

NUCLEAR SAFETY DIRECTORATE - BUSINESS MANAGEMENT SYSTEM		
ASSESSMENT GUIDANCE: ASSESSMENT PROCESS		G/AST/001
		ISSUE 002
Approved By: <i>R P Pape</i>	Dr R P Pape	Issue Date: 28/02/03
Open Government Status: Fully Open		Review Date: 28/02/06

1. Purpose & Scope

1.1 This guidance provides supporting information for procedure **AST/001** - "Assessment process".

2. Guidance

Assessment Process

1.1 A licensee's submission should already have been cleared by the licensee's due process. Any conditions attached by the licensee's independent NSC and INSA nuclear assessment should, with their resolution, form part of the case.

1.2 The assessor must fully understand what the licensee proposes to do and how the supporting documents are intended to demonstrate safety. The assessor may wish to conduct early discussions with the licensee and / or visit site / HQ to aid understanding of the licensee's case.

1.3 As a test of this understanding, and to make the eventual report self-contained, it is useful to **summarise the licensee's case and proposals** and prepare this early in the assessment.

1.4 Once the licensee's case is sufficiently understood, the assessor can determine what the assessment basis should be. The objective is to identify **standards and criteria** that can be demonstrated (or otherwise) and used as a yardstick for evaluating the case.

1.5 Overriding criteria are the logic and self-consistency of the case itself. One test of acceptability is to take the evidence provided

at face value and check if the conclusions flow from that evidence.

1.6 Other standards and criteria include licence conditions and SAPs, the licensee's own standards and criteria, engineering codes, and national / international standards.

1.7 Having decided on an assessment basis, the assessment continues by appropriate **appraisal** i.e. analysis of the claims in the case. This process can be thought of as addressing three questions:

- 1) Are the licensees doing the right thing? (are the objectives right ?)
- 2) Are the licensees doing things right? (is the detail right ?)
- 3) Are the licensees doing enough ?

1.8 The last question covers a variety of issues, such as has enough been done to satisfy the objectives, are the chosen standards and criteria appropriate and sufficiently satisfied, have claims been properly tested and checked, have all significant hazards been identified, is there enough engineering defence-in-depth, is the safety culture proactive enough, has there been enough and appropriate R&D for novel plant, etc.?

1.9 Key safety aspects should be identified by the assessor.

1.10 Reasons for agreement or otherwise with a licensee's case should be stated, along with appropriate evidence.

1.11 Claims made by a licensee should be supported by evidence. The assessor may wish to take into account sources of evidence additional to that provided by the licensee - if so this should be made clear in the assessment output. However, assessors should note that the licensee's safety case as documented must be self-sufficient, so they must ensure that any additional evidence which is necessary in order to make the case is incorporated within it.

1.12 Assessors should attempt to resolve all findings and concerns as far as possible during the assessment process and before they are converted to a formal recommendation. This gives the licensee a chance to clear up the matter at an early stage, and also assists transparency by avoiding surprises. In general, assurances and explanations should be confirmed in writing to provide evidence for

the benefit of corporate memory and the audit trail.

Time Allocation

1.13 The time required for the assessment process should be determined by the scope of the assessment (what is to be examined and why) and the depth required (which is warranted by the safety significance of the case).

1.14 The assessor needs to judge when he / she has done sufficient work to reach a supportable conclusion in relation to an agreed assessment objective. Sufficient time needs to be secured, in each case, for the reaching of this position.

In all cases, the assessor must be confident in the justification and substance of the conclusions reached, and in the recommendations accordingly made. Further information is available in the appendix.

3. The Mechanics of Assessment

The appended paper entitled '**The Mechanics of Assessment**', sets out a tried and tested approach, and offers practical advice in dealing with licensees.

4. Definitions

4.1 The appended paper entitled 'The Mechanics of Assessment', sets out a tried and tested approach, and offers practical advice in dealing with licensees.

