

NUCLEAR SAFETY DIRECTORATE - BUSINESS MANAGEMENT SYSTEM		
TECHNICAL ASSESSMENT GUIDE FAULT ANALYSIS		T/AST/044
		ISSUE 001
Approved By: <i>B J Furness</i>	B J Furness	Issue Date: 28/06/00
Open Government Status: Fully Open		Review Date: 28/06/03

Contents

Purpose and scope

SAPs addressed

Relationship to licence and other relevant legislation

Advice to assessors

Terminology for fault analysis

Role of 'fault schedule'

Structure of the Safety Analysis SAPs

Fault analysis general principles

Fault analysis does not stand alone

Importance of sound engineering and safe operation in fault analysis

Importance of completeness of the fault schedule (and supporting fault sequence schedule)

Value of, and dangers of, symptom-based analysis

Allowance in the safety case process for the unforeseen and unexpected

Allowance for internal and external hazards

Transient, radiological and bounding analysis requirements

Role of design basis analysis

Role of severe accident analysis for reactor and chemical plant

Role of PSA for reactor and for chemical plants

Criteria for acceptance of risk analysis

Checklist of questions

Appendix 1. Structure of SAPs safety analysis chapter

Appendix 2. Some generic fault analysis issues from chemical plant

Appendix 3. Definitions of fault schedule used in current licensees' safety-cases

References

1. Purpose and scope

1.1 Safety Assessment Principles (SAPs) 15 to 54 relate to accident analysis and comprise fault analysis principles (15 to 41), accident frequency principles (42 to 46) and assurance-of-validity principles (47 to 54). This Technical Assessment Guide (TAG) gives guidance on the interpretation of the fault analysis SAPs.

1.2 An analysis carried out following the fault analysis SAPs results (among other things) in a **fault schedule**, defined here to be *a list of initiating faults, together with the protection systems provided to prevent the release of radioactive material*. 'Initiating faults' includes internal and external hazards and human action (see Terminology section). This definition of fault schedule is discussed further below.

1.3 The TAG has three objectives:

1) to explain the central role of the fault schedule in distilling the results of the safety analysis.

2) to show the overall structure of the fault analysis SAPs and how its three major legs fit together and contribute to the fault schedule. These legs are design basis accident analysis (DBAA); analysis of severe accidents; and probabilistic safety analysis (PSA).

3) to advise on how SAPs 16 to 19 (and other SAPs as discussed below) can be used to check the validity of the fault schedule (or equivalent) prepared by the licensee and the use made of it in the safety case.

1.4 This TAG contains guidance to advise and inform NSD inspectors in the exercise of their professional regulatory judgement. Comments on this guide, and suggestions for future revisions, should be recorded on the appropriate registry file.

2. SAPs addressed

2.1 The principal SAPs addressed or drawn on in this TAG are P15 to P41.

3. Relationship to licence and other relevant legislation

3.1 Licence conditions 14 and 15 (preparation and review of safety case) apply plus LC 23 (preparation of a safe envelope for plant operation). LC 1 contains a comprehensive definition of 'operations'. Fault analysis should consider all operational states including normal operation, and the operations of shutting down or starting up. Foreseeable transients in the shut-down state, such as refuelling or maintenance, should also be considered.

4. Advice to assessors

4.1 Terminology for fault analysis

1) The SAPs define 'fault', 'fault condition', 'fault sequence' and 'initiating fault' as below:

Fault: Any unplanned departure from the specified mode of operation of a system or component due to a malfunction or defect within the system or component or due to external influences or personnel error.

Fault condition: When used without qualification, this means all design basis fault conditions and, where appropriate and as far as reasonably practicable, beyond design basis conditions also.

Fault sequence: A combination of events starting from an initiating fault and including any additional failures which may occur.

Initiating fault: The starting fault of a fault sequence. It may be a direct plant fault or a fault caused by an internal or external hazard or by human action.

2) 'Direct plant fault' implies the failure of a component to perform its duty for whatever reason. This corresponds to an occurrence which needs to be protected against to prevent an undesired end state (e.g. core damage, criticality, release of radioactivity etc). If occurrence goes completely unchecked, the undesired end state would occur (unless fortuitously prevented by something not claimed in the safety case). The protection could be equipment or people and will include detection and the means of delivering the safety function(s) (e.g. cooling or shutdown). The failure should be active (revealed) and call on a protection system. An unrevealed fault is not an initiating fault until it becomes active.

3) Assessors should be aware that the phrase 'initiating event' is sometimes met in a licensee's safety documentation as an alternative to 'initiating fault' in the above sense, with the phrase 'initiating fault' interpreted more narrowly. The licensee's documentation should include appropriate definitions.

4) 'Fault analysis' is not defined explicitly in SAPs and its meaning can depend on the context. For the purposes of this TAG it is defined in the following two senses (see **Appendix 1**)

a) Fault analysis (general) - the entirety of the analysis of faults, from cradle (identification of a list of initiating faults) to grave (comparison of analysis against engineering standards and against numerical risk criteria, and with assurances of validity);

b) Transient analysis - a technical description of how a fault develops with the physics, chemistry and engineering calculations which demonstrate how the plant behaves under that fault condition. The element of time is always present (otherwise the plant would never move from an initially safe state to some other one).

