NUCLEAR INDUSTRY ASSOCIATION AND INSTITUTE OF MECHANICAL ENGINEERS

"ZEN AND THE ART OF SAFETY CASE MAINTENANCE IN THE POST-NIMROD WORLD"

KEYNOTE SPEECH BY MR JUSTICE HADDON-CAVE

6th June 2017 – Birmingham Conference
Fit for Purpose Safety Cases in the Nuclear Industry

ABSTRACT

RAF Nimrod XV230 suffered a catastrophic mid-air fire whilst on a routine mission over Helmand Province in Afghanistan on 2nd September 2006. This led to the total loss of the aircraft and the death of all 14 service personnel on board. It was the biggest single loss of life of British service personnel in one incident since the Falklands War. The cause was not enemy fire, but leaking fuel being ignited by an exposed hot cross-feed pipe. It was a pure technical failure. It was an accident waiting to happen. The deeper causes were organizational and managerial and can be traced back to design flaws 30 years earlier.

Crucially, there was the outsourcing of the Nimrod Safety Case in 2004-05 which produced a large amount of paper which said that the aircraft was 'safe', when manifestly it was not. The Safety Case missed obvious risks. The military Safety Case regime had lost its way. It had led to a culture of 'paper safety' at the expense of *real* safety. It did not represent value for money. Its shortcomings included: bureaucratic length; obscure language; a failure to see the wood for the trees; archaeological documentary exercises; routine outsourcing to Industry; lack of vital operator input; disproportionality; ignoring of age issues; compliance-only exercises; audits of process only; prior assumptions of safety; and decorative 'shelf-ware'. *The Nimrod Review* recommended that Safety Cases should be renamed "*Risk Cases*" and conform in the future to the six Principles: **S**UCCINCT; **H**OME-GROWN; **A**CCESSIBLE; **P**ROPORTIONATE; **E**ASY TO UNDERSTAND; and **D**OCUMENT-LITE. Safety Case should be an aid to thinking, not an end in themselves. Like the Pompidou Centre in Paris, Safety Cases should have their workings visible on the outside. They should be a living thing. Safety Cases are bristling with risks. They require constant maintenance.

"A motorcycle functions entirely in accordance with the laws of reason, and a study of the art of motorcycle maintenance is really a miniature study of the art of rationality itself." (Robert M. Pirsig, Zen and the Art of Motorcycle Maintenance: An Inquiry into Values (1974))

'*God is watching the apples*'

1. Pupils at a local convent school had lined up at the cafeteria for lunch. At the head of the counter was a large bowl of juicy red apples. A nun had left a note beside the bowl which read, "*Take only one. God is watching.*" At the other end of the counter was a large bowl of chocolate chip cookies where a pupil had left a handwritten message which read, "*Take all you want. God is watching the apples.*"

2. Good afternoon. It is a privilege to be asked by IMechE (the Institute of Mechanical Engineers) and the NIA (Nuclear Industry Association) to speak to you about Safety Cases and the lessons learned from *The Nimrod Review*[1] at this important and appropriately named conference "*Fit for Purpose Safety Cases in the Nuclear Industry*"

Zen and the Art of Motorcycle Maintenance

3. This year has seen the death of the American philosopher, Robert Maynard Pirsig, who wrote *Zen and the Art of Motorcycle Maintenance: An Inquiry Into Values*[2] in which he explored the meaning of "quality" using the novel conceit of a motor-cycle journey[3]. His alter ego *Phaedrus* is driven insane by this philosophical question and subjected to electroconvulsive therapy. I hope this lecture will prove a little less painful.
4. Professor Pirsig describes the "*Romantic*"[4] (or Zen) approach to life, where one is focussed on being 'in the moment' and hopes for the best, and the "*Classical*" approach, where one is determined rationally to understand the inner workings. He pointed out that motorcycle maintenance was not simply a "knack" but an exercise in pure rationality. The book demonstrates that motorcycle maintenance, like building a safety case, may either be either dull and tedious or enjoyable and rewarding; it all depends on attitude.
5. If you display what Professor Pirsig would regard as a good attitude (and rationality) for the next 30 minutes, I might reward you with some PowerPoints. However, as some of you may know, I recommended in *The Nimrod Review* that the ubiquitous use of PowerPoints should be discouraged because it lead the audience to watch rather than think (especially after a good lunch).[5]

