

The Management of Ageing Combat Aircraft – the RAF Nimrod Story

“Have the courage to say no. Have the courage to face the truth. Do the right thing because it is right. These are the magic keys to living your life with integrity.” W. Clement Stone.

On 2nd September 2006, RAF Nimrod MR2 XV230 caught fire in mid-air over Afghanistan shortly after completing an air-to-air refuelling operation. The crew had time to declare Mayday and begin an emergency descent, but the aircraft exploded at 3000 feet altitude and all fourteen crew died.

This accident led to a detailed review by Charles Haddon-Cave into “the broader issues surrounding the loss of RAF Nimrod MR2 aircraft XV230 in Afghanistan in 2006”. His report¹, published in 2009 is one of the most outspoken and savagely critical of its kind. He described a long saga of bad original design, poorly conceived and implemented design changes, and manufacturing defects. This was combined with a series of incidents which should have generated strong warning messages. Lastly, when the Ministry of Defence (MOD) decided belatedly to produce a safety case for the Nimrod between 2001 and 2005, the result was described by Haddon-Cave as a “lamentable job” which missed the key dangers. The production of the safety case was described as a story of “incompetence, complacency, and cynicism”.

Haddon-Cave did not hold back from naming individuals and organisations that were culpable. “In this Report, I specifically name, and criticise, key organisations and individuals who bear a share of responsibility for the loss of XV230. I name individuals whose conduct, in my view, fell well below the standards which might reasonably have been expected of them at the time, given their rank, roles and responsibilities, such that, in my view, they should be held personally to account.”



Fig 1: RAF Nimrod MR2 XV230 (HMSO)

¹ The Nimrod Review, Charles Haddon-Cave QC, HMSO, London, 2009

The RAF's Nimrod MR2's role was anti-submarine warfare and anti-surface unit warfare. Its airframe was derived from the De Havilland Comet, so the Nimrod's lineage dated back to the 1950's. The Hawker Siddeley Nimrod MR1 entered service in 1969, and the upgraded MR2 variant entered service in 1979. Hawker Siddeley Aviation became part of BAE Systems in 1977.

By 2006, the Nimrod was nearing the end of its operational life.

Weaknesses in the original MR1 design dated back to 1969. A fundamental problem with the Nimrod's layout was that the fuselage space ('No 7 Tank Dry Bays') between the two pairs of Rolls-Royce Spey engines was extremely congested, and that the congestion included both hot gas ducts and fuel pipes.

Because the Nimrod was required to cruise around at low speed for many hours while airborne, it was designed so that two of its four engines could be shutdown, and then re-started quickly when needed. The Nimrod also had to cope with loss of a single engine when operating on only two engines. Hence, to enable mid-air engine re-start, very hot air could be bled from any one engine to start any of the other engines. This was achieved by means of a three-inch diameter steel duct known as the 'Cross-Feed Duct'. This was insulated with a glass fibre blanket and covered with a stainless steel sheath, where possible; elsewhere it was covered by metallic shrouds. The Cross-Feed Duct was fitted into the space between the engines. In the same space were fuel pipes supplying fuel for the engines. Despite this proximity of hot air ducts and fuel pipes, the No 7 Tank Dry Bays were not fitted with fire detection or fire suppression equipment.

Design changes were implemented over the decades which made the congestion and the fire hazard worse in this space between the engines. (See Figure 2.)

The first notable design change was in 1979, when the MR2 variant entered service, it was fitted with a 'Supplementary Conditioning Pack' (SCP) to provide cooling air to the Nimrod MR2's improved electronic systems. This Supplementary Conditioning Pack was powered by hot air bled off the Cross-Feed Duct – now called the 'Cross-Feed/SCP Duct'. The normal condition of this Cross-Feed/SCP duct when in flight was therefore that it would be hot and pressurised.

In practice, the insulation of the hot Cross-Feed/SCP Duct was imperfect; in service the glass fibre insulation got squashed causing the stainless steel sheath to get hot. Bellows units at bends in the duct were, in any case, less well insulated, or even completely un-insulated. Nevertheless, the existence of regions of insulation gave a 'false sense of security' – it was perceived that fire risk was minimised. Thus there were now normally-hot surfaces adjacent to fuel pipes, in a region without fire detection or fire suppression systems. Haddon-Cave was critical of BAE Systems for not identifying the fire risk and not installing fire detection and fire suppression equipment. Even worse, fuel leaks within the No 7 Tank Dry Bays could accumulate in-flight without any facility for drainage.