5) *Fault schedule* - the SAPs ^[1] contain references to a safety schedule and to a maintenance schedule, but not to a fault schedule except indirectly. In SAPs Glossary 'Safety system schedule' is defined as *a schedule which identifies the minimum safety system requirements for each of the initiating faults and internal and external hazards listed in the fault schedule*: but the term 'fault schedule' is not defined. Nor does there appear to be an agreed international definition, e.g. the IAEA consider 'fault schedule' a British term.

i) The definition of *fault schedule* given earlier (**paragraph 1.2**) is believed to sum up the intent of the SAPs.

ii) Alternative definitions are currently used by major licensees for nuclear reactor and nuclear chemical plant safety cases. These are given in **Appendix 3** for information.

iii) The definition of fault schedule in a particular safety case may incorporate *more* elements, or more detail, than the above definition: where it contains less, the licensee can be challenged to justify the omissions.

4.2 Role of the fault schedule

1) The fault schedule plays a central role in distilling the safety analysis. Its purpose is to record the plant's protection against the faults foreseen. A good fault schedule acts as a compact pointer to the analysis and protective measures, as a springboard for further analysis, and as a compact record of the protection provided. It is developed in different degrees of detail as the safety case evolves. This is an iterative process. The objective of the supporting safety analysis is to demonstrate that the plant has adequate protection against the faults foreseen.

4.3 Structure of the Safety Analysis SAPs

1) The Safety Assessment Principles ^[1] contain a chapter on Safety Analysis, consisting of an introduction (explaining the basic safety limit (BSL) and basic safety objective (BSO) concept, a section on normal operation and a section on accident conditions. **Appendix 1** shows this structure in detail.

2) The following points may be noted about this structure (see also **Appendix 1**):

i) The 'Fault analysis - General' principles (P15 to P19) are applicable to fault analysis as a whole:

a) The **scope** of accident analysis is set in P15. The term 'operating mode' is defined in SAPs glossary.

b) These general principles start from the premise that listing the faults, and fault identification, is the first step in guarding against them. A fault cannot be guarded against *directly* if it is not foreseen. It can be guarded against indirectly by robust engineering (this point is developed further below).

c) The **design basis accident analysis principles** (P20 to P27) are the subject of two further assessment guides ^[2,3]. **Refs 2 and 3** are drawn on as appropriate to make the present TAG self-contained.

ii) The **severe accident analysis principles** (P28 to P31) are the subject of a separate TAG ^[4].

iii) The **PSA principles** (P32 to P41) are the subject of a separate TAG ^[5].

iv) The **accident frequency principles** (P42 to P46) set basic safety limits (BSLs) and basic safety objectives (BSOs). **Appendix 2** of SAPs gives guidance. Discussions are on-going with regard to the 'large release' principle P44.

v) The **assurance of validity principles** (P47 to P55), like the engineering principles, underpin the above fault analysis principles and apply generally. The assurance of validity principles and the key engineering principles are considered self-explanatory so do not require further interpretation.

4.4 Fault analysis general principles

1) Fault analysis does not stand alone

i) The accident/fault analysis SAPs should not be considered in isolation: they are underpinned by the engineering SAPs and also by the life-cycle SAPs, in particular the key engineering principles and management of safety principles. The fault analysis principles P15 to P41 draw on ideas and themes which are developed in more detail in P61, P62, P64, P72, P81, P119, P120, P178 and P329.

2) Importance of sound engineering and safe operation in accident analysis assessment

i) Fault analysis cannot be considered in isolation: it is complementary to consideration of the engineering and also of the operation and life-cycle, in particular the key engineering principles and management of safety principles refer. Fault analysis requires analysis of both the logic of fault development and of the engineering ^[2,3]. Consideration of the engineering aspects is necessary at all stages. This part of the assessment can be iterative: ultimately it will include P61 to P314, but the key engineering principles P61 to P81 are useful as the initial focus. Satisfaction of the life cycle principles in general (P315 to P333) and the management systems principles in particular (P315 to P323) also need to be borne in mind as background to the fault analysis: they influence the realism of its assumed inputs.

ii) Engineering SAPs relevant to fault analysis include but are not limited to P61/ P62 on hazard avoidance / preferred hierarchy of protective measures; P65 addressing defence in depth; P67 addressing failure to safety; P68, P79 and P80 which address diversity, redundancy and segregation requirements; and P78 (the single failure criterion).

a) Principle P61 addresses hazard analysis, P62 fault tolerance. They generate an order of preference ^[3] viz:- prevent by removal of the hazard; else protect by engineering means; else mitigate i.e. guard against the consequences.

b) The defence-in-depth principle, P65, is primarily intended to protect against the expected. It can also provide powerful insurance against the unexpected (the unforeseen in design) especially when combined with good engineering practice (use of redundancy and diversity, avoidance of single failure, etc.).

