AN OVERVIEW OF THE UK REGULATORY EXPECTATION FOR DESIGN BASIS ACCIDENT ANALYSIS

Andy Trimble
Office for Nuclear Regulation, UK

Abstract - The UK Health and Safety Executive published its most recent regulatory expectations in the 2006 version of it's safety assessment principles (SAPs). This built on experience regulating the full range of facilities for which it is responsible. Thus the principles underpinning all regulatory safety case assessment are the same but the implementation differs depending on the application.

This paper will describe the published design basis accident analysis (DBAA) logic in context with other technical aspects of the regulatory expectation for safety cases. It will further illustrate the DBAA methodology with practical examples from actual experience on reprocessing plant gained over the last 15 years or so. Among the examples will be the relevance of conventional safety fault initiators to nuclear safety assessment. It will further demonstrate the derivation of facility limits and conditions necessary for nuclear safety.

Introduction

In the UK's nuclear regulatory regime, the Office for Nuclear Regulation (ONR) (formerly, The Health and Safety Executive's, Nuclear Installations Inspectorate) does not specify what should and should not be in a safety case [1]. However, the regulatory goals are set out in our Safety Assessment Principles (SAPs) [2]. These Principles were originally written for nuclear plant in design and were also used to inform periodic safety case reviews required under licence conditions. They are applied, proportionately, to all types of facility including power reactors, chemical plant, fuel fabrication facilities and waste stores.

In common with the goal setting principles of safety regulation in the UK, this is regulatory guidance which sets the regulatory expectation, not a rigid set of rules that need to be followed [6]. Rather, it is intended to assist both Nuclear Inspectors in setting consistent standards and to inform our licensees as to the benchmark they are expected to meet. In line with the injunction in UK safety law, all this is subject to the test "so far as is reasonably practicable" better known as As Low As Reasonably Practicable – ALARP (broadly equivalent to ALARA).

The Standard Licence

The heart of the regulatory control system is the licence and its attached conditions. The regulator can, at any time, attach to a licence conditions which appear necessary or desirable in the interest of safety. However, a standard set of licence conditions (LCs) [13] has evolved with the aim of producing consistent

safety requirements which are largely non-prescriptive, flexible and apply to all facilities. 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. 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, inspectors must make judgments about compliance with LCs. This is, in part, achieved using the relevant Safety Assessment Principles [2]. For example Principle FA.9 and the following SAPs paragraphs state that the purpose of Design Basis Accident Analysis is to provide information relevant to trip settings, plant operational limits (Operating Rules), plant operating instructions for fault conditions and the availability requirements for the sufficiency of safety systems. These form some of the fundamental safety controls on the relevant operations.

Technical SAPs - Definitions

In order to ensure proportionate protection for people and the environment and to set DBAA in context the following shows:

a. the key aspects and relationships DBAA has with other forms of analysis;
b. the key relationship with the engineering that delivers the safety function.

It is important that safety provisions reflect this holistic approach – which extends further than the aspects considered here.

The SAPs explicitly state that the technical (as opposed to organisational or cultural) aspects are fundamentally important to engineering a demonstrably safe, fault tolerant plant. The aspects considered here are:

a. Design Basis Accident Analysis (DBAA);
b. Probabilistic safety analysis (PSA sometimes known as QRA);
c. Severe accident analysis (SAA);
d. Good Radiological practice (GRP or Good Engineering Practice - GEP);
e. Waste Management.

Dealing with each of these broad areas in turn:

DBAA: is a robust demonstration of fault tolerance. It is intimately linked to the engineering that delivers the safety function by providing proportionate levels of protection. It also 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 DBAA 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. Thus the conservatism becomes a constraint or input on the engineering. DBAA is concerned with internal faults with larger harm potential and not normally with more minor events which are governed by radiological control arrangements [e.g. 9].

PSA: The main purpose of PSA is to demonstrate a balanced design (i.e. where there is no undue reliance on any particular safety feature) and that risks are minimised. The great strength of PSA is this overview. The real value is in the modeling itself and the insights this gives e.g. subtle cross plant interactions can be revealed. This is not covered by DBAA which deals with faults on a fault by fault basis.