BAE Systems sought to share blame for these design mistakes by stating that the design modifications had been 'accepted' by the Ministry of Defence in 1977-1978. Haddon-Cave did not consider that this absolved BAE Systems of its responsibility in respect of the poor design of the aircraft. The Cross-Feed/SCP duct represented a fundamental flaw in the design of the Nimrod aircraft and was the primary physical cause of the accident.

The next relevant design change was the installation of Air-to-Air Refuelling (AAR) capability. This was implemented as an urgent design change at the time of the Falklands War in 1982; it was conceived, designed and installed in 18 days. The temporary (1982) modification involved a refuelling hose passing through the aircraft cabin, which the crew had to step over. A permanent modification was implemented in 1989; both the temporary and permanent modifications were carried out by BAE Systems.

The fuel tanks were fitted with pressure relief valves ('blow-off valves') to prevent the tanks over-pressurising during AAR. Blow-off during AAR refuelling was seen as a potential hazard, because of the risk of fuel spillage. Also, there was significant concern about the design of the fuel pipe seals, which might cause leakage especially within the No 7 Tank Dry Bays. Either of these sources of fuel - blow-off during AAR or leaking seals - could have led to the fatal fire, although Haddon-Cave favoured blow-off during AAR as the cause.

So, in short, Haddon-Cave concluded that either AAR blow-off or fuel pipe seal failure led to fuel leakage, and the hot Cross-Feed/SCP ductwork provided a source of ignition that led to the fire and subsequent explosion.

There had been several other incidents of fuel leaks, damaged fuel pipe seals, and failure of the SCP ductwork, from which clear lessons should have been learned. However, it appeared no-one was taking a wide view of these incidents which were each treated as 'one-off' events.

So far, so bad: a less-than-perfect design with some less-than-perfect design changes over a 37 year operating history.

Haddon-Cave then turned his attention to the Safety Case for the Nimrod MR2, which was intended to identify, assess and mitigate catastrophic hazards which might occur to the aircraft. In plain language:

- What could go wrong?
- How bad could it be?
- What controls are in place to stop it happening?
- What if it happens? (i.e. contingency planning)
- Is the level of risk acceptable?

The definition of 'Safety Case' given by Haddon-Cave is more legalistic: ".....a structured argument, supported by a body of evidence, that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given environment" The Nimrod Safety Case was produced by a team consisting of people from BAE Systems and the Ministry of Defence's Nimrod Integrated Project Team (IPT), with QinetiQ Ltd as an independent advisor. He concluded that the Nimrod Safety Case was "a lamentable job from start to finish. It was riddled with errors. It missed the key dangers. Its production is a story of incompetence, complacency and cynicism." I have never seen, in any other inquiry report, such excoriating words as these.

It should be noted that the drive to produce Safety Cases within MOD projects came as a result of a political directive that military projects should be designed with civil safety standards in mind. Military projects should be "as civil as possible, as military as necessary". However, much of this

change of approach was aimed at new projects; in the case of Nimrod, however, it was necessary to produce a Safety Case for an aircraft that had been operating for over 30 years with a generally good safety record.

A key part of the Safety Case for Nimrod was its Safety Management System, the objectives of which were described as being:

- (1) To establish and maintain an effective management structure and organisation for implementing and promulgating airworthiness policy;
- (2) To assess the safety performance of the equipment and the safety management system itself by measurement and audit;
- (3) To provide for the documentation of the evidence for airworthiness in a Safety Case; and
- (4) To establish mechanisms for learning from the MOD's and others' experience in safety and airworthiness. The Safety Case itself was to be written in accordance with an MOD Standard, Def-Stan 00-56, which included a requirement for system hazard analysis and risk assessment.