3) Importance of completeness of the fault schedule (and supporting fault sequence schedule)

i) Modern approaches to accident analysis and prevention should all start by listing events (faults plus internal and external hazards) in order to prepare a corresponding safety schedule of protective measures. Principle P16 addresses the *preparation of the initial list of faults (including internal and external hazards and faults due to personnel error)* and states that *this should aim for completeness*. P22 requires that design basis fault sequences from these initiating faults be identified, principle P33 requires that a complete range of fault sequences be identified for PSA purposes. P22 and P33 advise further on how this is to be done.

a) Identification of fault sequences and scenarios is central to the further fault analysis and to the demonstration of the effectiveness of the safety schedule. Thus a 'fault sequence schedule' needs to be developed as part of the analysis.

b) As the plant design evolves, a list of the protective measures needed to guard against the identified faults and sequences is

developed: this list, together with corresponding operator actions, forms the safety schedule. The safety schedule thus contributes the 'list of protection systems' in the definition of the fault schedule (in **Section 1.3**). The safety schedule should be derived from the design basis analysis (P26 refers): it evolves as the design and plant life evolves.

c) The fault schedule sums up the analysis by listing the initiating events plus corresponding protective measures.

ii) Both design basis accident analysis and probabilistic safety analysis are vulnerable (as methodologies) to the following common methodological concern: if an initiating event, or fault sequence has not been foreseen, an accident may develop in a way the designers and operators did not expect, and for which the protection may prove inadequate. There are many examples of this. Some have had harmless consequences: the defence in depth provided on general engineering principles arrested the accident before it could escalate, with no injury to the workforce and either no or negligible release of radioactivity. Others have had significant consequences: barriers and defences have been breached, leading to an off-site release detected and halted by the outer defences. At Three Mile Island in 1979, an unanticipated chain of events, not adequately foreseen in the generic probabilistic safety analyses carried out in the URNS WASH-1400 report ^[6], led to a core melt unanticipated in the WASH-1400 PSA. The robustness of the containment, and other robust design features, prevented a significant release ^[7]. At Chernobyl in 1986 the accident had tragic consequences: successive safety systems were switched off in contradiction of designer's instructions ^[8]. Ironically, this was done in order to carry out a safety experiment.

iii) P16 states that the safety case should *demonstrate a systematic process for establishing the list of faults, which should aim for completeness*. The following points can be borne in mind in assessing the licensee's submissions:

a) Diverse fault identification processes are normally necessary. For chemical plants, a good core process is HAZOP; good diverse processes include plant walkdowns and (for mechanical equipment) failure mode and effect analysis (FMEA).

b) Having identified the faults, the next stage is to identify and analyse the fault sequences and scenarios that might flow from them, together with corresponding protection systems and safety measures. The analysis of fault sequences and scenarios should consider mitigated and unmitigated sequences and corresponding protective measures. This is an interactive process, feeding from, and feeding in to, the developing fault schedule.

c) At every stage of the safety case, the fault schedule needs to be transparent, inspectable and auditable. Its documentation needs to be *inspectable* so that its audit trail can refer back to the fault identification techniques (HAZOP, walkdowns, FMEA etc.) that generated it. Its documentation needs to be *auditable*, as does the process generating it, in that it needs to correspond to the reality of the plant as built (the hazard comes from the plant as built, not as designed). Conversely, the reality of the plant, as the design progresses, needs to reflect the fault schedule at the previous design stage.

d) As pointed out in **Ref 3**, elimination of faults by engineering design may usefully be carried out very early in the analysis (for example as a recommendation of a HAZOP meeting). It is nevertheless good practice to record that faults have been eliminated somewhere in the fault list or safety documentation.

e) DBA analysis and probabilistic analysis are both vulnerable to the following common cause: missing an unanticipated fault sequence.

This can be protected against to some extent by having systematic and diverse fault identification methodologies (for example HAZOP plus walkdowns) and secondarily by robustly engineered plant that satisfies the defence-in-depth principles. Sound engineering based on proven technology minimises the unforeseen happening. The robustness of the defence-in-depth serves as a useful insurance to prevent escalation of unexpected sequences should these develop. Use of an iterative fault identification process (developing more detail as the design progresses) is an additional safeguard.

iv) Reference 5 on PSA contains a detailed checklist of points to check the completeness of the list of initiating faults and the fault schedule.

