

NUCLEAR SAFETY DIRECTORATE - BUSINESS MANAGEMENT SYSTEM		
<b>TECHNICAL ASSESSMENT GUIDE</b> <b>TRANSIENT ANALYSIS FOR DBAs IN</b> <b>NUCLEAR REACTORS</b>		<b>T/AST/034</b>
		ISSUE 001
Approved By: <i>B J Furness</i>	B J Furness	Issue Date: 12/11/99
Open Government Status: Fully Open		Review Date: 12/11/02

## 1. Purpose and scope

1.1 This TAG provides guidance to assessment inspectors on the interpretation of the safety assessment principles covering transient analysis for design basis accidents in nuclear reactors. The TAG contains *guidance* to advise and inform NSD inspectors in the exercise of their professional regulatory judgement. Comments on this guide, and suggestions for future revisions, should be recorded on the appropriate registry file.

## 2. SAPs addressed

2.1 This guide discusses how principles 20-27 in the 1992 issue of NII safety assessment principles<sup>[1]</sup> are to be interpreted.

## 3. Relationship to licence and other relevant legislation

3.1 Licence condition 14 requires the implementation of adequate arrangements for the production and assessment of safety cases. Design basis analysis is a major part of most safety cases for nuclear installations.

3.2 Licence condition 18 requires adequate arrangements to be made for the assessment of committed effective dose equivalent for various classes of people. The doses to people who live round the site are calculated as part of the design basis analysis for the installation.

3.3 Licence condition 19 requires the safety of any new plant to be justified. If the equipment is installed to protect the reactor, its adequacy will probably be tested by design basis analysis. If the plant needs to be protected, the adequacy of that protection will probably be demonstrated by design basis analysis.

3.4 Licence conditions 23 and 24 provide for the submission of operating rules and operating instructions to HSE. The adequacy of these rules and instructions are often demonstrated by design basis

analysis.

#### 4. Advice to assessors

4.1 Design basis accidents are introduced when considering the need for and capability, as opposed to the reliability, of protection equipment. For every protection system, there is at least one fault which provides the specification of its capability. The design basis fault can be a reasonably realistic sequence or it can just be a simple set of bounding assumptions. The design basis concept has a more specific meaning in most countries outside the UK.

4.2 Following USA practice, design basis faults usually refers to fault sequences and analytical assumptions defined by the regulator as criteria which have to be met by a reactor design in order to be licensable. That reflects a prescriptive regulatory regime, which does not apply in the UK. Design basis analysis is often presented as being deterministic, with uncertainties in the analysis being covered by appropriate conservatism in the modelling. That can be difficult to prove. In the UK, it is the responsibility of the licensee to demonstrate that it applies.

4.3 However, the US interpretation of design basis faults was imported into the UK with PWR technology. The two different interpretations of the phrase can cause confusion. The difference in interpretation shows up particularly in the way transient analysis is done. When the design basis assumptions are imported, the transient analysis in support of PSA analysis will usually be done on a different basis, since it should be best estimate. Under the UK regime, the transient analysis supporting a probabilistic safety analysis (PSA) is essentially the same as that used in the analysis of design basis faults. The analytical assumptions are chosen by the licensee. They are then justified in submissions to NII.

4.4 In the US approach, the assumptions are imposed by the regulator, on the basis of providing a bounding assumption. A major distinction is then drawn between design basis analysis and best estimate analysis. That distinction is also made in the UK but not with such a clear cut difference. There is the concept of a confidence level for a calculation, which can be allowed to vary with fault frequency.

4.5 In the UK, safety submissions should demonstrate that the risk from a licensed nuclear installation is tolerable, in the sense of **reference 2**. It is the responsibility of the licensee to demonstrate that the installation is safe. We do not have the concept of licensability,

which is closely related to the US prescriptive regulatory regime. The risk limits of **reference 2** are to be applied to the sum over all faults for the entire reactor. Most safety submissions deal with only part of the plant or one particular type of fault. There should be suitable rules for allocating an appropriate fraction of the allowed risk to the part of the safety case being considered. While that could be based on the results of a PSA for the whole reactor, it would normally be based on allocating the risk equally amongst the different fault types.

