Evolution of the Air System Safety Case

Plan Design Enable

1

Learning Objectives

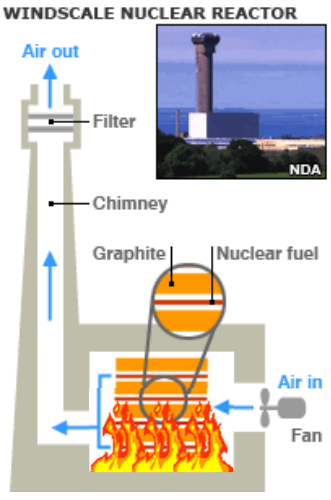
- To understand the applicability of the HSWA and Duty of Care
- To appreciate the relationship between prescriptive regulatory based approach and risk (goal-based) approach to safety management with its use of safety cases
- To appreciate the changes in safety management as a result of the Nimrod review

2

Introduction

- Strategy to Safety Management is linked to
  - The pace and complexity of technological advancement
  - The increasingly complex interdependencies between organisations and 'system of systems' considerations
- Pre-1940s
  - Industry sectors have been relatively stable with little change
  - Confidence in the prescribed solution
- Post-1940s
  - Great technological upheaval
  - Accelerating trend with growth of software applications.

Windscale Reactor Fire (10 October 1957)



- Nuclear Arms Race
  - Production of Plutonium 239
  - Graphite Control Rods
- New technology
  - Based loosely on existing reactors
- Reactor Fire!
  - ~1300 Celsius measured
  - ~20,000 Curies of radioactive material released into the atmosphere
- First hint of moving away from prescriptive regulatory approaches – Nuclear Installations Inspectorate

Aberfan (21 October 1966)

5

Aberfan: Origins of the Health and Safety Executive

The HSWA was formulated following Aberfan & also due to a number of defects in the statutory system as reported in the Robens Committee (1972), namely;

HSE
Health & Safety Executive

- Too much law, disparate across multiple organisations
- Existing law was unsatisfactory from a holistic perspective
- Lack of general provision for safety & health at work

New style regulation to encourage ‘safety principles rather than solutions’

6

Health and Safety at Work Act etc. 1974

- **Sections 2-6 apply to employers**
  - Safe place of work & Safe working environment
  - Safe systems of work, instruction, training, supervision
  - To ensure their activities do not endanger ***anybody***
  - To provide information to the public (non-employees) about risks that might affect their health and safety
  - To ensure supplied equipment is safe when correctly used
- **Section 7 applies to employees**
  - Must take reasonable care to ensure that they do not endanger themselves or anyone else who may be affected by their work activities
  - Must co-operate with their employers to enable the employer to comply with his statutory duties
- **Section 8: General Duties for everyone (inc. General Public)**
  - Not to intentionally or recklessly interfere with anything provided in the interests of health, safety or welfare

How To Comply With HSWA

- Many aspects of a Safety Management System can be seen to be responses to the requirements of the HSWA
- **Management of Health & Safety Regulations 1999** introduced to bridge gap with EU legislation, and clarifies HSWA requirements
- Organisations must have published Policy, covering:
  - Risk
    - Identification
    - Assessment
    - Minimisation
  - Procedures and facilities for safe handling, storage, transport
  - Product integrity regime
  - Surveillance (of health)
  - Information, instructions, supervision
  - Emergency procedures

Flixborough (1974): Chemical Plant Explosion

- Production of Cyclohexanol ($C_6H_{11}OH$) for Nylon manufacture
  - (volatile & flammable)
- Complications:
  - Crack in no. 5 reactor
  - "Temporary" bypass pipe to allow continued production during repairs
- 2 months later, pipe ruptured
  - 40 tonnes of cyclohexane leaked
  - Fuel-air explosion ~15 tonnes TNT
  - 28 Killed
  - 36 Seriously Injured

- Investigation and outcomes:
  - Management pressure
  - Regulations not suitable for size of plant
  - Adoption of a risk based approach to Major Accident Hazards
  - Demonstrate ALARP

Herald of Free Enterprise (1987)

- Ship departed with bow doors open (familiar operation)
  - Change in route
  - Change in organisation
  - Captain unaware
- Bow ballast filled due to lack of ramp
- Shallow seas around Ostend
  - "Squat Effect" - sucking ship lower in the water
- Water entered the vehicle deck
  - Free surface effect destabilises ship
  - Rapid capsize (90 secs)
  - 193 deaths – mostly hypothermia