4.2 NSC - Nuclear Safety Committee

4.3 INSA - Independent Nuclear Safety Assessment

4.4 SAPs - Safety Assessment Principles

4.5 R&D - Research and Development

5. Associated Documents

5.1 **AST/FWD** - Assessment Foreword

5.2 **AST/001** - Assessment Process

- 5.3 **AST/002** - Assessment Activity Management
 - 5.4 **AST/003** - Assessment Reports
 - 5.5 **AST/004** - Issues Recording Process
-

APPENDIX

THE MECHANICS OF ASSESSMENT

Introduction:

Assessment of nuclear safety cases is a fundamental and major component in the work of NII. It is appropriate therefore to consider how it should be undertaken, in order to:-

- a) maximise the effectiveness of available effort;
- b) promote consistency in the standard of assessment; and
- c) expose potential pitfalls and provide advice on ways to avoid them.

This guide does not set out 'the definitive way to conduct assessment'. Rather it presents one possible approach. It does however represent an approach that has evolved, by experience, trial, error and refinement, over many years.

It is important to recognise that assessment is undertaken by all NII inspectors whether they are working within their own particular specialism or not. Licensees are required to '....in respect of any operation that may affect safety, produce an adequate safety case to demonstrate the safety of that operation.....' (extract from Licence Condition 23). Hence safety cases, also referred to as safety justifications or safety demonstrations if they are part of a wider case, are produced in a wide variety of circumstances, covering a wide range of plants and activities both large and small. All inspectors therefore need to carry out assessments. Site or project inspectors generally assess cases where specialist skills are not needed, and call in specialists when they are. ***In this guide the term 'assessor' is used to refer to any inspector that carries out an assessment.***

The Nature of Assessment:

ASSESSMENT is the process NSD applies,

*To reach an **INDEPENDENT** and **INFORMED** judgement on the **ADEQUACY** of a nuclear safety case. (See **AST/FWD** for a formal definition)*

Independence is the stance that we take with respect to licensees, *information* is the input to the assessment process, and *adequacy* is the subject of the judgement that we deliver, representing the output from the assessment process and the input to the process of recommending a way forward such as seeking improvements where necessary. These three elements will be considered in turn.

1. **INDEPENDENCE:**

1.1 NII's basic independence derives from the reason why the organisation was originally set up. NII staff are required to be independent of licensees, and to be less affected than they are by the pressures that arise, most notably costs and deadlines. However these considerations still do have an effect, and we must guard against allowing them to degrade the quality of our assessments. Time pressures that licensees seek to impose upon us can have a major impact if we allow them to, and although it is sometimes appropriate to allow such pressures to influence the priority that is assigned, it is not appropriate to allow them to influence the scope or depth of assessment that the assessor considers necessary.

1.2 The need for independence can be recognised by considering the licensee's position. Licensees are responsible for safety, but they are also responsible for performance, cost, production, functionality, project duration and everything else. All these other factors relate to a plant *doing what it is supposed to do*, and therefore shortfalls or excesses are very conspicuous. Safety on the other hand relates to the plant being successful in **NOT doing what it is supposed NOT to do**, and shortfalls are not at all conspicuous until they cause an accident - when it is too late.

1.3 A second point is that a licensee's resources are always limited, and the needs of safety often conflict with the needs of one or more of the other factors.

Hence there exists for the licensee a potentially dangerous combination of circumstances, whereby,

1) ***safety must compete with all other requirements for limited resources, and***

2) ***inadequacies in safety are inconspicuous.***

1.4 In spite of a licensee aiming to achieve an adequate safety standard there remains therefore the risk that safety will take a lesser share of the licensee's attention than it should, either because resources are stretched, or because an inadequacy goes unrecognised, or both.

1.5 The necessity for an independent view should therefore be clear. The fact that NII is deliberately independent of licensees and has legal powers to enforce safety requirements may be seen as no more than appropriate compensation for all the factors that naturally conspire against safety. The principle underlying independence is "redundancy", in that if two independent people (or organisations) are satisfied as to the adequacy of safety of an installation, then the additional value provided by the second person relates directly to the absence of common-mode factors. These can never be eliminated completely, but a great deal can and should be done to minimise them.

