A REGULATORY VIEW OF DETERMINISTIC SAFETY ANALYSIS IN THE NUCLEAR INDUSTRY (SOME LESSONS FOR THE PROCESS INDUSTRY?)

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

The aim of this paper is to show the how engineering fault analysis forms a major plank in the safety assessment of Nuclear Plant and how such analysis may be carried out. The paper briefly outlines the regulatory and legal framework for UK nuclear licensed sites in our non prescriptive, goal setting safety regime.

HSE publishes a great deal of guidance. The prime relevant sources are Tolerability of Risk (TOR) and Safety Assessment Principles for Nuclear Plants (SAPs). This led to the development and application of internal guidance on Deterministic Safety Analysis (DSA) which has its roots in Nuclear Chemical Plant assessment and is based on considering design basis faults. Design basis faults are those that, without the appropriate safety systems, are foreseeable within a plant lifetime. DSA forms the major input into the quality required from any such safety systems required to prevent, terminate or mitigate fault sequences. This highlights DSA as the bedrock of safety analysis for nuclear plants which is consistent with international practice.

AIMS

This paper introduces a non probabilistic part of demonstrating safety which has been an underlying principle in the UK's approach to nuclear safety regulation. Here it is called deterministic safety assessment. It is usually complemented by a probabilistic analysis. As part of propagating sound practice and corporate learning, it seemed reasonable to share this way of thinking with the process industries. This is particularly relevant as the guidance stemmed from interactions between ourselves and Nuclear Chemical Plant licensees. The annex summarises the guide which may be bench marked against corporate safety assessment guidance.

In common with the goal setting principles of safety regulation in the UK, the guidance, summarised in the annex, is not a detailed prescription or a single permissible approach that needs to be followed. The guide is intended to assist HSE's Nuclear Inspectors in using consistent approaches to making judgments. In line with the injunction in safety law, all this is subject to the test "so far as is reasonably practicable", better known as As Low As Reasonably Practicable - ALARP (see later).

INTRODUCTION

The legal requirement for a safety case for UK Nuclear Installations stems from the conditions attached to Licenses granted under the Nuclear Installations Act 1965 (as amended). Such cases have been a feature of the licensing regime since its inception. The safety case is a key feature of nuclear safety regulation. The current licence requirement is for an adequate safety case for operations that may affect safety. The Health and Safety Executive's Nuclear Installations Inspectorate (NII) is charged, amongst other things, with administering this licensing function including assessment

of such safety cases. Regulating adherence to the conditions attached to licenses (including the safety case assessment) is part of the nuclear safety permissioning regime.

Licensees carry out their duty to protect workers and members of the public by establishing safety standards to ensure radiation doses from both accidents and normal operations are ALARP. NII's has a duty among other things to see that licensees develop, achieve and maintain such standards, to ensure that any necessary safety precautions are taken and to inspect and enforce safety law by means of its powers under the licence and relevant legislation. Thus, NII has to satisfy itself that the licensee is managing safety to an adequate standard, and take the necessary regulatory action to ensure standards are maintained and, where reasonably practical, improved. In all this, the licensee remains solely responsible for safety.

The point is that NII does not prescribe in detail how the licensees should comply with their legal obligations. It is for licensees to present their criteria and safety cases. NII then judges them against the SAPs [1] which are high level goals. NII has also developed a series of assessment guides to complement SAPs and assist in achieving consistency in a regime where there is considerable scope for flexibility and a need for judgment by the regulator. It is also important to realise that the ALARP principle drives an ongoing improvement in safety standards in the light of the current technical understanding, changes to limits and best practice.

THE STANDARD LICENCE

The heart of the nuclear regulatory control system is the licence and its attached conditions. NII can, at any time, attach conditions to a licence which appear necessary or desirable in the interest of safety. The most relevant here include:

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. LC1. INTERPRETATION

(1) In the conditions set out in this Schedule to this licence, unless the context otherwise requires, the following expressions have the meanings hereby respectively assigned to them, that is to say -

....."operations" includes maintenance, examination, testing and operation of the plant and the treatment, processing, keeping, storing, accumulating or carriage of any radioactive material or radioactive waste and "operating" and "operational" shall be construed accordingly;.....

c. LC14. SAFETY DOCUMENTATION

(1) Without prejudice to any other requirements of the conditions attached to this licence the licensee shall make and implement adequate arrangements for the production and assessment of safety cases consisting of documentation to justify safety during the design, construction, manufacture, commissioning, operation and decommissioning phases of the installation.

d. 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.