4) Value of, and dangers of, symptom-based analysis

i) 'Symptom-based analysis' is a phrase used to describe practical recovery operations, and originated following the Three Mile Island accident. It has come to mean a common-sense response to relieve an actually dangerous, or potentially dangerous, situation. For example, if something is getting too hot - switch off the power. If pressure is getting too high- lift a safety valve; and so on. This assumes that protection systems provided have not done this automatically.

ii) The TMI operators had found that they lacked information to identify the specific accident sequence that they had entered. Consequently they would have done better to look at symptoms at a crude level: "the pump systems haven't enough water, we will inject water." In this example, the operators and back-up would not need to know the specific fault causing the symptom to take corrective action to mitigate the accident. Symptom- based analysis can also be useful to avoid accidents (i.e. avoid escalation of a developing situation).

iii) However, there are dangers in symptom based analysis. "If a car is going too fast - brake" can be fatal on an icy road. "If Chernobyl reactor power is escalating and you no longer know what's going on, hit the emergency stop button". This last happened and according to some analysts may have pushed a very dangerous situation irrecoverably over the edge.

iv) The licensee's safety case for the whole plant will include emergency instructions. Creation of such instructions requires anticipation of events which may never happen or which may unfold in unexpected ways. These may rely implicitly or explicitly on symptom-based analysis. The right use of symptom-based analysis, and of the operator's discretion, has to be decided on a case-by-case basis, informed by questioning of the premises behind the instructions and recognising the legitimate role of the professional judgement of the licensee.

5) Allowance in the safety case process for the unforeseen and unexpected

i) The importance of completeness in the list of initiating faults (and in the fault sequences derived from them) has already been stressed. This completeness depends on the adequacy of the licensee's analysis and on the process for generating this analysis (P16 refers). The licensee's analysis should allow for human errors and omissions, and the licensee's process for generating the analysis needs to too. Recovery from errors requires the licensee to have procedures for validation (is it doing right things?) and verification (is it doing things right?). This process needs to include suitable procedures to guard against the unforeseen.

ii) Engineering defence for the unforeseen include: a) conservatism in the DBA analysis b) appropriate conservatism in the engineering; and (c) prudence in design e.g. well-tested approaches. Conservatism is mainly required to demonstrate that claimed protection *will* be effective rather than *is likely to* be effective. It provides assurance that the intent will be met.

iii) Safety management defence against the unexpected is primarily through good safety management which includes policy, planning etc. An important ingredient of

good safety management is a good safety culture in the workforce (the prudent, questioning, communicating attitude recommended by IAEA). More advice is distilled in SAPs P315 to P322.

iv) The chance of a mistake in analysis and/or a miscommunication may dominate in the quantitative analysis. For example, if there is a 1E-3 chance of an analyst making a significant mistake this is likely to dominate over the 1E-5 per year (say) that he/she calculates for the risk of an accident. A 'significant mistake' here means a mistake in analysis which happens also not to be guarded against by the engineering. The procedure for building the safety case should allow for this possibility.

6) Allowance for internal and external hazards

i) The fault schedule also needs to address both internal and external hazards (P16 refers principally, as do P61, P64, P72, P119 and P120 at the more detailed level, see Appendix). For internal hazards, T/AST/014^[9] advises on points to look for structured against seven key objectives. These objectives relate to fire prevention; fire control; fire consequences; explosions and missiles; toxic/ asphyxiant gases; dropped loads; and flooding and spray. For external hazards, T/AST/013 advises on corresponding points to look for. External hazards considered are seismic; aircraft crash; extreme ambient temperatures; flooding; extreme wind; and external missiles and explosion.

7) Transient, radiological and bounding analysis requirements

i) P17 and 18 advise on points to consider in assessing the adequacy of the supporting transient and radiological analysis: they are straightforward and require no further interpretation. SAP 19 advises on the use of bounding analysis. Experience with some safety cases reveals the following pitfall when bounding analysis is used.

- Suppose that the licensee's analyst identifies sequences A and B, with frequencies F and G and consequences X and Y. Suppose that frequency G is below F, and consequence Y is below X. The analyst is then tempted to ignore sequence B, arguing that it is 'bounded' by sequence A. But for correct comparison with a total numerical frequency standard (P42 or the licensee's equivalent) the frequency should be $F + G$ and not F.

ii) If the above pitfall is avoided, the frequency sum can become dominated by frequencies from low-consequence events. P42 proposes a set of consequence bands expressed as maximum effective doses (0.1 to 1 mSv, 1 to 10 mSv and so on up to 100-1000 mSv and greater than 1 Sv): use of these bands breaks up the calculation and assists realism.

4.5 Role of design basis analysis

1) **Refs 2 and 3** give guidance on DBA analysis. Key concepts are reviewed here with emphasis on how DBA analysis feeds from, and feeds into, the fault schedule (part of the two-way iterative process mentioned earlier).

2) In overview, the concept of DBA analysis is as follows:

i) A 'design basis fault or sequence' is defined in the Glossary of Terms in SAPs, viz. "a fault (sequence) which the plant is designed to take or can be shown to withstand without unacceptable consequence, by virtue of the plant's inherent characteristics or the safety systems."

ii) Analysis is required to demonstrate that an accident sequence is within the design basis. The essential idea is that all faults more frequent than certain cut-off frequencies must be considered and protected against. Corresponding DBA SAPs (P20 to P27) are given in **Appendix 2**.