Objectivity:

1.6 An important requirement to support independence is objectivity. We should be influenced by factual material much more strongly than by opinion, and should always seek factual support for any opinion expressed by a licensee in a safety case. An assessor is usually very conscious of the fact that a licensee is much more knowledgeable about the plant than the assessor is, and must, for the sake of independence, consciously guard against any tendency to defer to the licensee's opinion. If a licensee is confident of something then it should be possible to assemble the material that gave rise to that confidence, in order to convince the assessor. If such material cannot be assembled, then the opinion is unsupported.

1.7 A particular danger that arises from possible lack of objectivity occurs when the assessor's own opinion coincides with that of the licensee. We all have prejudices born out of our own particular background and experience, and whenever we find ourselves being influenced by "gut feel" or the like we should recognise that we may have departed from objective assessment. At such times we should be as forceful in questioning and demanding factual support for our own

opinions as we are those of the licensee, and as thorough in carrying out the assessment as when we disagree.

Assurances:

1.8 Care should be exercised when part of a justification is presented in the form of an assurance by the justifier without supporting documentary evidence. This situation usually occurs during discussions when the assurance is given verbally, and the assessor is expected to take the justifier's word for the matter in question.

1.9 It is very easy in these circumstances to ask for objective evidence, at which the assurer often takes offence at the implied lack of trust. The meeting can deteriorate very quickly after this if the situation is not handled with sensitivity. A person whose integrity is felt to have been challenged invariably reacts negatively, and responds at minimum with less co-operation, and possibly with downright hostility. Assessors should be aware of this danger, and when presented with an assurance should avoid implying any lack of trust - even if it seems that the assurance is unsupportable. Instead the assessment difficulties posed by assurances should be pointed out, namely:-

- 1) the ability to apply *independent* assessment, as we are required to do, is prevented;
- 2) the degree of objectivity in the safety case is reduced; and
- 3) the requirement for the safety case to be rebuilt from its source material at any time in the future is prevented.

1.10 When these difficulties are explained it is less likely that offence will be given, and supporting evidence, if it is available, will be more likely to be found by the assurer.

1.11 If no supporting evidence is available, then the assurance may still be accepted providing the following points can be established:-

- 1) the matter is not one that is central to the overall validity of the safety case. In other words the case would stand without the assurance, but it provides an additional element of comfort or an increased safety margin;

- 2) assurance is straightforward with little or no possibility of misunderstanding between the assessor and the justifier;
- 3) the assurance is indeed factual and not in any way dependent on the opinion of the justifier;
- 4) the justifier is personally qualified to make the assertion - it is not merely something heard from someone else.

1.12 When satisfied, the assessor should document the acceptance of the assurance in a formal manner, or request that the assurance be recorded in the minutes of the meeting with any necessary supporting information that is available. It is important that the record should name the individual making the assurance, not only to demonstrate a traceable reference in this respect but also to maintain the individual's awareness of formal responsibility as spokesperson for the 'body corporate' licensee.

1.13 If the matter is one that is central to the safety case, then the above arguments about independence, objectivity, and self support should be stressed, and it made clear that further evidence must be supplied, even, if necessary, by repeating and recording the process that led to the original assertion.

Assessment Approach:

1.14 It is seldom possible or necessary to assess a safety case in its entirety. Sampling is used to limit the areas scrutinised, to limit the total effort to be applied, and to improve the overall efficiency of the assessment process. If sampling is done carefully it can be expected to reveal generic weaknesses in the safety case as a whole. The majority of samples should be drawn from areas of high safety relevance since weaknesses in these areas are potentially very serious, but a few should also be taken from lower significance areas to check for possible neglect by the licensee.

1.15 An important application of independence is in the way that a safety case is assessed. For example, a licensee might submit a safety justification for an instrumentation channel as part of a wider safety case. In assessing its work, the assessor could check in great detail all parts and question and criticise according to the findings. However this process, although at first sight quite reasonable, suffers from a major lack of independence. It starts from an inappropriate

point, implicitly accepting the need for a justification at all, the suitability of the form of the justification, and the boundaries and assumptions implicit in the methods applied. The assessor is in danger of being "led by the nose".