In making its regulatory decisions NII must make judgments about compliance with LCs. This is, in part, achieved using the relevant Safety Assessment Principles. For example Principle 27 (P27) states the purpose of Design Basis Accident Analysis (part of Deterministic Safety Analysis) is to provide information relevant to trip settings, plant operational limits (Operating Rules) and plant operating instructions for fault conditions and P26 which addresses the minimum requirements for the sufficiency of safety systems .

TOLERABILITY OF RISK & SAFETY ASSESSMENT PRINCIPLES

Tolerability of Risk (TOR) originates from a recommendation in the 1986 report of the Sizewell Inquiry [3] into the UK's first Pressurised Water Reactor (PWR). Public comment was invited and TOR was republished [2]. It discusses how people normally approach risk, shows how industrial risks (and nuclear risks in particular) are regulated, the nature of risk from radiation and how these are calculated. In doing this it established three levels of risk:

a. a risk which is so great or the outcome so unacceptable that it must be refused altogether - which can be described as intolerable risks: these cannot be justified except in extraordinary circumstances

b. a risk which is or has been made so small that no further precaution is necessary - the "broadly acceptable" region where no *detailed* working is needed to show that risks are ALARP.

c. risks that fall between these two states, that have been reduced to the lowest level reasonably practicable taking into account the detriment of further risk reduction. The injunction laid down in safety law is that any such risk must be reduced so far as is reasonably practicable. This is the ALARP or Tolerability region

TOR goes on to quantify these regions for individual risks which, in turn, are interpreted into some of the quantitative limits found in SAPs. These are set out as basic safety limits (BSLs) and basic safety objectives (BSOs). There was no intent to imply that showing how these are achieved by probabilistic safety assessment (PSA) is the most important element of safety cases. Indeed, HSE has given other statements that emphasise the more deterministic underlying approach adopted in UK nuclear safety regulation [6]. This paper shows a way to meet that more deterministic aim.

SAPs are at the "Principle" level and are used to guide inspectors' assessment for all nuclear installations. They are intended to promote consistent regulatory decisions. They are <u>not</u> standards imposed on licensees but have been published so that anyone who is interested can be aware of the safety guidance against which licensees' safety cases will be judged. They are non prescriptive and are intended for use with new plant and major plant modifications. However, they are also used in safety reviews of older plant, required under licence conditions, for comparison with modern standards and to give a benchmark against which any argument on what is reasonably practicable can be set.

The bulk of the SAPs set out NII's views on good engineering practice and are regarded as the basis of safe design. It is only by matching the quality of the engineering to the harm potential of the operation that fault tolerance in the plant and its operation can be demonstrably met. This could be interpreted as a definition of

"deterministic" for these purposes. Also, the PSA should help in making decisions to achieve a balanced plant design, i.e. one with no undue reliance on any particular design feature. The PSA should also show that risk targets have been met.

To assist in meeting HSE's policies of consistency and proportionality NII has drafted a series of assessment guides. This paper is primarily concerned with the guide on Deterministic Safety Analysis, which helps define its role and the term deterministic.

TECHNICAL SAPs - DEFINITIONS

The SAPs explicitly state that the technical aspects are fundamentally important to engineering a demonstrably safe, fault tolerant plant. The aspects considered are [7]:

a. Deterministic safety analysis (DSA)

b. Probabilistic safety analysis (PSA sometimes known as QRA)

c. Severe accident analysis (SAA)

d. Good Engineering Practice (GEP)

e. Waste Management

Dealing with each of these broad areas in turn:

DSA: which by definition includes Design Basis Accident Analysis, is a robust demonstration of fault tolerance. It links directly to the engineering principles which call for a preferred series of responses to faults. These vary from designs that are inherently safe to those that may require operator intervention in the fault sequence. The important feature of DSA is that any uncertainty is allowed for by conservatism. Often this conservatism is in the input data and requires expert judgments about the degree of conservatism appropriate to any particular case. DSA is concerned with faults with larger harm potential and not normally with more minor events.