4.6 The division of safety analysis into design basis faults, severe accidents, and probabilistic safety analysis, is therefore largely a matter of convention. Most routine safety submissions to NII will use design basis methodology, rather than PSA techniques. A reliability assessment will also be supplied. Safety submissions are often concerned with the adequacy of engineered protection for specific faults. If individual faults meet the design basis criteria, it is believed that the total risk, as estimated by a PSA, will be acceptable. PSAs are then used to confirm the position or provide guidance on how to change the design basis procedure.

4.7 When designing a plant, PSAs can be used to demonstrate balance between the various fault types. When applied to existing reactors, balance may not be desirable. In an actual reactor, certain fault types are expected to dominate. Any argument for relaxation of protection standards over the design intent, on the basis that the fault in question is not a dominant one, should be resisted.

4.8 The wording of our principles is heavily influenced by our interest in licensing power reactors but the underlying ideas should have general application across nuclear installations. The licensees are expected to have equivalent guidance for their safety analysts and that guidance should be tailored to their specific interests.

4.9 Safety submissions are expected to follow the internal guidance of the licensee. Discussions between NII assessors and safety case authors should be primarily concerned with how the safety case authors are interpreting their internal guidance. Both our assessment principles and the licensees' guidance require judgement and are aimed at experienced engineers and scientists.

4.10 An NII assessor should interpret licensees' guidance in the light of NII's principles but should not assume that safety case authors have any understanding of our principles. If an NII assessor perceives differences between the licensees' guidance and our principles, and these differences cannot be regarded as a matter of interpretation, the

matter should be raised as a generic issue with NII management.

#### 4.11 Principle 20

1) P20 requires a demonstration that the claimed protection equipment is fit for its purpose and suggests that the design basis accident concept provides a standard way of doing that. Licensees are expected to have a declared procedure for carrying out design basis analysis. In particular, there needs to be a definition of what is meant by a design basis fault, in terms of probability of occurrence. There also needs to be a standard calculation procedure for the transient analysis, and an acceptance criterion, which the transient analysis has to demonstrate is met with a suitable level of confidence.

2) A robust demonstration is taken to mean that the calculation should be demonstrated, for example by sensitivity studies, to be insensitive to the uncertainties in the model. That would normally be interpreted as referring to the calculation procedure itself as well as the analyses of individual fault sequences. However, the assessor should be confident that the lack of sensitivity applies to the individual calculations. That can be based on arguments from physical principles, as well as computer calculations. Such arguments are to be encouraged, when reviewing calculation procedures.

3) The calculation procedures used for design basis analysis are aimed at providing pessimistic estimates for radiological consequences and need not necessarily be consistent with what is physically possible on the plant. The aim is to have a pessimistic estimate of the parameter of interest, usually temperature. The computer codes used in the analysis must have been verified and validated to a satisfactory standard prior to their use in plant safety analyses. This is discussed in a separate assessment guide<sup>[3]</sup>.

4) In the UK, the normal approach is to have a computer model that can be validated by the methods quoted in that guide and then to do design basis analysis with a pessimised version of it. The pessimism may take the form of assuming pessimistic boundary conditions but

that is not the only way of pessimising a best estimate model. The artificial features are included in the pessimised model in order to simplify the analysis or bound the uncertainties in the calculation.

#### 4.12 Principle 21

1) P21 provides the frequency criterion for the initiating events that need to be considered. It reflects the risk limits given in **reference 2**. If the fault frequency is low enough, then the confidence in the adequacy of the protection can be reduced. Three exclusions are listed. The first refers to plant failures with a frequency less than  $1E-5$  per reactor year (prry). The second is failure of structures which have gone through the special case procedure of P70. The special case procedure is usually applied to 'incredibility of failure' structures but the exclusion can be extended to 'high integrity' structures; i. e. those with an estimated failure rate of  $1E-5$  prry. The third exclusion is hazards, where the frequency cut off to be applied is explained in principles 119 and 120.

