

CONTROL OF OPERATIONS IN THE NUCLEAR INDUSTRY AND THE DERIVATION OF OPERATING RULES

Dr. Andy Trimble
HM Principal Inspector (Nuclear Installations), HM Nuclear Installations Inspectorate,
St. Peter's House, Balliol Road, BOOTLE L20 3LZ

In the UK nuclear industry safety is primarily regulated through conditions attached to the site licence. HSE's policy includes a need for consistency. All site licences require potentially hazardous plants and operations to have a safety case which adequately demonstrates safety and which identifies limits and conditions necessary in the interests of safety. These limits and conditions form the basis for safe control of operations that affect safety and are identified in Safety Assessment Principles. The philosophy for such limits and conditions are well understood in the nuclear power reactor industry and the international consensus is shown in guidance from the International Atomic Energy Agency (IAEA). However, applying that directly to nuclear chemical plants proved more challenging. This paper outlines the underpinning thinking from regulatory interactions with licensees and how this thinking is now more broadly applicable, and so more consistent, across the range of facilities the NII regulates. The underpinning intent is to show how similar thinking may be useful for other high hazard industries.

INTRODUCTION

This paper is intended to demonstrate how the fundamental thinking on regulation for nuclear power reactors has been modified to suit nuclear chemical plant. This paper is intended to allow managers and practitioners dealing with high hazard plants in the non nuclear sector to understand the principles and, if useful, to adapt and adopt the relevant parts of this practice. In common with the goal setting principles of safety regulation in the UK, this is embedded in HSE's Nuclear Installations Inspectorate (NII) guidance. It is not a detailed prescription or single permissible approach but it does represent regulatory thinking in the NII and is considered current good practice.

THE LAW

The heart of the nuclear regulatory control system is the licence and its attached conditions (LCs). This is granted under the Nuclear Installations Act for prescribed activities which enables licensing. The most relevant LCs here are:

a. *LC23. 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.*

b. *LC24. (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.*
c. *LC27. 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* (often referred to simply as Safety Mechanisms).

INTERPRETATION OF LICENCE CONDITION TERMS

OPERATING RULES (ORs):

– Limits which are parameter values which must not be exceeded or may need to be in a permitted range.
– Conditions which related to the permitted plant configurations. Often this is an availability constraint for safety equipment to be brought in and out of service for maintenance and test.

OPERATING INSTRUCTIONS (OIs): these (as referred to in LC24(2)) are not simply the instructions that the operator follows but a specific sub set of these that are necessary in the interests of safety and that implement the ORs. As such they are high profile and need to be at the forefront of the operator's mind, usually by highlighting them and requiring some form of record to demonstrate compliance.

SAFETY MECHANISMS (SMs): these are the engineered safety systems (often called protection) that prevent, terminate or reduce the consequences of faults.

These non prescriptive LCs do not give any indication about their level of significance. This is found in supporting guidance and good practice.

GUIDANCE

The primary guidance for Nuclear Inspectors are the Safety Assessment Principles [1] (SAPs). Principle 27 clearly links ORs to design basis (deterministic) fault analysis [4,5]. Thus ORs are limits and conditions related predominantly to faults and they will have the characteristics of the underpinning deterministic analysis from the safety case. The most relevant of which include:

a) a robust (engineering) demonstration of fault tolerance
b) assumes the worst case plant conditions, including allowable outages
c) uses conservatism to allow for uncertainty

Thus, ORs will be prudently based.

There is further international good practice given in the IAEA guide [2]. This establishes a number of regions within the progress of a fault where "rules" are required.

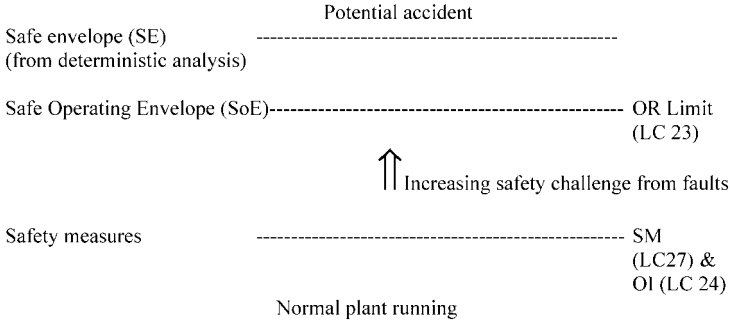

Figure 1. IAEA guide interpretation for UK regulatory practice for Limits

It is this concept that forms the model for benchmarking ORs. Schematically we interpret the guide.

The safe envelope may be likened to a fence protecting from an incline. Because the analysis that places the fence is deterministically derived, there is high confidence that provided the fence is not crossed, the operation is safe. On the other side of the fence, the operation may not be unsafe, yet there is the potential to "fall down the slope". If there are drivers to move the fence further towards the incline, there will be a need for more analysis or research work which may remove uncertainty and/or demonstrate whether the incline is more a cliff or a gentle slope.