PSA: The main purpose of PSA is to demonstrate a balanced design and it may also show that risks are minimised. The great strength of PSA is this overview. It is not covered by DSA which deals with faults on a fault by fault basis. Undue reliance should not be placed on the numbers produced by PSA. These numbers are usually rather uncertain and so, while they are very useful in comparative terms, they must be used with caution as a definitive quantification of the overall risks from the operation considered. PSA is usually carried out using best estimate data.

SAA: A severe accident is one which is not necessarily expected in a plant lifetime but has the potential for high doses or environmental damage. It is not necessary for this potential to be realised (Three Mile Island was a severe accident but there was no release of radiological significance). The prime difference between DSA and SA is in the way that data is used. SA is based on best estimates and as may well be bounded by the DSA if the level of conservatism is high. However, a sound understanding of the underlying phenomena during such accidents avoids the need for introducing unnecessary conservatism and hence unfruitful expenditure. The main aim of SA is to provide an input to emergency planning and to identify reasonably practical design improvements that can be implemented at reasonable cost.

GEP**:** In every industry there are both pressures to reduce costs and increase cost effectiveness. However, most companies and most industries set basic standards below which any design should not fall. This ensures that for harm potentials smaller

than would be covered by DSA, the learning experience of the company and/or the industry is taken into account. Often GEP is embodied in design manuals or company standards. Quality engineering should not stray outside this standard.

Waste Management: There are major additional external constraints as well as those required for safety. Much regulation is concerned with implementing government policy and GEP. Plainly, this also reflects public opposition to ill considered waste accumulation and storage (disposal is dealt with under Environmental Legislation administered by the Environment Agency).

DSA

This engineering fault analysis or Deterministic Safety Assessment forms the bedrock on which the safety case is built. The rigour in such analysis is directly linked to the harm potential or hazard. This is a key idea in deterministic analysis as harm potential is related primarily to the inherent characteristics of the processed material. It is a qualitative measure of the radioactivity (broadly equivalent to toxicity), mobility and driving force. Thus a mobile, highly active material which can undergo self heating (e.g. high level liquid waste) has a higher harm potential than low level solid waste encapsulated in cement. Although the guide gives broad classes of harm potential the reality is that harm potential is a continuous variable and we judge each case on its merits. The guide addresses the rigour and conservatism appropriate to the classes or categories of nuclear plants.

It is important to understand that DSA deals exclusively with faults - deviations from the operating envelope - and does not consider normal operation except as the state from which faults develop. Therefore, the only consideration or constraint DSA puts on normal operation is the plant state the fault starts from.

In order to carry out DSA on a process it is essential to have a sound technical understanding of that process and plant. Much of the basic information is either identical to that needed for design or closely related to it. There is an ongoing iteration between the designer and safety analyst in the search for a suitable and sufficiently safe design, one which is economic, environmentally acceptable and operable. The outcome is that the options for the underlying processes are assessed and an informed decision made about the preferred option (optioneering). There are similar considerations for existing plant in periodic review but the options for change in order to achieve ALARP will be limited by what already exists.

The DSA technique is conceptually simple and follows the logic in Figure 1. Decisions must be taken and in most cases their order is not vitally important. There is one exception to this. There is a decision node labeled "low consequence". The intention is to remove the analysis burden where the consequences are low. However, this decision must only be carried out after the harm potential or hazard has been judged. The intention is not to place high reliance on mitigation (often filtration on nuclear chemical plant) but rather to soundly engineer the process for defence in depth in the first place. This decision must only be taken in the light of the overall assessment. In case of doubt, we would expect the decision to be prudently based.

