Product/System Safety – Legal Duties & Liability

Raytheon

Martin S. Chizek, J.D., PE, CSP, CQE

- Product Liability
- Manufacturer Liability
- Professional Liability of Engineers
- Product/System Safety Program
- The Loss of RAF Nimrod XV230

29th International System Safety Conference
8 Aug 2011, Las Vegas, NV

Manufacturer Liability

- Theories of Recovery – Products Liability
  - Negligence (Fault)
  - Strict Liability (No Fault)
  - Restatement of Torts (2nd and 3rd)
  - Misrepresentation
  - Breach of Warranty (Implied or Express)

Negligence

- Negligence focuses on *Conduct*
- Plaintiff must prove that the Defendant

  owed the Plaintiff a ***DUTY***

  which the Defendant ***BREACHED***

  and

  that the breach of duty was the ***CAUSE***

  (both “But for” and “Proximate”)

  of Plaintiff’s ***DAMAGES***

Elements of Negligence (Fault)

- Duty
  - Our duty to others (the *Standard of Care*) is to act as a reasonable person would under the same or similar circumstances [as the person charged]
  - To act as a *Reasonable Person*, one must foresee the consequences of one's actions and be guided by balancing the risk of those actions to others against the utility of those same actions.

Elements of Negligence (Fault)

- Breach
  - The duty to others is breached if the jury finds that the actions of the person charged are not what a reasonable person would have done under the same or similar circumstances.
  - Determining whether a person's behavior is reasonable is an objective inquiry; it does not depend on what the person charged believed at the time, only what a reasonable person would have would have done under the same or similar circumstances.

Elements of Negligence (Fault)

- Causation
  - "But For" Cause (cause in fact)
    - But for the Defendant's breach of duty (or defective product), the Plaintiff would not have been harmed.
  - Proximate Cause (legal cause)
    - The Defendant's breach of duty (or defective product) must also be a *substantial factor* in causing Plaintiff's harm

      or
    - The harm to the Plaintiff must also be *assignable* to the Defendant's breach of duty (or defective product).

Proximate Cause not found when[1]:

- The harm was of a different type than reasonably anticipated
- The harm was caused to an unforeseeable person
- The harm was caused by the operation of intervening forces

Palsgraf v. L.I. Railroad

Elements of Negligence (Fault)

- Damages
  - Compensatory
    - Property Damages
    - Profit/Wage Loss
    - Medical and other Expenses; past and future
    - Pain and Suffering; physical and emotional
  - Punitive
    - Acts must be willful, wanton; show a callous disregard for safety

Strict Liability (No-Fault)

- Strict Liability focuses on *the Product*
- Plaintiff must prove that the Defendant sold a product

  which contains a **DEFECT**

  and

  that the defect was the **CAUSE**

  (both “But For” and Proximate)

  of Plaintiff’s **DAMAGES**

Strict Liability - Restatement of Torts 2nd § 402A

1. One who sells any product in a defective condition unreasonably dangerous to the user or consumer or to his property is subject to liability for physical harm thereby caused to the ultimate user or consumer, or to his property, if:
   - The seller is engaged in the business of selling such a product
   - It is expected to and does reach the user or consumer without substantial change to the condition in which it is sold
2. The rule stated in subsection 1 applies, although
   - The seller has exercised all possible care in the preparation and sale of his product.
   - The user has not bought the product from or entered into any contractual relationship with the seller.

Types of Defects

- Design Defects
  - Flaw in the intentional design of a product that makes it unreasonably dangerous. Exists in a product from its inception.
- Production (Manufacturing) Defects
  - The product does not conform to the designer's or manufacturer's own specifications or standards.
  - A product "contains a manufacturing defect when the product departs from its intended design even though all possible care was exercised in the preparation and marketing of the product."[2]
- Marketing Defects
  - Flaws in the way a product is marketed, such as inadequate safety warnings, improper labeling of products, insufficient instructions, or the failure to warn consumers of a product's hidden dangers. A negligent or intentional misrepresentation regarding a product may also give rise to a product liability claim.

Traditional Test for Design Defect

Consumer Expectations Test[3]

1. At the time of the use, the product was substantially the same as when it left defendant's possession;

   or

   Any changes made to the product after it left defendant's possession were reasonably foreseeable to defendant; and
2. The product did not perform as safely as an ordinary consumer would have expected at the time of use; and
3. The product was used (or misused) in a way that was reasonably foreseeable to defendant.

- Is an objective test of ordinary consumer's expectations; not dependant upon the subjective expectation of a particular consumer or user.
- Evidence of compliance with governmental or industry standards generally allowed as objective evidence of consumer expectations.
- "A product may be found defective in design, even if it satisfies ordinary consumer expectations, if through hindsight the jury . . . finds the risk of danger inherent in the challenged design outweighs the benefit of such design."[4]

Recent Test for Design Defect

Risk/Utility Test

- A finding of design defect may result from a demonstration that the risks inherent in the product's design outweigh the benefits of that design.
  - **The factors relevant to the risk utility analysis are[5]:**
    - The usefulness and desirability of the product – its utility to the user and to the public as a whole.
    - The safety aspects of the product – the likelihood that it will cause injury, and the probable seriousness of the injury
    - The availability of a substitute product which would meet the same need and not be as unsafe.
    - The manufacturer's ability to eliminate the unsafe character of the product without impairing its usefulness or making it too expensive to maintain its utility.
    - The user's ability to avoid danger by the exercise of care in the use of the product.
    - The user's anticipated awareness of the dangers inherent in the product and their avoidability, because of general public knowledge of the obvious condition of the product, or of the existence of suitable warnings or instructions.

Mfg and Design Defects - Restatement of Torts 3rd

- Product contains manufacturing defect when it departs from its intended design even though all possible care was exercised in preparation & marketing of product.
- Product is defective in *design* when the foreseeable risks of harm posed by product could have been reduced by adoption of a reasonable alternative design . . . and omission of the alternative design renders product not reasonably safe.
- Product is defective because of inadequate instructions or warnings when the foreseeable risks of harm posed by product could have been reduced by the provision of reasonable instructions or warnings . . . and omission of instructions or warnings renders the product not reasonably safe.

  - "Strict Liability" limited to claims of manufacturing defect
  - Does not include the "unreasonably dangerous" terminology of §402A.
  - Imposes a "risk-utility" test, while incorporating negligence concepts

Affirmative Defenses

- Plaintiff's Behavior
  - Contributory/Comparative Negligence,
    - Plaintiff's negligence played a significant role in causing the injury
    - States have different formulas for calculating Plaintiff's recovery
  - Voluntary Assumption of Known Risk
    - "if the user or consumer discovers the defect and is aware of the danger, and nevertheless proceeds unreasonably to make use of the product and is injured by it, he is barred from recovery ."[6]
  - Unforeseeable Product Misuse
    - The manufacturer will not be liable if the consumer's unforeseeable misuse of the product was the sole cause of the harm.
- State of the Art
  - The manufacturer used the best technology reasonably available and feasible for use at the time of manufacture.
- Substantial Change Doctrine[7]
  - Manufacturers or sellers cannot be held strictly liable if the condition of the product substantially changes in a way that is material to the accident after the product leaves their control.

Theories of Recovery – Product Liability

- Misrepresentation
  - A person who relies on false or misleading information conveyed by the seller and who is harmed by such reliance may recover for the misrepresentation.
    - Fraudulent misrepresentation occurs when the defendant knows that a statement is false, and intentionally misleads the plaintiff.
    - Negligent misrepresentation occurs where the defendant was negligent in ascertaining whether a statement was true.

- Warranty
  - If a product's quality is less than the representations made by the seller, the seller could be liable for breach of warranty. The Uniform Commercial Code (U.C.C.), which has been adopted in part by every state, provides the basis for warranties in the United States.
    - An express warranty is when the seller makes certain representations regarding the quality of a product.
    - An implied warranty of merchantability is a promise that a product sold is in good working order and will do what it is supposed to do.
    - An implied warranty of fitness for a particular purpose is a promise that a seller's advice on how to use a product will be correct.

