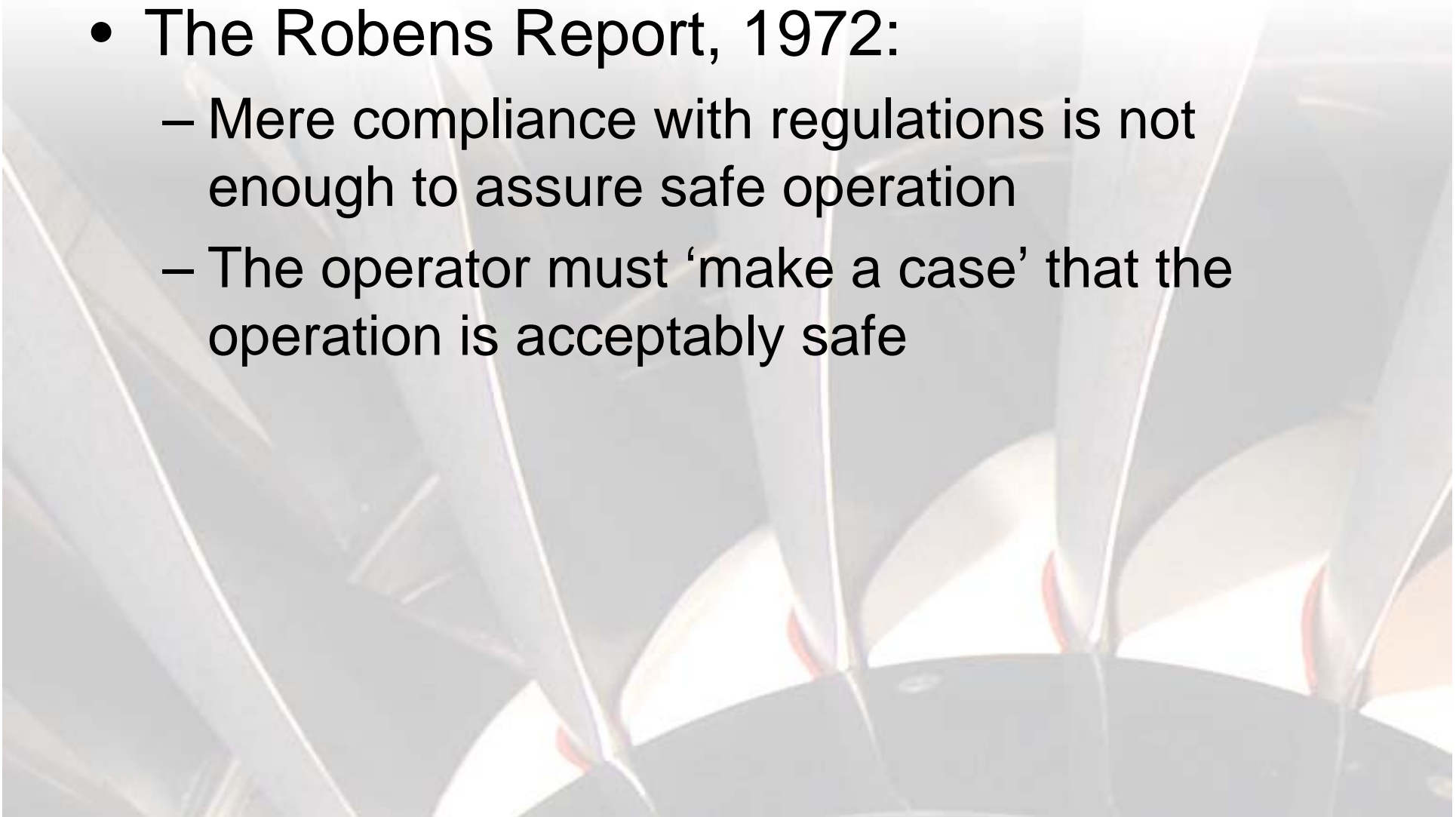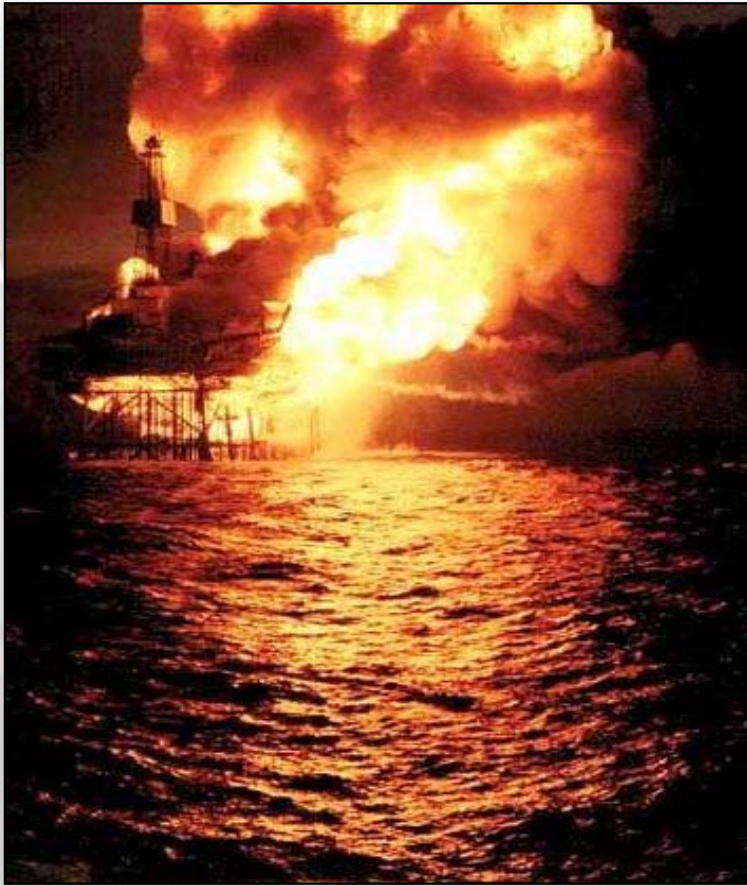# Safety Cases:
Beyond
Safety Management Systems

