

NUCLEAR SAFETY DIRECTORATE - BUSINESS MANAGEMENT SYSTEM		
TECHNICAL ASSESSMENT GUIDE DETERMINISTIC SAFETY ANALYSIS AND THE USE OF ENGINEERING PRINCIPLES IN SAFETY ASSESSMENT		T/AST/006
		ISSUE 03
Approved By: <i>M Weightman</i>	M W Weightman	Issue Date: 31/07/00
Open Government Status: Fully Open		Review Date: 30/07/03

1. Purpose and Scope

1.1 This guide gives specialist 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.

1.2 The term DSA has been coined to avoid the confusion of using DBA (as in the previous version of this guide) with a very similar term used in reactor safety work. In non reactor work, the terms DSA and DBA are synonymous (as applied in the previous version of this guide). The SAPs use the term DBAA, design basis accident analysis and so DSA incorporates DBAA and is closely related to it. In this guide the term deterministic covers qualitative and quantitative, non-PSA aspects of such assessments.

1.3 This guide does not explain the meaning and interpretation of each and every principle from SAPs, rather it lays down a logic to show both the possible content and interfaces DSA has with other parts of SAPs. Thus there are aspects covered in this guide which are not strictly DSA but are related to it and aspects that are DSA which are covered elsewhere (see **reference section**).

1.4 As with SAPs themselves, this interpretation of DSA relates primarily to plant design. However, in common with accepted practice, this guide also forms the benchmark for existing plant and there is guidance on how judgments may be made on reasonably practicable grounds in such assessments.

1.5 This guide supersedes the previous guide with a comparable designation^[1]. As with all guidance, inspectors should use their judgment and discretion in the depth and scope to which they apply this guide. It is important to stress that there is a wide variety of nuclear plant, so flexibility is also needed. Comments on this guide,

and suggestions for future revisions, should be recorded on the appropriate registry file.

2. SAPs addressed

2.1 The DBAA Safety Assessment Principles (SAPs) start at P20. Those that address the purpose of DBAA, and the means of identifying design basis fault sequences are:

“(P20) The analysis of design basis accidents should be carried out to provide a robust demonstration of the fault tolerance of the engineering design and the effectiveness of the safety systems.

(P21) The safety case should present a list of all initiating faults which are included within the design basis of the plant. All initiating faults identified under P16 {listing initiating faults} should be considered for inclusion in this list, but the following need not be included:

(a) faults internal to the plant which have an expected frequency lower than about 10^{-5} per year; and

(b) failures of structures, systems or components for which acceptable special case arguments have been made in accordance with P70. { ‘special case procedure’}

(c) hazards excluded in accordance with P119. {guidance for inclusion of internal and external hazards in DBA}

(P22) The design basis fault sequences should then be identified, starting with each design basis initiating fault and including as appropriate: failures consequential upon the initiating fault, failures expected to occur in combination with it due to having a common cause, and single failures in the safety systems in accordance with P78 {the single failure criterion}. The worst normally permitted configuration of equipment outages for maintenance, test or repair, should be assumed, and correct performance of safety-related and non-safety equipment should not be assumed where it would alleviate the consequences.

Sequences with very low expected frequencies need not be included.

(P23) The transient and other plant analyses (see P17 {need for various analyses}) of design basis fault sequences should be performed on a conservative basis, sufficient to provide a high degree of confidence that the requirements of P25 {characteristics of design basis fault sequences} will be met.”

2.2 The remaining DBAA SAPs address consequence and safety measure criteria, and are addressed in other Assessment Guides. A fuller appreciation of the scope can be gained by referring to **Appendix 1**.

3. Relationship to Licence and other Relevant Legislation

3.1 The main licence conditions (LCs) that relate to this guidance are shown below:

1) 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.

2) 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; ...

3) 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.

4) 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.

3.2 These LC requirements are linked to the DBAA SAPs in P27 which states the purpose of DBAA is to provide information relevant to trip settings, plant operational limits (Operating Rules) and plant operating instructions for fault conditions and in P26 which addresses the minimum requirements for the sufficiency of safety systems .

3.3 Thus these conditions require written safety cases for all safety-related operations during all stages of plant life, and these cases must **adequately demonstrate** safety (Licence Condition 23).