The foundation for all this work is fault identification. The main characteristics we seek are that this has been carried out in a structured and comprehensive way. Such techniques might include HAZOP (Hazard and Operability studies) and FMEA (Failure Mode and Effect Analysis). In each case it is important that the individuals involved understand the underlying processes in the plant. The result should be a list of all potential faults for the plant (which may be grouped). As the design evolves the

balance of faults changes and so further fault identifications are carried out. In addition, the act of analysing the fault may identify further faults or knock on effects. These should also be analysed. It is very important to ensure that a change on one part of a complex plant does not have an unanalysed knock on effect on another part. The faults so identified become the Fault Schedule. The analysis takes each fault or groups of faults and analyses them in a technique very akin to event tree analysis. The technique simply assumes the fault initiation occurs and examines how the plant responds (usually without any safeguard). Depending on the harm potential of the sequence being considered, the safeguards are then put in place as part of the design and their quality constraints flow from their safety function (see later). One of the key aspects of this type of work is the iteration between the analysts and the designers or operators in the search for improvements to meet ALARP.

The options for dealing with faults during iteration are prioritised on what is known as the P61/P62 hierarchy (relating to Principles P61 and P62, in SAPs). P61 says, in essence, that faults should be avoided by safe passive means if possible. P62 says that the sensitivity to faults should be minimised. These concepts should be at the front of every engineer's mind when designing or analysing plant. It is a drive toward inherent safety (see Annex). It is difficult to overestimate the importance of this hierarchy and this has been the thrust of several initiatives on the part of HSE for some years [4,5]. Intrinsic or inherent safety should be the goal of all designers.

For plants which already exist (especially nuclear plants where access is often either difficult or impossible) the response to this hierarchy can be different to that for plants in design. At this stage the Reasonably Practicable or ALARP principle takes effect. Whilst the ALARP concept from TOR is easy to understand, in DSA the concept is not so easy to apply. The surrogate developed from many years of experience has been to establish the "modern standard". This is compared with what exists and those modifications that improve safety are highlighted. The judgment about what to implement is a combination of the balance of plant life, the hazard potential, the current deficit in performance, costs and benefits. The judgments in nuclear plant are often made on the basis of national and international experience. It is important to note, that it may be acceptable to partly meet the safety shortfall where a safety gain can be made at reasonable cost. However, a case based on cost-benefit analysis alone is unlikely to be sufficient since it would not normally address the deterministic drivers.

In summary the fundamental DSA technique is simple:

a. assume the fault occurs with the worst consequences (usually qualitatively).

b. assume the worst allowable plant state in terms of feeds, impurities, plant availability and other conditions including start up and shut down .

c. develop a technical description of how a fault develops and the engineering calculations which demonstrate how the system or plant behaves under that fault condition. Do not assume any control or safety provision operates correctly. Often this will be a transient analysis.

d. define the safety systems available to prevent, terminate or mitigate the fault on the basis of its significance.

e. determine if these meet the characteristics of quality safety systems e.g. P61/P62 hierarchy, single failure proof, diverse, redundant, segregated, capable of detecting the fault under fault conditions and so on. For more frequent faults, single failures in the safety system is assumed. This is one route for deciding how many redundant trains will be needed in some safety systems. In particular, safety related items which are maintained on line should be assumed to be in the worst maintenance state.

f. assess the effectiveness of the safety systems on a proportionately conservative basis to demonstrate adequate performance.

g. judge the adequacy of the safety systems against the Principle 25 criteria of no dose and at least one barrier intact except in the most severe cases and, ideally, having an accident rate less than 10^{-7} per annum for major accidents. For lower consequence faults such a frequency is likely to be both unnecessary and expensive given the potential harm from that fault. It is often the case that surrogate or subordinate rules can be developed to help engineers and analysts demonstrate adequate reliability.

In many cases faults can be considered as transients from steady state and modeling the time variation of some parameters can vary from simple to extremely complex. The more complex calculations are often carried out with computer codes e.g. Computational Fluid Dynamics (CFD). If such codes are used, they should be validated (ensure the code models plant behavior as accurately as possible with due conservatism) and verified (ensure that both the code and the input data are as correct as possible).