Dmitri Zotov

Origin of 'Safety Case'

- The Robens Report, 1972:
  - Mere compliance with regulations is not enough to assure safe operation
  - The operator must 'make a case' that the operation is acceptably safe
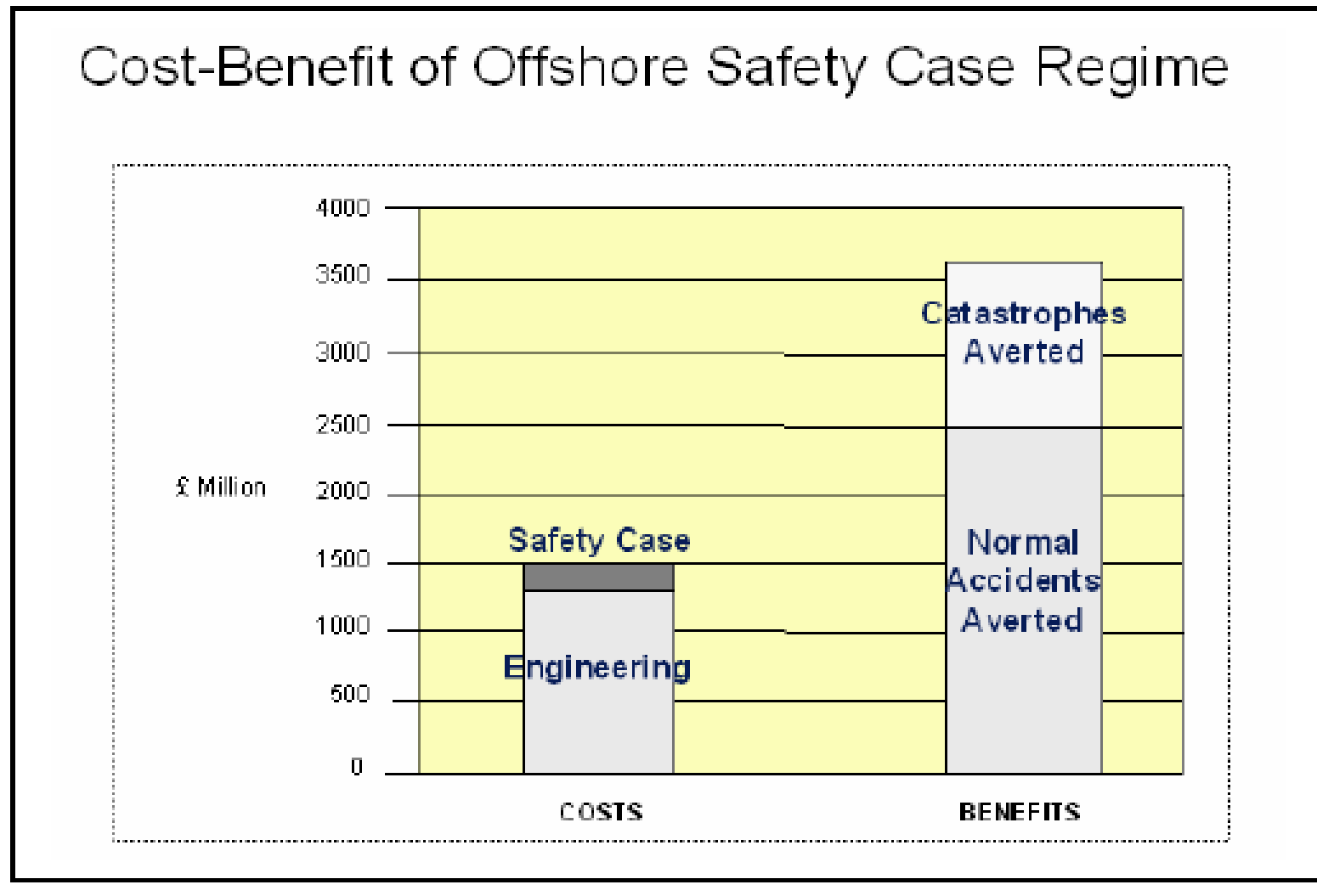
Why a Safety Case? Piper Alpha