Nimrod XV230

6. On 2nd September 2006, the maritime reconnaissance aircraft *RAF Nimrod MR2 XV230*[6] suffered a catastrophic fire and exploded in mid-air whilst on a routine mission over Helmand Province in Afghanistan. The crew had had no chance of controlling the fire. It broke out in a part of the lower fuselage of the aircraft which was unreachable and not covered by an automatic fire suppression system. It was the biggest single loss of life of British service personnel in once incident in theatre since the Falklands War in 1982. The cause was not Taliban fire, or friendly fire, but a pure tech failure - fuel leaking onto hot cross-feed pipes. .
7. My inquiry team had valuable assistance from the MOD, US military, NASA, the HSE, the CAA, Lord Cullen and others.

[1] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/229037/1025.pdf
[2] First published in 1974.
[3] From Montana to Northern California.
[4] *Gestalts*
[5] *The Nimrod Review*, Chapter 28, Recommendation 28.2.
[6] *Nimrod MR2* aircraft were specialized RAF reconnaissance aircraft which were manufactured in 1960s and in active service until recently.

Seven steps to loss of XV230

8. We investigated 30 years of history of the aircraft, its design, maintenance and operation. This was accident waiting to happen. We discovered the following concatenation of seven factors which fatally combined over three decades to cause this catastrophic loss:

   (1) **Poor design** and modifications from 1960s onwards gave risk to the risk of fuel coming into contact with 400 degree hot pipes in the bottom of the fuselage at any time.

   (2) There was **history of fuel leaks** in 1970s and 1980s which did not ring alarm bells (and had become 'the normalization of deviance').

   (3) There was an **increase in operational tempo** in late 1990s and early 2000s with the heavy use of Nimrod aircraft particularly in theatres such as Kosovo, Afghanistan and Iraq.

   (4) There were increasing **problems of maintenance** of an increasingly aging aircraft, with its out-of-service date being regularly extended.

   (5) There were meanwhile **distractions of major organizational change and cuts** in funding in the MOD in 2000-2005 following the Strategic Defence Review of 1998.

   (6) There was the **outsourcing of the Nimrod Safety Case** in 2004-5 which produced a large amount of paper which said that the aircraft was safe – but it manifestly was not. The Safety Case missed obvious risks.

   (7) And then on 2nd September 2006, following **air-to-air refueling**, the inevitable happened.

Safety Case regime had lost its way

9. I felt strongly that the Safety Case regime had lost its way. It had led to a culture of 'paper safety' at the expense of *real* safety and did not represent value for money. Indeed, Safety Cases had had become positively dangerous and lulled people into a sense of false security. They were generally big fat, glossy, consultant-produced documents which said the kit was "safe" when manifestly it was not.

Nimrod Safety Case

10. There were four particularly troubling features of the Nimrod Safety Case:

    (1) The Nimrod Safety Case was entirely outsourced to the original aircraft manufacturers, who took 4 years to complete it and charged several hundred thousand pounds.

    (2) None of the operators, *i.e.* personnel or engineers at RAF Kinloss (the home of the Nimrod MR2 fleet) had had any involvement *at all* in drawing up the safety case; indeed, very few even knew of its existence.

    (3) The so-called 'completed' safety case was handed over and signed off during a PowerPoint session on a warm afternoon.

    (4) 40% of the risks were not closed off or mitigated properly, including the fatal one. Crucially, the Nimrod Safety case did not address the absence of a fire suppressant system in the bay in question, notwithstanding the obvious risks

presented by the juxtaposition of fuel and high temperatures in close proximity. The best opportunity to identify the fatal risk was lost.

Shortcomings

11. In *The Nimrod Review*, I outlined a dozen shortcomings in military Safety Cases generally[7]:

(1) **Bureaucratic length**: Safety Cases and Reports are too long, bureaucratic, and repetitive and comprise impenetrable detail and documentation. This is often for 'invoice justification' and to give Safety Case Reports a 'thud factor'.