Uncertainties which lead to undue constraints on operations can often result in research and development either to look at ways of better preventing or terminating the fault or to reduce conservatism in the analysis by increasing confidence in the underpinning data. Also, the conservatism in the analysis helps develop a design that is robust and can tolerate unforeseen faults e.g. Three Mile Island's containment was not designed for the potential hydrogen ignition insult but, because the design was conservative, it tolerated it. Managing conservatism is covered further in the annex.

The results of such analyses give outputs that put constraints on the operations in question. These are referred to in total as the Safe Operating Envelope for the plant or operation. Licence Condition 23 calls for Limits and Conditions and these are usually derived from the DSA as shown in Figure 1.

CONCLUSION

Deterministic Safety Analysis is a very wide ranging technique intended to demonstrate the robustness of nuclear plant to tolerate relatively frequent faults. The technique is quite different to the more usual fault trees used for PSA (QRA) and serves a different purpose. DSA requires a detailed and comprehensive professional knowledge of how the operations (plants) respond to faults. This can involve anything from simple hand calculation to complex CFD computer models. The rigour and conservatism is a matter of judgment but increasing rigour and increasing conservatism is expected as the harm potential and uncertainty increase.

ANNEX - EXTRACT FROM THE GUIDE

This guide gives inspectors an interpretation of deterministic safety analysis (DSA) together with many of the associated engineering principles used in the assessment of licensees' safety cases. DSA will be used for the integrated concept of a robust demonstration of plant fault tolerance.

SAPs use the term DBAA, design basis accident analysis and so DSA incorporates DBAA and is closely related to it. Deterministic covers qualitative and quantitative, non-PSA aspects of assessments.

There are two functions of DSA that together encapsulate its essence:

a. DSA, together with the engineering justification, as presented in safety cases, provides a robust demonstration of fault tolerance in a proportionate manner;

b. DSA is an input into the engineering design to allow a judgment about the quality that needs to be built into the plant and thus achieve adequate reliability.

General: It is important to note that DSA and the inherent safety of the plant tend to deal with non trivial accidents with the aim of providing defence in depth in a proportionate manner. If the resulting plant is engineered on a sound, robust basis then good engineering practice should ensure less significant events are catered for. PSA should also catch any other identified fault.

It is also important to note that the order of the steps in the logic in Figure 1 is not usually important and that iteration will mean revisiting many aspects as designs evolve. The diagram does not show the multiple iterations that may be necessary.

In DBAA and DSA, uncertainties are dealt with by conservatism in the transient and radiological analyses. Similarly, P82 states that "The design should be conservative . . . ". It is convenient to distinguish between these "conservatisms". The analysis conservatism is preferred as it then permeates through to the engineering to deliver the safety function. Conversely, the margins built into the engineering using such features as robust, prudent design and large factors of safety to generate margins can make an equally valid contribution. It is always possible to balance one against the other or to balance conservatisms within analyses. Therefore, both conservatism and the engineering margins must be judged to yield an outcome that is both safe with an appropriate over design but not so over engineered as to make the outcome disproportionate, illogical or unworkable.

Source ID & Operating modes: The practice of identifying fault types or groups by identifying the characteristics of the activity source (see also Harm Potential later) with a top down approach is one of the key differences between a deterministic case and PSA. It is linked to P19 where faults are analysed as fault groups by taking the characteristics of the most restrictive fault as representative of the group. This allows analysis to be carried out in a comprehensible and suitably robust manner with a clarity that is often difficult with probabilistic techniques.

All initiating faults: This is the bottom up form of initiating fault identification and should generate a comprehensive and near complete overall fault schedule. There are different interpretations of SAPs for DSA purposes:

a. use either the full fault listing as the fault schedule;

b. use the listing derived from the P15 technique; or

c. use the reduced set which has been subject to the engineering out and low consequence filters to generate the fault schedule.