- On 6 July 1988, a series of explosions and fires destroyed the Piper Alpha oil platform and killed 167 people.

- The modern Safety Case has been influenced by the recommendations of the Cullen Inquiry into the Piper Alpha disaster.

- Lord Cullen noted in his report that compliance with detailed prescriptive regulations was not sufficient to ensure safety.

- Safety Case needed to be owned by the operators and was to be a "living document".
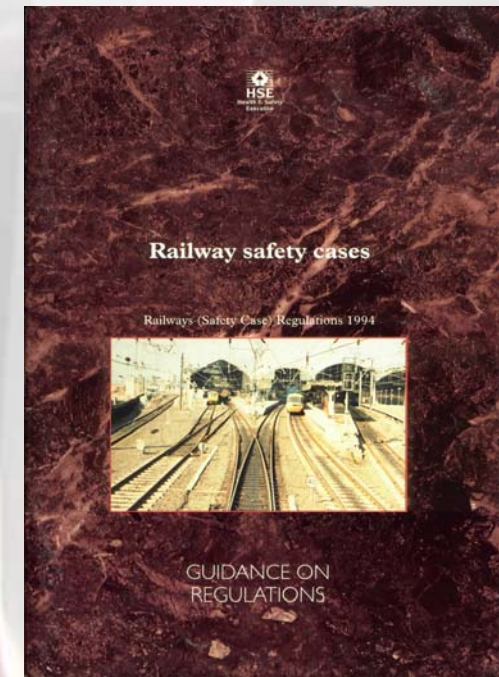
Modern Offshore Safety Management Practices

- Operator responsible for safety.

- Responsibility to demonstrate case for safety via a performance based Safety Case – that is, demonstrate fitness for its intended context of use.

- Use of formal and structured hazard identification and analysis techniques.

- Results of hazard analysis used to drive design.