The Safety Case was to have a pyramid structure to be “credible, complete, consistent, and comprehensible”, comprising four levels:

- Safety Evidence – the foundation of the Safety Case, including all analysis, records and data.
- Safety Argument – Justification that the Safety Evidence is sufficient to demonstrate that the equipment is tolerably safe.
- Safety Case Report – A summary of the Safety Argument, including all salient issues and any recommendations for future work.
- Safety Statement – A certificate of acceptance from the Integrated Project Team Leader, stating that the equipment is tolerably safe.

For old aircraft such as Nimrod, there was an ‘implicit safety case’ by virtue of its previous operation, which Haddon-Cave describes as ‘something of an oxymoron’, that is, a Safety Case implied detailed analysis, and an ‘implicit safety case’ did not. A review of the ‘implicit safety case’ was to be completed by April 2004, and a Safety Report was to be issued.

A problem here is that the MOD was both the ‘operator’ and the ‘safety regulator’, so the MOD could re-interpret these requirements as it saw fit.

A Nimrod Project Safety Working Group (PSWG) was established, reporting to the Integrated Project Team Leader, to produce the Nimrod Safety Case in the period 2001 to 2005 (that is, before the accident). The Nimrod Project Safety Working Group therefore had a marvellous opportunity to identify and perhaps rectify the fire hazards in the No 7 Tank Dry Bays, but it failed to do so.

The main steps in production of the Nimrod Safety Case were as follows:

1. First, the Nimrod PSWG issued, in February 2002, a Safety Management Plan in which the conclusion of the Nimrod safety case was given – before the work had been done! – as follows: “By virtue of a range of traditional methods, there is a high level of confidence in

the safety of the Nimrod aircraft.” This made it clear that those involved in producing the Nimrod Safety Case thought they knew the answer at the outset; that is, the Nimrod had been in service since 1969, so it had to be safe.

2. Next, The Nimrod PSWG issued a ‘Hazard Identification report’ in April 2003. Six further reports on hazard analysis and hazard mitigation were issued in September 2004, completing BAE Systems’ input to the exercise. Regarding the fire risk in No 7 Tank Dry Bays, where the fatal fire arose, BAE Systems provisionally assessed the risk of fire as ‘improbable’, although this was one of the ‘open’ items. At no stage was the catastrophic risk of fire created by the hot Cross-Feed/SCP Duct and the Air-to-Air Refuelling modifications ever properly identified, assessed or addressed. Nevertheless, at a two-day meeting with the MOD Nimrod Integrated Project Team and QinetiQ Ltd to present the results of the Nimrod Hazard Identification Report at a ‘Customer Acceptance Conference’ on 31st August and 1st September 2004, BAE Systems said the Nimrod was ‘acceptably safe to operate’. MOD and QinetiQ Ltd simply accepted that BAE Systems had completed their task, and so the reports were signed off as complete.
3. Finally, although over 40 per cent of the hazards remained ‘open’ in the BAE Systems reports (meaning there were unresolved issues), the Nimrod Integrated Project Team sentenced these issues, and the Nimrod Safety Case was declared complete in March 2005.

So, on what basis did the Nimrod Integrated Project Team accept the level of fire risk in the No 7 Tank Dry Bays? This was the crux of the issue – how did this fire risk get missed? The answer to this is that the approach adopted was highly superficial indeed. No detailed assessment was ever carried out:

- a. During inspection visits to operational Nimrod aircraft, the BAE Systems team had indeed noted that in the No 7 Tank Dry Bays were congested areas with “a potential for hot air, fuel and hydraulic leaks and possible fire”. However, and without any further analysis, this risk was assigned an ‘initial probability’ of ‘improbable’. This risk category was important: an ‘improbable’ likelihood of occurrence was equated to a ‘tolerable’ risk, so no further action was required.
- b. This initial review was later used by BAE Systems’ Nimrod Safety Manager, Frank Walsh, as the basis for sentencing the ‘open’ hazards on behalf of the Nimrod Integrated Project Team (step 3 above of the production of the Nimrod Safety Case). Hence, on the basis of an initial assessment during an inspection visit, and without any further analysis, the risk of fire in No 7 Tank Dry Bays was deemed to be ‘tolerable’.