1.16 It is more productive to start by considering the nature of the plant or system and the hazard(s) that are involved. Then without even reading (much of) the documentation it is possible to draw up a tentative structure for a possible safety justification weighted in those areas most directly related to safety, i.e. effectively an outline specification for a safety justification that the assessor might prepare. What is necessary at this stage is little more than a contents list, enhanced by indications of safety significance and envisaged complicating factors, and it can usually be produced fairly quickly. It is generated by asking questions such as *What is the source of danger? How can it materialise? What would be needed to eliminate the hazard? What sort of protection could be provided? What can go wrong?* etc. Success depends on a knowledge of the hazards concerned and the means by which they can be controlled, a good imagination, and a mentality that is directed at failure rather than success - compulsive worriers and deep pessimists apply here! This latter quality is often very difficult for new assessors to acquire, since the activities that they have generally been used to are geared to success.

1.17 It is important to recognise that the objective of this process is not to set out an expectation of how the licensee should approach the justification, it is purely to have something against which the licensee's work can be compared, since ***a procedure that involves the comparison of two independent structures is much more powerful, particularly in revealing omissions, which are of course not mentioned at all and often represent the most serious of shortcomings, than merely checking a single structure.*** Furthermore, shortcomings in the assessor's own thought processes revealed by scrutiny of the licensee's work represent lack of vision on the part of the assessor, and a self-examination with respect to how they occurred can pay significant dividends over the years in improving assessment skills.

1.18 The licensee's work can certainly be checked, but now in an active manner and to more purpose, with emphasis in those areas of high safety relevance. Additionally the implicit assumptions and boundaries in the work will be more likely to be revealed where they differ from the assessor's own thoughts. All such assumptions and boundaries revealed in this way should be tested objectively for

validity, as should explicit assumptions that are documented as underlying the safety argument. The same process should be applied at several stages throughout the assessment in an iterative manner, as more detailed knowledge is gained about the plant or system and the way it works.

1.19 In this way deliberate attention to independence leads to greater efficiency in that effort is expended in direct relation to safety impact. The additional effort required to draw up the independent structure at each stage is very small as it amounts to little more than a list of topics to be considered, with additional notes to flesh out each resulting from the assessor's own deliberations.

1.20 The assessor should also try, where relevant, to ensure that the independent structures overlap to some extent the specialist areas of other assessors. This is to avoid 'assessment gaps', where two complementary assessors each assume that the other will address points at or near the specialism boundaries. The real world and real plants do not separate themselves conveniently into the areas that assessors (and licensees) separate themselves into, so care is needed to ensure comprehensive coverage of all areas of legitimate safety concern. At each such point the assessor should check that concerns that emerge at or near such boundaries are being addressed by other appropriate assessors, or should address them personally.

Assistance to Licensees:

1.21 A situation which often occurs after a legitimate objection has been raised by an assessor and has been accepted, is that a licensee will ask for assistance with respect to what needs to be done to satisfy the assessor's concern. This is a fair question for a licensee. An obstacle has been reached and must be overcome by as quick and painless a means as possible. It is potentially a dangerous question for an assessor however, since it threatens their independence. An assessor who indicates explicitly what is required, and has this advice taken by the licensee, is risking putting forward a proposal that *will not be subject to independent assessment*. Furthermore, shortcomings that come to light in the assessor's suggestion, especially if they degrade safety, will reflect badly on both the assessor and NII. Hence assessors should try, at least initially, to restrict their advice to clarification of the safety principle which is being pursued rather than to the identification of specific engineering solutions.

1.22 However it is unhelpful and against the principle of openness (and also understandably regarded as perverse by licensees) to insist

on keeping a potential solution secret, in the hope that it will occur independently to the licensee.

1.23 A way round this dilemma is to explain clearly the safety concern that underlies the objection, and to put forward one's idea for satisfying the concern on the strict understanding that although it *appears* to suffice, no guarantee of acceptability is to be assumed by the licensee, and that if it is taken up then it remains the licensee's responsibility to justify it, and it will be assessed as the licensee's own proposal. The assessor should also take particular care to be fully objective in carrying out the assessment as there will clearly be a predisposition to accept it. It might well be advisable to seek a second opinion from a colleague, if one is available, with the appropriate specialist knowledge. In fact it is wise to carry out the required assessment informally *before* making the suggestion, both to avoid the embarrassment of rejecting one's own suggestion, and to foresee any caveats that might apply so that they can be passed to the licensee along with the suggestion.