3.4 Adequacy is judged on a technical basis using the underlying concept of goal setting. These goals are set by SAPs and there is compelling advice [2] that avoidable inconsistencies between licensees' criteria and SAPs should be minimised. Thus, we might reasonably expect an adequate safety case to mirror much in SAPs.

4. Advice to Specialist Inspectors

4.1 This is expanded in **Appendix 1**. In seeking this robust demonstration of plant fault tolerance the key ideas and concepts are:

1) the importance of the P61 / P62 “hierarchy” (hazard avoidance and fault response);

2) the concept of a robust demonstration of safety vested in safety measures, the need for which is derived from a technical description of how faults develop with the technical calculations that demonstrate how the plant behaves;

- 3) the degree of robustness and rigour expected in a safety case based on tiering as a measure of the harm potential which is a function of radioactive inventory, radio toxicity, “driving force” and mobility;
 - 4) reliance on prevention rather than mitigation unless there is no reasonably practicable alternative;
 - 5) the P25 success criteria of no dose except in the most severe cases and no more than 100 mSv to a member of the public and 200 mSv to a worker
 - 6) the inclusion of a final reliability step as a check for the adequacy of safety measures;
 - 7) preference for an “event tree” type of analysis to complement fault tree analysis;
 - 8) inclusion of As Low As Reasonably Practicable (ALARP) guidance consistent with other assessment guides.
-

Appendix 1 - Further guidance to assessors

5.1 Introduction

- 1) This appendix contains further guidance for specialist inspectors in the assessment of licensees' deterministic safety analysis cases linked to the associated engineering justification.
- 2) There are two functions of DSA that together encapsulate its essence:
 - i. DSA, together with the engineering justification, as presented in safety cases, provides a robust demonstration of fault tolerance in a proportionate manner;
 - ii. 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.

3) It is difficult to show the entirety of the principles applicable to DSA although some other relevant technical guides are shown in the reference section.

5.2 Guidance Layout

1) a logic **flow diagram** to highlight the relationships between the main principles that are expected in DSA (Page 6) with some further universal principles that underpin the logic;

2) an expansion of the terms and ideas used in the logic flow diagram;

3) an interpretation of the overall principle of “reasonably practicable” for application to existing plant which is consistent with that in other assessment guides;

4) an alternative approach to another form for DSA which is different to that implied in SAPs but consistent with their intent.

5.3 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 radiological practice should ensure less significant events are catered for to demonstrate the adequacy of the safety systems. The PSA should also catch any other identified fault.

5.4 It is important to note that the order of the steps in the logic is not usually important and that iteration will often mean revisiting many aspects as designs evolve. This is expected, particularly on larger projects. For simplicity the flow diagram does not show the multiple iterations that may be necessary in the design process, for example, to optimise the safety provisions by introducing changes to climb the P61/P62 hierarchy (see later) or balance out one fault provision against another. There are other principles that cross reference the DBAA principles e.g. P120 et.seq. and P325 et.seq. These are not shown in

the diagram.

5.5 In DBAA, and thus DSA, uncertainties are dealt with by appropriate conservatism in the transient and radiological analyses (para 45). Similarly, P82 states that "The design should be conservative ..1. ". It is convenient, for the purposes of this guide, to distinguish between these "conservatisms". The analysis conservatism is preferred since it then permeates through to the engineering intended to deliver the safety function. Conversely, the margins built into the engineering to deliver that function using such features as robust, prudent design and large factors of safety to generate engineering margins can make an equally valid contribution depending on the safety function(s) being considered. 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. Inspectors must take the holistic view of the engineered outcome and balance both conservatism and engineering margins with due over design to ensure proportionate reliability.

5.6 Other SAPs applicable to the logic:

- 1) P47 & P48 Validity of analysis
- 2) P49 Knock on effects of faults
- 3) P50 Feasibility of claimed actions in response to faults
- 4) P51 et seq. Ongoing data validity
- 5) P86 et seq. Data and modeling
- 6) P181,182 Fault detection & termination
- 7) P191, 192 Relationship between measured variable and plant behaviour
- 8) P196, 197 Reliability of safety systems

5.7 Interpretation of principles and terms for the purposes of this work (Refer to logic flow diagram).

- 1) **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 a PSA. It is often linked to P19 where faults are analysed as fault groups by taking the characteristics of the most restrictive fault as representative of the entire group. This technique allows analysis to be carried out in a comprehensible and suitably robust manner with a clarity that is often difficult with probabilistic techniques. This can be considered as top down analysis.