Benefits of a Safety Case Regime

Source: DNV

History Of Safety Cases And Regulation -
Typical UK Reactive Sequence
Accident - Enquiry - Act of Parliament - Guidance

Potential Problems

- Cost
- Ownership
- Competency
- Move to non-prescriptive regulation

Safety Cases in Civil Aviation

- Part Safety Cases:
  - Eurocontrol: RVSM
  - UKCAA: unusual operations
- Delayed introduction of a full Safety Case regime:
  - Absence of formal Inquiries in recent years
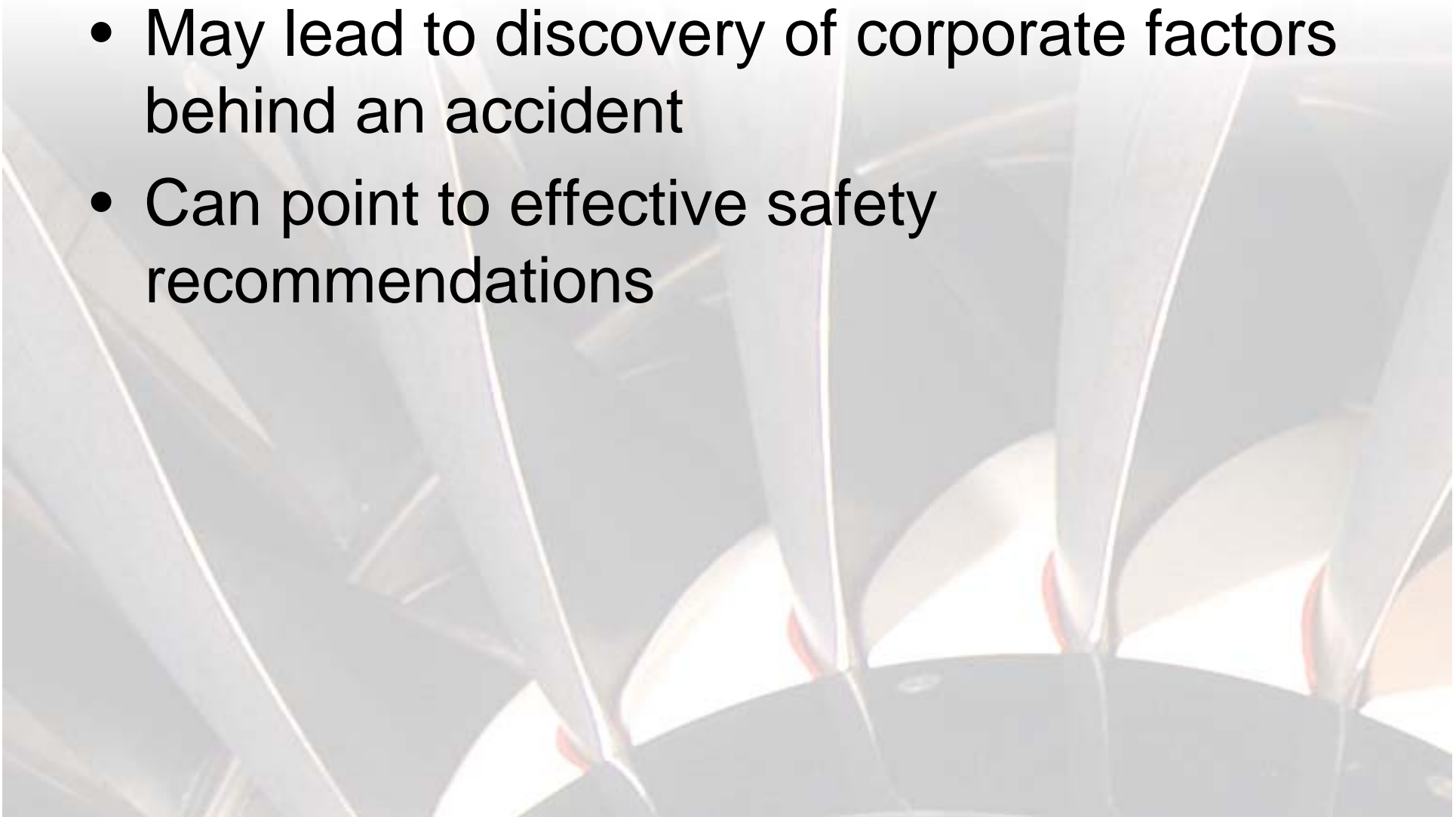 - Emphasis on SMS

Safety Case or Stand-alone SMS?