2) When considering what is meant by an initiating event, it should be noted that design basis analysis is top down. The analysis starts with mechanisms for releasing radioactivity and the engineered systems provided to prevent the mechanism from operating. It deals with fault types and the systems designed to protect against them. It does not usually deal with failure of individual items of plant. The analyst will also be expected to use an understanding of the way the plant behaves, in order to limit the number of initiating events being considered. P21 refers to an initiating event, which implies a single fault. The assessors should give some thought to fault combinations in the appropriate frequency range.

3) When deciding what is to be regarded as an initiating event, licensees should not be allowed to subvert the aim of any frequency cut off criterion by subdivision of initiating events. The application of a frequency cut off criterion is the modern version of the old claim that certain fault sequences were incredible and need not be protected. When applying the cut off criterion, the totality of faults should be encompassed within a reasonable number of initiating events. A typical number would be

around 20.

4) The aim is a simple argument with relatively few sequences; defined as the design basis sequences. This is recognised as a strength, but also a weakness, in the approach. A PSA usually takes the alternative approach. It starts with failure of individual items of plant and explores what happens. This results in a voluminous list of sequences, which can be difficult to keep track off. Provided the results tie up, the two types of analysis support one another and provide a desirable redundancy in the safety argument. If the results do not tie up, the licensee should be requested to supply an explanation.

#### 4.13 Principle 22

1) P22 explains how to develop the fault sequences. The principle is, if in doubt, make the pessimistic assumption. There should be high confidence that the protection system has sufficient capability. However, in difficult cases, the analyst should be aware of the  $1E-7$  per reactor year cut off on fault sequences. The proposed procedures in P22 should be regarded as a first pass. If there is a potential common mode failure, it should be assumed to occur. For example, a hot gas release would normally be assumed to fail all the protection equipment in the quadrant into which it occurs.

2) The single failure criterion should then be applied. A certain amount of judgement is also needed on that. The worst single active failure should certainly be assumed but passive failures are more negotiable. The advice is to think in terms of fault frequencies, bearing in mind the  $1E-7$  pry cut off on sequence frequency. If the worst passive failure is not assumed, justification for not doing so should be supplied. The justification will almost certainly be based on estimated fault frequencies. Since our principles were formulated, the single failure criterion has been expanded to provide deterministic reliability criteria, which can be used as a substitute for a PSA.

3) Maintenance is often a disputed area, particularly for reactors designed prior to 1980. The phrase used is 'normally permitted'. This should be taken to mean maintenance states, which are not time limited by the

operating rules. It does not apply to 'urgent maintenance' states, which arise when equipment fails and continued operation is time limited. However, this raises the issue of what percentage of the time a reactor can then be allowed to be in the 'urgent maintenance' state before such states have to be included within the design basis. An acceptable figure would be about 1%.

4) Failure to meet that should be taken as an indication that extra safety equipment should be installed. It may be possible to argue for a lower confidence level in the design basis calculation and thereby redefine urgent maintenance states. Such arguments need special treatment.

5) NII safety assessment principles are aimed primarily at new plant. The preferred approach for complying with P22 is for protection equipment to have 1 out of 4 redundancy. The design basis procedure would then assume that one of the four trains is failed as a consequence of the fault, a second train is assumed failed to comply with the single failure criterion and a third train is assumed to be out for maintenance. That is an ideal, rather than a requirement, particularly when considering existing reactors. Whether post trip cooling equipment is failed as a consequence of a fault can be analysed and the probability of its failure estimated. Time at risk arguments will be allowed, when considering maintenance outages.

6) The protection systems on current reactors often fail to meet that ideal. This principle therefore causes problems. Maintenance assumptions tend to take the strain. The licensees should have specific guidance on the allowed reductions in the redundancy of safety systems. NII assessors are expected to exercise judgement, based on perceived frequencies, against the  $1E-7$  per year cut off for fault sequences to be analysed by design basis techniques.

7) The final point in P22 is the role of equipment that is not declared to be safety equipment. Two types of equipment are covered by that. The first is equipment that is present but is not formally claimed in the safety documentation. In a PSA, such equipment can be

claimed with a low reliability. In design basis analysis, it cannot. A licensee can always upgrade the status of the equipment but it must be done before it is claimed in design basis analyses. This is not often a problem when defining system capability.

