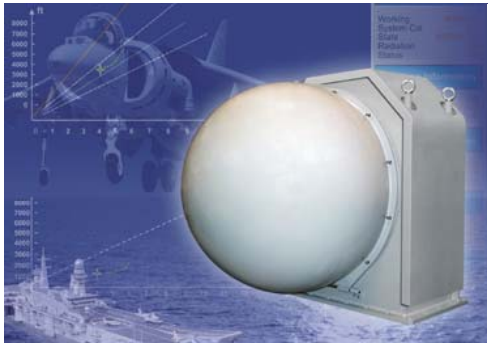
Assuring Operational Systems – - a Safety Case Study

Simon Di Nucci

System Software Technology Conference 2008

QinetiQ

Presentation Contents



QinetiQ

01 Scenario – a Safety Case

Standard practice in the UK Ministry of Defence is to assure equipment quality by generating a compelling case to support claims that specific requirements are met. An example of this is a ***Safety Case***:

"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 operating environment."

02 The Task

We were asked to assure the safety of a system for guiding aircraft onto ships in bad weather. This was to consider the whole ship/equipment/aircraft system of systems, taking into account:

- Human factors.
- The operating environment.
- Operating procedures.
- Maintenance & Management.

An Operational Safety Case (OSC) was needed.

03 Requirements

The System was being procured to enhance the capability of Aircraft operating from Ships. The System consisted of:

- A navigation Beacon, to locate the ship.
- A Radar to guide the Aircraft's approach to the Ship.

We were to assess the safety of Aircraft operating from the Ship:

- When shore-based diversion airfields were available.
- When no diversions were available.

03 Requirements – Risk Targets

	Catastrophic	Critical	Marginal	Negligible
Frequent	A(1)	A(3)	A(7)	B(13)
Probable	A(2)	A(5)	B(9)	C(16)
Occasional	A(4)	B(6)	C(11)	C(18)
Remote	B(8)	C(10)	C(14)	D(19)
Improbable	C(12)	C(15)	D(17)	D(20)
Incredible	C(21)	D(22)	D(23)	D(24)

04 Problems to Overcome

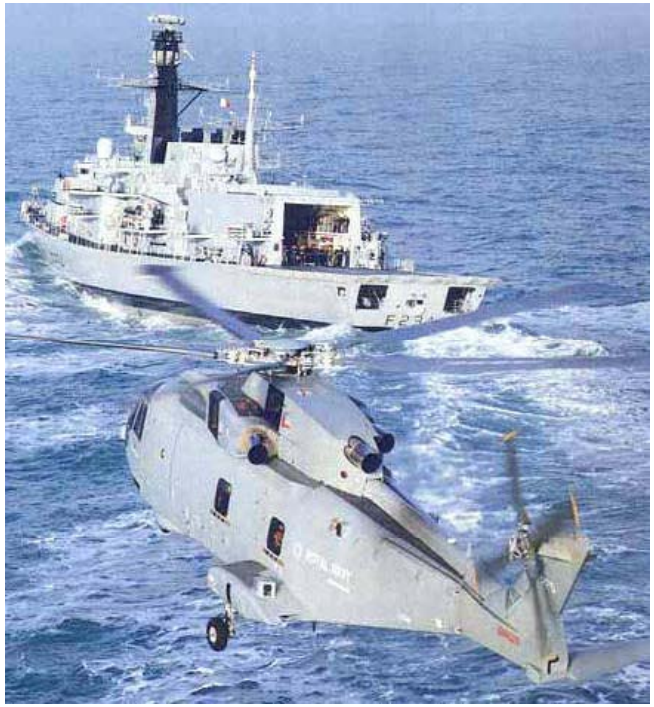
The Radar and Beacon had equipment safety cases, but:

- They did not consider operational issues (e.g. procedures).
- Each equipment was assessed in isolation.