It is very tempting to believe the figures produced by PSA. However, there is no basis for this and the numbers, useful in comparative terms, are little more than a crude estimate of the overall risks from the operation under consideration for comparison with criteria. It is carried out best estimate as far as possible.

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 (in these definitions, Three Mile Island was a severe accident but there was no significant radiological release). The prime difference between DBAA and SAA is in the way that data is used. SAA is based on best estimates and as such may well be bounded by the DBAA 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 SAA is to provide an input to emergency planning and to identify reasonably practical design improvements that can be implemented at reasonable cost.

GRP {GEP}**:** Because we deal with radiological hazards it is referred to here as Good Radiological Practice (GRP) although it is more commonly known as Good Engineering Practice (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 DBAA, the learning experience of the company and/or the industry are taken into account. Often GRP is embodied in design manuals or company standards. Quality engineering should only stray outside this standard with sound reason. There is also the concept of the "modern standard" which simply asks "what would the facility look like if it were designed today". This includes changes to engineering standards as well as progress in safety thinking nationally and internationally. The modern standard is used as a benchmark against which ALARP may be judged. Thus, the engineering is required to provide appropriate engineered provisions to deliver the safety function, reliably and with an appropriate, proportionate capability.

Waste Management: There are major additional waste management constraints as well as those normally required for safety. Much of the regulation is concerned with implementing government policy and GRP. Plainly, much of this reflects public opposition to careless waste accumulation and storage (disposal is dealt with under Environmental Legislation administered by the Environment Agencies). These aspect is becoming more and more relevant in the UK with its legacy of facilities designed before independent nuclear regulation.

DBAA

The detailed guidance for nuclear inspectors is found in T/AST/006 [3]. This is currently in revision following the revision to SAPs although there is nothing that detracts from the underpinning thinking in the current guide. There is a cross reference table on the web that allows the new SAPs principles to be read across to the previous ones as an interim measure [4].

This engineering fault analysis that the guide refers to as “Deterministic Safety Assessment”, includes DBAA and 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 to the inherent characteristics of the material with that potential. This is a measure of the activity (broadly equivalent to inventory), radio toxicity, mobility and driving force under the prevailing conditions. Thus a mobile, highly active material which can undergo self heating e.g. high level liquid waste, has a higher harm potential than intermediate 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 contains guidelines on the rigour and conservatism appropriate to the classes or categories of nuclear plants.

It is important to understand that DBAA deals exclusively with faults and does not consider normal operation except as the state from which fault sequences develop. Therefore, the only consideration or constraint DBAA puts on normal operation is this "fault starting" condition. The initiating fault frequency lower bound for DBAA is given in principle FA.5 as 10E-5 p.a. and the dose boundary in principle FA.2. However, it is accepted that it is disproportionate for all sequences to have the same rigour in their analysis resulting in extensive, highly diverse and redundant quality safety systems, and so, for infrequent faults (initiating frequencies <10E-3) a single line of defence is adequate provided doses are not excessive whereas, at higher initiating frequencies two independent lines of defence are more appropriate. If potential doses are extremely high, then each of these lines of defence may themselves be diverse and / or redundant to improve their reliability (capability is an engineering function). In addition, the higher the hazard or potential dose, then the more regulators will insist on a robust case which infers engineered provisions in preference to human interaction (subject to ALARP). However, should time be a factor, then is may be acceptable to argue that to achieve a timely hazard reduction, the balance may favour other approaches [10].

The DBAA technique is conceptually simple and can follow logic in the flowchart at Figure 1. Certain decisions must be taken and in most cases the order in which they are taken 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. The engineering inherent safety hierarchy tends to drive towards this approach with a preference for prevention over termination and finally mitigation (see later). Therefore, 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.