As Haddon-Cave noted, “All three phases of the Nimrod Safety Case were fatally undermined by an assumption by all the organisations and individuals involved that the Nimrod was ‘safe anyway’.” In particular, the BAE Systems work was incomplete and contained “numerous systemic errors”.

He also noted the budget constraints that the Nimrod Safety Case project was working within. In October 2001, at the outset of the project, MOD only wanted to spend £100000 to £200000 over six months, whereas the Harrier safety case cost £3 million and took three years. Although the final costs and timescales for the Nimrod Safety Case did exceed these initial MOD aspirations, it is nevertheless an indication that MOD considered that the Nimrod Safety Case was a ‘rubber-

stamping' exercise; the Nimrod had been operational since 1969 – so it must be safe. And, in any case, Nimrod MR2 was near the end of its operational life.

Haddon-Cave named three individuals in BAE Systems, three individuals in the MOD Nimrod Integrated Project Team, and two individuals in QinetiQ Ltd as the key people in the debacle of the Nimrod Safety Case. “The best opportunity to capture these serious design flaws in the Nimrod fleet, that had lain dormant for the decades before the accident to the XV230, was squandered.”

The role of QinetiQ Ltd as Independent Safety Auditor throughout this exercise is of interest. When QinetiQ's representative Martin Mahy raised concerns about the Nimrod risk assessment methodology in November 2003, the Nimrod Integrated Project Team Leader, Group Captain (later Air Commodore) George Baber, said, “I don't need to get independent advice from QinetiQ, I can go elsewhere”, and referred to “bloody QinetiQ” and said “QinetiQ is just touting for business”.

QinetiQ's response to this warning from Group Captain George Baber seems to have been conciliatory. Subsequently, QinetiQ went to “extraordinary lengths” to keep the Nimrod Integrated Project Team Leader happy and were “eager to please”.

Nevertheless, in 2004, QinetiQ's Martin Mahy again challenged aspects of the Nimrod Safety Case, including the need to provide sufficient identification and risk mitigation of hazards. BAE Systems' Nimrod Safety Manager, Frank Walsh, replied in an email, “Your full guidance would produce a ‘gold-plated’ solution that.....would not represent value for money”.

Later, however, QinetiQ clearly softened their tone, and in June 2004 Martin Mahy wrote to Frank Walsh to say that, “Provided all the risk mitigation evidence is included in the final safety case report, I don't foresee any difficulties.....in the sign-off of the baseline safety case.”

QinetiQ's Martin Mahy could not be present at the Customer Acceptance Conference on 31st August and 1st September 2004. Another QinetiQ person stepped in at the last moment, and the only briefing he received was that Mahy told him, “66 per cent of the Nimrod risk mitigation work is outstanding”. In this conference, BAE Systems gave very optimistic presentations about the work done, while remaining light on details. Haddon-Cave notes that at no stage in the Customer Acceptance Conference did BAE Systems give information about how many hazards had been ‘closed’, how many were still ‘open’ or ‘unclassified’, and how much work remained to be done even in broad percentage terms. In particular,

“I have been driven to the regrettable conclusion that it was, in fact, a deliberate and conscious decision by the senior BAE Systems representatives present (namely Chris Lowe, Richard Oldfield and Eric Prince) not to mention or otherwise draw the Customer's attention to the large percentage of hazards which it had left “Open” and “Unclassified”. The motive was simple: it was embarrassing to reveal the actual figures and it might lead to an unseemly argument with the Nimrod IPT representatives as to whether the task had been properly completed by BAE Systems and whether final payment could be made.”

This is a most damning conclusion. Basically, BAE Systems connived to present as positive a picture as possible so that a payment milestone could be deemed to have been passed. In the meeting, both the Nimrod Integrated Project Team and QinetiQ agreed that “the aims and objectives of the project

had successfully been achieved". So why did neither QinetiQ nor members of the Nimrod Integrated Project Team challenge the BAE Systems' presentation?

The answer seems, amazingly, to be that, at the time of the presentation, the final BAE Systems Nimrod safety analysis reports had not yet been issued, and they were not actually issued until three weeks later. So, the minutes of the Customer Acceptance Conference recorded the agreements of both the Nimrod Integrated Project team and QinetiQ to a set of safety analysis reports, although neither party had yet seen the final version of those reports, and those final reports still left a number of hazards as 'open' or 'unclassified'.