- Investigation:
  - No appreciation of change in operations/environment
  - No "door closed" indicator light on bridge
  - Management pressures (overworked staff)
  - Requirement for assurance to Port Authorities

Piper Alpha Platform Fire (1988)

- Piper Alpha was a large North Sea oil platform that started production in 1976
  - produced oil from 24 wells
  - acted as a central node in network
  - upgraded in 1980 with a Gas Recovery Module

- Prelude:
  - Fortnightly overhaul of LPG Pump A not completed (temporarily sealed)
  - Not reported to duty custodian
  - Entire supply now depended on Pump B

Situation occurs:

- Pump B stopped suddenly
- Pump A switched on
  - No apparent reason to not use Pump A
- Overpressure led to leak and subsequent explosion

Piper Alpha Platform Fire (1988)

- Lack of space led to module being placed by the Control Room
  - Control Room destroyed by initial explosion

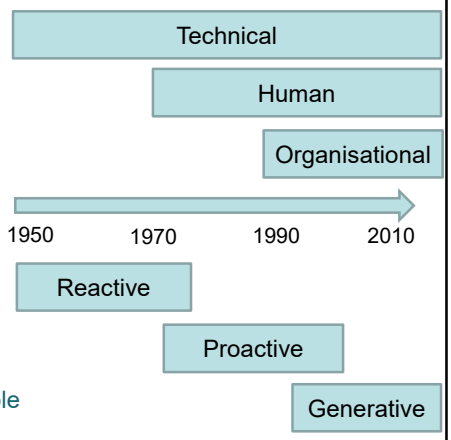
- No communication to other wells
  - Oil continued to be pumped to Piper Alpha
- No activation of suppression system
  - Automatic Fire Control System set to manual due to divers in the water
- No order to evacuate

- Within 22 minutes of initial explosion, a 2nd explosion engulfed the platform
- 167 died, 59 survived

- Investigation and outcomes:
  - Followed regulatory standards but change in use failed to recognise local interactions and risks
  - HSE remit extends beyond UK borders
  - Requirement for Safety Cases HSE Offshore Installation (Safety Case) Regulations 1992

Evolution of Safety Thinking

- Change in Emphasis
  - **Technical** – mechanical and electrical failures
  - **Human** – workload and human error
  - **Organisational** – role of management etc. in accidents
- Change in outlook
  - **Reactive** – prevent reoccurrence of previous accidents
  - **Proactive** – analyse performance to prevent impending accidents
  - **Generative** – analyse trends to enable proactive management of safety



Prescriptive vs. Risk Based Standards

- "Older" style of regulation followed **PRESCRIPTIVE** rules
  - **Regulator** prescribes particular detailed solution
  - **Duty Holder** ensures that standards are followed and produces evidence that solution has been appropriately implemented
  - Driven by accident history (Reactive)
  - Regulators actively involved in drafting (lack independence)
- "Newer" style of regulation is **PERFORMANCE** (risk based) oriented
  - **Regulator** defines overall targets
  - Nature of the technical solution is left to the operator
  - **Duty Holder** selects most appropriate methods and processes and produces valid and coherent argument of safety with supporting evidence (i.e. safety case)
  - Proactive approach
  - Regulator maintains independence

Prescriptive Standards

- Can be sufficient if:
  - There are few companies in a regulated sector
    - Regulator has good oversight of each company's activities
    - There are few differences between companies
  - Systems (technical and social "components") are relatively stable
    - High degree of confidence in prescribed solution
    - Little drive to innovate

- Unsuitable for general regulation of most sectors
  - Too many differences between products / solutions
  - Too many technologies
    - Business pressures for innovation

- Does not actually manage safety (identify and reduce risk)
- Nor does it challenge the status quo

Risk-Based Approach

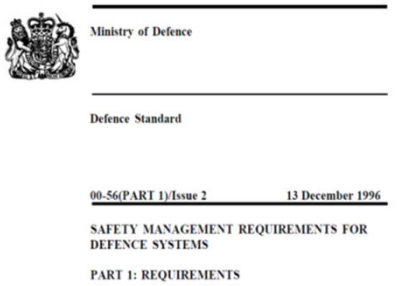
- Enables companies to develop solutions suitable for their business
  - Input from regulator is at strategic policy level, e.g. top-level goals

- Makes it clear that companies have liability
  - Not "we complied with your standards" argument

N.B. In reality, we use a combination of prescriptive and risk based approaches to safety

MOD Safety Cases

- Since Def Stan 00-56 Iss1 – April 1991
- Safety Case required –
  - "The Safety Case shall provide a well organised and reasoned justification clearly showing that ***the proposed system*** is acceptably safe."
  - Technologically focussed – "to demonstrate that the system is tolerably safe"
  - Contracted-out, supplier document
  - 'Managed' in-service
- Growing desire for Safety Cases for Legacy Systems



Ministry of Defence

Defence Standard

00-56(PART 1)/Issue 2 13 December 1996

SAFETY MANAGEMENT REQUIREMENTS FOR DEFENCE SYSTEMS

PART 1: REQUIREMENTS

Words of Warning!!