In order to carry out the analysis on a process it is essential to have a sound technical understanding of that process and the associated 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 both a suitable and sufficiently safe design, one which is economic, environmentally acceptable and operable. In DBAA the main concern is safety in the fault condition. 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 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 outcome of the fault identification should be a compilation 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 consequential effect on another part. 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 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 safety systems other than high reliability passive features such as shielding). Depending on the harm potential of the sequence being considered, the safety systems are then put in place as part of the design and their quality constraints flow from their safety function (see later).

The options for dealing with faults during iteration are prioritised on what is known as the inherent safety hierarchy (relating to Principles EKP.1 - 5 in SAPs) which may be summarised:

The design should be such that hazards are avoided (intrinsic or inherent safety);

- The design should use passive features without undue reliance on control or safety systems;
- Any failure or fault should produce no significant deviation other than an indication that the fault has happened;
- 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*;
- Administrative safety measures are an option where there is no reasonable alternative;
- Finally, mitigation is then taken into account.

Note: Filtration falls into the final category not the 4th (*). The aim is to be as near the top as possible.

In other words, these SAPs say faults should be avoided by safe passive means if possible and that that the sensitivity to faults should be minimised. This hierarchy should be at the front of every engineers mind when designing or analysing designs. This provides a driver towards inherently safer facilities. It is difficult to overestimate the importance of this hierarchy and this has been the thrust of several initiatives for some years [5]. Intrinsic and inherent safety should be the target for all facilities. The practical outcome is to drive the safety systems closer to the part of the operation where the faults initiate before considering safety systems that act later or further on in the fault sequence.

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 principle is conceptually simple, in a DBAA the concept is not so easy to apply. The surrogate developed from many years of experience has been to establish the "modern standard". The modern standard simply asks “what would the facility look like if designed today?”. Thus, it involves not just changes to published engineering codes and

standards but also advances in safety thinking, nationally and internationally. This is compared with what exists (a gap analysis) and those modifications that improve safety are highlighted. The judgment about what to implement is a combination of the balance of plant life, the potential hazard, the current deficit in performance, costs and benefits. The judgments in nuclear plant are often made on the basis of experience both national and international. 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. Equally, a case based on cost-benefit analysis alone is unlikely to be sufficient.

In summary the fundamental DBAA technique is simple:

a. assume the fault occurs with the worst possible harm potential (usually qualitatively). Often this will be a design limit for the facility or a parameter derived from the design limit;

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. Put in place the safety systems;

d. determine if the safety systems meet the inherent safety hierarchy;

e. determine if these meet the characteristics of quality safety systems e.g. single failure proof, diverse, redundant, segregated, capable of detecting the fault under fault conditions, provide sufficient defence in depth and so on. For more frequent faults (>10E-3 initiating frequency), single failures in the safety system are 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. judge the adequacy against the SAPs Target 4 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.