2. INFORMATION:

2.1 Normally a great deal of information is potentially available, both within a submission and from its references. In essence though what an assessor must be taken not to be distracted by unhelpful information. Information about hazards really needs is information about hazards and their defences. Associated information is necessary to set these aspects into a specific context, but care and their potential consequences establishes the *significance* of the assessment task, whilst information about defences, which may be in the form of systems, procedures, or merely arguments, establishes the potential *complexity* of the assessment task. These two features together enable a judgement of the total *assessment effort* that would be needed without the need for sampling (see 'Assessment Approach' above), and the available time then allows the *degree of sampling* to be determined.

2.2 Judgement is necessary both in deciding whether to assess a particular safety case at all - significance is the usual criterion here though there can be others - and in the time and hence degree of sampling that should be allocated if it is assessed. However, whatever cases and samples are assessed, it is important always to apply sufficient rigour to arrive at defensible judgements, since they may well be challenged either at the time or at any time later. Shortage of time may restrict the range of cases or the areas that are sampled, but should never restrict the depth and rigour of assessment.

2.3 A further aspect that requires separate consideration is presentation, i.e. the quality of the submission itself. Is the material comprehensive? If not is the missing information or assumed prior knowledge already to hand? Is it comprehensive, coherent, accurate and consistent? Is it adequately structured from an assessment point of view? This information determines the *difficulty* of the task. If the task is judged too difficult then the licensee should be approached to present the material in a better or more comprehensive form. It is not profitable to apply effort that can as easily or more easily be applied by the licensee. Furthermore it is the licensee's responsibility to demonstrate the safety of the plant, and a badly presented safety case prevents that responsibility being fulfilled. It should be remembered that the licensee should have reached a properly objective and valid conclusion as to the safety of the plant. Our job is to be satisfied, independently, that the licensee's opinion is soundly based. This is important. It is easy to become enmeshed in the process whereby the licensee is trying to convince us that the plant is safe, whereas in fact *we should be judging whether or not the licensee has achieved the necessary confidence, in a proper and demonstrable manner, that it is safe.* The difference may be subtle, but it has particular significance when information is presented in a form that makes assessment difficult. An assessor should not be unduly reticent in rejecting a poor safety case, and should argue that since its purpose is to document the basis of the licensee's belief in plant safety, it does not fulfil that purpose in its current form. The specific shortfalls should be indicated clearly by the assessor to support the rejection. This is a much more effective stance to take than merely to complain that the licensee has made the assessor's task difficult. Such complaints do not usually elicit much sympathy.

2.4 Note that in order for a safety case to be effective it must provide three elements: *Safety Requirements, Evidence and Argument* (Ref 1). These normally exist at several levels of detail, from overall plant to specific subsystem. The safety requirements represent the licensee's perception of the objectives to be met, and may be explicitly stated or implicit, in which case they should be self evident, for example to meet established company criteria and demonstrate that risks are ALARP. The evidence must always be explicit, and either stated in the case itself or referenced from it. The evidence is the raw information or data that underpins the ability to show that the safety requirements are met. The argument must also be explicit, and at the higher levels should be in the safety case itself rather than referenced from it, although more detailed level arguments may well be referenced out. The argument is what links the evidence to the requirements, it is what does the 'showing' in showing the safety

requirements are met - it 'tells the safety story'. Although it is relatively rare for any of these elements to be missed completely, it often happens that they are out of balance. This particularly applies between evidence and argument, cases often consisting either of vast amounts of factual material with very little in the way of argument, or very extensive argument with little factual support.

2.5 In gathering information of all kinds it is necessary to work in a proactive manner to avoid implicitly accepting licensees' judgements - by seeking answers to questions - and *not* by mere passive reading. The process is an iterative one and is closely linked to the independent safety justification structures discussed earlier under 'Assessment Approach'. The questions should be hierarchical in nature, starting with general matters - *What are the hazards? How can they cause harm? What does safety depend on? What can go wrong?*; and progressing to more detail as the exercise proceeds - *Is it always available? How can we be sure? How does it work? What does it depend on? Is that always available? What would happen if? How can consequences be prevented/mitigated? etc*; and always *Are associated risks as low as reasonably practicable (ALARP)?* If an independent safety justification structure has been prepared as discussed above, then the questions will follow naturally when this is compared with the licensee's approach.