Professional Liability of Engineers

- Legal Duty (Standard of Care)
  - NJ Model Civil Jury Charge 5.52
    - An engineer has the duty to have and to use that degree of judgment, knowledge and skill which engineers of *ordinary ability* possess and exercise, *in the same or similar communities*, at the time the engineer performs his/her services. This is the standard by which to judge the engineer in this case.
    - The law does not expect or require perfection. Unsatisfactory results, alone, are not necessarily evidence of lack of skill or proper care.

Professional Liability of Engineers

– NJ Model Civil Jury Charge 5.52 (cont'd)

- If in the exercise of his/her judgment an engineer selects one or two or more courses of action, each of which under the circumstances has substantial support as proper practice in the engineering profession, the engineer is not negligent even if the course chosen produces a poor result.
- If the exercise of an engineer's judgment causes him/her to do that which standard engineering practice forbids, he/she is negligent.

Professional Liability of Engineers

– NJ Model Civil Jury Charge 5.52 (cont'd)

- Usually it is necessary to establish the standard of care by expert testimony, that is, by testimony of persons who are qualified by their training, study and experience to give their opinions on subjects not generally understood by persons who lack such special training or experience.

Professional Liability of Engineers

- Contractual Duty
  - If design professionals fail to perform their duties under a professional services agreement, they may be sued for breach of contract.
  - In the absence of a total lack of performance, most breach of contract claims against the engineer will be based upon negligent performance of the contract.

Professional Liability of Engineers

- Contractual Duty (cont'd)
  - The Plaintiff will generally establish the engineer's breach of contract by introducing evidence showing that the engineer failed to use reasonable care in the performance of his/her contractual obligations, or that the engineer's performance fell short of applicable professional standards.[8]
  - Suits against design professionals frequently allege liability based upon the failure of the design to comply with the mandates of codes or regulations.[9]

Professional Liability of Engineers

- Contractual Duty (cont'd)
  - Contractual language may elevate the "standard of care" by which the engineer will be judged[10].
    - Perform consistent with "the highest professional standards" or "nationally recognized firms with specialized expertise".
    - Contracts which employ such words as "ensure", "guarantee", "warrant", "achieve" and similar variants may be held to elevate the standard of care and create an express warranty.

Gross Negligence

- Case Law Regarding Design Professionals and Gross Negligence is Sparse
  - "Gross negligence" is the *failure to exercise slight care.*[11]
  - Gross negligence "is that degree of negligence which shows an utter disregard of prudence amounting to *complete neglect of the safety of others*."[12]
  - Gross negligence is "something more than the failure to exercise slight care . . . There must be an element either of malice or willfulness of utter and wonton disregard of the rights of others as from which it may be assumed the act was *malicious or willful".*[13]
  - If, in the judgment of the Board, a licensee, firm, entity, or person representing same . . . demonstrates carelessness which is in *reckless disregard for the safety, property or lives of others*, or is so great it appears to be a *conscious violation* of other people's property, or rights to health, safety or welfare, the Board may deem such neglect to be gross negligence.

    (OK Brd of Professional Engrs, Rule 245:15-23-5).

Professional Liability of Engineers

- Liability of Employee Engineers[14]
  - As a general rule, when an engineer negligently performs services on behalf of his firm or employer, the individual allegedly suffering damage from the engineer's negligent performance may sue the company and/or the individual engineer.
  - Typically, in the case of an engineering firm in private practice, the firm's professional liability insurance carrier will respond to claims against any past or present principal, partner, director, officer, or employee acting within the scope of their duties.

Product/System Safety Program

- Product Codes and Standards
- Hazard Identification
  - Hazards arising from *Intended Use*
  - Hazards from *Reasonably Foreseeable Misuse*
- Hazard Risk Assessment
  - Estimate *Probability of Occurrence,* and
  - *Seriousness of Harm*
- Hazard Risk Mitigation
  - Design Out the Hazard
  - Provide Guards and Interlocks
  - Provide Warnings and Instructions

Product Codes and Standards

As Part of System/Product Safety Program:

- Statutory Regulations (OSHA, FDA, etc.)
- Industry Standards (ANSI, NFPA, MIL-STD, etc.)
- Safety Factors (Limit Loads, Pressure Vessels, Stress, Yield, etc.)
- Checklists

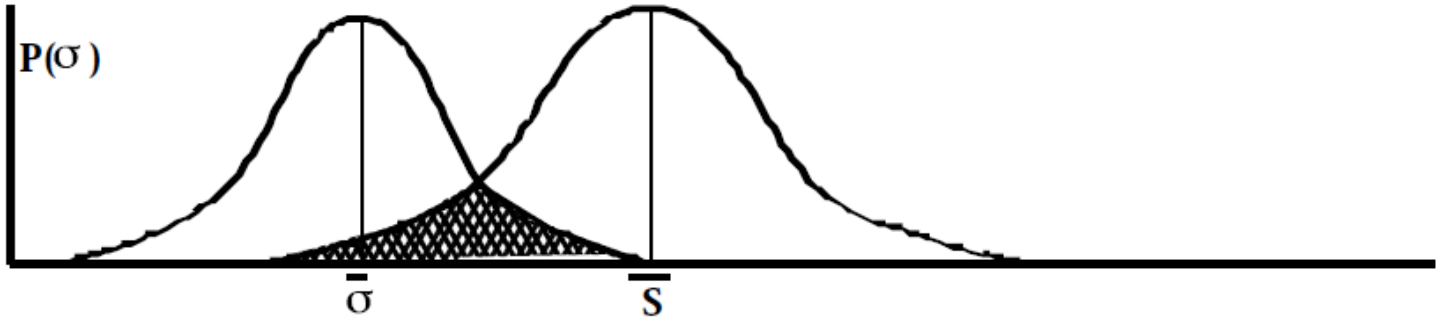


Figure 1. The Probability Distributions of Stress and Strength Showing Substantial Overlap
[Juvinall & Marshek, 1991, p. 225]

Product Codes and Standards

As Part of a Liability Prevention Program:

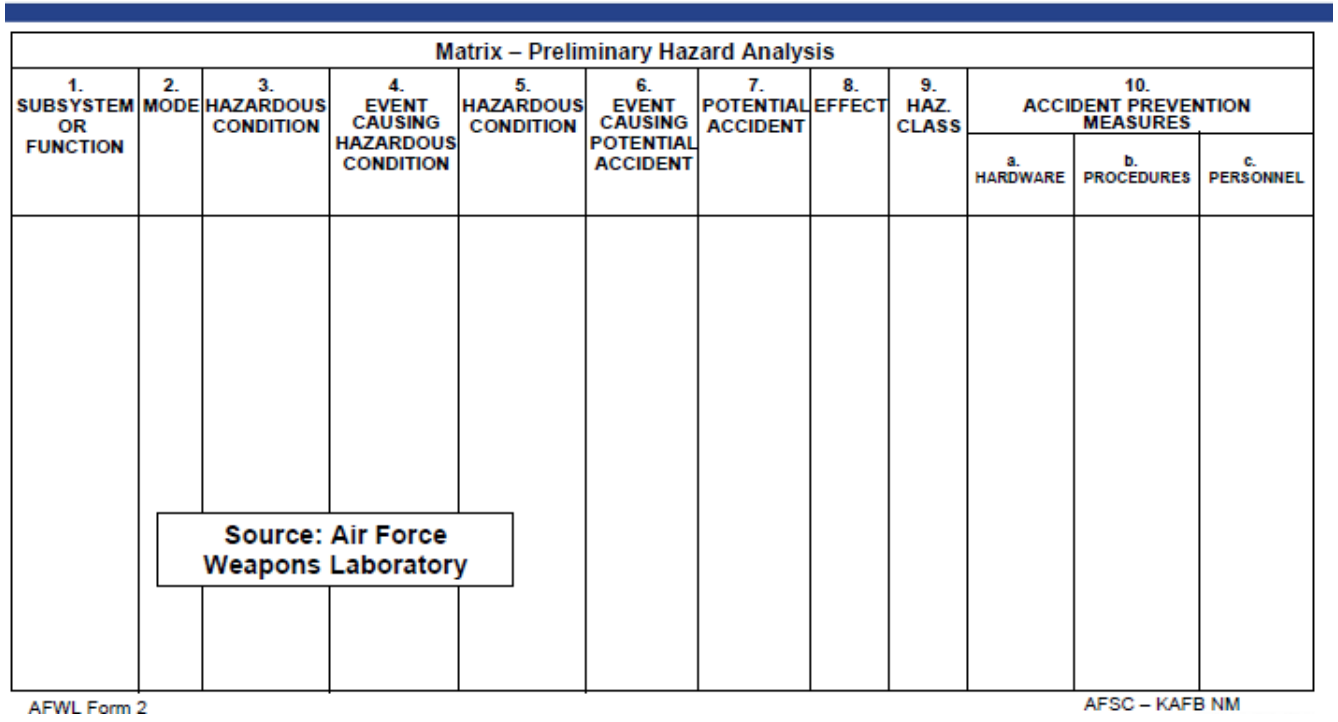
- "The fact that a particular product meets or exceeds the requirements of its industry is not conclusive proof that the product is reasonably safe. If fact, standards set by an entire industry can be found negligently low if they fail to meet the test of reasonableness."[15]
- Production (Manufacturing) Defects - The product does not conform to the designer's or manufacturer's own specifications or standards.
- Evidence of compliance with governmental or industry standards is generally allowed as objective evidence of consumer expectations.
- Suits against design professionals frequently allege liability based upon the failure of the design to comply with the mandates of codes or regulations.[14]

