

BACKGROUND TO AND EXPERIENCE USING THE NII'S NEW SAFETY ASSESSMENT PRINCIPLES – LEARNING FOR THE HIGH HAZARD SECTOR?

Dr Andy Trimble
HM Superintending Inspector (Nuclear Installations), HM Nuclear Installations Inspectorate, Redgrave Court, Merton Road, BOOTLE L20 7HS

In January 2007 HSE's Nuclear Installations Inspectorate (NII) had redrafted and reissued its safety assessment principles (SAPs) following more than 10 years of use for the previous version. This paper reviews the drivers and outcomes from this exercise and also reviews experience in the first year of use in the nuclear chemical plant sector. We also review the way forward with our subsidiary technical assessment guides (TAGs) which complement the SAPs and further assist safety assessment in the nuclear sector.

The inspectorate now even better placed to carry out its work in a consistent and targeted manner. The clarity in regulatory expectation brought by the new SAPs has been welcomed in many quarters and our inspectors have also welcomed the increased clarity they bring. Overall, we believe that, once complete, the package of SAPs and subsidiary technical guides are as good as any in the world and form a sound basis for the inspectorate to move forwardand meet the challenges that face it. The lessons learned will also apply, selectively, in many other parts of the high hazard industries.

BACKGROUND AND INTRODUCTION

In the nuclear regulatory regime, the Health and Safety Executive's (HSE) Nuclear Installations Inspectorate (NII) does not specify what should and should not be in a safety case [12]. However, the regulatory goals are set out in our Safety Assessment Principles (SAPs) [e.g. 1]. These Principles were originally written for nuclear plant in design and they were also used to inform periodic safety case reviews required under licence conditions.

We decided, in the light of the experience gained over the last decade or so, to review our Principles and to make them more relevant to the environment in which we now regulate. It is important to note that the initial reviews showed that most of the original Principles are still relevant but could be made clearer in their application to the wide variety of plant we now regulate. We had already addressed some omissions in our subsidiary guidance [e.g. 9,10].

Whilst these new SAPs [5] (SAPs 06) were written explicitly for the nuclear sector, there are many parts that take on board thinking from the non nuclear high hazards sector

and other parts that complement the high hazard sector thinking. Therefore, companies are encouraged to review their corporate safety processes against SAPs 06 (bearing in mind they are set as regulatory guidance) and, where appropriate, incorporate the applicable thinking into their own guidance and standards.

DRIVERS

The SAPs have evolved over time:

- 1979: first produced for nuclear reactors
- 1983: first produced for nuclear chemical plant
- 1988: the 1979 version modified following Sizewell B inquiry
- 1992: combined version produced, taking account of the Tolerability of Risk [2] framework

However, the 1992 SAPs have remained unchanged until 2006. Although they have needed expert interpretation from time to time, they have served us well in setting regulatory expectation for nuclear facility safety cases.

Increasingly, the 1992 SAPs were being used for assessing safety cases that had design elements that were constrained by what existed – for example, decommissioning safety cases [3]. In addition experience showed that safety thinking was developing and the SAPs were not giving best advice to our inspectors. Therefore, the NII has devoted scarce resource to this work to reap the long term benefit.

The prime drivers for change and sources of reference were:

a) IAEA standards: NII's policy is that our guidance will be consistent with the international atomic agency standards which provide an international benchmark. These IAEA documents have been evolving and continue to do so. This has been a driver to try and make the latest SAPs version easier to change by making them web based to avoid republishing a paper document. This does not mean that our SAPs are an attempt to clone the IAEA guidance – rather they reflect the safety thinking in the IAEA standards.
b) Increased emphasis on decommissioning: With the advent of the Nuclear Decommissioning Authority the level of decommissioning activity has risen significantly and we considered that there was sufficient experience to make it worthwhile incorporating our latest thinking into the new SAPs.
c) Aspects that had been part of regulatory good practice but not yet incorporated into SAPs:
   Leadership and Management of Safety
   Regulatory Assessment of Safety Cases
   Radiation Protection
   Accident Management and Emergency Preparedness
   Radioactive Waste Management