There were some more steps in the completion of the Nimrod Safety Case (and yet more opportunities missed) but basically the deal was done, and in March 2005 the Nimrod Integrated Project Team declared that the Nimrod Safety Case was complete. A strong impression of completeness was given: "...all potential safety hazards have been identified, assessed and addressed.....the aircraft type is deemed acceptably safe to operate....."

Eighteen months later, Nimrod XV230 caught fire and exploded over Afghanistan.

None of the individuals and organisations (MOD, BAE Systems and QinetiQ) involved in this sorry saga deserves any credit. All were, to varying degrees, complicit in a story of "incompetence, complacency, and cynicism". And, of course, everyone had felt the Nimrod was 'safe anyway' because it had been operating since 1969.....

Final sign-off, and therefore responsibility, had been carried out by Group Captain (later Air Commodore) George Baber, who later claimed he had been "hoodwinked" by BAE Systems' Frank Walsh. Haddon-Cave said that Baber "bears the lion's share of the blame", but that this must be put into context. The project was complex and over-stretching, and he also had to deal with increasing and extremely challenging operational demands supporting aircraft in conflicts in both Afghanistan and Iraq, including unscheduled modifications and other operational requirements. He was responsible for an annual budget of £200 million and an acquisition programme of £500 million. He was travelling a great deal. There is, therefore, probably some implied failure of delegation.

Haddon-Cave also pointed his finger at organisational causes of the accident. There had been some significant organisational changes in the RAF – a move from a function-based organisation to a multi-discipline project-based organisation, and larger structures created by Joint Service (that is, navy/army/air force) organisations, and 'whole-life' equipment management, and finally a lot of outsourcing of work to industry. Thus there had been a period of intense, major organisational changes which left many people unclear about where responsibilities really lay. On top of this there had been significant budget cuts following the 1998 Strategic Defence Review.

As a result of these changes, 'airworthiness' of aircraft within the RAF fleet became a casualty, and it was no longer always uppermost in the minds of personnel in the MOD and RAF. In particular, the changes led to expectations that the Nimrod Integrated Project Team would deliver the Nimrod Safety Case at minimum cost and with minimum necessary upgrades to the aircraft. George Baber told Haddon-Cave that, following the re-organisations, there was a "lack of supervision" from his superiors and he felt "abandoned". 'Airworthiness' just became another part of the tri-Service SHEF

function². Haddon-Cave blamed the Chief of Defence Logistics for this loss of focus. The post of Chief of Defence Logistics was held by two people during the relevant period: General Sir Sam Cowan, and Air Chief Marshal Sir Malcolm Pledger.

The RAF's initial Board of Inquiry (which preceded Haddon-Cave's report) made recommendations, amongst which were:

- Nimrod Air-to-Air refuelling was stopped.
- In-flight use of the Cross Feed/SCP Duct was also stopped.
- A complete review of the Nimrod Safety Case was begun.

Haddon-Cave made further, very wide-ranging recommendations to improve safety and airworthiness. These recommendations included aspects of safety principles, military airworthiness, safety cases, ageing aircraft, personnel, engagement with industry, procurement, and safety culture.

Haddon-Cave noted parallels between Nimrod and other major accidents such as the Herald of Free Enterprise, the King's Cross fire, BP Texas City and, in particular, the Columbia Shuttle accident in 2003. He espoused the adoption of 'Four Key Principles':

1. Leadership – strong clear leadership from the very top.
2. Independence throughout the regulatory regime
3. People (not just Process and Paper)
4. Simplicity – regulation, processes and rules must as simple and straightforward as possible.

He recommended a new Military Airworthiness Authority, with clearly identified Airworthiness 'Duty Holders', to bring coherence, governance, and responsibility.

² SHEF is Safety, Health, Environment and Fire.