These faults or fault groups are then associated with their protection to generate the overall schedule. For the purposes of DSA either of the second two reduced set fault listings would be adequate. The key aspect is that a formal fault identification system has been used. The aim of the fault schedule is to show how faults have been identified and traced through the analysis. It is acceptable, and often desirable, to group faults rather than repeatedly analyse similar faults. Demonstration of completeness is still required.

It is important to note that initiating faults may originate in one plant on a multi plant site before propagating to where the consequence could potentially be realised. This should be covered by appropriate interface arrangements if the fault is not traced through the complete fault sequence.

Engineer out: (or design out) it is important to distinguish between faults which cannot happen, often because of technical choices to achieve inherently safer plant, and those which are very remote such as incredibility of failure cases (IOF). Faults which are engineered out are related to both of these. It then becomes physically impossible, provided the passive engineering and system configurations are maintained, for the fault to develop. Thus, the analysis should show the engineering and system configuration can be preserved and any change to these configurations should be assessed with the safety functions clearly in mind before changes are made. If gross failure would invalidate the case, in the absence of an IOF case, it may be necessary to make an incredibility of gross failure[1] (IOGF) argument. In all such cases maintenance would be expected to cover assurance of continued function by reference to appropriate schedules and, if necessary, repairs would be expected in a short timescale to keep the safety case valid or, if this is not possible, there should be another equivalent way of assuring continued safety function.

Low consequence: (not part of DSA) these are fault sequences, assessed on a conservative basis, unlikely to give doses in excess of the Ionising Radiations Regulations (IRR) annual whole body limits (or equivalent if other limits are more restrictive). Much depends on the assessment techniques but the aim is to remove the analysis burden where the upper consequence bound is low. Good practice should give an adequate answer in such cases. However, for any fault which passes this test (yes leg), there should be some form of safety measure. The quality and reliability expected from that safety measure should be proportionate to the harm potential. Care must be taken to account for the harm potential under consideration before deciding the fault is low consequence.

IOF: (not normally part of DSA) these arguments should be extremely rare but, if used, do need to be rigorous (P70). By convention, the failure frequency associated with such cases is taken to be 10^{-7} p.a. Thus an IOF argument is automatically taken down the BDBA leg. It is difficult to see how to avoid a severe accident analysis since the fault is likely to be severe and should be analysed as a severe accident.

[1]IOGF is used in this guide as shown (there are other interpretations). An example might be where a case depends on a static pressure generated by the pipe configuration to ensure a positive pressure gradient into the active medium under all reasonably foreseeable conditions. Thus the pipe configuration must be maintained yet the pressure would not be compromised by, say, a minor valve leak or a pin hole in a weld. A guillotine break would invalidate the case and is GROSS FAILURE.

It is also acceptable in some circumstances to use a multi legged argument (similar to an IOF argument). In these circumstances, where no single leg of the argument is sufficient to support the case, it may be possible to show that a combination of nominally lower quality safety provisions can cumulatively give the same degree of safety assurance as a smaller number of more robust systems. The legs of such a case should be as independent as possible to avoid common cause effects.

Severe accident analysis and Beyond Design Basis Analysis (BDBA) are not part of DSA. Both are carried out on a best estimate basis. Often BDBA will be bounded within the conservatisms of the DSA. BDBA is not expected outside PSA.

The basis for safety assessments has been established both in law and in published documents. Thus, the rigour expected can be judged on the basis of radioactive inventory, radio toxicity, "driving force" and mobility - the harm potential.

a. Highest tier: typically, operating reactor cores, highly active plant and equivalents2, unplanned criticality - full application of DSA with all assumptions rigorously justified. Full conservatism in analysis unless there is a sound justification for the values and / or modeling chosen. Codes and calculations should be fully validated.

b. Intermediate tier: typically reactor waste stores, medium active plant and equivalents[2] - DSA to be applied as far as is possible, assumptions must be reasonable and capable of justification. A due level of prudence would be expected in the assumptions and analysis. The modeling should be shown to be appropriate.

c. Lowest tier plant: typically low active waste handling, other low active plant and equivalents - detailed DSA is often not justified on the grounds of harm potential although it would be expected if the unit operations were being used elsewhere and the potential faults had already been modeled there (the cost of transferring the expertise is minimal) or where the analysis is very simple and easy to perform. Use "conservative best estimates" if the analysis is done at all.