2) **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:

- i. use either this full fault listing as the fault schedule;
- ii. the listing derived from the P15 technique
- iii. use the reduced set which has been subject to the engineering out and low consequence filters to generate the fault schedule.
- iv. In some cases two fault schedules may result - one for PSA and one for DSA (see later). These are then associated their protection to generate the overall schedule^[15].

3) For the purposes of DSA either of the second two reduced set fault listings are adequate although, in practice, it may be easier to list the full identified fault set which is that used for Probabilistic Safety Assessment (PSA). However, there is no doubt that the PSA works from the full fault set. The key aspect is that a formal fault identification system or systems have been employed. Techniques such as Event Tree Analysis, Hazard and Operability studies (HAZOP), Failure Mode and Effects analysis (FMEA), Reliability Centered Maintenance (RCM) are all applicable for identifying faults and should aim for completeness. The aim of the fault schedule (wherever it is in the logic) is to show how faults have

been identified and traced through the analysis process. It is acceptable, and often desirable (see above), to group faults rather than repeatedly analyse similar faults time after time (usually under the P19 bounding case logic). However, demonstration of completeness is still a requisite.

4) 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 from initiation through the complete fault sequence.

5) **Engineer out:** (often known as design out) it is important to distinguish between faults which cannot happen, often because of technology 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 these. They are those where it is physically impossible, provided the engineering and system configurations are maintained, for the fault to develop. Most often this will be achieved using passive engineered features. Thus, the analysis should show the engineering and system configuration can be preserved to guarantee the impossibility of the fault and so are safety related. Any proposed change to these configurations should be assessed with the safety functions clearly in mind before actual 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 failure¹ (IOGF) argument. In all such cases maintenance would be expected to cover assurance of continued function in appropriate schedules and, if necessary, repairs would be expected in a short timescale to keep the safety case valid or there should be another equivalent way of assuring continued safety function.

6) **Low consequence:** (not part of DSA) these are fault sequences, assessed on a conservative basis, that are unlikely to give doses in excess of the Ionising Radiations Regulations (IRR) annual whole body limits (or equivalent if other limits are more restrictive) and in many cases these doses are likely to be of the same order as those

for normal operations. Plainly, much depends on the assessment techniques but the aim is to remove the analysis burden where the upper consequence bound is low. Good radiological practice should give an adequate answer in such cases. (It can also be acceptable to use these limits as a surrogate for the P25(b) “no dose” assessment - see also ALARP guide.) 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. (see also Engineer out, degree of rigour, and other assessment guides). Care must be taken to account for the harm potential under consideration before deciding the fault is low consequence.

7) **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 against a fault is automatically taken down the BDBA leg. It is difficult to see how to avoid some sort of analysis, such as severe accident analysis, if appropriate, since the fault is likely to be severe and will need to be analysed as a severe accident (otherwise why go to the time and expense of an IOF argument).

8) it is also acceptable in some circumstances to use a multi legged argument (which has similar characteristics 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 these nominally lower quality safety systems can cumulatively give the same degree of safety assurance and reliability as a smaller number of more robust systems. It is important that the legs of such a case should be as independent as possible to avoid common cause effects.

9) Severe accident analysis and Beyond Design Basis Analysis (BDBA) are not usually part of DSA. They are both carried out on a best estimate basis. Other assessment guides apply⁹. Often the BDBA will be bounded within the other conservatisms of the DSA. BDBA is not normally expected outside PSA. Conversely,

faults beyond the design basis will need to be addressed in the PSA^[7] and may need analysis as severe accidents. In addition there may also be faults that need to be analysed because the DSA provisions have failed. This may require judgment about the degree of conservatism in the DSA itself.

10) The basis for safety assessments has been established both in law ^[3] and in published documents ^[4,5]. Thus the degree of rigour expected can be judged on the basis of radioactive inventory, radio toxicity, “driving force” and mobility - the *harm potential*.

- i. 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 or modeling chosen. Codes and calculations should be fully validated.
- ii. Intermediate tier: typically reactor waste stores, medium active plant and equivalents - 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.
- iii. 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.

This has established the tiering related to operations that might reasonably fit in each tier.

11) 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). This is consistent with other guidance.