(2) **Obscure language**: Safety Case language is obscure, inaccessible and difficult to understand.

(3) **Wood-for-the-trees**: Safety Cases do not see the wood for the trees, giving equal attention and treatment to minor irrelevant hazards as to major catastrophic hazards, and failing to highlight, and concentrate on the principal hazards.

(4) **Archaeology:** Safety Cases for 'legacy' platform often comprise no more than elaborate archaeological exercises of design and compliance documentation from decades past.

(5) **Routine outsourcing**: Safety Cases are routinely outsourced by Integrated Project Teams (IPTs) to outside consultants who have little practical knowledge of operating or maintaining the platform, who may never even have visited or examined the platform type in question, and who churn out voluminous quantities of Safety Case paperwork (referred to by the consultants in question as 'bumpf' and outsized Goal Structured Notation charts) in back offices for which IPTs are charged large sums of money.

(6) **Lack of vital operator input**: Safety Cases lack any, or any sufficient, input from operators and maintainers who have the most knowledge and experience about the platform. In his comments on the Nimrod XV230 BOI Report the Commander-in-Chief Air Command, Sir Clive Loader, said, correctly in my view, that any review of the Nimrod Safety Case "*...must involve appropriate air and ground crews in order to ensure that current practices are fully understood; those personnel, after all, both know most about how our aircraft are operated and flown, and also have the greatest personal interest in having levels of safety with which all involved are comfortable.*" Operators at RAF Kinloss were not even aware of the existence of the original Nimrod Safety Case.

(7) **Disproportionate:** Safety Cases are drawn up at a cost which is simply out of proportion to the issues, risks or modifications with which they are dealing.

(8) **Ignoring age issues**: Safety Cases for 'legacy' aircraft are drawn up on an 'as designed' basis, ignoring the real safety, deterioration, maintenance and other issues inherent in their age.

(9) **Compliance only:** Safety Cases are drawn up for compliance reasons only, and tend to follow the same, repetitive, mechanical format which amounts to

[7] *The Nimrod Review*, Chapter 22 (para. 22.7 *ff.*)

no more than a secretarial exercise (and, in some cases, have actually been prepared by secretaries in outside consultant firms). Such Safety Cases tend also to give the answer which the customer or designer wants, i.e. that the platform is safe.

(10) **Audits:** Safety Case audits tend to look at the process rather than the substance of Safety Cases.

(11) **Self-fulfilling prophesies**: Safety Cases argue that a platform is 'safe' rather than examining why hazards might render a platform unsafe, and tend to be no more than self-fulfilling prophesies.

(12) **Not living documents**: Safety Cases languish on shelves once drawn up and are in no real sense 'living' documents or a tool for keeping abreast of hazards. This is particularly true of Safety Cases that are stored in places or databases which are not readily accessible to those on Front Line who might usefully benefit from access to them.

Criticisms not new

12. Many of these criticisms were not new, nor confined to Safety Cases for military platforms.

13. A number of similar criticisms of Safety Cases were highlighted in the evidence before Lord Cullen in the *Ladbroke Grove Inquiry*[8]. Lord Cullen's report highlighted that operators were not thinking constructively about safety.

(1) **First, Safety Cases had a tendency to become bureaucratic with unnecessary detail**. Lord Cullen said: "*... I do not consider that it is necessary for the detail of the examination, assessment and control of individual risk to be set out in the safety case. There is an existing tendency for safety cases to become bureaucratic and I have no wish to encourage that tendency. It should be sufficient if the safety case points to the methods which have been used and to where the details can be found.*"

(2) **Second, operators too often relied on outside experts for the writing of their Safety Cases**. Lord Cullen quoted the words of one expert witness, Mr. Brown, Assistant Chief Inspector of Railways, who told the Inquiry that the use of outside consultants to produce safety cases was "*...completely ineffective. I think if people do not actually do this process in-house and do not involve all parties in it, it will not work. And I have got personal experience of that*". Lord Cullen also referred to a report which he had commissioned from Entec, which stated: "*If employees are involved in producing the safety case (rather than just being told about it) they would have 'ownership'. This can bring stronger commitment to the arguments*". Lord Cullen quoted Mr Brown, who remarked that failure on the part of management to ensure that "*the message gets through*" to all levels was" *...very much related to the failure to involve everybody in the process and very much the failure of constructing documents that people could find accessible and understandable and, crucially, helpful*". Lord Cullen referred to the evidence of other senior executives who remarked they had been surprised at just how valuable the input of employees had been.