Codes & Standards serve as a floor, not a ceiling, for liability.

Hazard Identification

As Part of System/Product Safety Program:

- Preliminary Hazard List (PHL)
- Preliminary Hazard Analysis (PHA)
- Hazard Checklists
  - Energy Sources, Substances, Electrical, Fire, Ergonomic, etc.



Matrix – Preliminary Hazard Analysis

1. SUBSYSTEM OR FUNCTION	2. MODE	3. HAZARDOUS CONDITION	4. EVENT CAUSING HAZARDOUS CONDITION	5. HAZARDOUS CONDITION	6. EVENT CAUSING POTENTIAL ACCIDENT	7. POTENTIAL ACCIDENT	8. EFFECT	9. HAZ. CLASS	10. ACCIDENT PREVENTION MEASURES		
									a. HARDWARE	b. PROCEDURES	c. PERSONNEL

Source: Air Force Weapons Laboratory

AFWL Form 2

AFSC – KAFB NM

Hazard Identification

As Part of a Liability Prevention Program:

- Identify Hazards Arising from Intended Use
  - During the Life Cycle of the Product
    - Shipping → Assembly/Install → Testing → Intended Uses (& Misuses) → Service/Maintenance → Disposal
  - By Considering Reasonably Foreseeable:
    - Product Environments
    - Product Users
    - Product Uses
- And Reasonably Foreseeable Misuse
    - Including Foreseeable Alteration of the Product

Hazard Risk Assessment

As Part of System/Product Safety Program:

- Standard Hazard Analysis Techniques
  - System/Subsystem Hazard Analysis
  - Fault Tree Analysis, FMECA
  - Operating & Support Hazard Analysis
  - Etc.

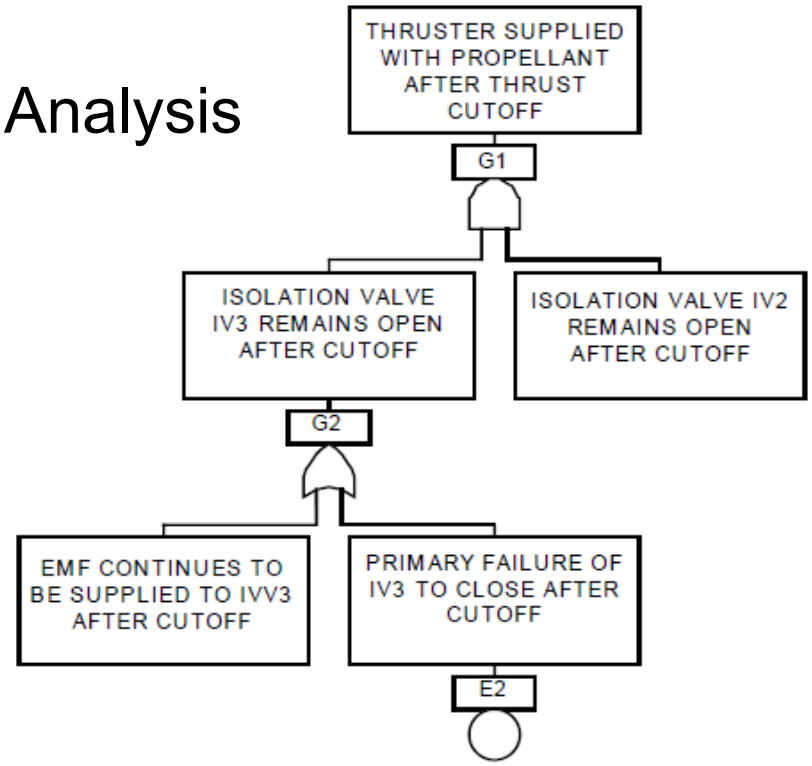
CATEGORY / FREQUENCY	(1) CATASTROPHIC	(2) CRITICAL	(3) MARGINAL	(4) NEGLIGIBLE
(A) FREQUENT ($X > 10^{-1}$)				
(B) PROBABLE ($10^{-1} > X > 10^{-3}$)				
(C) OCCASIONAL ($10^{-2} > X\ 10^{-3}$)				
(D) REMOTE ($10^{-3} > X > 10^{-6}$)				
(E) IMPROBABLE ($10^{-6} > X$)				

UNACCEPTABLE

UNDESIRABLE

ACCEPTABLE WITH REVIEW

ACCEPTABLE WITHOUT REVIEW



Hazard Risk Assessment

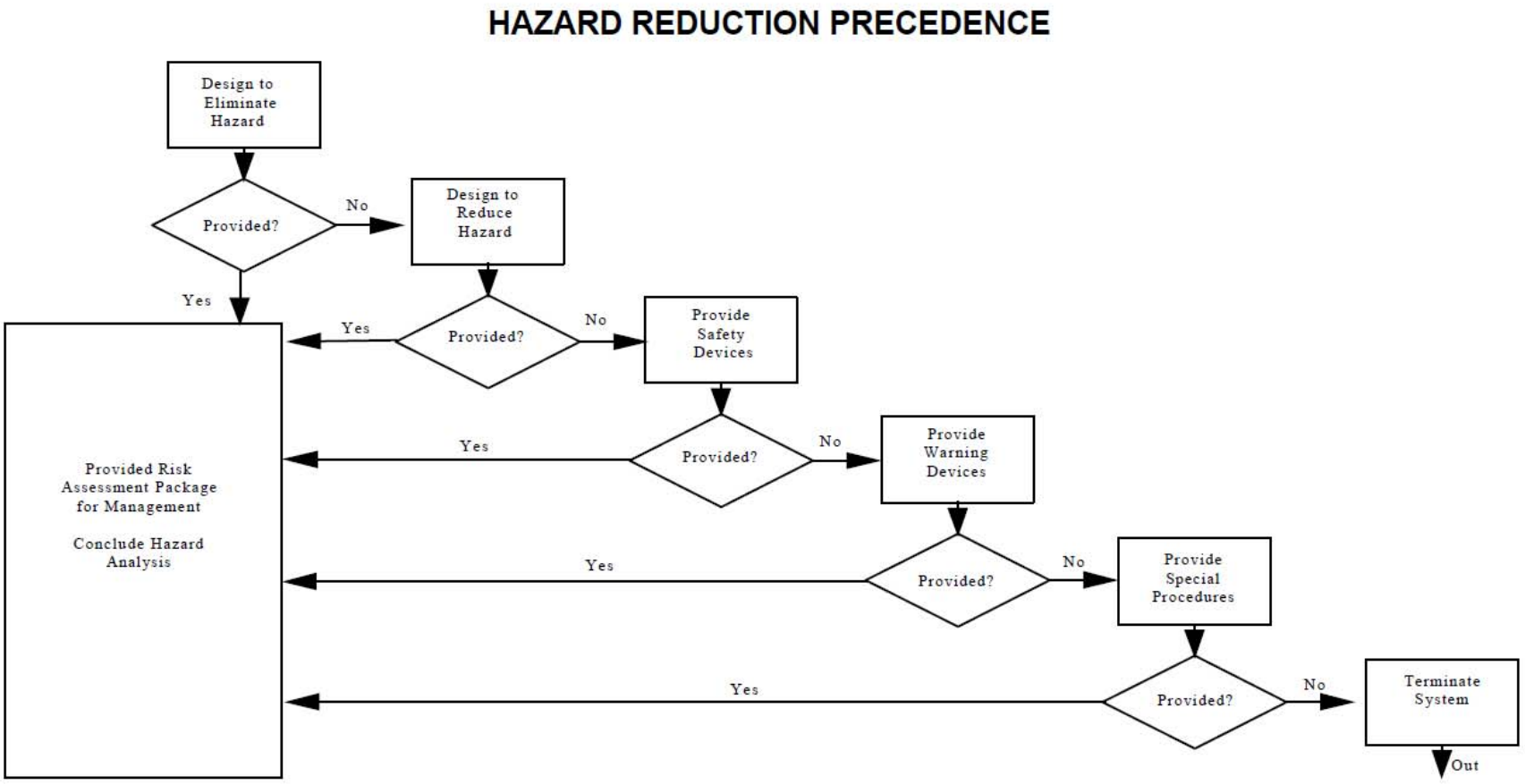
As Part of Liability Prevention Program:

- Product is defective in design when the foreseeable risks of harm posed by product could have been reduced by adoption of a reasonable alternative design
- The manufacturer will not be liable if the consumer's *unforeseeable misuse* of the product was the sole cause of the harm.
- State of the Art Defense - The manufacturer used the *best technology reasonably available* and feasible for use at the time of manufacture.
- While the first incident of misuse may not make the misuse sufficiently foreseeable to require remedial action, the more misuses that occur, the more it can be argued that the misuse has become "reasonably foreseeable".
- A product may be found defective in design, even if it satisfies ordinary consumer expectations, if through hindsight the jury . . . finds the *risk* of danger inherent in the challenged design *outweighs the benefit* of such design.

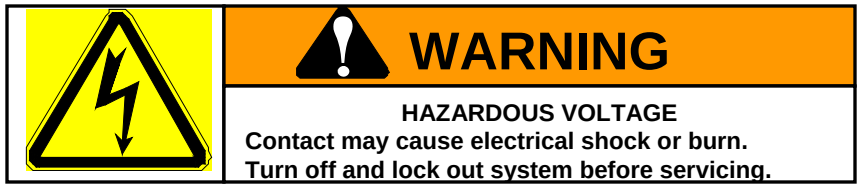
Hazard Risk Mitigation

As Part of System/Product Safety Program

AND Part of a Liability Prevention Program:



Warning Label per ANSI Z535[16]



- Must Communicate
  - Type of Hazard
  - Magnitude or Risk
  - Action to Avoid/Minimize the Risk
- Use Proper Signal Word
  - **CAUTION** indicates a *potentially* hazardous situation which, if not avoided, may result in *mild or moderate injury*
  - **WARNING** indicates a *potentially* hazardous situation which, if not avoided, could result in *death or serious injury*
  - **DANGER** indicates an *imminently* hazardous situation which, if not avoided, will result in *death or serious injury*

Restatement of Torts 3rd - Product is defective because of inadequate instructions or warnings when the foreseeable risks of harm posed by product could have been reduced by the provision of reasonable instructions or warnings.

The Loss of RAF Nimrod XV230

- A Case Study of a Safety Case

An Independent Review into the broader issues surrounding the loss of the RAF Nimrod MR2 Aircraft XV230 in Afghanistan in 2006.[17]

– *Charles Haddon-Cave QC*

The Incident

On 2 September 2006, RAF Nimrod XV230 was on a routine mission over Helmand Province in Southern Afghanistan in support of NATO and Afghani ground forces. Approximately 1½ minutes after completion of Air-to-Air Refuelling from a Tristar tanker, she suffered a catastrophic mid-air fire, leading to the total loss of the aircraft and the death of all 14 on board.

The crash site was secured by a nearby NATO unit, but no survivors were found. The crash site was in a known area of Taliban activity, and initial priorities were the recovery of the crew's bodies, personal effects, classified documentation, flight recorders and other equipment. A detailed photographic record of some key parts of the wreckage were made, but most of the aircraft wreckage was removed from the site by the Taliban and local villagers.

The Board of Inquiry

The Board of Inquiry (BOI) findings were made public on 4 December 2007. The BOI concluded that the loss of XV230 was caused by:

1. *Fuel Source*: The escape of fuel during Air-to-Air Refueling, occasioned by an overflow from the blow-off valve to No. 1 tank, causing fuel to track back along the fuselage, or alternatively, a leak of fuel from the fuel system (fuel coupling or pipe), leading to an accumulation of fuel within the No. 7 Tank Dry Bay.
2. *Ignition Source*: The ignition of that fuel following contact with an exposed element of the aircraft's Cross-Feed/Supplementary Cooling Pack (SCP) duct.

The BOI also found that a 'Safety Case' prepared in respect of the Nimrod MR1 and MR2 aircraft between 2002 and 2005, the Nimrod Safety Case, contained a number of significant errors.