12) Of particular importance are P61 & 62 - these give the preferred response to faults. Use of dose minimisation by introducing modification factors into the release calculations should not be the first option in a DSA case. This is because such analysis 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. Therefore, it is prudent to adopt the approach that prevention is better than cure and so the following hierarchy has been developed based on these principles:

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

13) The aim is to be as near the top of this list as possible. Plainly, this is not exactly what the SAPs say but it 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 such as filtration is the only high reliability safety measure but *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. See also multi legged arguments above in **paragraph 7**)*. Rarely should mitigation be the sole safety measure for faults analysed by DSA even though some of the other safety measures may not be claimed directly in the analysis. Thus the outcome should be a plant or operation which has defence in depth (P65) in a proportionate manner. 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 [4,6].

14) The output from DSA is included in the schedule of safety systems and may be compared with the safety measures derived by other means (see appropriate assessment guides and equivalent standards). The expected outcome would be a list of faults related to the claimed protection (see also fault schedule above). 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 specialist inspectors in the assessment of licensees cases for adequacy and sufficiency is extremely important in seeking a holistic view of the safety case. Conversely, the basis for trip settings, limits, Operating Rules (ORs), Operating Instructions (OIs) and Emergency OI's (EOI's) are included in this assessment.

15) **Numeric Reliability:** This is part of the ongoing iteration (iteration is not shown on the flowchart) in the search for adequacy and sufficiency as part of the design process. The main use in this context is to ensure that the application of the robust engineering principles has produced a reliable, workable solution, the realization 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 in this context (10^{-7} p.a. - Sizewell B public Inquiry [2]) but pragmatically, provided there are sufficient non-quantified safety measures, subject to ALARP, then a numeric value lying proportionately, based on the tier in which the fault is judged to lie, between the Basic Safety Objective (BSO) and Basic Safety Limit (BSL) given in P45 (Plant Damage Frequencies) would normally be good enough. For example, if a sequence initiates at 10^{-1} p.a. then to achieve a sequence frequency of 10^{-7} p.a., the safety systems should ideally deliver up to 10^{-6} pfd and 10^{-3} to achieve the BSL. 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 other alternative, judgment should be used to designate a suitably conservative reliability figure (P40 & P70). However, this judgment would be expected to be the exception rather than the rule.

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

How the fault, if it develops, is terminated or mitigated:

- i. 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);
- ii. what engineered provisions are provided to detect and, if necessary, terminate the fault (see P61/62 hierarchy), what operator actions (if any) are required and, finally, how the effects are mitigated;
- iii. 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)

17) 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. It does not follow the same logic as fault tree analysis. Thus, the outcome can be seen as somewhat diverse from fault tree treatments used in isolation. Fault tree techniques are not particularly helpful in this type of analysis, although they can support it by developing the logic whereby specific engineered provisions or operator actions might fail.

18) 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 such a correspondence should continue throughout plant life

5.8 ALARP for existing plant

1) The approach for existing plants to demonstrate ALARP is:

- i. establish the existing standard - this includes not only changes in the published standards but also the "standard" "*what would the plant look like if it were designed today*". Thus the entirety of this guide (and others) may be taken to apply to assessment for such plants by influencing the "standard". This is a driver for optioneering studies which may establish alternatives which meet the safety intent in a different manner from the existing "standard". To ensure the demonstration required by LC23, this optioneering should be transparent.

- ii. examine the plant and establish what safety improvement is reasonably practical in terms of changes (see also ALARP guide). This should be on a twofold basis - first, if the plant continues to the end of its expected life (usually 25 or 30 years as a design life, although this may be longer for some plants such as waste stores). 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 (rule of thumb) the overall total plant life as twice the design life or a further 20 years, whichever is longer.
- iii. if the plant operates beyond the expected life then those modifications required for the extended life should be carried out as well as any others that have become reasonably practical in the light of changing standards and knowledge.

2) It would be unusual for the entire design concept of a plant to be changed and similarly, radical change to many plants will be impractical. Thus, in the majority of cases, the reasonably practicable options will be limited. The yardstick is usually the P61/62 hierarchy of preferred responses to faults. Thus the arguments for existing plants would be expected to contain similar arguments 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 same safety function.

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

- i. that reliability cannot be proven;
- ii. that the doses incurred to carry out such modifications to provide the target reliability could prove prohibitive;
- iii. that the increment in hazard potential during the modification would be unacceptable.