[8] *The Ladbroke Grove Rail Inquiry, Part 1 and Part 2* (2001 *ff.*), Lord Cullen

(3) **Third, Safety Cases tended to be compliance-driven, *i.e.* written in a manner driven primarily by the need to comply with the requirements of the regulations, rather than being working documents to improve safety controls.**

(4) **Fourth, audits of Safety Cases were inadequate and confined to process rather than product**. Lord Cullen said: *"Auditing is a vital component in both the management and the regulation of safety."* He explained that audit was, on the one hand, a quality assurance exercise and, on the other, a compliance process. Lord Cullen quoted the evidence of a number of witnesses, including Major Holden, Transport Safety Consultant, formerly Inspector of Railways, who drew attention to weakness in auditing: *"My concern has been that there has been a lack of penetration in the audits, which have tended to chase paper trails rather than check that what should be going on the ground is, in fact, going on. This lack of penetration may, in part, be due to the lack of skill of the auditors but it may also lie in the belief that all that is required is a pure compliance audit of the accepted safety case. The vital question as to whether or not the safety case itself is adequate and appropriate to the circumstances is seldom asked".*

Goal-structured notation

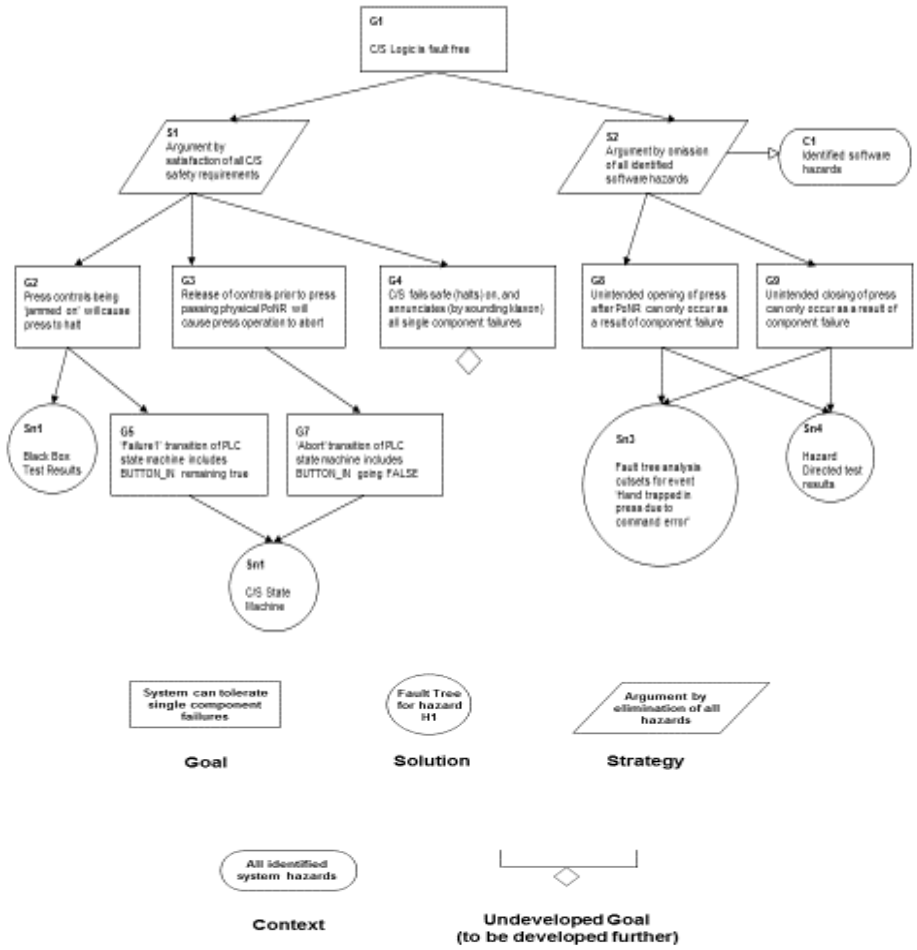
14. I want add a couple of words of caution about Goal-Structured Notation ("GSN") [9]:

(1) First, **GSN can become a self-fulfilling prophesy**. The ultimate goal (G1) of the fault-tree analysis is to prove the subject is 'fault free', *i.e.* the kit, system or activity is safe. But one must always be careful to ensure that *logic* drives the *answer*, not vice-versa.