Decommissioning
Control and Remediation of Radioactively Contaminated Land

d) Improved presentational consistency: The basis of any safe facility is sound engineering (reflecting the Good Practice thinking in Reducing Risks, Protecting People [4] - R2P2) and so the engineering has been brought forward in the layout of the new SAPs. Similarly, people are key to any safe operation and so the people and organisational aspects, embedded in the leadership and safety case SAPs have also been brought forward in the layout. Finally there were minor internal inconsistencies between sections, for example, there were concepts in one part of the 1992 SAPs that were principles in one section and comparable concepts were supporting guidance in another. Whilst this did not detract from the value of the concepts, they had the potential to send inconsistent messages. The overall editing in the new SAPs has been a difficult and demanding task but we are convinced the outcome is now consistent enough and sends a much more coherent message than before.

Also the following occurred during the process of revision and were incorporated into the thinking as far as possible:

e) WENRA reference levels: NII is also committed to being consistent with the reference levels set by the Western European Nuclear Regulators Association. Although these apply only to existing power reactors and waste there are elements that represent international regulatory consensus on good practice and so, where appropriate, they have been incorporated into SAPs 06.

f) Potential new power reactor build: With the government's intention that the UK should build new nuclear power reactors there was a need to make our SAPs more transparent to an international audience of power reactor vendors who may not be familiar with the UK regulatory regime.

It is important to note that there has been no significant change in the underpinning law and, in particular, the so far as is reasonably practicable (better known as ALARP) obligation still remains. Also, in line with R2P2, ALARP is more than cost/benefit analysis. In most cases relevant good practice will be more important. Because SAPs06 reflect the most up to date thinking, they also reflect good practice. Therefore, part of good safety practice will be found in SAPs.

Similarly, because this work was primarily about incorporating present practice and consolidation, SAPs 06 did not automatically make current safety cases out of date. However, what we do expect is that licensees and other relevant duty holders will review their own criteria – bearing in mind the intent of SAPs – to see if there are improvements that can reasonably be put in place. We do not expect to see wholesale changes to licensees' safety documentation, either in the underpinning guidance or the safety cases which they support.

It is also important to stress that SAPs are assessment guidance for NII's assessors (as well as being adopted or recognised by other regulatory stakeholders in their spheres of responsibility). Therefore, they should not be used as design guides or to underpin operations. Duty holders are expected to develop their own criteria.

REVISED SAPS STRUCTURE

The Document structure is:

Introduction
Fundamental Principles
Leadership and Management for Safety
The Regulatory Assessment of Safety Cases
The Regulatory Assessment of Siting
Engineering Principles
Radiation Protection
Fault Analysis
Numerical Targets and Legal Limits
Accident Management and Emergency Preparedness
Radioactive Waste Management
Decommissioning
Control and Remediation of Radioactively Contaminated Land
Glossary, Annex etc

Following a period of extensive public engagement SAPs 06 have been published on the web (now the definitive version). Also published were:

- Resolution of comments from public engagement [11]
- Table linking 2006 and 1992 SAPs [8]
- Explanatory Note on Numerical Targets and Legal Limits [7]
- NSD Guidance on Demonstration of ALARP (T/AST/005 revised [6])

There were, among other things, commitments to carry forward some comments and some of the principles in the 1992 SAPs into supporting technical assessment guides (TAGs). There are processes in place to sentence these and the outcome will be published on the web.

It is important to recognise that ALARP is driven by HSE corporate thinking and T/AST/005 interprets this for then nuclear sector where there have been very specific challenges to interpretation over the years. So this document incorporates such thinking reflected in SAPs.

What is more significant from a usability point of view is the more consistent high level definition of a Principle. These are highlighted in the text and numbered with the relevant good practice below. This lends a clarity and consistency to the document that would be difficult to achieve in any other way. This clarity will be continued into TAGs to form a coherent and consistent suite of documentation covering the regulatory assessment technicalities either in greater detail or to give a different perspective and logic on how SAPs relate to each other and how they might be applied.