For the purposes of P25 dose assessments there should be no doses from design basis fault sequences except in the most severe case where they should not exceed 100 mSv on a conservative basis (P25b). The equivalent dose for a worker should not exceed 200 mSv on a conservative basis (P25c). (These can be considered success criteria and may be compared to the BSO and BSL, although such comparisons are very inexact).

Of particular importance are P61 & 62 - these give the preferred response to faults. Use of dose minimisation by introducing mitigation factors into the release calculations should not be the first option in a DSA case. This is because such analysis does not take account of defence in depth and cannot usually be shown robust unless there is a guarantee that the physical phenomena modeled in the justification will be those prevailing during that fault. Thus, it is prudent to adopt the approach that prevention is better than cure. The following hierarchy has been developed:

[2] equivalence can be demonstrated by example where plutonium plants and HA plants have similar rigour in their analyses. The term equivalent is used to ensure every plant either has a "home" or is outside this regime because it has no safety significance in DSA. However, there may well be cases where inactive operations are claimed as safety measures and these should be engineered to a proportionate standard depending on the degree of reliance placed on them and the harm potential of the associated operation(s).

a. the design should be such that hazards are avoided (intrinsic or inherent safety);

b. the design should use passive features without undue reliance on control or safety systems;

c. any failure or fault should produce no significant deviation other than an indication that the fault has happened;

d. the plant should be brought to a safe state by continuously available safety measures or, if not practical, safety measures that need to be brought into operation;

e. administrative safety measures are an option where there is no reasonable alternative;

f. finally, mitigation (filtration / scrubbing) is then taken into account.

The aim is to be as near the top of this list as possible. This is not exactly what SAPs say but represents a strongly preferred interpretation. As a matter of good practice mitigating systems such as filtration and / or personal protective equipment (PPE) would be expected and it may well be that credit can and should be taken but they should not be the first "port of call". There will always be cases where mitigation is the only high reliability safety measure. This does not mean that there should be any lessening of effort to enhance the quality of the engineering higher up the hierarchy (even if it cannot be shown to be fully effective as a high quality system). Hence, only rarely should mitigation be the sole safety measure for faults analysed by DSA. Thus the outcome should be a plant or operation which has proportionate defence in depth (P65). This will be driven by the principles that allow no single failure to compromise the safety function (P78) and the best use of segregation, diversity and redundancy (P68, 79, 80 & 81). This hierarchy is consistent with HSE guidance.

The output from DSA is included in the schedule of safety systems and may be compared with the safety measures derived by other means. The expected outcome would be a list of faults related to the claimed protection often embodied in the Fault Schedule. There is an interface here, between the analysts and the other engineering specialisms who take the DSA output as an input. Iteration between the DSA inspector and other inspectors in the assessment of licensees cases for adequacy and sufficiency is extremely important in seeking a holistic view. The basis for trip settings, limits, Operating Rules (ORs), Operating Instructions (OIs) and Emergency OI's (EOI's) are included in this assessment.

Numeric Reliability: This is part of the ongoing iteration in the search for adequacy and sufficiency. The main use is to ensure that the application of the robust engineering principles has produced a reliable, workable solution being measured by this somewhat diverse technique. Ideally the overall numeric reliability at which the fault is realised to non trivial consequences should be at frequencies below which the figure ceases to have significance 10^{-7}p.a. but pragmatically, provided there are sufficient non-quantified safety measures then a numeric value lying proportionately between the BSO and BSL given in P45 - Plant Damage Frequencies would normally be good enough. There may be cases where very significant deterministic arguments cannot be quantified. In such cases full account should be taken of past precedent and, if there is no alternative, judgment should be used to designate a conservative reliability (P40 & P70). This judgment would be expected to be the exception.