The Board of Inquiry

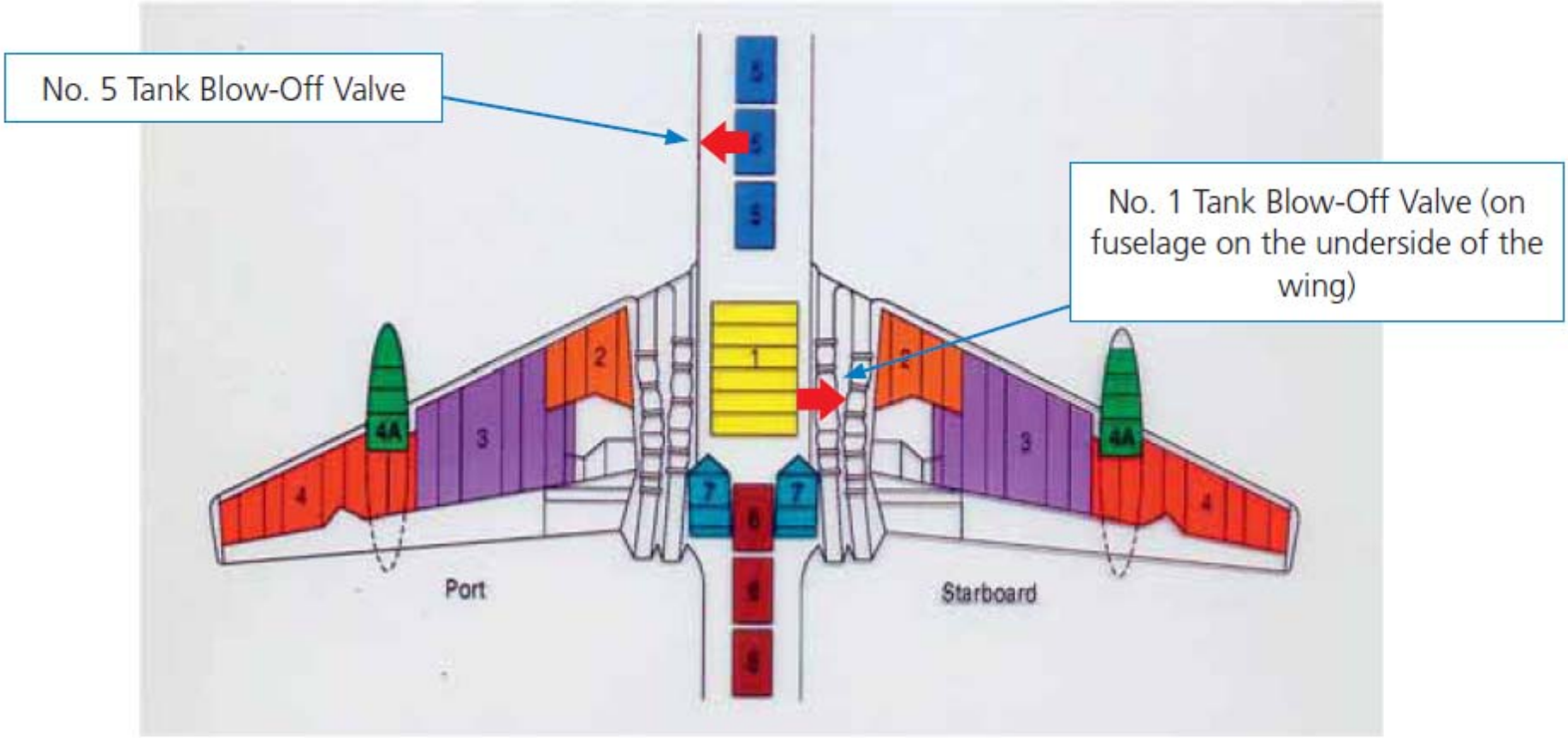


Figure 5.1: Location of Nimrod Fuel tanks

The Root Cause

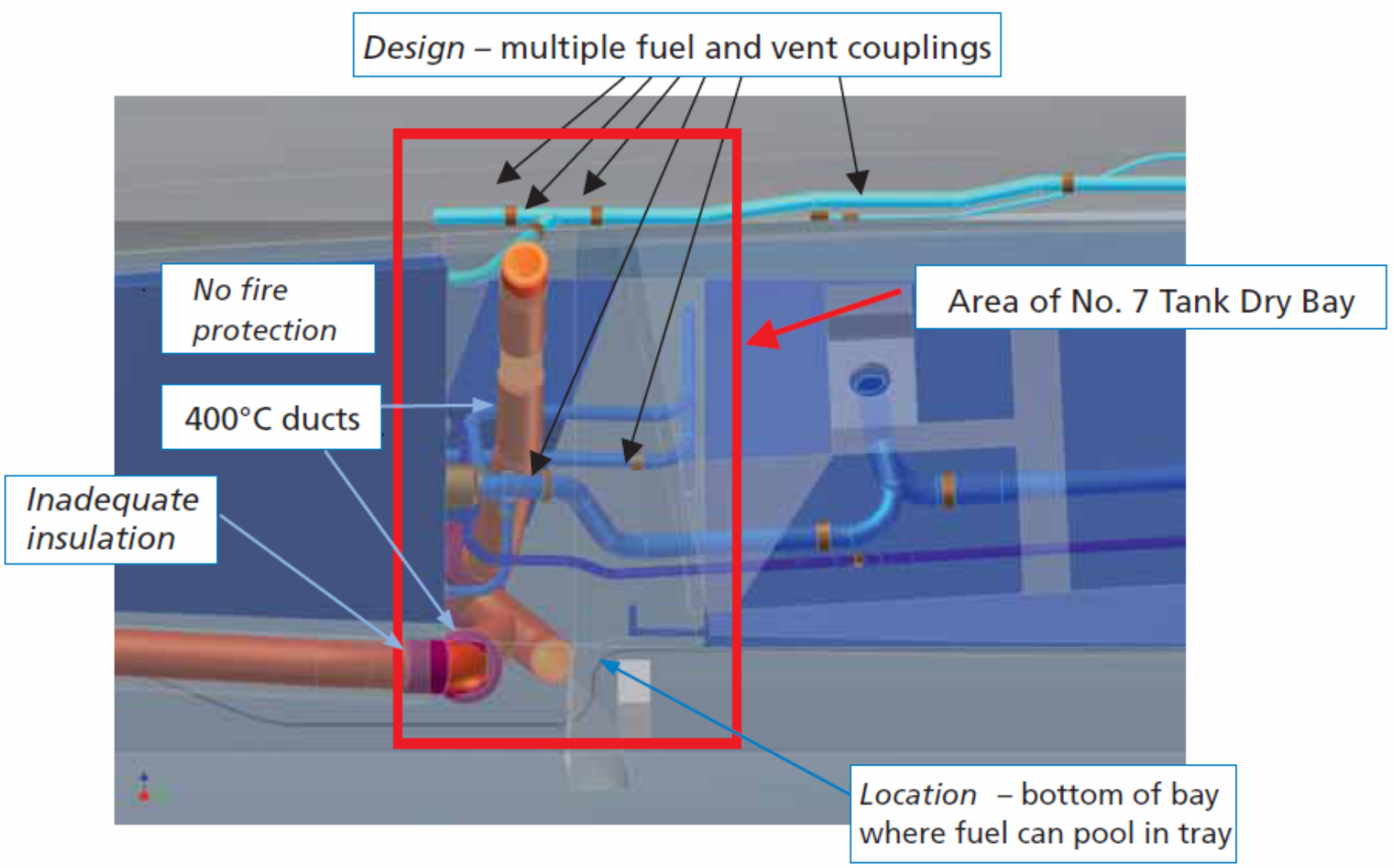


Figure 4.13: No. 7 Tank Dry Bay (Design Features)

The Nimrod Safety Case

The drawing up of a 'Safety Case', to identify, assess, and mitigate potentially catastrophic hazards before they could cause an accident, was mandated for military aircraft and other military platforms by regulations introduced in September 2002.

The Nimrod Safety Case was drawn up between 2001 and 2005 by BAE Systems (Phases 1 and 2) and the MOD Nimrod Integrated Project Team (Third Phase), with QinetiQ acting as independent advisor. The cost was in excess of £400,000 (~ $600k). Three organizations were involved in drawing up the Nimrod Safety Case:

1. **The Nimrod IPT**, which was the 'Integrated Project Team' within the Defence Logistics Organization, with specific responsibility for the Nimrod MR2 and R1 fleets.
2. **BAE Systems**, which was the Design Authority (DA) for the Nimrod aircraft and formally tasked by the Nimrod IPT to draw up the Nimrod Safety Case for the two aircraft types.
3. **QinetiQ**, which acted as 'independent advisor' to the Nimrod IPT in relation to the Nimrod Safety Case.

"The Nimrod Safety Case process was fatally undermined by a general malaise: a widespread assumption by those involved that the Nimrod was 'safe anyway' (because it had successfully flown for 30 years) and the task of drawing up the Safety Case became essentially a paperwork and 'tickbox' exercise."

The Nimrod Safety Case was Drawn Up in Three Phases:

Phase 1 conducted by BAE Systems (April 2001 to April 2003):

Following initial scoping and formalization of Phase 1 of the Nimrod Safety Case task, BAE Systems carried out zonal inspections of Nimrod aircraft and delivered a 'hazard identification' via a Zonal Hazard Analysis Report to the Nimrod IPT in April 2003.