Having a Safety Case does not necessarily mean you are safe !!!!

Air Safety Case Study

NIMROD MR2 SAFETY CASE

Warning this session contains an image depicting death that some may find distressing.

Nimrod MR2 XV230

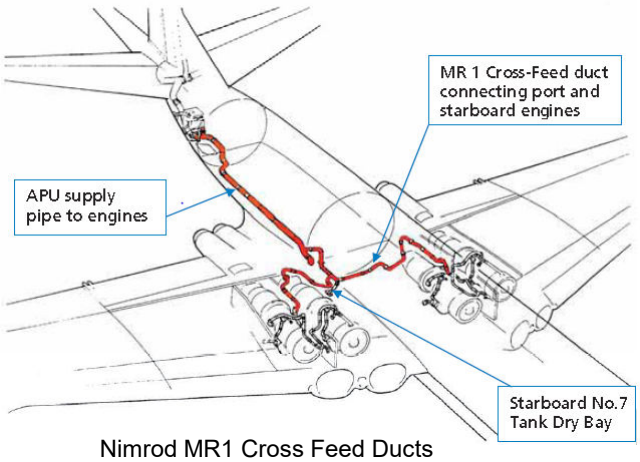
Nimrod had a 'fully substantiated' Safety Case

"ACCEPTABLY SAFE TO OPERATE & MAINTAIN UP TO RETIREMENT FROM SERVICE" 6th PSWG - 15 Dec 2004 BSC – Nimrod IPTL [Source H-C Nimrod Rpt]

The Cost – 14 Lives Lost

21

What Went Wrong?