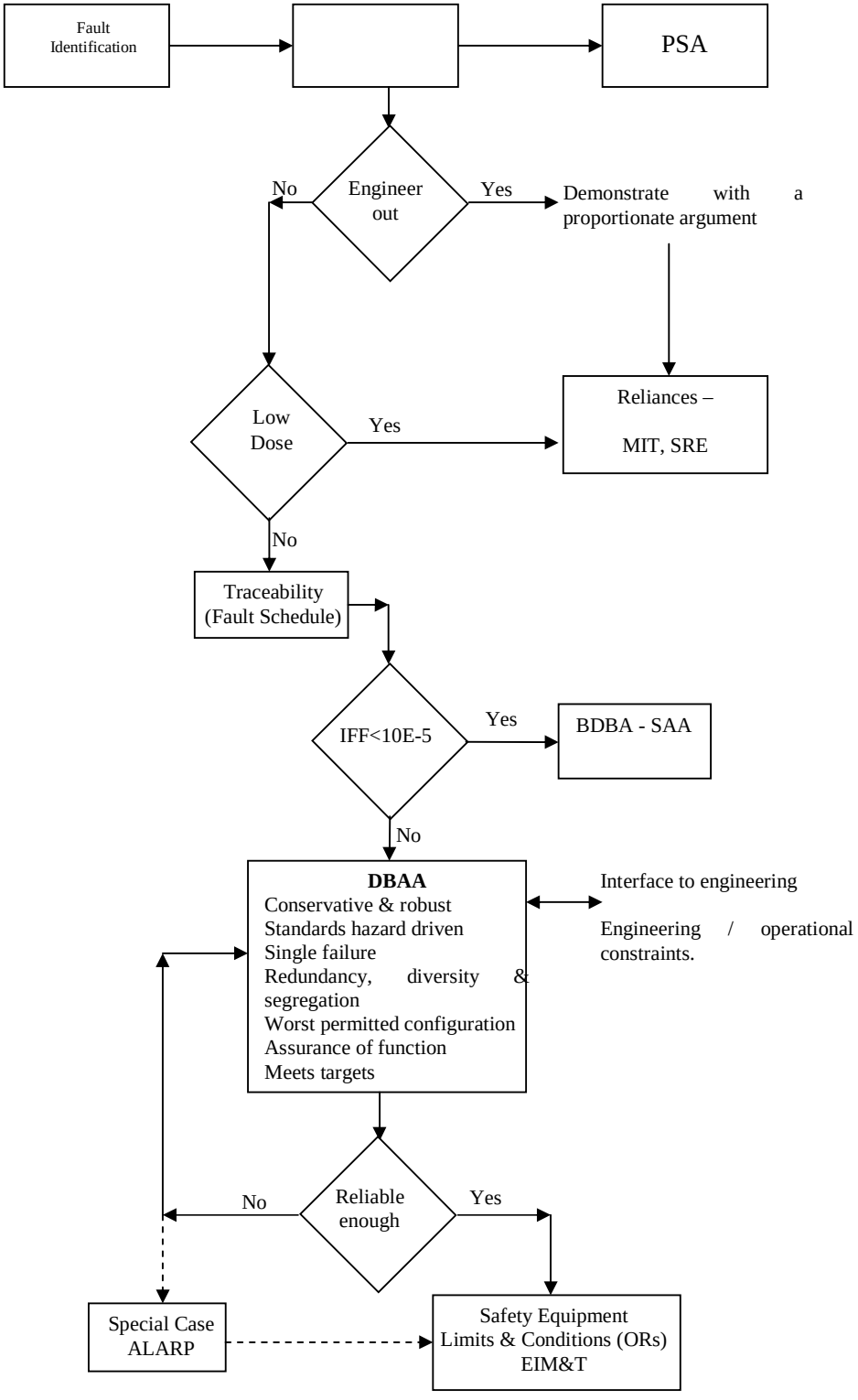


Figure 1: DSA Logic diagramme

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 would have tolerated it.

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 should be derived from the DBAA as shown in Figure 1.

LC 23 defines Operating Rules (ORs) as Limits and Conditions.

a. Limits are operational parameters such as temperature, pressure or concentration that operations must be controlled within in order to remain within the safe operating envelope;
b. Conditions are plant configurations that must be complied with in order to ensure the safe operation of the plant.

Both of these are primarily derived from the DBAA although there are a number of exceptions. Most notable will be the feed specification for the facility. This forms the basis for both the underpinning design and the analyses on which the ORs are based. The regulatory guidance [11] is being developed to bring it further into line with good international practice [12] and should be available by the time this paper is published.

Practical Examples

Here we consider how “conventional hazards” affect the nuclear analyses. Most conventional safety matters that affect nuclear safety fall into one of two categories:

a. Failure prevents the safety function being delivered e.g. electric power or steam supplies;
b. A reactive chemical or mechanical device interacts with the facility to initiate or aggravate a fault.

There are a number of these which are generic to most reprocessing facilities, some of which are covered below.

Hydrogen: The UK convention on hydrogen is that it should be controlled to 25% of the lower flammable limit (LFL) – 1%. Similarly we have accepted that reaching the LFL is acceptable under fault conditions provided the nuclear safety case is robust and conservative. In other words, the LFL is unlikely to be breached in practice. These are broadly equivalent to the limits used in conventional industry. The difference in the nuclear field is that we require this robust safety case to demonstrate that such levels will be achieved. It is worth noting that there is no distinction between radiolytic hydrogen and hydrogen from other sources e.g. reagent hydrogen or from battery charging. Our licensees have developed methodologies for meeting these limits [e.g. 7].