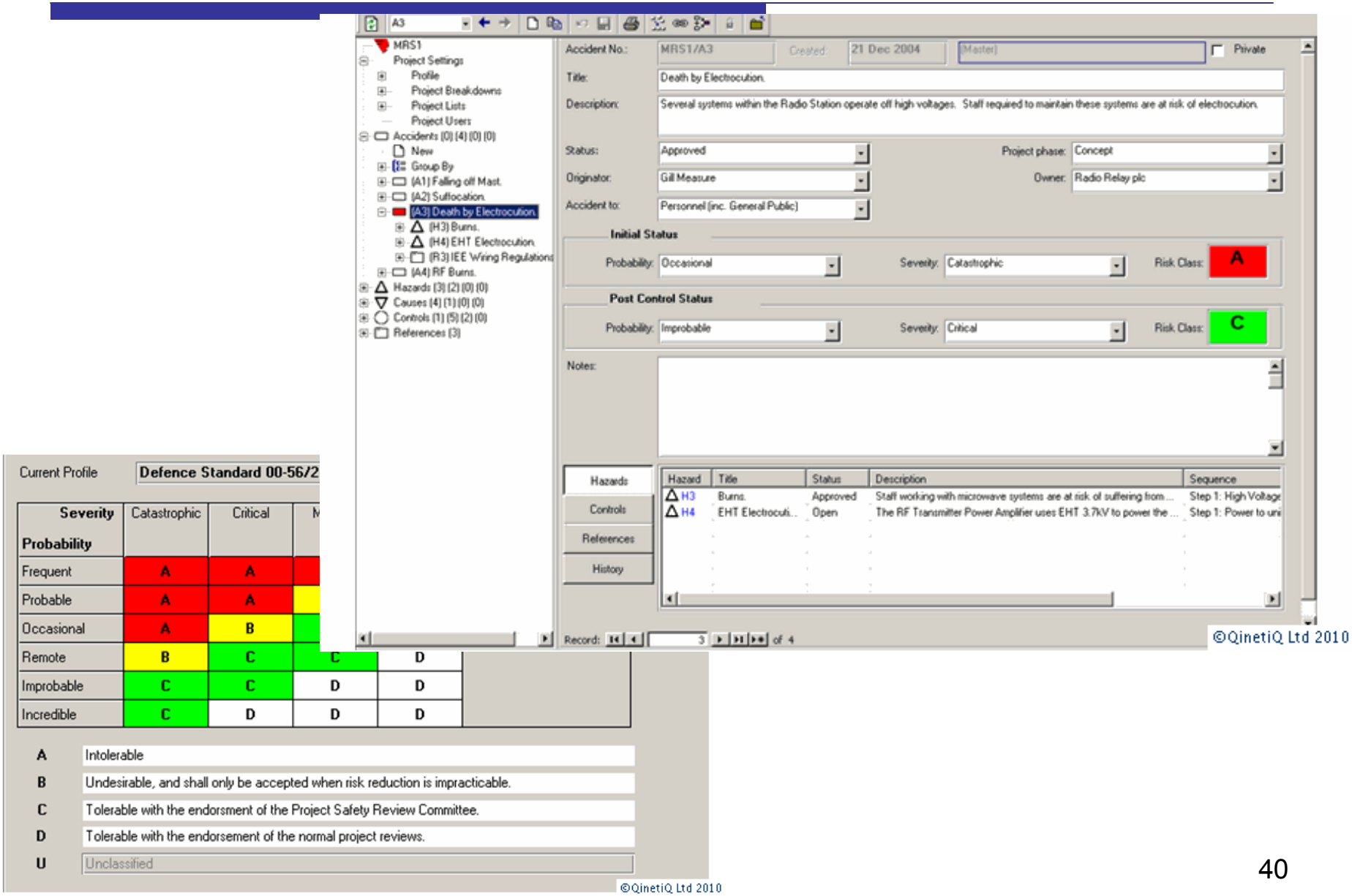
Phase 2 conducted by BAE Systems (August 2003 to September 2004):

Conducted 'hazard analysis' and 'hazard mitigation' exercises at its offices, culminating in the population of a database (CASSANDRA) and the delivery of six written Reports to the Nimrod IPT, comprising its completed work on the Nimrod Safety Case, in September 2004.

Third Phase conducted by the Nimrod IPT (September 2004 to March 2005):

Following handing over of the Nimrod Safety Case Reports by BAE Systems to the Nimrod IPT and the 'signing-off' of the task (supported by QinetiQ), the Nimrod IPT then proceeded to sentence the remaining hazards left "*Open*" by BAE Systems, and the Nimrod Safety Case for both Nimrod MR2 and R1 was declared completed in March 2005.

Cassandra Database



Phase 1 – Hazard ID and Initial Assessment

Phase 1 involved the identification and initial assessment of hazards, the production of the Fault Tree and the completion of the ZHA. An important element of this phase was said to be the visit to, and assessment of, an MR2 and an R1 aircraft. Specific deficiencies in Phase 1 included the following:

1. The general approach was flawed from the outset, the task was wrongly regarded as essentially a documentary exercise. The ZHA was an 'inspect and record' process with photos and notes, but no analysis.

2. The man-hours estimate was inadequate; the task was inadequately resourced; there was no continuity of personnel.

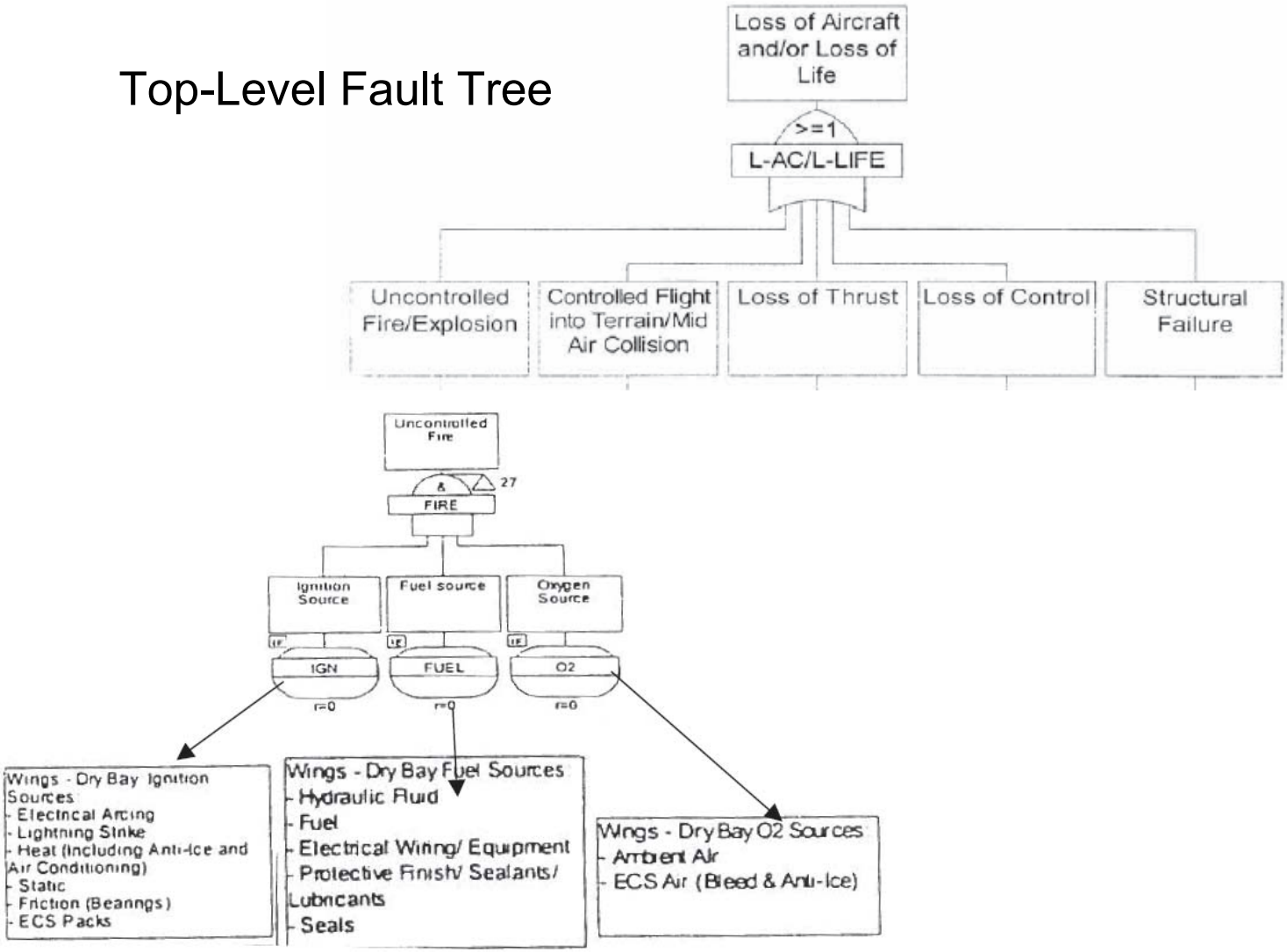
3. The zonal inspections were unsound, superficial and carried out by personnel with little practical knowledge of the aircraft. There was little operator/maintainer input.