3) Principle P21 (a) provides a criterion for determining design basis accidents - *any accident*

triggered by an initiating event which is expected to occur with frequency 1 in 100,000 per year or greater is a DBA in the sense that the consequences flowing from it must be shown to be acceptable. In this context 'acceptable' means not only that the risks are both tolerable and ALARP, but also that the consequences of the accident, should it occur, are within specific levels to be established by the designer as part of the design basis for the plant.

i) Historically, such consequences had for example related to the magnitude of the dose experienced by someone at the site boundary. In addition, workforce consequences need to be addressed; and also physical barriers to escape of radioactivity should so far as possible remain intact. P25 (**Appendix 2**) sets out corresponding "consequence criteria".

ii) The frequency criteria for choosing DBA are further refined in other SAPs. P119 specifies that initiating events with an annual frequency below 1 in 10 million per annum need not be considered at all; and P120 allows an initiating frequency of 1 in 10,000 for natural hazards, for comparison with P25 (see Appendix 2).

4) The concept of 'a design basis fault or sequence' can be made more specific by reference to the concept of a 'design basis initiating fault' (DBIF). Ref 2 expands this concept and sets out NII's position on design basis accident analysis (expanding on principles P20 to P27).

i) The Safety Assessment Principles refer to 'design basis' faults, i.e. "faults that the plant is designed to take or can be shown to withstand without unacceptable consequences, by virtue of the plant's inherent characteristics or the safety systems". Similarly, accidents (or fault sequences) that the plant is designed to withstand without unacceptable consequences are termed design basis accidents (or fault sequences). 'Unacceptable consequences' are those that breach principle P25. 'Initiating faults' are those identified by P16 with the exception of those excluded by P21.

ii) Having identified the design basis initiating faults, sequences arising must be considered as explained in P22. A 'design basis' analysis is carried out deterministically using conservative assumptions (as explained in detail in P22 and P23) ^[3]. Its purpose is to demonstrate first, that the fault tolerance of the plant is robust (has large margins and has defence in depth); secondly that its safety systems are robust; and thirdly, the limits to safe operation of the plant.

iii) Simple qualitative checks of the design basis provisions and analysis are possible (see also **Refs 2 and 3**). One test is found by combining P22 and P78 to give the following test: For any design basis initiating event, with the plant in its worst normally permissible operating state, then a single failure in the safety system should not lead to unacceptable consequences when calculated deterministically by a conservative route. Another test of a design basis event is that any design basis fault sequence: (a) the integrity of the physical barriers to radioactive release is maintained and the fault consequences limited as required by P25; and (b) no safety-related component (or structure or system) required to prevent or mitigate the fault sequence will be caused to operate outside the conditions for which it has been qualified (P325 refers). During a design basis event or sequence, at least one barrier to the release of radioactivity must remain intact. Other checks are in **Ref 3**.

5) **Ref 3** further expands **Ref 2** by identifying the integration of DBA with the engineering principles. Having classified an initiating event as a design basis fault, **Ref 3** identifies the next step as to analyse it robustly, with a view to preventing it from arising (first choice subject to reasonable practicability, unless consequences are negligible) otherwise protecting against it (second choice).

6) The goal of DBA analysis can be defined as *to analyse faults in a robust conservative (pessimistic) manner so as to show unequivocally that sufficient engineering safeguards are provided, and to demonstrate that all reasonably practicable means to mitigate the hazard have been adopted.*

7) For both reactor and chemical plant this robust conservative review of the design is to be supplemented both by severe accident analysis, in sufficient realism to inform accident

management strategy (see P29 and **Ref 4**), and by a probabilistic treatment which facilitates consideration of adequacy, sufficiency and balance [5].

4.6 Role of severe accident analysis for reactor and chemical plant

1) As noted earlier, **Ref 4** gives guidance on severe accident analysis. **Ref 4** also proposes and explains the following definition of severe accident: *an event or sequence of events that, through loss of control of plant conditions, creates a potential for the release of sufficient nuclear material to the environment to enable a person off-site to release a dose equivalent of 100 mSv or greater.*

2) The principles of severe accident analysis apply equally to reactor and to chemical plant although, in practice, control of the severe-accident risk from a reactor can be more demanding to control because of the shorter timescales over which accidents can develop. Good quantitative analysis can therefore be very important (especially if the time for things to go very wrong is very short).

4.7 Role of PSA for reactor and for chemical plants

1) Because of the different nature of the risks, stemming for example from the difference in timescales over which severe accidents may develop, the depth of the probabilistic analysis can differ for reactor and chemical plant, so that different degrees of rigour can be appropriate. For reactors, a consensus of what constitutes 'good practice' in PSA has grown up, key features of which are captured in SAPs P32 to P41.

2) The SAPs make no distinction between chemical and reactor plant, the same standards must apply to both. The depth of the analysis may differ, reflecting the principle of proportionality. In chemical plant, it has become customary for probabilistic concepts to be used to support analysis in less depth than for power reactors.