(2) Second, **GSN can become too complex**. I have seen GSN drawings that are yards long (and are barely held up by Blue-Tack). It is easy to become seduced and mesmorized by complexity. But remember, there is a false comfort in complexity. Simplicity is your friend, particularly in a complex environment.[10]

[9] https://www-users.cs.york.ac.uk/tpk/dsn2004.pdf

[10] *"Any intelligent fool can make things bigger, more complex, and more violent. It takes a touch of genius – and a lot of courage – to move in the opposite direction."* (E.F. Schumacher).



The University of York

15. I shared the concerns of Professor John McDermid and Dr Tim Kelly at York University[11]:

    (1) **First, 'legacy' Safety Cases should focus on identifying hazards**, their potential causes, controls and mitigation, and assessing the priority areas where remedial action is needed to reduce risk to an acceptable level, *i.e.* where controls or mitigations are deemed inadequate.

    (2) **Second, it is counter-productive to try to 'reverse engineer' the Safety Case** which should have been produced at the time the system was developed.

    (3) **Third, it is important to look at the problem from the operational end** (this is, after all, where the risks actually manifest themselves) and to ask what information is needed to support risk management, *e.g.* equipment safety cases, evidence of training, *etc.*

    (4) **Fourth, no system is absolutely safe**. Indeed, systems are normally released with limitations. Accordingly, the Safety Case should argue that *"the risks are controlled"*, not *"the system is safe"*, and should indicate those areas where remedial action is needed to achieve an acceptable level of safety.

[11] *The Nimrod Review*, Chapter 22 (para. 22.16 *ff.*)

(5) **Fifth, the focus needs to be on decision-making**, both decisions as to the acceptance of risk and decisions as to the deployment of resources to reduce risk. Priority attention must be given to the most significant risks. This is the real point underlying ALARP.16 Better methods and procedures for communicating risk information to senior management must be employed.

Are Safety Cases Working?

16. I commend to you Dr Tim Kelly's article "*Are Safety Cases Working?*"[12] in which he sets out seven classic 'traps' to avoid:

(1) ***The "Apologetic Safety Case":*** Safety Cases which avoid uncomfortable truths about the safety and certifiability of systems in production so that developers do not have to face the (often economically and politically unacceptable) option of re-design (*"X doesn't quite work as intended, but it's OK because..."*).

(2) ***The Document-Centric View:*** Safety Cases which have as their aim to produce a document. Dr Kelly describes this as 'the biggest bear-trap'. The goal of Safety Cases should not simply be the production of a document; it should be to produce a compelling safety argument. We should not be reassured by "*paper, word-processor files, or HTML documents*". There was a danger of "*spending a lot of money to produce a document*" of no safety benefit.

(3) ***The Approximation to the Truth:*** Safety Cases which ignore some of the rough edges that exist. For example, Safety Cases which claim in a Goal Structured Notation diagram that 'All identified hazards have been acceptably mitigated'19 and direct the reader to the Hazard Log when, *in reality*, the mitigation argument is not so straightforward.

(4) ***Prescriptive Safety Cases****:* Safety Cases which have become run-of-the-mill or routine or simply comprise a parade of detail that may seem superficially compelling but fails to amount to a compelling safety argument.

(5) ***Safety Case Shelf-Ware:*** Safety Cases which are consigned to a shelf, never again to be touched. The Safety Case has failed in its purpose if it is "*so inaccessible or unapproachable that we are happy never to refer to it again.*"

(6) ***Imbalance of skills:*** The skills are required of both someone to develop the Safety Case and someone to challenge and critique the assumptions made. Too often, the latter skills are missing.