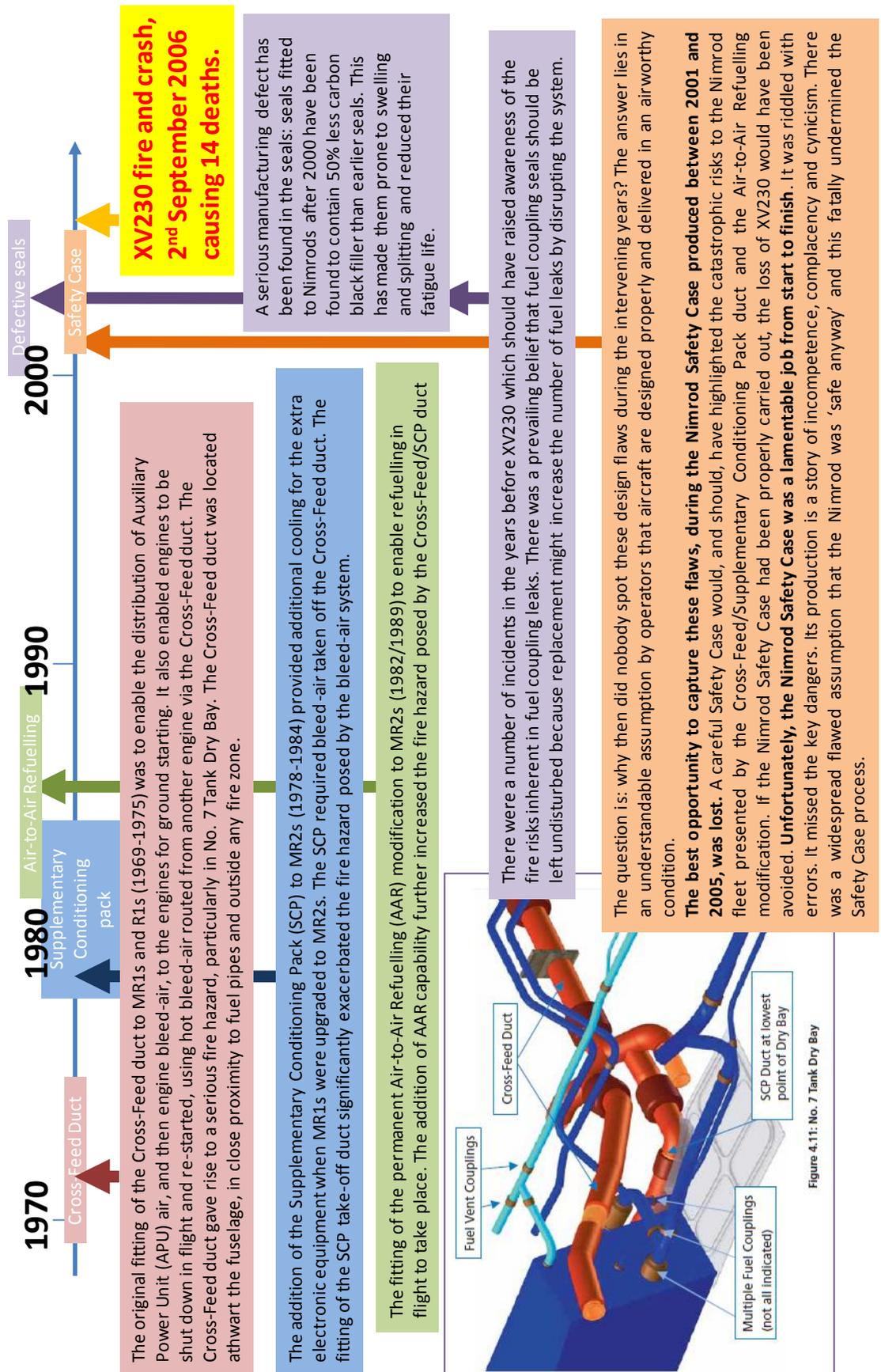


Fig 2: Timeline of key events leading to the Nimrod XV230 accident, with extracts from the Hadden-Cave report

THE MEANING OF SAFETY IN A MILITARY ENVIRONMENT

The Nimrod accident led to very thorough investigations and great soul-searching amongst all the people involved, directly and indirectly.