- iv. 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.

5.9 Alternative Approach

1) Experience shows that there is an alternative method for analysing faults (c.f. 5.3 para 16) which does not spring directly from the SAPs yet is consistent with its intent. It has been extremely useful in analysing faults for which no initiating frequency can sensibly be determined (although this does not make it any less useful if a frequency can be determined). Often the inability to derive an initiating frequency can be because the fault has been engineered out.

2) The technique is simply:

- i. examine the operation being considered and determine the harm potential;
- ii. determine the features that prevent that harm potential from being realised (referred to as "reliances");
- iii. compare these reliances with the P61/P62 hierarchy and demonstrate how the hierarchy has been addressed;
- iv. analyse the reliability of the safety features to ensure the engineering can deliver. Thus if no initiating frequency can be derived and the engineering can deliver a proportionate reliability in conformance with **5.7.15** then the outcome can be judged satisfactory.

3) Such analysis would also be expected to show conformity with all the other relevant DSA characteristics shown earlier, particularly a demonstration of continued function where the fault has been engineered out.

4) Often it is useful to use the P19 bounding case concept in such cases to simplify the analysis and make it more transparent.

6. References

1. T/AST/006 Issue 2 dated May 1999:DBA: INTEGRATION with ASSOCIATED ENGINEERING PRINCIPLES, G A Trimble. On BMS
2. Sizewell B Public Inquiry Report by Sir Frank Layfield, Dept of Energy, Library SPH
3. R v Board of Trustees of the Science Museum
All England Law Reports. 10 Sep. 1993, part 3, 853-861.
4. Reducing Risks, Protecting People HSE 1999
5. Safety and Health at Work : Report of the Committee 1970-1972 (Robens, A. report). HMSO, 1972, Cmnd 5034.
6. Successful Design for Health and Safety (to be published) HSE

Current related Assessment Guides:

7. T/AST/030 - Probabilistic Safety Analysis (Fully closed)
8. T/AST/003 - Safety Systems (Fully closed)
9. T/AST007 - Severe Accident Analysis (Fully closed)
10. **T/AST/034** - Transient Analysis for DBAs in Nuclear Reactors
11. T/AST/035 - Operating Limits for Nuclear Power Plant (Fully closed)
12. **T/AST/036** - Diversity, Redundancy, Segregation and Layout of Mechanical Plant
13. T/AST/037 - Heat Transport Systems (Fully Closed)
14. **T/AST/023** - Control of Processes involving Nuclear Matter
15. **T/AST/044** - Fault Analysis

History:

Issue 2: First formally approved version for use

Updates Issue 2 to Issue 3:

1. remove explicit references to chemical plants and add reactor examples to make the guide more universal
2. include in the DBA success criteria in the key ideas and concepts, namely no release, <100/200 mSv and no barrier breached & at least one intact
3. makes clear the difference between analysis conservatism and engineering margins and the DSA preference.
4. makes defence in depth EXPLICIT
5. includes the legal background for Harm Potential (often known as Hazard) from the Science Museum judgment and Reducing Risks, Protecting People
6. includes PPE as mitigation and low in the P61/P62 Hierarchy
7. optioneering transparency to demonstrate ALARP.
8. inherently safer operations made explicit and referenced to P61/ P62 Hierarchy
9. multi legged safety argument guidance where no single leg would be good enough
10. explicitly refers to the design analysed being that which exists throughout plant life.
11. IOF frequency convention changed to 10^{-7} from 10^{-6} .
12. the term DSA used to avoid confusion with a similar term used in reactor work. DSA and DBA are synonymous for non-reactor purposes as in Issue 2 of this guide.
13. the meaning of "conditions" in LC 23 for the purposes of DSA clarified.
14. the term deterministic is defined for use in this guide.
15. worker dose limits for P25 changed from 250 to 200 mSv on expert radiological

protection advice.

16. recognises that faults which initiate in one plant on a multi plant site may be realised elsewhere and that these should be traceable.

17. recognises P15 as a top down form of analysis

18. IOGF defined for the purposes of this guide

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. Conversely, a guillotine break at an appropriate point in the pipe geometry would compromise the pressure gradient, hence the safety case would no longer be valid.

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).

Flow Diagram - NSD BMS T/AST/006

DSA