4. The project planning was poor; the project management was inadequate; there was insufficient guidance for staff; there was no sensible priority given to the high risks. The initial identification of 1,300 'hazards' by the BAE Systems Phase 1 team further demonstrated a lack of competence and basic understanding as to what they were doing.

5. There was disagreement, confusion, and dissent between those involved as to how to proceed; the personnel involved were insufficiently trained and inexperienced.

Phase 1 – Hazard ID and Initial Assessment

Top-Level Fault Tree



Phase 2 – Hazard Analysis & Mitigation

The Phase 2 work by BAE Systems suffered increasingly from planning, management, execution, resource, time and attitude problems, which seriously affected the quality of the work done. The task was not completed by the 31 August 2004 deadline. The end product was both seriously deficient and defective in three principal respects:

1. BAE Systems' final Reports contained a big hole: over 40% of the hazards remained *"Open"* and over 30% of the hazards remained *"Unclassified"*. All these hazards had a potential severity rating of *"Catastrophic"*.

2. BAE Systems' 'hazard analysis' and 'hazard mitigation' exercises (summarized in documents called 'Pro-Formas' which underpinned, but did not accompany, the final Reports) contained numerous, systemic errors of fact, analysis and risk categorization.

3. BAE Systems failed properly to assess and address the critical fire hazard relating to the Cross-Feed/SCP duct in the starboard No. 7 Tank Dry Bay which probably caused the loss of Nimrod XV230 (Hazard H73). BAE Systems' provisional assessment of Hazard H73 as *"Improbable"*, *i.e.* as a Class C 'tolerable' risk, was seriously erroneous. Hazard H73 was, however, included in the large block of *"Unclassified"* and *"Open"* hazards in the final Reports because of the lack of time for BAE Systems' Electrical Systems Department to complete their assessment.

Phase 2 – Handover to Customer

At a two-day meeting with the Nimrod IPT and QinetiQ to present the results of its work on 31 August 2004 to 1 September 2004 (and at a subsequent meeting on 10 November 2004), BAE Systems represented that it had completed the task satisfactorily, that all hazards had been 'appropriately identified, assessed and addressed', and that the Nimrod MR2 and R1 could be deemed *"acceptably safe to operate"* and ALARP, subject to the carrying out of specific recommendations.

This was not a full or accurate picture: BAE Systems *deliberately* did not disclose to its customer at the meeting the known figures for the large proportion of hazards which it had left *"Open"* and *"Unclassified"* (many with only vague recommendations that 'further work' was required) or otherwise draw attention to the large gaps remaining in its analysis.

The Nimrod IPT and QinetiQ were content simply to accept that BAE Systems had completed the task and to agree to 'sign off' the final Reports without sufficient inquiry, or asking for any underlying material, or even carefully reading the final Reports themselves (which would have alerted them to the substantial proportion of *"Open"* and *"Unclassified"* hazards and large amount of work remaining to be done).

Phase 3 – “Sign Off” and Closeout of Hazards

Once the Nimrod IPT appreciated the number of *“Open”* hazards, it subsequently proceeded to sentence the remaining 43 out of 105 hazards which had been left *“Open”* by BAE Systems (including Hazard H73) on a manifestly inadequate, incorrect and unsatisfactory basis.

At no stage during the Nimrod Safety Case process did BAE Systems, the Nimrod IPT or QinetiQ, ever properly identify, assess or address the serious and long-standing catastrophic risk to the Nimrod fleet represented by the Cross-Feed/SCP duct and the Air-to-Air Refueling modification.

Zonal Hazard Analysis Worksheets

2. Hazards Subsumed & Description *(Taken from: M:\MBU\Design\Airworthiness\Flight Safety\NIMROD\hazard log\MAJOR HAZARDS (SCOTT)\zonal hazard.xls)*

	Hazard No. NM/H**	Hazard Title	Description	A/C type	Cause *(hazard- Section 3)*
A	367 (photo Dcp0221)	Fire/Explosion - Fuel or hydraulic leak onto Hot Engine Bleed Pipe	Potential fuel or hydraulic leaks from fuel pipe joint, Flap hydraulic pipelines or No 7 Tank main feed fuel pipe immediately above the HP, High Temp engine bleed take-off port or associated ducting potentially causing an uncontrolled fire or explosion.	Both	Fluid Leak (C, F)
B	498 (photo Dcp0312)	Multiple systems in very close proximity	In an area closely packed with flight control cables and pulleys, hydraulic services, unprotected electrical cables and hot air ducting there exists a potential for hot air, fuel or hydraulic leaks and possible fire.	Both	Fuel Leak (All)

3. Key Potential Hazards simplified

(List the potential hazards identified & the simply described potential causes)

	Potential Hazard *(taken, or assumed, from hazard description)*	Potential Cause *(taken from subsumed hazard Description)*	Failure Level
A	Fire/Explosion	Fuel Leak onto electrical circuits/cables	Double
B	Fluid Contamination	Fuel Leak onto electrical circuits/cables	Single
C	Fire/Explosion	Fuel Leak onto Hot ECS Duct	Single
D	Fire/Explosion	Fuel Leak onto Control Cables	Single
E	Fluid Contamination	Fuel Leak onto Control Cables	Single
F	Fire/Explosion	Hydraulic Leak onto Hot ECS Duct	Single
G	Fluid Contamination	Hydraulic Leak onto electrical circuits/cables	Single

U		AvP970 Chapter 715 Fire Precautions Leaflet 715/2	***Fire Zones**: Any region in which a single failure of an installation or any part of it could result in a fire or break out of existing controlled fire (e.g., combustion chamber) into the aeroplane shall be regarded as a fire zone.* *There is, however, the risk that a severe danger of fire may be present in certain other regions due for example to the necessity for the location of pipes carrying inflammable fluids near to a non-flameproof motor with the result that only a single failure could lead to a catastrophic fire.*

Supporting Annexes Were Incomplete

10B.18 Annex B stated in relation to Hazard H73 (one of the 32 open hazards left *"Unclassified"*):

HAZARD I/D	ZONE DESCRIPTION	*SEVERITY*	PROBABILITY	HRI	RECOMMENDED HAZARD STATUS
H73	**Zone 513/613 Interacting System** Hazards – No. 7 Fuel Tank	CATASTROPHIC	UNCLASSIFIED	–	OPEN

10B.19 Annex C stated in relation to Hazard H73:

Hazard Ref (H...)	Control Ref (C...)	Recommendation: (See Individual Safety Cases Baseline Hazard Log Entry for full recommendation)
73	100	• From the photographic evidence obtained during the zonal hazard review at RAF Kinloss & Waddington, it appears that there are potentials for fire hazards on the R Mk 1 and the MR Mk 2 aircraft. Further investigation is required to confirm that the potential loss due to the contamination of the various services in the zone (514/614) would not be a hazard to the aircraft. • Further analytical techniques are considered necessary in order to categorise the risk of the specific fire/explosion hazard identified.

Specific Errors in the Nimrod Safety Case (NSC)

"The NSC did not correctly categorise the potential threat to the aircraft caused by the co-location of fuel and hot air system components within the No. 7 Tank Dry Bay, in contravention of design standards in effect at the time of modification. Aircraft are required to be designed such that any potential single-point ignition risks are mitigated by *inter alia* fire detection and protection systems.

The NSC quoted the potential for fuel system leakage as 'Improbable', which is defined as '*Remote likelihood of occurrence to just 1 or 2 aircraft during the operational life of a particular fleet*'. The BOI's analysis of fault data, however, indicated an average of 40 fuel leaks per annum for the Nimrod MR2 fleet between 2000 and 2005.

The NSC stated that the Cross-Feed duct was only pressurised during engine start, not taking into account the lengthy periods it can be pressurised (at a working temperature of up to 420°C) when feeding the SCP.

The NSC noted as mitigation for Zone 614 hazards (which included the starboard No. 7 Tank Dry Bay) the provision of an aircraft fire detection and suppression system, when neither existed within Zone 614.