Also given the new way of presenting the Principles at a reasonably high level, then the amount of detail that can be included in the good practice and leave a document of manageable size was limited. Thus a comparison of the new SAPs with the 1992 version will show a number of omissions. For example, principle P45 which dealt with plant

damage will be covered in TAGs where it can be more fully expounded for the range of facilities NII regulates. If necessary, there will be separate parts of TAGs covering certain generic plant, typically, power reactors, defence facilities and chemical plant.

The 1992 SAPs established the link between Tolerability of Risk and SAPs. This sent the unfortunate message in some quarters that the principal need in a safety case was to show compliance with the numerical analysis even though the introduction stated clearly this was not the intention. Therefore, in SAPs 06, we adopted a structure that better reflects the importance of the various aspects of safety management. However, it is important not to over compensate and neglect the rest of the Principles. In all cases a balance appropriate to operations and facilities under consideration needs to be struck. Assessment inspectors are always encouraged to take this holistic view when carrying out their work.

Although the new SAPs have expanded to 139 pages from 47, most of this expansion is due to the inclusion of material formerly elsewhere (e.g. [9,10,12]) and to greater clarity because we better have shown the underpinning thinking and defined many of the terms used. This is of particular importance to those who may be entering the UK nuclear industry for the first time as most of our established licensees have an understanding of our regulatory expectations for their operations. This is relevant not only to potential new build but also to companies entering the decommissioning field engendered by the Nuclear Decommissioning Authority's bidding process. To further aid understanding we have explained the underpinning thinking for the principles. Most often this is at the *"dialogue"* at the beginning of each relevant section e.g. the introduction to fault analysis at paragraphs 496 to 503. However, it is important not to overlook the underpinning philosophy in the introduction. There is much of value here including a closing statement:

> *"The principles are written bearing in mind the content of safety cases likely to be submitted to the NII. However, dutyholders may wish to put forward a safety case that differs from this expectation and, as in the past, the inspector will consider such an approach. In these cases the dutyholder is advised to discuss the method of demonstration with NII beforehand. Such cases will need to demonstrate equivalence to the outcomes associated with the use of the principles here, and such a demonstration may need to be examined in greater depth to gain such an assurance. An example of such a situation is the greater use of passive safe concepts."*

However, there is compelling guidance that, in essence, says [13] – bearing in mind the different purposes for which they are intended, there should be the minimum of differences between licensees' safety criteria and the NII SAPs. Plainly, it is each parties' interest to avoid extra work and the resulting delays if the outcome can be achieved in a more productive, mutually understood way. Thus NII often has such understandings with existing licensees to ensure that, when there are differences, then these are mutually understood. Establishing such understandings can be a long and challenging process.

Also in the introduction is a section on proportionality – an HSC policy imperative. Unlike the IAEA which publishes different documents for different facilities, HSE publishes general documents such as SAPs and applies proportionality. Thus the extent and rigour

expected in any safety case will be in broad proportion to the underpinning hazard, among other things. This in turn is related to the harm potential of the materials being handled and the conditions under which they are handled – which is a way of defining hazard. In other words, the hazard is a function of the radio toxicity, mobility and driving force(s) under the plant conditions being considered and is consistent with legal interpretation of the Health and Safety at Work Act [17]. This policy has driven NII assessment for many years [14].

Although we use the word safety, this term includes regulating waste management on licensed sites and the final sections of SAPs demonstrate this. To ensure minimal regulatory overlap we have involved the Environment Agency in our development process and continue to do so as we develop the supporting TAGs. This should mean that the expectation from regulators should be consistent and minimise the regulatory burdens on industry.