8) The second type is control equipment. It is assumed that the requirements of principle 73 are met. Design basis analysis does not identify the specific initiating event. Control equipment can be the cause of an initiating event. If there is any equipment that is common to the control system that can cause a fault and the safety system claimed to protect that fault, the protection system should be assumed to have been failed by the initiating event.

9) The control equipment on nuclear reactors is usually designed, built, maintained and operated to safety grade standards. It is also often under continuous test. However, it can be the cause of the initiating event and its complexity rules out a claim for safety grade status. Failure modes are difficult to analyse. Design basis analysis must consider two situations; one with the control systems functioning as normal, the other with them suffering total failure. The frequencies will be, and can be claimed to be, different. Any such claim will need special consideration.

10) A controversial issue, when considering control equipment, is the possibility of partial failure. This has been a particular problem for AGR fuel routes, where assuming the worst possible failure at the worst possible time can be very difficult to protect against. In the extreme, the control system is being assumed to act maliciously. An NII assessor should consider this possibility and form a view on the credibility of the failure modes involved. If the sequence frequency is greater than  $1E-5$  per reactor year, it should be taken as a design basis fault.

#### 4.14 Principle 23

1) P23 covers transient analysis. The way the calculation is done should be based on standard procedures proposed by the licensee and under its quality control

procedures. NII agrees safety cases, not procedures, but an NII assessor should know what the procedures are and accept that they are suitably pessimistic. These procedures are crucial to the acceptability of any transient analysis in support of a safety case. The analysis should use approved codes in an approved manner. The assessor should have confidence in the specialist working groups who approve the codes and their usage. Such codes will have gone through the validation and quality control procedures discussed in the assessment guide on this subject<sup>[3]</sup>.

2) The analysis needs to identify the barrier preventing release of radioactivity to the atmosphere that is being considered and the system preventing its failure, whose capability is being demonstrated by the analysis. Typical examples of barriers in reactors are the fuel cladding and the primary pressure boundary. If the fault frequency is high enough, the analysis needs to demonstrate independence between the two or more barriers being claimed.

3) Having identified the barriers and shown them to be independent, the next stage is to identify failure mechanisms for these barriers and the acceptance criteria for each such mechanism. The aim of the transient analysis is then to provide a pessimistic estimate of the parameter, or combination of parameters, causing failure.

4) An obvious example is fuel temperature. A confidence level of around 0.1% is being sought and it is very difficult to do that by statistical techniques. The heat transfer is not linear enough. This is particularly so when you have a liquid coolant, which can go through the nucleate boiling crisis. The confidence can be based on suitable assumptions being made in the analysis or an insight into the energy balance. It will always require professional judgement by the assessor but previous practice should act as a guide.

5) Normal statistical techniques can often be applied to the energy input. It is easy to choose a suitable confidence levels for the decay heat. It is more difficult to handle power distribution throughout the core. There are

systematic variations, random variations, and uncertainties. Each of these needs to be handled against a 2 sigma confidence level by the licensee's procedure. An approach for the systematic is to do a large number of fuel cycle calculations and deduce distributions for axial and radial form factors. These predictions can be checked to a certain extent by reactor instrumentation, provided a suitable reactor exists to provide relevant data.

6) The randoms and uncertainties have to be estimated in some way. This can be based on theory or theory backed up by reactor measurements. To do this accurately can be difficult. The parameters are not independent and correlation effects must be included. Also, the distributions can be truncated by the need to be consistent with reactor measurements. For example, flow and power in a channel would be independent but together they determine temperature and it is under operator control. The licensee should have a procedure for handling that and some means of demonstrating the resulting confidence level.

7) When performing such statistical exercises, one issue needs to be clear in the submission. There can be an acceptance criterion like 'the probability of Magnox ignition shall be less than 1%'. The 1% can refer to the probability of the peak element or the sum of the probabilities for all elements. If it is the latter, the number of standard deviations the peak pin has to be from the ignition temperature has to be large because of the number of elements involved. It may be possible to model the peak element but use a revised acceptance criterion. The population being considered in any statistical analysis needs to be identified unambiguously.