This is the scenario that nearly befell XV227 on 22 November 2004, when it suffered a major hot air duct failure in a section of the Cross-Feed/SCP just aft of the elbow at the bottom of No. 7 Tank Dry Bay due to corrosion. The hot air leak of gases up to 420ºC caused serious damage *inter alia* to numerous proximate fuel seals in No. 7 Tank Dry Bay. XV227 was fortunate not to have been lost entirely."

Erroneous Hazard Control & Final Risk Probability

Evidence for Mitigation of hazards

Hazard No	Hazard	Control	Post Control Status
H73	Z514/614 Interacting Systems Hazards	1. Systems maintained iaw Nimrod maintenance procedures AP101B-0503-1. 2. Aircraft fire detection and suppression system.	Remote

"Of the 25 instances where this is repeated, only six of those zones possess a fire detection and suppression system; the other 19 do not. Therefore, the above entry was seriously flawed in three respects.

1. First, the reference to *"Aircraft fire detection and suppression system"* as a hazard control was in many cases, including Hazard H73, a glaring factual error.
2. Second, the inclusion of *"Systems maintained iaw Nimrod maintenance procedures AP101B-0503-1"* was inappropriate as a hazard control.
3. Third, the setting of *"Remote"* as a Post Control Status was inappropriate and illogical since in many cases this was merely the 'initial probability' set on CASSANDRA."

Criticisms of BAE Systems

"BAE Systems bears substantial responsibility for the failure of the Nimrod Safety Case. Phases 1 and 2 were poorly planned, poorly managed and poorly executed, work was rushed and corners were cut. The end product was seriously defective.

1. There was a big hole in its analysis: BAE Systems had left 40% of the hazards *"Open"* and 30% *"Unclassified"*. The work was, in any event, riddled with errors of fact, analysis and risk categorisation.
2. The critical catastrophic fire hazard relating to the Cross-Feed/SCP duct (Hazard H73) had not been properly assessed and, in fact, was one of those left *"Open"* and *"Unclassified".*
3. Further, at handover meetings in 2004, BAE Systems gave the misleading impression to the Nimrod IPT and QinetiQ that the task had been properly completed and could be signed off and deliberately did not disclose to its customer the scale of the hazards it had left *"Open"* and *"Unclassified"* (many with only vague recommendations that 'further work' was required). The Nimrod IPT and QinetiQ representatives were lulled into a false sense of security. These matters raised question marks about the prevailing ethical culture at BAE Systems.

Three key BAE Systems management personnel involved in the Nimrod Safety Case bear primary responsibility for the above matters and are the subject of significant criticism: (1) the Chief Airworthiness Engineer; (2) the Task Leader; and (3) the Flight Systems and Avionics Manager."

Criticisms of QinetiQ

"QinetiQ also bears a share of responsibility for the failure of the Nimrod Safety Case.

1. QinetiQ failed properly to carry out its role as 'independent advisor' and, in particular: failed to clarify its role at any stage;
2. Failed to check that BAE Systems sentenced risks in an appropriate manner and included risk mitigation evidence in its Reports;
3. Sent someone inadequately briefed to the critical handover meeting;
4. Failed to read the BAE Systems reports or otherwise check BAE Systems' work properly;
5. Failed to advise its customer properly or ask any intelligent questions at the key handover meetings;
6. Subsequently 'signed-off' BAE Systems' work in circumstances where it was manifestly inappropriate to do so: in particular, without even having read any of the BAE Systems Reports and contrary to relevant regulations and standards.

Two key QinetiQ personnel involved in the Nimrod Safety Case bear primary responsibility for the above matters and are the subject of significant criticism: (1) the Task Manager and (2) the Technical Assurance Manager."

Criticisms of Nimrod IPT

"The Nimrod IPT bears substantial responsibility for the failure of the Nimrod Safety Case.

1. The Nimrod IPT inappropriately delegated project management of the Nimrod Safety Case task to a *relatively junior person* without adequate oversight or supervision;
2. Failed to ensure *adequate operator involvement* in BAE Systems' work on Phases 1 and 2;
3. Failed to project manage properly, or to act as an 'intelligent customer' at any stage;
4. Failed to read the BAE System Reports carefully or otherwise check BAE Systems' work;
5. Failed to follow its own Safety Management Plan;
6. Failed properly to appoint an Independent Safety Advisor to audit the Nimrod Safety Case; and *signed-off BAE Systems' work* in circumstances where it was manifestly inappropriate to do so.
7. Subsequently, the Nimrod IPT sentenced the outstanding risks on a manifestly inadequate, flawed and unrealistic basis, and in doing so mis-categorised the catastrophic fire risk represented by the Cross-Feed/SCP duct (Hazard H73) as *'Tolerable'* when it plainly was not. The Nimrod IPT was sloppy and complacent and outsourced its thinking.

Three key Nimrod IPT personnel involved in the Nimrod Safety Case bear primary responsibility for the above matters and are the subject of significant criticism: (1) the Nimrod IPT Leader, (2) the Head of Air Vehicle, and (3) the Safety Manager."

DefenseNews

BAE, QinetiQ May Face Charges in Crash[18]

Families of 14 Killed in Aircraft Disaster Eye Criminal, Civil Actions

By Andrew Chuter

Published: 2 November 2009

LONDON - British contractors BAE Systems and QinetiQ could face a corporate manslaughter charge following the publication of a report on the crash of a Nimrod MR2 aircraft that claimed the lives of 14 military personnel.

Lawyers representing the families of those killed in the 2006 crash in Afghanistan said they were considering pursuing civil or criminal corporate manslaughter charges against the companies after a Ministry of Defence-commissioned report condemned their performance in conducting safety checks on the Royal Air Force surveillance plane.

The Nimrod crashed after a catastrophic midair fire on board the aging four-engine jet aircraft. The fire apparently started when an overflow of fuel ignited following an air-to-air refueling. The MoD has admitted liability for the crash and is negotiating with the families over compensation.

The report by Charles Haddon-Cave, a lawyer, blasted the performance of the MoD, BAE and QinetiQ in reviewing the Nimrod fleet's safety in the period of 2001-05.

In an unusual move, it named the executives and military personnel it deemed largely responsible for the mistakes.

. . . To make the case stick, he said, they would have to establish **gross negligence** linked to death and prove it was part of a long-term pattern of behavior.

References

1. Sweet, Schneirer, *Legal Aspects of Architecture, Engineering and the Construction Process*, 8th Edition (2009).
2. Restatement (Third) of Torts, Manufacturing and Design Defects.
3. California Civil Jury Instructions § 1203, *Strict Liability, Design Defect, Consumer Expectation Test*.
4. Soule v. General Motors, 882 P.2d 298 (1994).
5. Dan B. Dobbs, *The Law of Torts*, West Hornbook Series (2000).
6. Restatement (Second) of Torts §402A and Comments (1965).
7. Glassey v. Continental Insurance Company, 176 Wis. 2d 587, 601, 500 N.W.2d 295 (1993).
8. Prince, *Defective Products, Fraud and Misrepresentation Claims in Minnesota*, 29 Hamline L. Rev. 261 (2006).
9. Lee, Berg*, The Practitioner's Guide to Colorado Construction Law, Chapter 8, Architect/Engineer Liability (2005).*
10. American Bar Association, *Design Professional and Construction Manager Law*, 2007.
11. Driggers v. Southern Ry. Co., 169 S.C. 157, 160, 168 (1933).
12. Wallower v. Martin, 206 Va. 493, 497-498 (1965).
13. City of Middlesboro v. Brown, 63 S.W.3d 179, 181 (Ky. 2001).
14. National Society of Professional Engineers, A. Schwartz, *Liability of Employed Engineers*.
15. Dudley Sports Co. v. Schmitt, 279 NE2d 266 (1972).
16. ANSI Z535.4-2007, *American National Standard for Product Safety Signs and Labels* (2007).
17. Charles Haddon-Cave QC, *The Nimrod Review*, Ordered by the House of Commons, 28 October 2009.
18. Defense News, Electronic Edition, 2 Nov 2009, Army Times Publishing Company.