3) It is a very useful step for a licensee proposing to use a less deep PSA, or a simplified PSA, to *declare the standards its PSA has to meet*, since in this way any limitations of methodology can be explored with NII in advance:

i) For example, crude bounding rather than conservative best-estimate analysis may be used. This implies that P35 is not met, and also that the "risks" as estimated from the PSA may not reflect the true risks (be an artefact of the calculation method);

ii) When crude bounding analysis is used in PSA, the total frequencies for comparison with a licensee's numerical frequency acceptance standard can be dominated by frequencies from relatively low-consequence events (see discussion of P19 above). It is open to the licensee to propose and justify pragmatic ways round the difficulty (for example, when adding frequencies from relatively low-consequence events, to "weight" the frequencies being added according to their bounding consequences (so helping to meet the spirit of P42 although not meeting its letter). An important point to look for is that the assumptions in the licensee's analysis should be explicit, rather than implicit.

iii) Whatever depth PSA is taken to, it should take good account of dependent failures. In particular it must allow for limitations on reliability imposed by dependent failures.

4) To summarise: in principle, there is no objection to a chemical plant licensee applying probabilistic arguments differently from the 'PSA best practice' found in power reactors; but if it does so the standards it proposes for its PSA should be declared up-front, so that the SAP PSA principles can be used as a standard to evaluate them.

5) Use of a less than full PSA can lead to difficulties:

i) One of the objectives of fault analysis in general and PSA in particular is to determine the contribution of individual fault sequences to the risk, so as to check for a balanced plant design (P32 refers). The dominant sequences may arise from different categories of faults and hence these should be evaluated on a consistent

basis. A conservative approach (such as DBA analysis or PSA based on bounding analysis), has the potential to lead to the situation where sequences may become dominant as a result of the conservatism rather than the plant design. In other words, what appears to dominate may be a feature of the analysis and not of the plant. Accordingly, best estimate data, both in terms of reliability data and plant performance, should be used in probabilistic fault studies wherever possible (P35 refers). If there is uncertainty in data, however, interpretation should err on the conservative side.

ii) It can be more difficult for the licensee to demonstrate the absence of a 'cliff edge' effect (that is to say, in accordance with SAP P121, that there will not be a disproportionate increase in risk from an appropriate range of events which are more severe than the design basis event). It has previously been accepted that one satisfactory approach to the demonstration of absence of an adverse cliff edge effect is via a full PSA ^[10]: a PSA which does not address internal/ external hazards cannot readily do this, and may also miss a major contribution to risk.

4.8 Criteria for acceptance of risk analysis

1) DBAA and PSA have different purposes and quantify analysis in different ways. Satisfaction of accident consequence and frequency criteria is a *necessary* but not a *sufficient* condition for the demonstration of tolerability and ALARP. The licensee must also satisfy engineering principles.

2) Conversely, probabilistic quantification is not always possible. It is acknowledged that it is difficult to quantify certain very remote sequences which the licensee has foreseen and argued to be remote on "deterministic" grounds. In chemical plant, for instance, accidental criticality in the process is analysed by defence-in-depth whose individual 'legs' often involve purely deterministic arguments. For example, a criticality safety-case may claim that containers are safe-by-shape, so that criticality is impossible without some moderator; etc. The licensee's analysis can then focus on the way that these defences can be by-passed, by human, procedural or mechanical error. NII can assess adequacy using the hierarchy of protection ideas in SAPs (see **Ref 3** for further details and examples). The fault schedule serves to focus these ideas and to provide a two-way audit trail.

3) An alternative form of "deterministic" argument is to demonstrate that simultaneous occurrence of multiple contingencies is necessary for the event to occur, and that such contingencies are appropriately remote even if not readily quantifiable. The acceptability of such arguments, and the reasonable practicability of no further action, can be judged on a case-by-case basis, taking account of consequences should the coincidences nevertheless occur, and also taking account of the possibility of common-mode faults.

i) The phrases 'likely', 'unlikely', 'remote' and 'very remote' are sometimes met with in chemical plant safety cases. For example 'likely' faults can be those faults with an estimated frequency greater than 0.01 per year; 'unlikely' with a frequency less than or equal to 0.01 per year but above 0.0001 per year; 'remote' with frequency less than or equal to 0.0001 per year but above 1E-7 per year; and 'very remote' meaning with frequency less than or equal to 1E-7 per year. Corresponding phrases in reactor cases are 'frequent' for faults with a frequency greater than 1E-3 per year, 'infrequent' etc. Use of such phrases has the advantage of conveying ideas in familiar but precise language. If such phrases are used it is necessary for the licensees to explain them and use them consistently. Safety cases should be challenged if the licensee does not explain what such phrases mean.

4.9 Checklist of questions

1) Questions to ask of a safety-case are partly technical (what to look for), partly strategic (how to act on the information). This TAG, and the supporting references, has advised on the technical aspects. The strategic aspects are addressed in Staff Notices, and also in AGP00 ^[11]. The objective is to assemble the *evidence* needed to form an overall judgement on the suitability of the safety case provided.