- A Safety Case is analogous to a Business Plan
- An SMS is analogous to a FMS
- An FMS won't buy you much without a Business Plan
- An SMS won't but you much without a Safety Case
- ***An SMS is part of a Safety Case***

Safety Cases in Civil Aviation

- Eurocontrol
  - Partial Safety Cases, e.g. RVSM
  - Draft Safety Case manual
- UK CAA
  - Safety Cases required for Aerodromes and Air Traffic Services
  - Under consideration for flight ops and maintenance
- FAA
  - Guidance on Safety Cases for airworthiness standards (followed by ADF)
- Australia
  - CASA :- NAS
  - Air Services:- RVSM

Why It Matters to Investigators

- May lead to discovery of corporate factors behind an accident
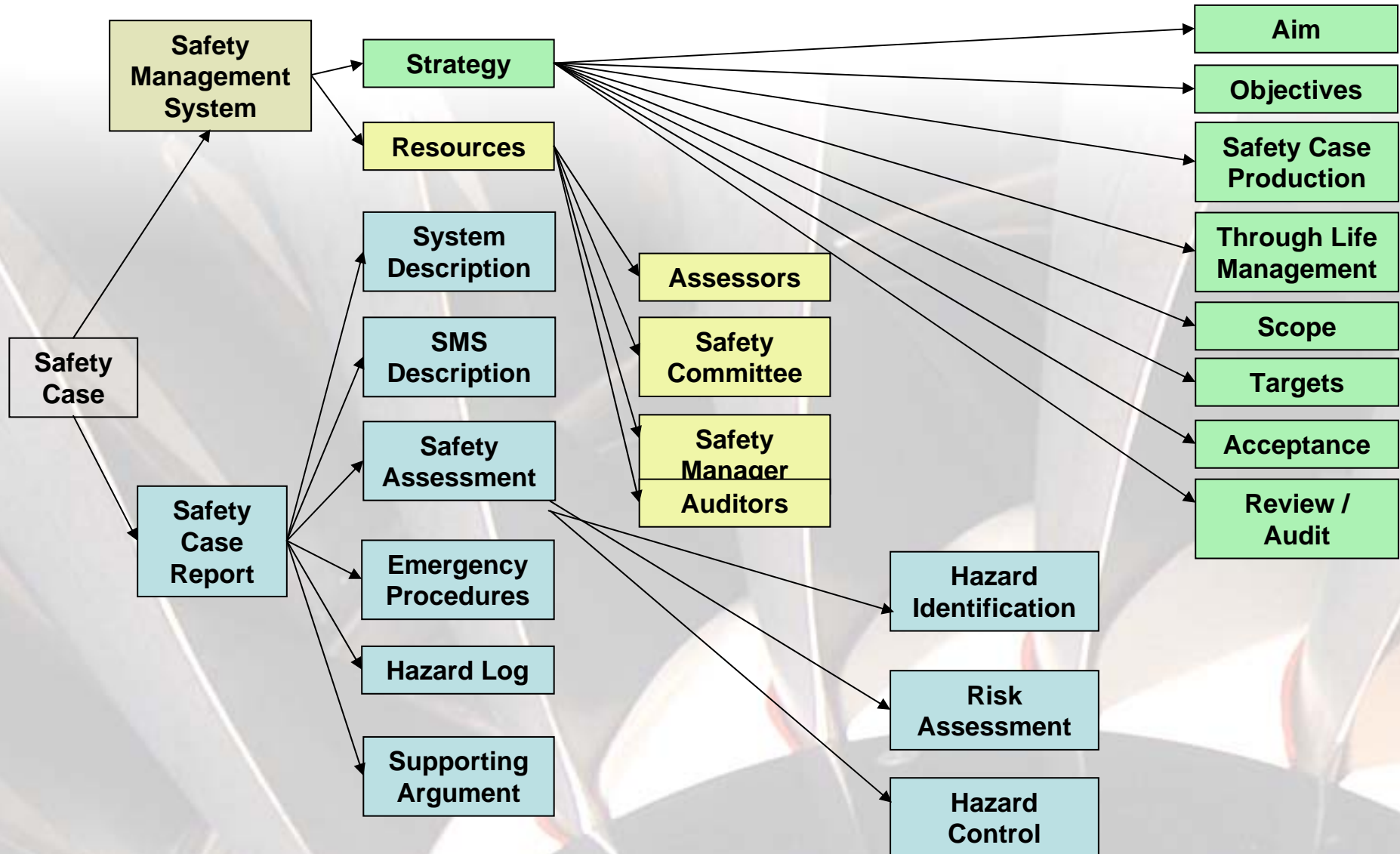- Can point to effective safety recommendations