In plant handling solutions of plutonium or other alpha emitters in closed tanks, it is often difficult to back fit a purge to control hydrogen concentration from radiolysis. It is acceptable to use lines intended for other functions e.g. pressure or level indication (provided the primary safety function is not compromised), to supply enough air to control the hydrogen below the LFL.

Cranes: As facilities develop and age there is often a need to either replace or add to the exiting plant and equipment. In common with most chemical plant this drives the need for construction cranes. The threat is either crane collapse or impact between the crane load and a sensitive operation. In the UK our sites are limited in area and so, particularly with older facilities, they tend to be relatively close together. This is particularly the case when decommissioning. Our view is that cranes near sensitive, high hazard should be avoided if possible as the consequences can be serious. To this end our licensees have gone to extreme lengths to avoid larger cranes, instead using jacking arrangements or lifting frames [8] and other means to minimise the use of mobile cranes.

There are some preferences for using cranes which include:

a. Remove or minimise the hazardous inventory in the potentially affected plants.
b. Avoid the use of cranes or, where necessary, minimise the size and reach of smaller cranes used to erect other lifting devices.
c. Where cranes must be used ensure they are used in the safest possible way e.g. limit travel, are operated by reputable contractors, are controlled on site according to good crane practice and are only used under well defined weather conditions.

Reactive chemicals: Probably the most interesting are the nitrogen based chemicals used in the salt free flow sheet for THORP. Hydrazine, hydroxylamine and hydrazoic acid are present either as reagents or as decomposition products. They represent a direct safety implication as reagents because their instability makes them potentially a fire hazard. This fire hazard could not only have the direct effects of the fire itself but also represent a loss of control with the potential for criticality in the separation plant.

Similarly, they decompose to ammonium compounds in the process which, with the nitric acid based flow sheet, produce ammonium nitrate. Ammonium nitrate in sufficient quantities and under the right conditions is a low grade explosive. Fortunately, most of today's nuclear chemical plants are small enough for this to be no more than a minor concern.

In addition, the odourlesss kerosene (used in the solvent extraction process), when mixed with ammonium nitrate forms the industrial explosive ANFO (ammonium nitrate – fuel oil). This further goes to highlight the importance of good solvent control in reprocessing plant. However, the nuclear safety case does need to demonstrate adequate control over these phenomena and that the DBAA criteria are met.

The solvent control example highlights one other aspect of nuclear chemical plant that is not so prevalent in power reactors, namely, facility – facility interactions. On a multi facility site, such as Sellafield, faults initiated on one facility can propagate to another and there must be an adequate analysis to cover this resulting in suitable and sufficient safety systems to deal with it (SAPs principle ST.6).

Conclusion

In the UK, DBAA is a nuclear industry wide technique that is intended to demonstrate the robustness of nuclear facilities to tolerate relatively frequent, potentially serious faults. Although the form of analysis varies across the facilities we regulate the overall intent is the same. The technique is quite different to the fault trees used for PSA (QRA) which serve a different purpose. It requires a detailed and comprehensive professional knowledge of how the operations (plants and facilities) respond to faults. This can involve

anything from simple hand calculation to complex computer models. The rigour and conservatism is a matter of professional judgment but increasing rigour and increasing conservatism is expected as harm potential and uncertainty increase.

The output of DBAA are both the operational and engineered controls necessary for robust safety in nuclear facilities. In addition, the level of examination, maintenance, inspection and testing to achieve appropriate capability and reliability should also flow from the same analysis and its associated engineering. Thus, there should be an assurance that facilities operated in compliance with these parameters should be safe from internal faults in all reasonably foreseeable circumstances.