2) Questions for an assessor to consider could include:

i) (on the general fault analysis - technical)

a) How far is the case compliant with the key requirements of SAPs 15 to 42:

- how well does it meet the scope/ fault list/ fault schedule principles P15 to P19?
- does it contain a design basis accident analysis compliant with P20 to P27?
- are beyond-DBA and severe-accident analysis addressed compliant with P28 to P31 (or if not, at least sufficiently well to inform severe accident management)?
- how far are the requirements for formal probabilistic safety-analysis compliant with P32 to P41 met, (see T/AST/030 ^[5])?

b) is the analysis validated and verified, and compliant with the assurance-of-validity principles P47 to P55?

c) does the analysis cover transient operations as well as normal operations (for example fault development during maintenance or standby or start-up/ shut-down)?

ii) (on the fault schedule - technical)

a) How does the licensee demonstrate that the process generating the list of faults is comprehensive?

- If the process is comprehensive how can I test if it is correctly applied?
- If it is not comprehensive how can I press for improvement?

b) If the list of faults seems to be incomplete:

- is it incomplete in reality and if so what are the implications for the process by which the schedule was produced?
- how significant to safety might the omissions be?
- what further information do I require from the licensee to resolve this?
- is the licensee aware of the omission and if so how does the licensee justify the omission?

c) Despite all precautions and licensee arrangements, the list of faults may in reality be incomplete. To guard against this:

- do the licensee's emergency arrangements appear adequately simple, wide-ranging and robust?
- are robust detection systems in place to detect anomalous behaviour?
- has the licensee in place a sensible basket of symptom-based protective features?
- does the licensee permit symptom-based emergency response? (if so how is this controlled and is the operator's

discretion appropriate? if not is the operator over-fettered?)

d) Consequences need to be calculated as part of the fault analysis:

- do the consequences appear reasonable from the information supplied?
- are they sensitive to any special assumptions?

iii) (on chemical plant probabilistic assessment - technical)

a) If a full PSA is not attempted but numerical estimates are provided

- do the calculated risks meet the numerical BSLs/BSOs in the accident frequency criteria, P42 to P46
- if so, how robust is the calculation?

b) If internal and external hazards are not included in the fault schedule

- what is the justification for this omission
- what information is provided instead?

c) Has the licensee complied with fault analysis related generic issues (for example, **Appendix 2**)? This Appendix lists examples drawn from experience with chemical plant safety cases.

Appendix 1. Structure of the SAPs safety analysis chapter

A1.1 The structure is revealed by the following indented list:

INTRODUCTION

defines and explains basic safety limits (BSLs) and basic safety objectives (BSOs) for the risks from normal and from accident conditions

NORMAL OPERATION

P6 to P14

+ Assure validity SAPs P47 - P55

+ Engineering SAPs

+ Management of safety SAPs

ACCIDENT CONDITIONS

Fault analysis (general)

ÿ Scope (P15)

ÿ Fault schedule related:

List initiating faults (P16)

Identify fault sequence (P16)

Carry out transient fault analysis (Note 2):

Analyse each fault sequence

P17, P18, P19 apply

DBA analysis

P20 - P27 supported by engineering principles

Covered by T/AST/003 and **T/AST/006**

BDBA analysis (severe accident analysis)

P28 - P31 covered in T/AST/007)

Probabilistic Safety Analysis

P32 - P41, covered in T/AST/030

Numerical principles

P42 - P46

Assurance of validity P47 - P55

- These are underpinning principles

- Similarly the engineering principles and life-cycle principles underpin all the analysis

A1.2 Notes on above:

1) '**Fault schedule**' means *a list of initiating faults, together with the protection systems provided to prevent the release of radioactive material.* 'Initiating faults' includes both plant-initiated faults and internal and external hazards. The fault schedule thus consists of two parts: **a listing of initiating faults and hazards**, plus the **safety schedule** which identifies the protection systems and safety measures

2) 'Transient fault analysis' means *a technical description of how a fault develops with the engineering calculations which demonstrates how the plant behaves under the fault conditions.*

3) Paragraphs 43 to 51 of SAPs link P15 to P55 back to the fundamental principles 4 and 5 and set the context.

Appendix 2. Some generic fault analysis issues from chemical plant

A2.1 During assessment by NII of the periodic safety reviews produced by licensees for nuclear and chemical plant, 'generic issues' (relating to more than one plant) have been raised, regarding shortfalls that NII has required the licensees to rectify in order to gain agreement to the safety cases.

A2.2 For chemical plants, particular shortfalls in methodology relating to fault analysis have been

- 1) the absence of design basis analysis;
- 2) fault schedules which fell short of SAPs requirements for fault sequences (in particular, by not including internal or external hazards as initiating events);
- 3) fault schedules which address shut-down or maintenance inadequately: there is a tendency to underestimate danger when plant is in those states;
- 4) and a simplified PSA approach which also fell short of the SAPs intent of an integrated analysis.
 - i) In this simplified approach, consequence analysis is first applied to accident and fault scenarios. Consequence analysis is intended to reveal which scenarios lead to significant radiological releases (releases to the public or the workforce which exceed target levels set in the licensee's company standards) and which do not. Mitigated release sequences (allowing for the protection equipment) and unmitigated release sequences are both considered. Scenarios with significant releases are next analysed by constructing fault trees, and probabilistic methods are used to identify the frequencies of the scenarios and demonstrate that these frequencies are below the licensees' target levels.
 - ii) In applying the above methodology, the main hazards to the plant are identified and analysed separately. The effect is to spread the PSA out among a number of separate hazard analyses.
 - iii) However, the intent of the SAPs is an integrated

analysis, allowing for interactions where appropriate of initiating events and also for internal and external hazards. This is missed when the PSA is reported in separate hazard analyses: it is difficult to demonstrate the absence of interactions among the separately-analysed hazards, for example.