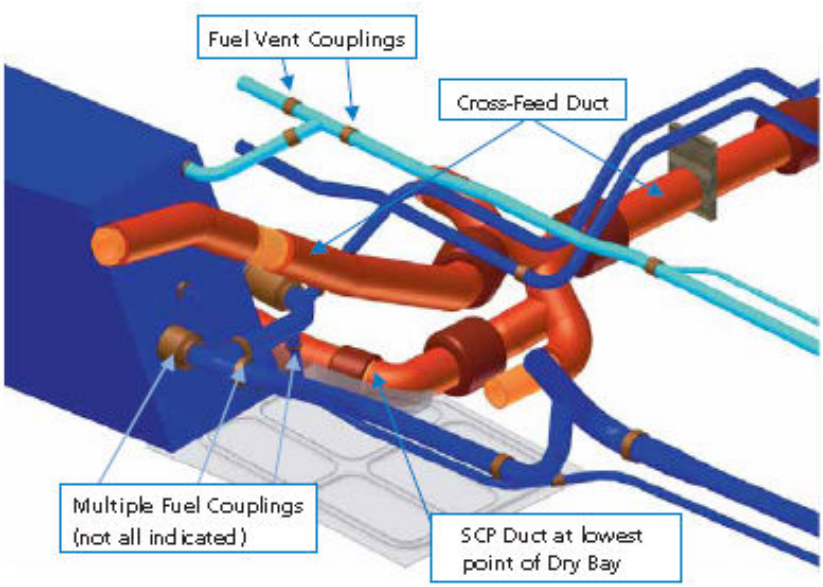


Nimrod MR1 Cross Feed Ducts

22

ASMT | Safety Case Evolution

SNC·LAVALIN ATKINS

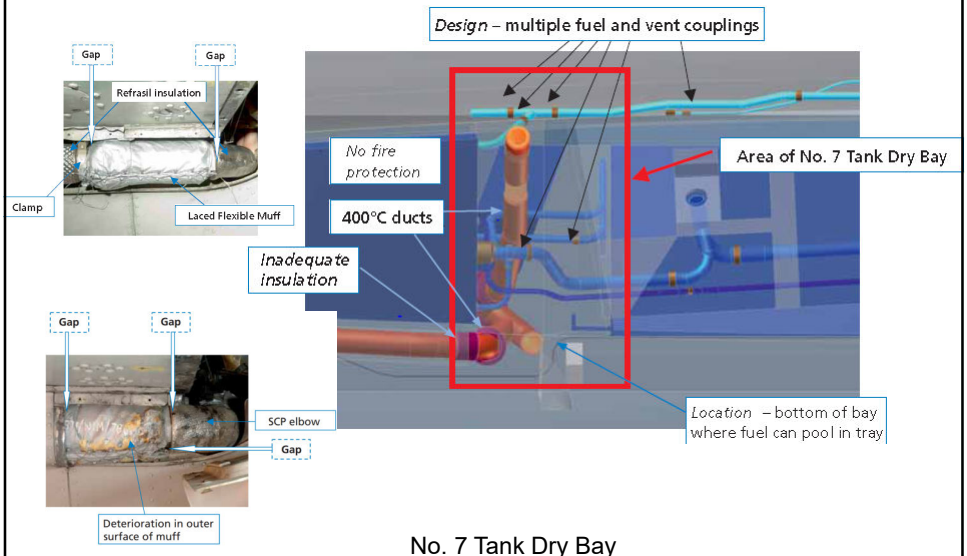


No. 7 Tank Dry Bay

ASMT | Safety Case Evolution

SNC·LAVALIN ATKINS

What Went Wrong?



No. 7 Tank Dry Bay

Summary

The Aircraft:

- Ac flying as designed
- Maintained iaw ADS
- Operated correctly
- Emergency drills carried out correctly
- But ac and all crew lost

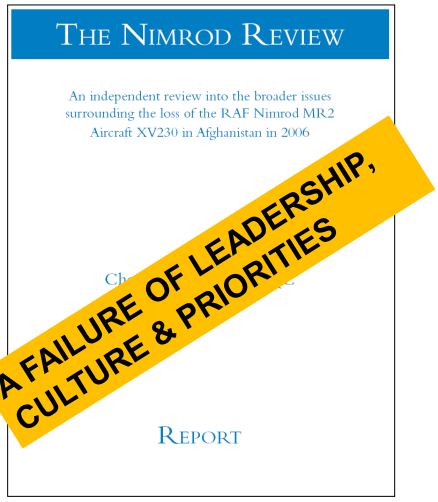
The Safety Case:

- Did not reflect as designed & built standard of ac
  - Said ac had fire detection & suppression equipment
- Did not reflect how ac was operated
  - Hot air duct only used for engine start
- Did not reflect current condition of ac
  - Duct insulation worn and had gaps.

Source: MASSC

The Nimrod Review

Charles Haddon-Cave QC



Create MAA

Recommendation 21.A.1: A Military Airworthiness Authority (MAA) shall be established as soon as practicable which comprises the single regulator authority responsible for regulating all aspects of Airworthiness across the three Services and DE&S and reporting direct to 2nd PUS.[10] The MAA shall subsume all the roles and responsibilities currently undertaken by ACAS and by: (i) the Equipment (Dir Air Systems and the MAR); (ii) Flight Operations (DARS); and (ii) Airspace Management (DAATM) Regulators and the three Services RTSAs.

Extract from Haddon-Cave Nimrod Review

Military Aviation Authority
MAA

Recommendations

WS	Title
	MAA-LED WORKSTREAMS
1	Create MAA
2	Establish Duty Holders
3	Rewrite AW regulations
4	Deliver Pan Defence Aviation Reporting System – EMS
5	Ac PT Manpower and Responsibility Review
6	Establish a new Joint Independent Accident Investigation Process
7	Airworthiness Training Review and Implementation
8	Develop Ac certification system and Safety Cases
9	Review Airworthiness of aging Ac Fleets
10	Develop MOD AW Risk Mgmt system
	CROSS-CUTTING WORKSTREAMS
11	Key Safety Principles and MOD Governance Arrangements
12	Safety Culture
13	Interfaces with Industry and Acquisition Reform
14	Safety Case
15	Personnel
16	Independent Regulation
17	Responsibility and Accountability

Have we Achieved the Learning Objective?

- To appreciate why the Safety Case approach to safety management was developed in favour of prescriptive approaches
- To appreciate the change in air safety management as a result of the Nimrod review
- Points covered by this presentation:
  - Several major disasters highlighted failings of existing regulations
  - Existing regulations failed due to over-prescriptive approach
  - Safety Case concept is now applied to most of British Industry & MOD
- Brief overview of cause and fallout from Nimrod XV230 accident

Questions?