References

[1] Technical assessment guide T/AST/051, Guidance on the purpose, scope and content of nuclear safety cases. http://www.hse.gov.uk/nsd/tast051.htm

[2] Safety Assessment Principles for Nuclear Facilities 2006 Edition, Revision 1 http://www.hse.gov.uk/nuclear/saps/saps2006.pdf

[3] Deterministic safety analysis and the use of engineering principles in safety assessment http://www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast006.pdf

[4] 1992 to 2006 SAPs Cross-reference Table http://www.hse.gov.uk/nuclear/saps/crossreference.pdf

[5] The storage of Liquid High Level Waste at BNFL Sellafield – an updated review of safety. A report by HM Nuclear Installations Inspectorate. HSE February 2000.

[6] Trimble G A, Proc HAZARDS XX Symposium Series 154 P236 – 246, Background to and experience of using the NII's new safety assessment principles – Learning for the high hazard sector? I Chem E 2008

[7] ID Kempsell, MJ Wakem, MP Fairclough, JM Ingram, Proc HAZARDS XVI, Symposium Series 148, P523 – 540, Hydrogen Explosions - An Example of Hazard Avoidance & Control, I Chem E 2001

[8] e.g. http://www.mammoet.com/Default.aspx?tabid=692

[9] Ionising Radiations Regulations 1999 (IRR99) SI 1999 No. 3232

[10] Trimble A, Proc HAZARDS XIX, Symposium Series 151 P792 ff , Summary of the current position on decommissioning safety cases and the control of operations. I Chem E

[11] T/AST/035 Issue 2, The Limits and Conditions for nuclear plant safety. http://www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast035.pdf

[12] IAEA "Operating Limits and Conditions and Operating Procedure for Nuclear Power Plants", IAEA Safety Standards Series, Safety Guide No. NS-G-2.2 http://www-pub.iaea.org/MTCD/publications/PDF/Pub1100_scr.pdf

[13] Licence Condition Handbook http://www.hse.gov.uk/nuclear/silicon.pdf

Acknowledgment

Thanks go to many in ONR for help and advice in developing this paper and the guide it describes. The opinions here are those of the author.

Disclaimer

No part of this paper should be taken as definitive interpretation of policy, UK law or their application.

SAPs
Engineering & DBAA

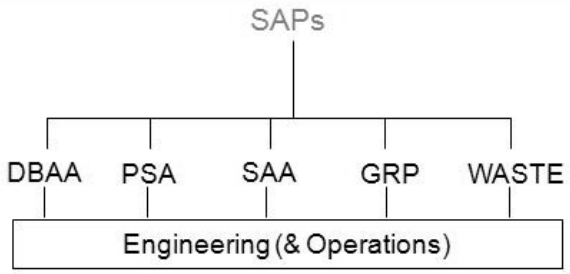
Dr Andy Trimble
HM Superintending Inspector
(Nuclear Installations)

Office for Nuclear Regulation
An agency of HSE

CONTENTS

- Context setting & Underlying thinking
- Interpretation
- Conclusions
- Closing thought

Office for Nuclear Regulation
An agency of HSE



Office for Nuclear Regulation
An agency of HSE

Proportionality

Based on Hazard: Hazard = Harm Potential

Harm Potential is a function of the intrinsic material properties under the prevailing conditions:

- radioactive inventory,
- radio toxicity
- "driving force" and
- mobility.

For example: these are all High for Highly Active Liquor – Hence rigorous & robust case,

conversely

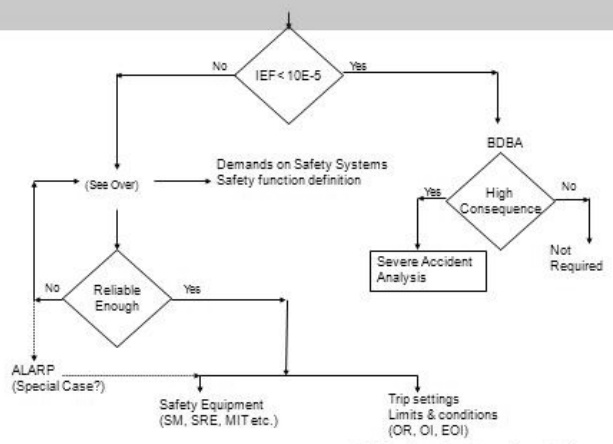
- Mobility is LOW for Glass and the plant is passively safe (walk away)