8) Turning to heat removal, the main parameter is flow, with heat transfer being an important secondary and correlated effect. For fuel temperature calculations, it should be biased two sigma low. When considering feed stocks, it would be biased three or four sigma high. The design basis fault for that should assume failure of a feed pipe. For gas cooled reactors, heat transfer arguments usually centre round the possibility of flow stagnation. The confidence in the calculation is based on having flow stagnation for longer than is physically reasonable and

then biasing subsequent flows low by one or two sigma. If the core flow is a balance between two large flows, the calculation procedure should explain how the flow is biased. Total reliance on a computer calculation in that situation should be regarded with suspicion, unless backed by suitable arguments.

9) For liquid cooled reactors, there is the further complication of widely varying heat transfer coefficients. This is particularly related to the boiling crisis. Such conditions need special treatment to ensure pessimism. The licensees' procedures should explain how the modelling is to be pessimised and the assessors should be confident that it is pessimistic for the range of faults considered. That judgement can be based on appeals to experiments, to sensitivity studies, or to an understanding of the energy balances.

10) When dealing with structures, similar principles apply but the issues can be different. The assessor should be convinced that the failure mechanism and its relationship to pressure and temperature has been established. What is the combination of parameters that is being pessimised in the computer model? If a structure is important in determining radiological consequences, it needs to be subjected to design basis analysis for the faults concerned. Deterministic criteria, such as required by design codes, can be difficult to incorporate in fault studies arguments, with their concern for failure probabilities.

11) Design basis analysis for structures is therefore not developed to the same extent, as it is for fuel temperature assessment. The uncertainties in the transient analysis are often comparably minor compared to those in the structural integrity part of the calculation but difficulties can arise. For insulated structures, there may well be large uncertainties in what insulation is present and its condition. The solution there is to analyse a range and choose the worst one. Choosing the range of possible configurations should be covered in the licensees' procedure documentation. NII's acceptance that a suitable range has been chosen may well involve considerable engineering judgement.

12) Another specialised area is modelling free convection in large but non standard geometries. That is a code validation problem and is covered by the assessment guide on that subject<sup>[3]</sup>. There needs to be suitable experimental support and free convection is very scale dependent. The assessor will need to judge the adequacy of the experimental support.

13) Failure of some structures is regarded as incredible. The probability of failure has to be around  $1E-7$  pry. This raises the question of the confidence level required of the transient analysis. There are three parts to that, the fault frequency being considered, the confidence level of the calculation and the failure probability of the structure, given that the acceptance criterion is met. If confidence levels around 0.1% are required of the transient analysis then the standard procedures described in **reference 3** will suffice. If  $1E-7$  pry is being required, the calculation has to be a very simple one and general confirmation by a hand calculation ought to be possible.

14) The acceptance criterion for structures may well depend on the presence of cracks. That will have its own probability. The confidence level of the calculation can be allowed to vary to compensate for the change in frequency of the combination of the fault and the crack. Alternatively, the design basis accident may be different in the two cases, reflecting a change in the frequency of the initiating event, which needs to be considered.

#### 4.15 Principle 24

1) P24 covers the radiological release calculations. It is the subject of another assessment guide. The wording is more prescriptive than it needs to be but it reflects the procedures used by the UK nuclear generators. The usual design intent for a protection system is the prevention of a breach in the fuel clad. Therefore no radiological calculations are required. That cannot be applied universally. Some criterion based on radiological release is needed.

2) Traditionally, UK safety assessors have used the concept of avoiding any need for controls beyond the detailed emergency planning zone or even beyond the

site fence. P24 gives an typical example of such a criterion. The licensees' guidance should have something equivalent. This is usually referred to as requiring that an ERL should not be exceeded in design basis faults. The conversion of the radiological source term to the ERL dose needs to be specified unambiguously in the licensees' guidance and agreed as being acceptable by NII.

3) Radiological release calculations for reactors and their fuel routes are the result of three separate calculations. The first considers release from the fuel to the primary containment. The second is the release from the primary containment to the environment. The third is the relationship between radioactivity released to the environment and the dose for comparison with P42. The first will use a computer code backed by suitable experiments. The second can either be a bounding assumption based on assuming no plate out within the primary containment or it can be based on suitable experiments. The third is based on an approved calculation. The first two depend on the fault. The third is site specific and is usually quoted as conversion factors for the various isotopes.