The safe operating envelope is set back from the safe envelope by the extent of the largest reasonably foreseeable transient. This can be a very simple time based calculation e.g. based on the response time of the safety measures and the rate of change, or on conventions such as that in criticality [3]. This is the aspect that requires most engineering judgment and in the power reactor aspect of our work, it takes a great deal of time and effort. For example, there is economic benefit in generating electricity to maximize the coolant temperature to the steam boilers and this governs the fuel temperature — a vital safety parameter. Conversely, in most chemical plants there is no great drive in this direction — there is no economic advantage in running a highly active storage tank of self heating liquor close to its boiling point and there are many economic and safety advantages in not doing so.

The safety measures are those engineered (SM) and administrative arrangements (OI) that are the normal method of keeping the operation within the SoE. This is where we see a significant difference between power reactors and nuclear chemical plant. The margin on a power reactor is generally small and the safety measures are close to the SoE. This is not usually the case on most nuclear chemical plant. In fact what the figure does not show is that further instructions (OIs) would be expected both between exceeding the safety measure and the OR and beyond. The form of these instructions varies to give the maximum assistance to the operator in order that the fault may be terminated and the plant brought under normal control with the minimum of disruption.

TYPICAL ORs

For nuclear chemical plants there are a number of expected "standard" ORs on most operations with radioactivity.

a) A feedstock rule: Although this is not strictly in accordance with the method shown, it is the basis of the safety analysis on which the ORs are derived. Therefore, to ensure the analysis remains valid and the operation remains within the SoE, this becomes an OR.
b) A shielding rule: because penetrating radiation has the potential to harm then an OR will be necessary for most operations. The typical form might be "All significant sources of radiation shall be shielded". This covers such aspects as the passive shielding, shield doors, containers and transport flasks. The OIs would be expected to cover the specifics of each shielding system in a proportionate manner. An equivalent to shield doors in conventional industry might be where air lock doors provide a barrier to toxic release, then there may well be a condition rule that only permits one door open whilst the toxic material is present to maintain the containment function. Obviously, the first option should be to remove the hazard.
c) A ventilation discharge rule: all plants containing more than a trivial quantity of radioactivity are expected to be ventilated as part of their containment. A typical form might be "In any single event the stack discharge must not exceed (a limit)". This should ensure that public doses are minimised in the case of faults. There is no expectation that such a limit will be breached because of the drive towards defence in depth from the deterministic approach. It is also a very good example of how the OR tends to be related to consequences whereas the associated safety measures, in compliance with the deterministic methodology, tend toward the initiating fault. There could be equivalent conventional systems for dealing with biologically active species where similar constraints could apply.

In the UK's goal setting safety regime the regulator does not prescribe what ORs should be or how they should be framed. Rather, there is an ongoing evolution in pursuit of risks being 'As Low As Reasonably Practicable' (ALARP) — in compliance with the overall legal provision in the Health and Safety at Work Act — to set the basis of how they are derived and thus, how they might meet regulatory expectation.

OPERATING RULE PRACTICE

ORs, being based in the deterministic analysis, are expected for faults with a reasonable initiating frequency (usually taken to be greater than 10^{-3} p.a.) and with potential consequences greater than statutory dose limits. In line with HSE's policy of proportionality, less frequent initiating faults with higher doses will also be associated with ORs. For faults initiating with a frequent less than 10^{-5} p.a. and with potential consequences less than statutory dose limits there may well be OIs but ORs are not usually expected. Between these, there is may be faults or groups of faults that need to be judged on a case by case basis.

LC 24 requires that there are OIs to ensure the ORs are implemented. LC 25 calls for operational records and Good Practice dictates that there is demonstrable compliance with the ORs. Hence there are a number of characteristics of sound ORs:

a) there must be a means for demonstrating compliance. Most often the instrument or activity should be explicitly recorded at regular intervals or when that activity is carried out. Whether that is an electronic or manual record is not of major concern provided the record is adequately secure.
b) The OR must be in a form that the operator can comply with it. In other words, it must be clear what the limit or condition is and the way in which compliance can be secured.
c) There should also be suitable means for returning the operation to a safe state. Since breaking the OR is not yet of itself a realised hazard to people, then recovery to some stable state should be possible. Otherwise the plant has not been correctly designed, operated or constructed.
d) The OR should be explicit and timely — there is no point in an OR that can only be shown to have been complied with by a calculation after the event.
e) Operators also need a knowledge of ORs in order to deal with unforeseen problems or faults. In some cases there may be the need to breach some limit or condition to take the plant back to a safe state. Such breaches need to be carefully considered and, if possible, alternative and/or temporary safety systems put in place to do all that is reasonably practicable to avoid harm.