2.6 The review should be regarded as an interrogation, or a directed investigation, where the assessor maintains control at all times but is sensitive to the significance of points that arise. Unexpected information will come to light, and it is appropriate to allow this to influence the direction of the investigation. The independent justification structure should be added to, amended or refined at such times, the assessment process in this way always remaining active and iterative.

2.7 The assessor should at all times guard against lapsing into mere passive reading. This can represent a most inefficient way of working. Time can be wasted by being sidetracked into unproductive byways, and the assessor's creative and imaginative talents can be dulled by the attention being controlled in a guided tour rather than by allowing it the freedom to explore its own chosen paths.

3. ADEQUACY:

3.1 It is the responsibility of the assessor to judge when and if a safety case is adequate and the associated risks shown to be ALARP. Although it can be assumed that the licensee believes a submitted

safety case to be adequate, the assessor must have in mind a clear and independent image of what adequacy means, and must be able to recognise when it has been achieved. If there are documented standards, criteria and/or guidance (licensees' own; SAPs; HSE's, including 'Tolerability of Risk' (TOR) and 'Reducing Risks, Protecting People' (R2P2); national or international) that are relevant in a particular area then these may be called upon to help establish an appropriate benchmark. If not then an appropriate and justifiable benchmark still needs to be developed, using whatever existing material is available together with objective judgement, taking account of the nature and age of the plant, the nuclear hazards involved, and the worst-case accident consequences and their likelihood.

3.2 Licensees become justifiably frustrated when presented with seemingly endless and unconnected questions, and by objections that they fail to understand, when there is no clear indication of the objective that is being sought. In questioning or objecting to a safety case therefore the assessor should take pains to indicate, when it is not self evident, what the underlying concern is in each case. *If the licensee can discern the logic behind each line of enquiry a constructive and helpful response is much more likely.* It is regrettable perhaps but nevertheless a fact that very often the particular questions that are asked or objections that are raised are caused by misinterpretations or misunderstandings, the causes of which can lie with the assessor or with the wording of the safety case. In such cases a clear indication of the assessor's concerns prevents the licensee and assessor becoming entangled in a web of increasing and futile confusion which can be very damaging to mutual respect, and therefore to effective progress.

Material Presented:

3.3 Care should be exercised in being unduly influenced by the amount of material presented in a safety case, especially when a particular aspect of a wider justification is being assessed. A licensee may supply a surprisingly large amount of information pertaining to a particular aspect of a system, and it is easy to accept the necessity for such information and assess it at face value. In this case a disproportionate amount of effort can easily be expended in matters of little safety importance. Licensees sometimes submit a mass of material that has not been produced especially for the safety case but already exists, often in the hope (a) that the sheer quantity will cover any points that the assessor might raise, and/or (b) that the assessor will do the necessary legwork to extract the essential and relevant information and thereby, in effect, make the safety argument on behalf

of the licensee. This sort of danger illustrates well the need for an independent view of what is expected and for *active* assessment - the assessor needs to maintain control at all times - a lapse into passive review of whatever is presented severely reduces effectiveness in these circumstances. Note also the points made earlier under 'Information' about the three elements of an effective safety case - safety requirements, evidence and argument. In a good case these are well balanced. A severe imbalance is often a sign that the material has not been prepared with the intention of forming a safety case. It should always be remembered however that the assessor's expectations may be wrong and the licensee's treatment right, in which case the error will soon be spotted, but without an independent view the assessor will be guided implicitly by the licensee's material.

3.4 Conversely the licensee may neglect or deal superficially with an area that the assessor feels should be addressed in more detail, but may be persuaded - perhaps almost without consciously realising it - that such treatment is inappropriate. This often happens when an assessor has pointed out an apparent omission on the licensee's part, and the licensee, being subject to normal human nature, seeks to justify the original neglect of the matter by playing it down. This point is not intended to imply any dishonesty on the licensee's part - the process is a subjective one - a person is easily persuaded to the view that something that was not thought of does not matter. The assessor however should guard against being as easily persuaded, especially as the justification is often highly subjective in these circumstances. This point relates back to the earlier discussion on objectivity

3.5 The important thing to keep in mind is the HAZARD. The assessor should maintain a firm mental grasp of that, apply assessment effort accordingly, and judge that the case is adequate only when all associated concerns have been satisfied.