Finally, we have clarified links to the law. This can be seen, for example, in references to nuclear site licence conditions and to dose limits from the Ionising radiations regulations [15]. In particular, some of the basic safety levels (BSLs – the levels our policy say should not normally be exceeded and equate broadly to the limit of tolerability from R2P2/TOR [4]) in the targets section have a designation BSL(LL) indicating their link to the law. This clarity helps inspectors to know when to insist on further improvements and how stringently they should pursue these. It also makes a more consistent approach to safety that is more transparent to all stakeholders.

SAPS AND TAGS

Although we have already published our TAGs (e.g. [6]) they are now inconsistent with the new SAPs (although that does not detract from the guidance in them). NII has now embarked on a process of revision. The content, approach and timetable for bringing these into the public domain is being developed and this is planned to produce a coherent and more comprehensive suite of documents that will also help our stakeholders understand our expectations.

The outline plan is:

By mid 2008 – first tranche of TAGs to be on the web for comment. These will include most of those relevant to new build as this is seen as the area of most pressing need.

By 2009 – all TAGs to be drafted and ongoing maintenance work to be undertaken based on experience and feedback.

This programme will be driven by the priorities at the time. Although this appears an easily achieved timescale, such tasks are not simple and our experience with the SAPs shows that being consistent across a suite of documents is not simple – especially when different TAGs may be drafted by several different authors working in separate technical disciplines. Pragmatically, we may need to tolerate minor inconsistencies to get the benefit of having a set of published documents. In line with SAPs 06 we would expect to revise this suite on the web and the definitive versions will be the electronic web documents.

In practice, some of the more significant TAGs (e.g. [14]) are in a late stage of drafting and may well be put out for comment earlier. As with the SAPs we are involving

other regulatory agencies including the environment agency and the defence nuclear safety regulator (DNSR). As before, this should optimise regulatory demands on duty holders and thereby minimise regulatory compliance costs because these regulatory expectations should be more consistent.

The NII is prepared to put scarce resource to this work to gain the longer term benefits. However, this in itself will almost certainly generate further work with licensees to ensure their criteria are consistent enough even though minimal change may be required.

EXPERIENCE

It will have become obvious that since SAPs 06 have not significantly changed our guidance and thinking, that the effect on our work should be minimal. What has happened is that new inspectors, who usually start in assessment roles, now have much clearer and consistent guidance which assists their rapid development. This is crucial as the inspector age profile is skewed towards retirement and the need for knowledge management becomes ever more acute. As a result, NII is recruiting to address this and new inspectors can look towards a career in regulation with greater certainty of what is expected from them technically.

Our licensees, who were consulted about the SAPs 06, have also been reviewing their criteria to help meet the compelling advice to avoid inconsistencies between that and our SAPs. At least one is taking the opportunity to revisit their understandings with us. This work will underpin the way we regulate. If licensees present safety cases that meet our expectations or are to a comparable standard, then the assessment work is made a great deal easier and safety is better assured (provided the safety cases are implemented as intended). There is no safety benefit for either party to have long drawn out debate about methods and processes that do not deliver safety in operations. Thus, we are piloting an assessment approach that considers not only the paperwork but involves assessment inspectors taking a much higher role in safety case implementation. This is not something new but a change of emphasis to promulgate good practice more widely.

DISCUSSION

It is important to summarise the role of SAPs:

SAPs are	SAPs are NOT
Regulatory safety goals	Design criteria
Regulatory assessment guides	HSE guidance to dutyholders
Guides for regulatory judgments	Mandatory standards
Assistance in judging ALARP	To be met unconditionally
To be considered holistically	To be considered separate good practices
For regulatory use	To be adopted wholesale

Our expectation (as in the 1992 SAPs) is that modern facilities should have little difficulty in meeting these regulatory expectations. However, older facilities built to earlier standards will be judged against SAPs 06 and our expectation is that licensees should be able to demonstrate they have done (or will do) all that is reasonably practicable to reduce potential harm to people. SAPs 06 will be used as a benchmark as has always been the case. The clarity of this set of SAPs should help licensees and potential licensees understand our regulatory expectation.