Office for Nuclear Regulation
An agency of HSE

Inherent Safety Hierarchy (see also EKP 1 – 5)

- The design should be such that hazards are avoided (intrinsic or inherent safety);
- The design should use passive features without undue reliance on control or safety systems;
- Any failure or fault should produce no significant deviation other than an indication that the fault has happened;
- 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;
- Administrative safety measures are an option where there is no reasonable alternative;
- Finally, mitigation is then taken into account.

Office for Nuclear Regulation
An agency of HSE

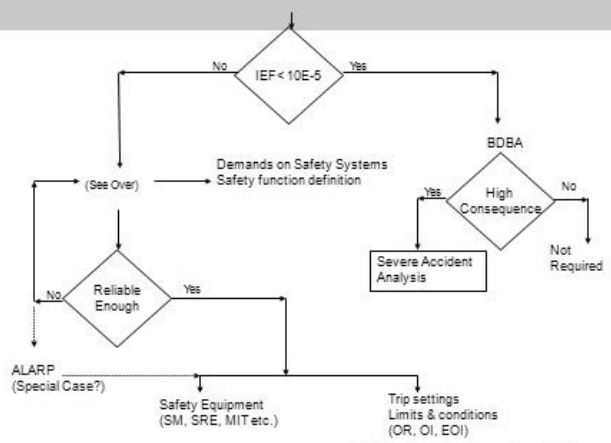


Office for Nuclear Regulation
An agency of HSE

DBAA

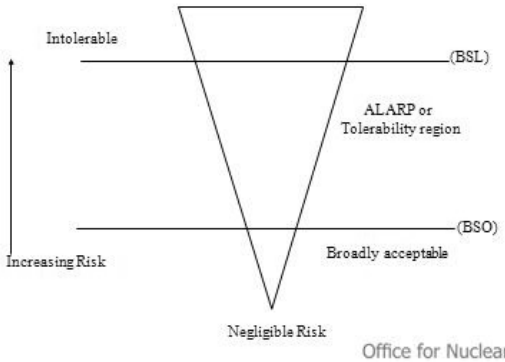
- Conservative & robust
- Standards related to hazard (ALARP)
- Safeguards as high up Inherent safety hierarchy as possible
- Single failure
- Redundancy, diversity, segregation
- Multiple physical barriers
- Worst permitted plant configuration
- No breach & at least one barrier intact (Target)
- No dose except in most severe cases (Target)
- Assurance of continued function

Office for Nuclear Regulation
An agency of HSE



Office for Nuclear Regulation
An agency of HSE

TOR Framework



Office for Nuclear Regulation
An agency of HSE

CONCLUSIONS

The case should show the prime DBA characteristics being ROBUST and FAULT TOLERANT (infers optioneering) thus, a sound technical justification will be required to underpin the case

So ALARP (SFAIRP) can be achieved and thereby compliance with the law.

Thus meeting HSE's policy of securing compliance with the law in line with the principles of proportionality, consistency, transparency and targeting on a risk related basis.

Office for Nuclear Regulation
An agency of HSE

CLOSING THOUGHT

"HSE {ONR} does not advocate relying solely on quantified risk assessment, particularly as this may be misused to justify poor practice when factors relating to good engineering practice in design or construction may be more meaningful. It is our view that probabilistic estimates, particularly with such low numbers, must always be treated with caution as there are inevitably high levels of uncertainties in both the data they are based upon and the calculational models which produce them. Safety cases must therefore be primarily based on other elements such as defence in depth and good engineering practice. Probabilistic or quantified risk assessment should only be on input in the overall case. The normal approach used for nuclear installations of robust engineering design, defence in depth and the use of deterministic conservative assessments of both normal operation and fault behaviour, with probabilistic risk assessments to judge the significance of uncertainties, should be sufficient to ensure public protection both now and in the future".

Office for Nuclear Regulation
An agency of HSE