Prior to the accident, concerns were raised by people who knew what they were talking about (QinetiQ) to those in positions of authority – and the concerns were rebuffed. The apparent confidence in the safety of the systems was based on prior successful operation, but the apparent confidence was at least partially a bluff; project pressures about costs and programmes were almost certainly the real drivers.

‘Normal’ civilian safety certification (or licensing) practices did not apply. Nobody had ever suggested that military aircraft should be licensed by the UK Civil Aviation Authority. Combat aircraft had their own safety licensing regimes. And yet there was also, somehow, a political and public expectation that the standards of safety should in some way be comparable to civil standards. In the United Kingdom, the Ministry of Defence had gone so far as to say that safety standards should be ‘as military as necessary, as civil as possible’.

How realistic is this? Everyone knows that combat aircraft have to face (potentially) much greater risks than commercial airliners. Is it realistic to think about applying a similar approach to their licensing and operation?

In a military environment there is an expectation of risk because, inescapably, that is what combat involves. Does this make those engineers who are involved in military safety assessment and analysis less thorough in their approach? I am suggesting here that BAE Systems engineers working on the Nimrod Safety Case had another ‘reason’ not to regard the Nimrod Safety Case as a hugely important piece of work; namely, they may have thought that any identified risks in their safety analyses will have been much less significant than combat risks, for example the risk of a Nimrod being shot down by a ground-to-air missile. (This false ‘reason’ would be in addition to two other false ‘reasons’: First, the Nimrod was ‘safe anyway’, and second, it was near the end of its operational life. The latter implies some sort of judgment about residual ‘time at risk’.)

Also, it is implicit in safety analysis that identified weaknesses will be rectified; this will cost money, yet ultimately there are overall budget constraints. After all, Group Captain George Baber had potentially much bigger things to worry about than the Nimrod Safety Case – he had responsibilities for Nimrods flying in hostile environments over Iraq and Afghanistan. For George Baber, I wonder, could it have come down to a choice between either spending money on urgent operational (combat) requirements, or else spending money on the urgent mitigation of ‘theoretical’ risks?

The principal requirement in any safety justification is that the design is *fit-for-purpose*. The Nimrod No7 Tank Dry Bay design failed a basic ‘fitness for purpose’ test.

Haddon-Cave wrote that the Nimrod’s ‘implied safety case’ was an oxymoron. Maybe this comment can be extended more generally: What does it mean to have a safety case for combat aircraft – that is, for activities that are inherently dangerous? Is ‘combat aircraft safety case’ also an oxymoron? Do we really understand what ‘safety’ means in a combat aircraft setting?

A difficulty here can be the conflation of two issues: *fitness-for-purpose* and *risk-based safety justification*. Sometimes (though not necessarily in these examples) it can appear to senior management that a particular safety concern has been derived solely from risk-based safety analysis, and not from a review of fitness-for purpose. Senior management may think the concern is about a hypothetical fault sequence expressed in terms of probability or fault frequency, unless it is made very clear where the engineering issues lie.

A further difficulty for senior management is that they may be asked to make decisions about expenditure on design improvements based on detailed technical analyses which they will almost certainly not have sufficient time to read and fully understand.

Safety analysts need to be very clear and concise about their safety concerns; they need to be able to express them in basic engineering terms such as ‘Nimrod No 7 Dry Tank Bay is a major fire risk yet there is no fire detection or fire suppression’. The real problem for Nimrod was that the designs were not fit-for-purpose³.

Regarding risk-based safety criteria, the philosophical basis of safety and risk in hazardous civilian industries is well understood and numerically defined⁴. Perhaps, for combat aircraft, there should also be a first-principles-based set of risk criteria, particular to combat aircraft and equipment, using a cost-risk-benefit approach, which addresses both initial design and subsequent modification work in the context of combat risk. Existing defence safety standards, such as the UK’s Def Stan 00-56, rely heavily on civilian safety standards⁵. This seems to me to be unrealistic.

³ Just for clarity: I am not necessarily saying that a failure to explain the deficiencies in clear engineering terms was a problem in this example – but it can be.

⁴ See for example *The Tolerability of Risk from Nuclear Power Stations*, HMSO, 1992, and *Reducing Risks, Protecting People*, HMSO, 2001

⁵ At time of writing, Def Stan 00-56 is under review.