There is one area where there may seem to be a contradiction. This is where risks increase, usually temporarily, in order to gain an overall benefit. This is seen most often in decommissioning [3] where the hazard needs to be managed by removing the facility's radioactive contents. Such actions can represent a reduction in safety on such ageing facilities but are a necessary part of achieving a long term stable state for their contents. Such situations are now better understood and where activities to reduce long-term risks mean risks rise in the short term, efforts should be made to carry out the activities such that the risks are minimised both in magnitude and time. It is important to stress (SAPs para 637):

> *"High risks that would exceed BSLs if evaluated as continuous risks should be avoided except in special circumstances. These circumstances should be justified in advance. They may include situations not originally foreseen in the design of the facility, or which are unavoidable because of the need to increase risks for a short time to reach a safer state in the long term."*

One theme that runs through this paper has been the holistic view that inspectors take in doing their assessment. This comes out very strongly in SAPs:

> *"Priority should be given to achieving an overall balance of safety rather than satisfying each principle or making an ALARP judgment against each principle. The principles themselves should be applied in a reasonably practicable manner. The judgment using the principles in the SAPs is always subject to consideration of ALARP."*

This simply acknowledges that engineering and management of safety are a matter of expert judgement to optimise the compromises that must be made to achieve a safe, workable, affordable environmentally friendly operation that delivers for the dutyholder. Inspectors realise that they need to judge whether or not such a balance has been struck.

Nuclear installations are in the high risk category in the Management of Health and Safety Regulations Approved Code of Practice (ACoP) [16]. However, they are not alone. Therefore, it is a logical deduction that other facilities may benefit from the nuclear experience now embedded in these new SAPs. Therefore, comparable high hazard industries are invited to review their corporate guidance and standards as a learning exercise so that they may be better able to demonstrate ALARP. Plainly, as with nuclear installations, not everything applies to every facility, discrimination should prevail.

POTENTIAL APPLICATIONS

As an example of how some of the concepts might be applied both in the nuclear and non nuclear sectors, consider the "technical" principles. These can be broken down into a number of broad categories [14]:

a. Design Basis accident analysis (DBAA)
b. Probabilistic safety analysis (PSA sometimes known as QRA)
c. Severe accident analysis (SAA)
d. Good Engineering Practice (GEP)
e. Waste Management

The first three are complementary forms of fault analysis. Dealing with each of these broad areas in turn:

DBAA: is a robust demonstration of fault tolerance. It links directly to the engineering principles which call for a preferred series of responses to faults. These vary from designs that are inherently safe to those that may require operator intervention in the fault sequence. The important feature of DBAA is that any uncertainty is allowed for by conservatism. Often this conservatism is in the input data and requires expert judgments about the degree of conservatism appropriate to any particular case. DBAA is concerned with faults with larger harm potential and not normally with more minor events. This methodology has much in common with Layers of Protection Analysis (LOPA) (although the output is different) which is already a well accepted methodology in the high hazard industries. In the nuclear sector DBAA is the bedrock of fault analysis and is used to derive the operating parameters for plant control.

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

SAA: A severe accident is one which is not necessarily expected in a plant lifetime but has the potential for high doses or environmental damage. It is not necessary for these doses or environmental damage to be realised. The prime difference between DBAA and SAA is in the way that data is used. SAA is carried out on a best estimate basis and may well be bounded by the DBAA if the level of conservatism is high. However, a sound understanding of the underlying phenomena during such accidents avoids the need for introducing unnecessary conservatism and hence unfruitful expenditure. The main aim of SAA is to provide an input to emergency planning and to identify reasonably practical improvements that can be implemented at reasonable cost. There may be cases where this may influence the options at the design stage of a project.

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

be covered by DBAA, the learning experience of the company and/or the industry are taken into account. Often GEP is embodied in design manuals or company standards. Quality engineering should not stray outside this standard. Nuclear safety cases have a significant section on engineering substantiation to demonstrate GEP has been met and that then engineering will continue to deliver the appropriate safety function for the foreseeable future (usually taken by convention at 10 years minimum). This has similarities with vessel inspections and lifting inspections carried out in the non nuclear sector - which are often not possible on nuclear process plant as access can be highly restricted due to radiation.