(7) ***The illusion of pictures:*** People are 'dazzled' by complex, coloured, hyper-linked graphic illustrations such as Goal Structured Notation or 'Claims-Arguments-Evidence' which gives both the makers and viewers a warm sense of over-confidence. The quality of the argument cannot be judged by the node-count on such documents or number of colours used.

17. In a recent monograph on Safety Case depictions, Ibrahim Habli and Dr. Tim Kelly emphasised: "*There can sometimes be an illusion of truth with GSN (and other graphical) depictions of an argument*".[13]

[12] https://www-users.cs.york.ac.uk/~tpk/2008scscarticlekelly.pdf

Safety Cases are invaluable

18. Let me be clear: Safety Cases and the Safety Case regime and methodology are invaluable tools in modern risk management. Safety Cases are here to stay. Properly used, they provide an invaluable intellectual and practical structure for analysing, anticipating and ameliorating risks. However, like so many 'paper-based' solutions, they are open to abuse and lassitude and can become a 'comfort blanket' to keep one warm from the chill of having to face the realities of multifarious risk. In some domains, Safety Cases had become part of the problem, not the solution. So it was that I came to make some far-reaching recommendations in *The Nimrod Review*.

Recommendations

19. I recommended that Safety Cases in the future should be brought in-house, re-named "*Risk Cases*" and accord with the following six principles (with the acronym "SHAPED")[14]:

> **S**UCCINCT
> **H**OME-GROWN
> **A**CCESSIBLE
> **P**ROPORTIONATE
> **E**ASY TO UNDERSTAND
> **D**OCUMENT-LITE

20. I set out below my full list of Recommendations regarding best practice for Risk Cases[15]:

> **Recommendation 22.1:** The Safety Case concept should be retained by the MOD, provided it is brought in-house, slimmed down, and made consistent both with the Recommendations below and the Recommendations in **CHAPTER 21** that there should be a single, concise, through-life "*Risk Case*" for each platform owned by the Regulator, and backed up by a single Risk Register.
>
> **Recommendation 22.2:** Safety Cases should be re-named "*Risk Cases*" in order to focus attention on the fact that they are about managing risk, not assuming safety.
>
> **Recommendation 22.3:** "*Risk Cases*" should henceforth be drawn up and maintained in-house by the Regulator/Services and not outsourced to Industry. All Safety Cases which are currently being managed or drawn up by Industry should be re-named and brought in-house.
>
> **Recommendation 22.4:** Front Line maintainers and operators should have a major role in drawing up and maintaining "*Risk Cases*".
>
> **Recommendation 22.5:** Business Procedure (BP) 1201 and other relevant regulations should be redrafted to reflect the principles relevant to "*Risk Cases*" outlined above, namely that "Risk Cases" should be Succinct, Home-grown, Accessible, Proportionate, Easy to understand and Document-lite (SHAPED).

---

[13] https://www.researchgate.net/publication/4292988_Safety_Case_Depictions_vs_Safety_Cases_-_Would_the_Real_Safety_Case_Please_Stand_Up
[14] *The Nimrod Review*, Chapter 22 (para. 22.37)
[15] *The Nimrod Review*, Chapter 22 (para. 22.38)

Recommendation 22.6: The definition of a Safety Case in Defence Standard 00-5646[16] should be replaced with the following simple definition of Risk Case**:** *"A Risk Case is reasonable confirmation that risks are managed to ALARP."*

Conclusion

21. Remember you have as many, lengthy Safety Cases and Fault-Tree analysis as you want. But, as the Defence Nuclear Safety Regulator, Commodore Andrew McFarlane, said to during *The Nimrod Review* and I quote in my Report: *"Safety is delivered by people, not paper"*.

22. Finally, let me leave you with you three pertinent quotes from Robert Pirsig:

"The more you look, the more you see."

"Familiarity can blind you."

"Some things you miss because they're so tiny you overlook them. But some things you don't see because they're so huge."

CH-C
London
June 2017

[16] Defence Standard 00-56, paragraph 9.1: A Safety Case itself is defined in the military context as *"a structured argument, supported by a body of evidence, that provides a compelling, comprehensive and valid case that a system is safe for a given application in a given environment"*