A Way to Focus the Mind:

3.6 A very powerful self-test that the assessor can apply in helping to decide whether or not adequacy has been achieved is to imagine that a serious accident has occurred, and that the cause has been traced to the particular system being assessed. The big question is - how justifiable is the assessor's acceptance of the system?

3.7 This exercise should not be treated as merely academic. If such an event occurred then the assessor's work would indeed be called into question. It might be thought that by the fact of the accident

itself the assessment must have been inadequate, but this is not so. A genuinely adequate system can fail, and multiple safeguards can fail simultaneously. Adequacy does not imply perfection, it represents an appropriate improbability of dangerous failure. In other words, the fact of failure does not in itself prove inadequacy, but points either to inadequacy or to sheer bad luck. The assessor's task would be to convince a court that the assessment carried out was such as would have been done by a reasonable person with appropriate qualifications and experience, exercising discretion as permitted by instructions, on the basis of the state of knowledge prior to the event. If an assessor can feel reasonably comfortable with the judgements made in these circumstances then the process has gone far enough.

Record Keeping:

3.8 The need for a comprehensive written record is of paramount importance and should be clear from the above argument. If an accident occurs it is likely to be long after the justification and its assessment have been carried out. Even if the assessor had a defensible position at the time, poor record keeping might make this difficult or even impossible to establish. The assessment records need not all be included in the final assessment report or note, they can be kept as part of the background material. However they must be kept on the appropriate official file, so as to be accessible at any time in the future. What is required is to indicate clearly the basis of the assessment conclusions - *This is what I think, and this is why I think it.*

3.9 A further point about records is that pros as well as cons should be recorded, so as to present a balanced picture overall.

Implied and Actual Plant Safety:

3.10 It should always be borne in mind that *safety is a feature of the plant and its operation, and not of the abstracted safety case.* Working remotely, from information in reports and other documents, it is possible to be insulated from the reality of achieved nuclear safety, becoming preoccupied with the correctness and adequacy of the documented safety case in isolation.

3.11 The relationship between the plant and its associated safety justification is not always as rigid as might be assumed, the justification sometimes representing a claimed state or expectation that may not be fully attained in practice. These considerations apply with regard to design intent and implementation, which may not always

be the same; and to operational claims, which may not always be borne out in practice. Appropriate measures should therefore be taken to verify or otherwise test the claims made, preferably by direct inspection, or by assistance from the appropriate site inspector.

3.12 Inspection in support of assessment should be against specific rather than general plant features. A powerful technique to apply is "deep thin slice" sampling, where deliberate scrutiny of a number of detailed matters across a narrow field is applied as a test of the licensee's adherence to declared procedures, principles and claims. In spite of the narrow view taken this technique is very good at revealing generic weaknesses. When a weakness is found it should be pursued in some detail; it is most unlikely to be an isolated case even though the licensee may well claim it to be so. Whenever sampling is used it should be as part of a predetermined plan, and where time is limited the number of samples should be reduced rather than the depth of each sample. Generally three or four samples are sufficient for most inspection purposes, and should be chosen by the assessor unless there is an overriding reason for the licensee to choose them, in which case it must be ensured that there is no possibility of favourable selection occurring. If weaknesses are found then it will probably be necessary to take further samples to ascertain how widespread they are, but the new samples need only be reviewed for the particular weakness rather than in the same detail as the original samples.

4. Conclusion:

4.1 This Appendix has examined what are considered to be the three core elements of effective assessment, namely independence, information, and judgement of adequacy. It should be noted however that although they have been addressed separately they are not in practice separate. They represent complementary aspects of the iterative assessment process of information gathering and judgement making, undertaken in ways that capitalise on our independence from licensees.

References:

Ref 1: "Arguing Safety - A Systematic Approach to Managing Safety Cases" by T P Kelly September 1998.
University of York Dept. of Computer Science.