Waste Management: There are major additional external constraints as well as those required for safety. Much regulation is concerned with implementing government policy and good practice. Plainly, this also reflects public opposition to ill considered waste accumulation and storage (disposal is dealt with under Environmental Legislation administered by the Environment Agencies). This is becoming and increasingly large part of the work in the nuclear sector.

These aspects are often found in high hazard industry although the "labels" may be different. However, it is good practice to critically examine corporate standards against a range of good practice and such concepts are one input.

CONCLUSIONS

The inspectorate now even better placed to carry out its work nationally and internationally in a consistent and targeted manner. The clarity in regulatory expectation brought by the new SAPs has been welcomed in many quarters and our inspectors have also welcomed the increased clarity they bring. Overall, we believe that, once complete, the package of SAPs and subsidiary technical guides are as good as any in the world and form a sound basis for the inspectorate to move forward and meet the challenges that face it. The lessons learned will also apply, selectively, in many other parts of the high hazard industries.

REFERENCES

1. Safety Assessment Principles for Nuclear Plants HSE 1992 ISBN 0 11 882043 5
2. The tolerability of risk from Nuclear Power stations HMSO 1988 ISBN 0118839289
3. G A Trimble, SUMMARY OF THE CURRENT UK POSITION ON DECOMMISSIONING SAFETY CASES AND CONTROL OF OPERATIONS *Proc HAZARDS XIX* 792ff
4. Reducing Risks, Protecting People (R2P2) HSE 2001 http://www.hse.gov.uk/dst/r2p2.pdf
5. Safety Assessment Principles for Nuclear Facilities 2006 Edition HSE http://www.hse.gov.uk/nuclear/saps/saps2006.pdf
6. T/AST 005 Issue 3, NSD GUIDANCE ON THE DEMONSTRATION OF ALARP http://www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast005.pdf

7. Numerical targets and legal limits in Safety Assessment Principles for Nuclear Facilities, An explanatory note HSE December 2006 http://www.hse.gov.uk/nuclear/saps/explanation.pdf
8. SAPS 206 Edition – Stakeholder comments resolution http://www.hse.gov.uk/nuclear/saps/publiccomments.pdf
9. Management of radioactive materials and radioactive waste on nuclear sites http://www.hse.gov.uk/nsd/waste1.pdf
10. Decommissioning on nuclear licensed sites http://www.hse.gov.uk/nsd/decomm1.pdf
11. 1992 to 2006 SAPs Cross-reference Table http://www.hse.gov.uk/nuclear/saps/cross-reference.pdf
12. TECHNICAL ASSESSMENT GUIDE T/AST/051, GUIDANCE ON THE PURPOSE, SCOPE AND CONTENT OF NUCLEAR SAFETY CASES http://www.hse.gov.uk/nsd/tast051.htm
13. Sizewell B Public Inquiry Report by Sir Frank Layfield, Dept of Energy
14. T/AST/006 Issue 03, DETERMINISTIC SAFETY ANALYSIS AND THE USE OF ENGINEERING PRINCIPLES IN SAFETY ASSESSMENT http://www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast006.pdf
15. Work with ionising radiation. Ionising Radiations Regulations 1999. Approved Code of Practice and guidance L121 HSE Books 2000 ISBN 0 7176 1746 7
16. Management of health and safety at work. Management of Health and Safety at Work Regulations 1999. Approved Code of Practice and guidance L21 (Second edition) HSE Books 2000 ISBN 0 7176 2488 9
17. R v Board of Trustees of the Science Museum All England Law Reports. 10 Sep. 1993, part 3, 853–861.

ACKNOWLEDGMENT AND DISCLAIMER

Thanks go to many in HSE's Nuclear Installations Inspectorate for help and advice in developing this paper, in particular Mr G J Vaughan. The opinions here are those of the author. No part of this paper should be taken as definitive interpretation of HSE or NII policy, the law, or their application.