DSA needs to show on a system by system basis (selected from the fault schedule or a group of faults) and for each fault associated with the selected system:

a. how the fault, if it develops, is terminated or mitigated: one expected technique is to assume the initiating event happens and follow how the plant reacts. This requires a technical analysis of the variables such as flow, mechanical loads, temperature / heat and rates of reaction and can be summarised as “a technical description of how a fault develops with the engineering calculations which demonstrate how the system or plant behaves under that fault condition” . The technique used must be appropriate to the underlying process(es);

b. the analysis continues with the engineered provisions are provided to detect and, if necessary, terminate the fault (see P61/62 hierarchy), what operator actions are required and, finally, how the effects are mitigated;

c. how the limits and conditions are set and how these plant items achieve the claimed reliability to meet such demands. Conditions refer to plant or system configurations that describe the safe working envelope of the operation(s) being considered.

These are all done on the basis of worst normally permitted states in terms of plant configuration and plant inputs. This is the main constraint DSA puts on normal operation. This technique is akin to event tree analysis since it represents a sequence in time with multiple potential outcomes depending on success or failure of the engineered provisions and operator actions. The outcome can be seen as somewhat diverse from fault tree treatments in isolation. Fault tree techniques are more useful in supporting the logic where engineered provisions or operator actions might fail.

Inspectors should be able to satisfy themselves that the plant which has been analysed is that which has been designed. This correspondence is vital to ensure the validity of the analysis and this correspondence should continue throughout plant life

The approach for existing plants to demonstrate ALARP is:

a. establish the existing standard - this includes not only changes in published standards but also the “standard” “what would the plant look like if it were designed today”. This drives optioneering studies which may find alternatives which meet the safety intent differently to the existing "standard". To ensure the LC23 demonstration this optioneering should be transparent.

b. examine the plant and establish what safety improvement is reasonably practical in terms of changes. This should be on a twofold basis - first, if the plant continues to the end of its expected life. Second there will be further modifications that might be made if the plant were to operate longer. In this case, the reasonably practical modifications should be listed taking the overall plant life as twice the design life or a further 20 years, which ever is longer.

c. if the plant operates beyond the expected life then those extended life modifications should be carried out as well as others that have become reasonably practical in the light of changing standards and knowledge.

It would be unusual for the entire design concept of a plant to be changed and radical change to many plants will be impractical. Thus, the reasonably practicable options

will be limited. The yardstick is the P61/62 hierarchy of preferred responses to faults. So arguments for existing plants should be similar to those for plant in design but the comparison with the P61/62 hierarchy and considerations of what is possible, or reasonably practical, may give different safety measures to achieve the safety function.

There may be cases (particularly when assessing older plant):

a. where reliability cannot be proven;

b. where the doses incurred to carry out such modifications to provide the target reliability could prove prohibitive;

c. where the increment in hazard potential during the modification would be unacceptable.

In such cases it will be necessary to make a proportionate argument on the basis of ALARP. Such arguments should include consideration of partial achievement to achieve a safety gain as well as full implementation. This is because partial achievement may be at reasonable cost without other undue detriment.

REFERENCES

1. Safety Assessment Principles for Nuclear Plants HSE 1992

2. The Tolerability of Risk from Nuclear Power Stations HSE 1992

3. Sizewell B Public Inquiry Report by Sir Frank Layfield Dept of Energy

4. INSIDE PROJECT AND THE INSET TOOLKIT: CEC Environment programme 1990-94, Contract No. EV5V-CT94-0416 "Inherently safer approaches to the design of chemical process plant" HSE Contract No 3225/R71.04

5. DRAFT Health & Safety Guide: Successful Design for Health & Safety
To be published.

6. Evidence from the Health and Safety Executive To the HOUSE OF LORDS SELECT COMMITTEE ON SCIENCE AND TECHNOLOGY, Inquiry on The Management of Nuclear Waste. Para 25 Submitted by: Jenny Bacon, Director General Health and Safety Executive. January 1998

7. 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

ACKNOWLEDGMENT AND DISCLAIMER

Thanks go to very many in HSE's Nuclear Installations Inspectorate for help and advice in developing this paper and the guide it describes. 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.

Figure 1 – DSA Logic Diagram