The Ansett Case Study

- TOC analysis led to a very few core problems, but a large number of recommendations to address them
- All of the recommendations relating to the airline could be distilled into
  - Airlines should be compelled to operate within a Safety Case

What Is A Safety Case?

– "A documented body of evidence that provides a demonstrable and valid argument that a system or equipment is tolerably safe for use: within a defined envelope, throughout the proposed life of the equipment". (UK MoD JSP 430).

- The body of evidence that the system is safe, together with the argument that makes sense of the evidence.

• No reference to Regulatory compliance: the exact opposite to an Exposition.

Structure Of A Safety Case

Exposition, SMS and Safety Case

Exposition:

Term used by NZ CAA, and EASA (Maintenance regulations only)

A document

- Demonstrating compliance with Regulations
- Detailing Company structure, and
- Procedures which will be followed

Underlying Assumption: that compliance with the Regulations will assure safety

Exposition, SMS and Safety Case

Safety Management System:

- A function of service provision which ensures that safety risks have been identified, and the hazards driven down as far as reasonably practicable

- Assumption behind stand-alone system: that operating with a SMS, within a regulatory structure, will assure safe operation
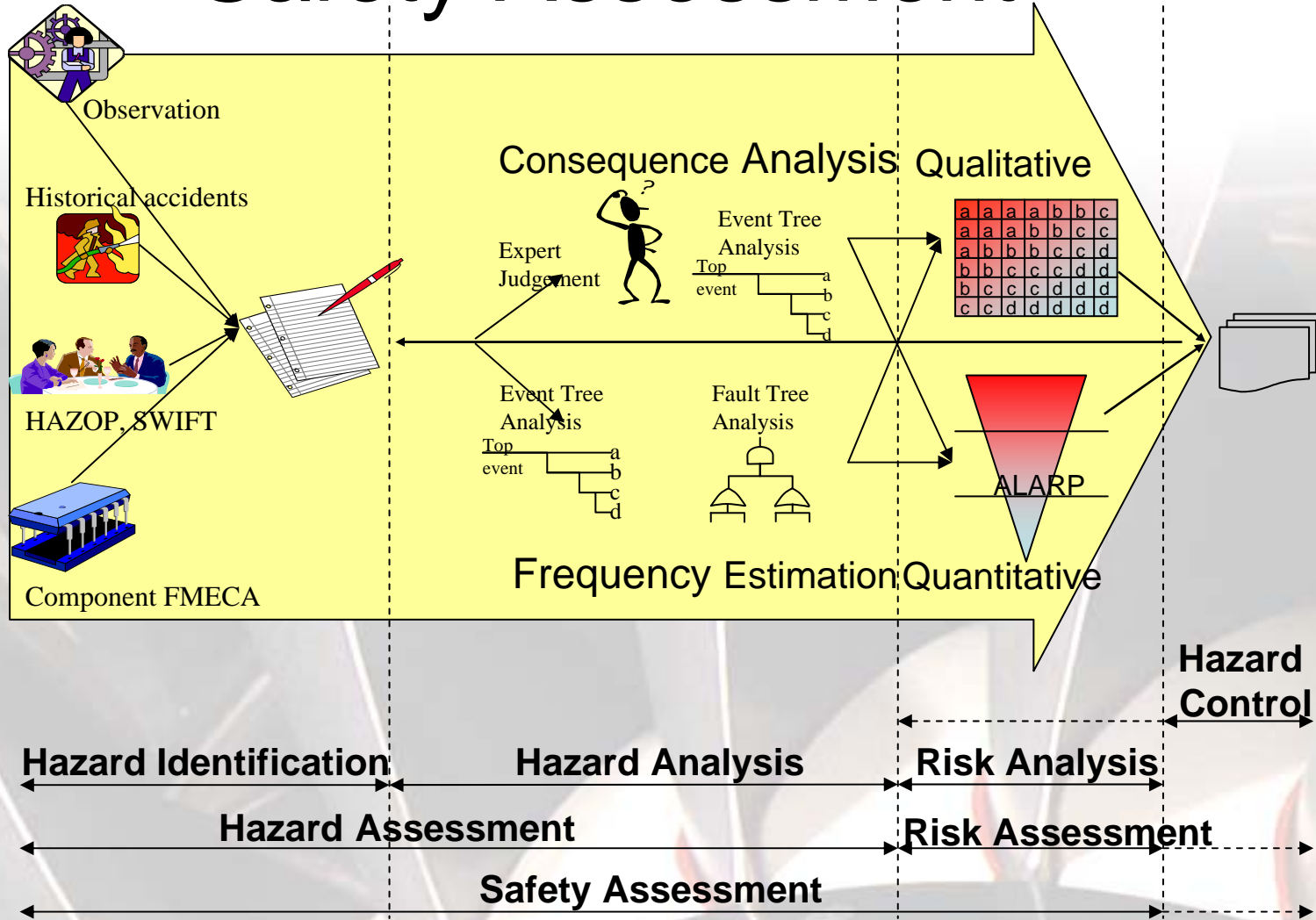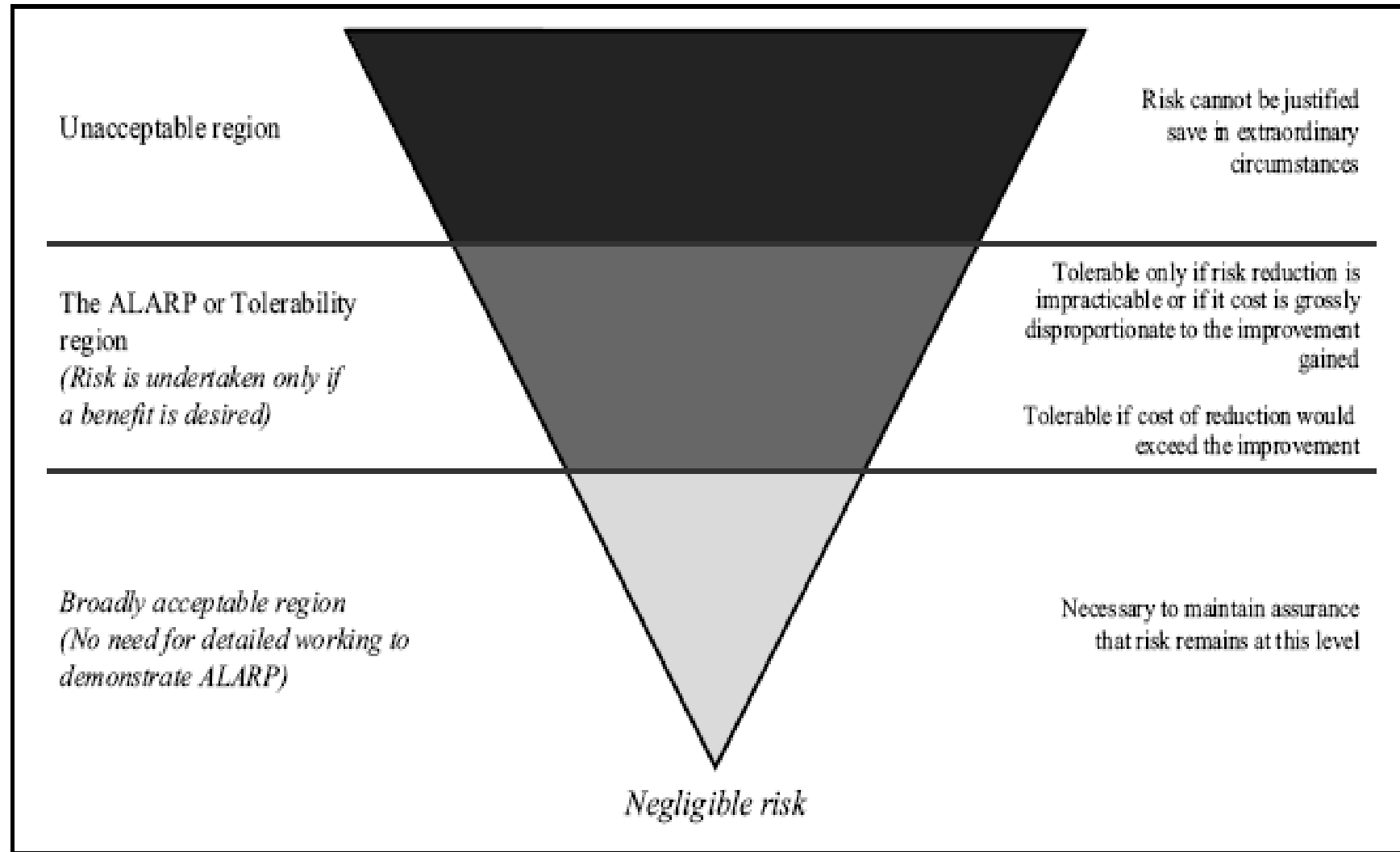
Safety Case, Exposition and SMS