iv) A further difficulty arises in the reporting, in the individual hazard analyses, of “fault schedules”. These follow the definition in **Appendix A3.2** and report the protective measures against fault sequences rather than against initiating events. It is not suggested that it is wrong to report this information: what is missing is an overall list, of initiating faults plus protective equipment, in the parent document (as with the fault schedule approach suggested in this TAG).

A2.3 The following points may be borne in mind when considering the adequacy of the fault schedule and of a simplified PSA:

1) The fault schedule should include a complete listing of all faults identified, including internal and external hazards (SAP P16 refers): all faults listed need to be considered in subsequent analyses. Traceability from hazard identification to and from hazard analysis is necessary.

2) Traceability by bounding faults should be explicit. Special attention may be needed for sequences which have a strong time dependence or rely on sequential operations. Consider event trees to supplement fault trees in appropriate instances.

3) Provide sensitivity analysis (SAP P38 refers, also P62 and P167 refers). Consider qualitative as well as quantitative sensitivity-analysis, for example the qualitative use of fault trees (using cut set listings to highlight and audit the logic), and algebraic or numerical importance analysis based on the cut sets analysed.

i) Importance analysis can be algebraic or numerical. Algebraic importance analysis involves setting up an algebraic/ arithmetical statement of the way that the numerical risk is built up, in order to capture the significant contributions to risk compactly and transparently. This is done with reference to combinations of cut sets. Numerical importance analysis means tabulating the numerical measures of importance in the

PSA analysis.

4) Occupancy rules for calculating the risk to workers are necessary in hazard analysis. Only where direct control of occupancy is in force should it be assumed that occupancy is less than 100%.

A2.4 The potential for common-cause failure should always be borne in mind in fault analysis. This topic is covered by SAPs P80 and P81, further advice is in **Refs 2, 3 and 5**.

Appendix 3 Definitions of fault schedule used in current licensees' safety-cases

A3.1 As noted in the main text, nuclear chemical plant and nuclear power station licensees have developed different definitions of fault schedule useful to their purposes, and which reflect the different ways that, historically, safety cases have been developed for nuclear chemical plant and nuclear power stations. Two of these definitions are given here for information.

A3.2 From a nuclear chemical plant licensee, the fault schedule definition developed is *a relatively brief but comprehensive listing of fault sequences arising from internally initiated events, along with the safety measures which protect against each sequence.*

A3.3 From a nuclear power station licensee, the fault schedule definition developed is more detailed. Summarising and paraphrasing, *a fault schedule is a comprehensive schedule of initiating events which have the potential to give rise to a radiological release, together with the corresponding lines of protection. Categories of fault need to be identified for the fault schedule. For reactor plant twelve categories are identified, each category being broken down further into individual initiators.*

- *The twelve categories are: spurious reactor trips; feed system faults; steam system faults; water ingress and other overpressure faults; primary coolant flow faults; reactivity faults; single quadrant / circuit faults; loss of grid connection; depressurisation faults; faults arising in essential systems; fuel route faults; internal hazards; and external hazards). Each of these categories is further subdivided into more specific faults.*
- *For process plant, the fault schedule is to be replaced by comprehensive hazard and interlock schedules.*

References

1. HSE, 'Safety assessment principles for nuclear plants', HMSO 1992.
2. 'NII Design basis assessment principles for internal faults' Appendix 1 of T/AST/003, 'Safety Systems'. [Appendix 1, 1995, has been issued earlier to British Nuclear Fuels plc as a NII position statement for chemical plant].
3. **T/AST/006**, 'Design basis accident analysis: integration with associated

engineering principles (with particular reference to chemical plant)'.

4. T/AST/007, 'Severe accident analysis'.

5. T/AST/030, ' Probabilistic safety analysis'.

6. 'Reactor Safety Study: An assessment of accident risks in U.S. commercial nuclear power plants', 9 vols., USNRC report WASH-1400, NUREG-75/014, October 1975.

7. IEEE, 'Spectrum special issue: Three Mile Island and the future of nuclear power', IEEE Spectrum volume 16 no 11, Institute of Electrical and Electronic Engineers, USA.

8. Richard F Mould, 'Chernobyl: the real story', Pergamon Press 1988.

9. T/AST/014, 'Internal Hazards'.

10. T/AST/013, 'External Hazards'.

11. Assessment Guide AGP 000 'A guide to assessment by the NII of licensees' safety cases for nuclear installations' (ASD Assessment Report No. 281/97).