4) In the first part, the main pessimism is obtained by overestimating fuel temperature in the normal way. When there are significant levels of oxygen in the primary circuit, overestimating temperature may not be pessimistic, since the rate of formation of  $U_3O_8$  goes through a maximum with temperature. The procedure should maximise the amount of fuel at the worst temperature. A typical approach would be to overestimate temperatures but then assume that any fuel above the worst temperature is at the worst temperature. It would depend on the temperatures being predicted whether that was a reasonable approach or not.

5) Once the temperatures are overestimated, the release rate need not be pessimised much. Using one sigma confidence would be good enough and even a best estimate could be allowed when the over estimate in temperature is believed to compensate for uncertainty in the radiological release modelling. By its nature, there are no cliff edges or sudden changes in the results of that

modelling.

6) All the fission products that are released from fuel pins will not necessarily escape to the atmosphere. For most faults, only a very small percentage will do so. The rest will plate out on surfaces inside the pressure vessel, particularly on the boilers. Modelling of plate out can be difficult and, while sophisticated codes exist, judging the pessimism in the model is usually done on the basis of understanding experiments. In the absence of suitable experiments, plate-out would normally be assumed to be zero. If plate-out is claimed, there will need to be an approved calculation for it. The approval can be done by a suitable group of specialists within the licensee's organisation. An assessor can rely on that group or make arrangements to have the modelling underwritten by independent specialists.

7) In many calculations, claims are made on filters. This should preferably be based on measurements on the plant, mainly to check they have been installed correctly. In the absence of such tests, high efficiencies should be regarded with suspicion. The assessor needs to check whether the filters have ever been tested under the conditions envisaged in the fault, in terms of temperature, humidity and dust loading. A design basis fault, or faults, may need to be devised for filters.

8) The dispersion calculations can be best estimate. The required pessimism is obtained by assuming pessimistic occupancy factors.

#### 4.16 Principle 25

1) P25 gives the acceptance criteria for design basis analysis. A barrier can either prevent a radiological release or reduce the amount of radioactivity released. The second part of P25 defines what is meant by an effective barrier, when the retention is not 100%. For example, a fuel pellet provides a barrier by retaining much of the radioactivity until the fuel melts. A filter train is a more obvious example of a barrier which reduces, rather than prevents, a release.

2) In practice, when considering reactor faults, there are

well known acceptance criteria, which depend on the fault type. These should be spelt out in any safety submission on fault studies. Examples would be 1350 C for clad melt in an AGR, the 2200 F criterion used for depressurisation faults in PWRs, or the 1% probability of Magnox ignition in pressurised faults in a Magnox reactor.

3) Therefore, while the second criterion provides the underlying concept, for the majority of faults, the first criterion is the one that is applied. In principle 25 b), the phrase 'most severe' can either be interpreted as referring to the low frequency of the fault or the low probability of a significant release following a frequent fault. Principle 42 is an elaboration of that idea and can always be used as an alternative safety argument.

4) The third criterion given in P25 concerns operator doses. On reactors, this is not a major interest for design basis analysis. The obvious fault in this category is failure of the protection systems preventing operator access to high radiation areas. The capability of such systems is rarely analysed. The reliability of these systems has to be analysed but the safety case usually assumes that failure of such systems leads to a fatality with a probability of unity.

5) Another possible concern is the effect of radiological releases from the reactor or fuel route facilities on operators. There are general studies to support the contention that, provided off site doses are controlled, on site doses from such accidents are acceptable. The design basis concept could be applied but the two consequences are clearly related to one another. In making that judgement, assumptions have to be made on the effectiveness of evacuation and mustering procedures for people on site but they are not fault specific.

6) The final concern on operator doses arises from recovery actions following faults. The strategy is to avoid having to make such claims by improving engineered protection but, where that cannot be done, operator doses are estimated. A design basis accident could be designed for that purpose but it is rarely necessary.