Examining a Safety Case

- Documentation:
  - Organisation Description/Intent
  - Operating History and Incidents
  - Safety Cases and Hazard Assessments (components)
  - Emergency and Contingency Arrangements
- Argument showing that evidence proves safe operation
- Safety Management System
- Risk assessment and review

Safety Assessment

Observation

Historical accidents

HAZOP, SWIFT

Component FMECA

Consequence Analysis Qualitative

Expert Judgement

Event Tree Analysis
Top event
a
b
c
d

Event Tree Analysis
Top event
a
b
c
d

Fault Tree Analysis

a	a	a	a	b	b	c
a	a	a	b	b	b	c	c
a	b	b	b	b	c	c	d
b	b	c	c	c	d	d
b	c	c	c	d	d	d
c	c	d	d	d	d	d

ALARP

Frequency Estimation Quantitative

Hazard Control

Hazard Identification   **Hazard Analysis**   **Risk Analysis**

Hazard Assessment   **Risk Assessment**

Safety Assessment

As Low As Reasonably Practicable

Unacceptable region — Risk cannot be justified save in extraordinary circumstances

The ALARP or Tolerability region
(Risk is undertaken only if a benefit is desired) — Tolerable only if risk reduction is impracticable or if it cost is grossly disproportionate to the improvement gained — Tolerable if cost of reduction would exceed the improvement

Broadly acceptable region
(No need for detailed working to demonstrate ALARP) — Necessary to maintain assurance that risk remains at this level

Negligible risk

Setting ALARP Levels

UK Rail has set target levels in two ways:

- Small operator: qualitative
- Large operator: quantitative

Eurocontrol has set quantitative levels:
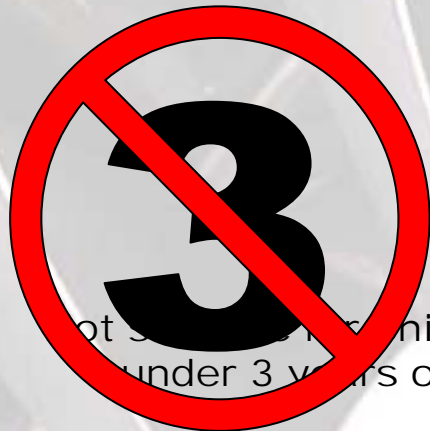
- Intolerable: 2 x TLS
- Acceptable: .02 x TLS

A Safety Case needs to be Pragmatic

A Safety Case needs to be Pragmatic

Summary

- Safety Case to prove operations are adequately safe is world's best practice
- Being progressively mandated in hazardous industries world-wide
- In accident investigation, comparing the Safety Case with reality can give clues to what went wrong
- Safety Recommendations made in terms of modifying a Safety Case may have generic application