The concepts underpinning ORs are not complex but the their framing is an acquired skill. ORs need to be cast so that the safety intent is clear and unambiguous but not so tightly worded that there might be frequent or unintended technical breaches (ones which breach the wording of the OR but do not breach the safety intent) which do not actually compromise safety. If there are such regular breaches, then the duty holder (Licensee) needs to consider whether or not the plant is as robustly protected as the analysis might indicate. One of the most useful techniques is to include a short description or commentary to allow the relevant operators to understand the purpose of the OR.

It has been the practice in certain parts of the nuclear power industry to embody certain limits and conditions in “special” Instructions. Whilst this is perfectly acceptable, the fact that the compliance means is labeled an instruction does not necessarily tie it to LC 24. In many cases these are treated as compliance with LC 23. What is important is the safety function performed, not its label.

DISCUSSION

ORs have been a part of the nuclear industry armoury for controlling operations since the earliest days. The label has become so well established that even when reviewing our licenses we have chosen to keep the title rather than use limits and conditions from the LC because the term is so well understood. However, there is still the implication that ORs are some form of high level OI. This is simply not the case and it is important to

keep the licence shorthand in mind at all times when dealing with ORs — they are Limit and Conditions (although this paper has dealt almost exclusively with limits).

The prime concepts that would seem universally useful would include:

a) The safe envelope and safe operating envelope. Colleagues who have been in other industries see this as a sound way to improve corporate and operator understanding of where operations and plants should be at any point in time.
b) The safety measures which can be a combination of engineering and administrative controls. However, the deterministic approach drives towards engineered systems that either (in order of preference) stop the fault initiating, stop it propagating, terminate its progression or deal with the consequences — a drive towards inherently safer operations. Often defence in depth is a combination of several of these.
c) The strong link between the analysis and the safety measures. These safety measures are derived from the underpinning robust demonstration of fault tolerance which is characteristic of the deterministic approach.

NII's approach to OR breaches is guided by HSE's enforcement policy and strategy [6,7]. Among the factors taken into account are:

a) The risk gap — basically, how significant is the breach
b) The track record of the duty holder
c) Strategic factors such as public expectation and whether the underpinning weaknesses been addressed in a timely manner.

Thus, not every breach will result in strong regulatory action although that is one of the options for enforcement.

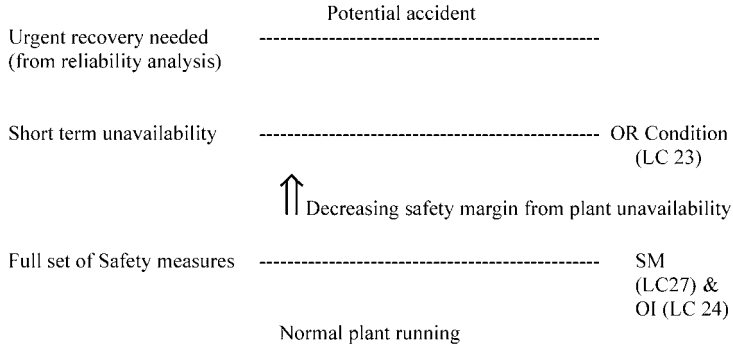

Figure 2. IAEA guide interpretation for UK regulatory practice for Conditions

CONCLUSION

This short paper has outlined the thinking in the nuclear industry for safely controlling operations. Whilst it is not a universal solution on its own, the concepts and practices would appear useful to high hazard industries in general and may be helpful to them in meeting their legal duties under the law.

ACKNOWLEDGMENT AND DISCLAIMER

Thanks go to very many in HSE's Nuclear Installations Inspectorate and BNFL for help and advice in developing this paper. The opinions here are those of the author. No part of this paper should be taken as definitive interpretation of HSE or NII policy, the law, or their application.

REFERENCES

1. Safety Assessment Principles for Nuclear Plants HSE 1992
2. IAEA 'Operating Limits and Conditions and Operating Procedure for Nuclear Power Plants', IAEA Safety Standards Series, Safety Guide No. NS-G-2.2
3. 10CFR Section 50.68 Page 763 USNRC
4. The Use of Deterministic Analysis in Safety Cases for High Hazard Plant, G A Trimble. Proceedings of a conference on Safety Cases: Cross Industry comparisons of best practice. IBC 2001
5. Trimble G A, A regulatory view of deterministic safety analysis in the nuclear industry (some lessons for the process industry?) Proc. HAZARDS XVI P754ff
6. Policy Statement, Our approach to permissioning regimes, HSE 2003 http://www.hse.gov.uk/enforce/permissioning.pdf
7. The Enforcement Management Model, Operational Version 3, HSE, http://www.hse.gov.uk/enforce/emm.pdf