7) Operator doses may well be of greater interest on

chemical plant and formulating a design basis accidents to test the protection may have a role there. The concept would be the same. It would be a matter of whether the system is complicated enough to justify doing so formally. (T/AST/006 addresses DBA for non-reactor plant).

#### 4.17 Principle 26

1) P26 reminds assessors of the desired end result but the wording does not reflect the standard approach in safety cases. Safety functions are usually identified, independent of specific faults. It is a top down approach. There should be two diverse means of achieving the function. This gives a list of systems, which will be discussed in the safety report. Design basis analysis will identify the minimum capability for each of these systems, based on a design basis fault, which is introduced for the purpose.

2) There may be several different fault types and, although one will be limiting, the others need to be recorded. The system will be designed with suitable redundancy to achieve that capability. The original safety report should state what was being assumed by the designers and, if there is subsequently a change for any reason, the reference safety statement should be updated. Assessors need to check that these procedures are being followed. If a requirement is relaxed, the licensee should demonstrate that another fault type has not become the limiting one.

3) Design basis analysis requires the analyst to identify the limiting fault. This could be done by taking many sequences and working out the capacity required for each one and identifying the maximum. In practice, identifying the limiting fault is usually done by logical argument, not by checking long lists. NII assessors have to judge the quality of the logical argument.

4) P26 requires operator actions to be identified. This should be a matter of installing suitable alarm systems. Operators are trained to respond to alarms. How they do so is covered by station operating instructions. Only in important cases would such instructions appear in the operating rules. If an operator action is identified, then the

analysis should estimate the time available for such action, after the alarm comes up. As required by principle 77, operator action should not be claimed, unless 30 minutes is available to diagnose the fault and initiate action. The thirty minute rule is often a major input to the definition of the design basis accident.

5) While the reactors are at power, the thirty minute rule usually prevents the operator being part of front line safety systems. On shutdown reactors the operator is often part of the front line safety systems. This is because of the time available. The design basis analysis is concerned with estimating that time. That part of the safety argument tends to be straightforward. The time depends on decay heat in a straightforward way. There should be an operating rule dealing specifically with shut down reactors.

#### 4.18 Principle 27

1) P27 is a continuation of P26. Design basis analysis will often be used to justify trip settings and operating conditions. The analysis can either assume the current arrangements in the ORs and justify them, or the analysis can be the source of the numbers that appear in the ORs. Either way, the analyst should explicitly state what the OR numbers are being assumed to be. OR numbers can be changed from time to time and it is then important to know all the faults which might be affected.

2) When determining the value for the trip settings to be quoted in the operating rules, allowance has to be made for instrument error, setting error, and drift. That can be included in the transient analysis or left to the operator to add in. The fault analyst may or may not be making a suitable allowance. If no statement is made, the assessor should assume that no allowance has been made and the safety case author must propose and justify a suitable allowance.

3) When determining operating limits, allowance has to be made for instrument uncertainty. That should include both steady state uncertainties and any time lags due to rapidly changing conditions. The latter are usually taken care of by the transient analysis but reactor control

systems can be difficult to model and some allowance should be made for that. The fault analyst should normally be able to advise, based on knowledge of the ability of the codes to model operational transients. The trip settings and the operating limits must be taken as a single package.

4) Operating instructions following a fault should be based on responding to alarms and will use any available measurements of conditions inside the core. That is usually straightforward for faults considered by the designer. If special transient analysis is necessary, best estimate analysis and sensitivity studies is the preferred approach. Design basis analysis is used when demonstrating compliance with the thirty minute rule of P77, but beyond that, its application is limited when considering operator actions. Use of design basis analysis, which is designed to be pessimistic, can positively mislead operators.

## **5. References**

1. HM Nuclear Installations Inspectorate: Safety Assessment Principles for Nuclear Power Reactors, ISBN 0 11 882043 5, 1992.
2. Health and Safety Executive: The Tolerability of Risk from Nuclear Power Stations, ISBN 0 11 886368 1, 1992.
3. T/AST/042 Technical Assessment Guide on 'Validation of Calculation Methods, Design Data, Models and Codes'.