In particular the Radar equipment safety case predicted that the Radar software would need to have a specific Software Integrity Level, but:

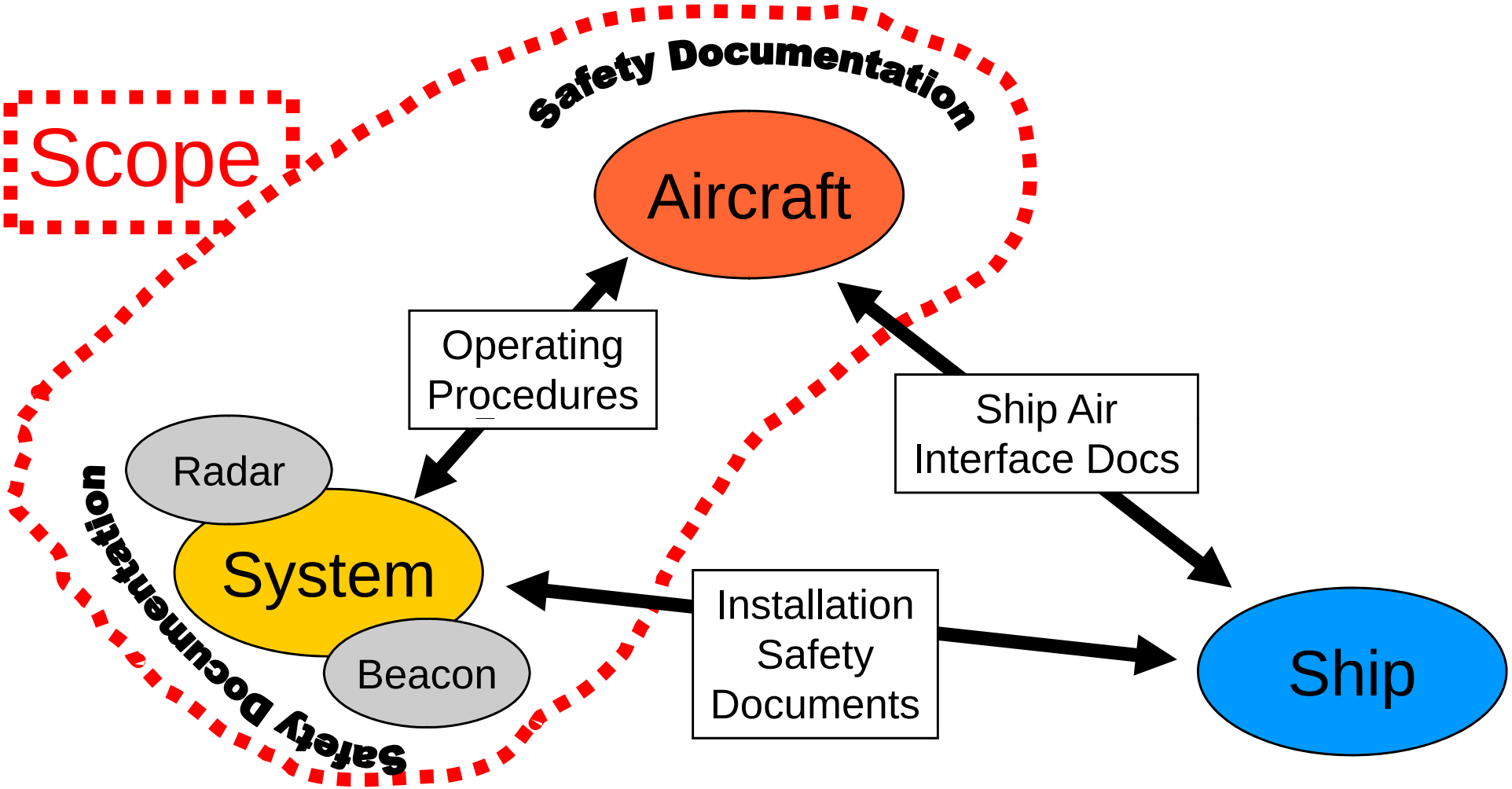
- We could not find enough analysis or evidence to confirm this.
- The Radar was a ‘COTS’ product, so it could not be changed.

05
Approach to the Task

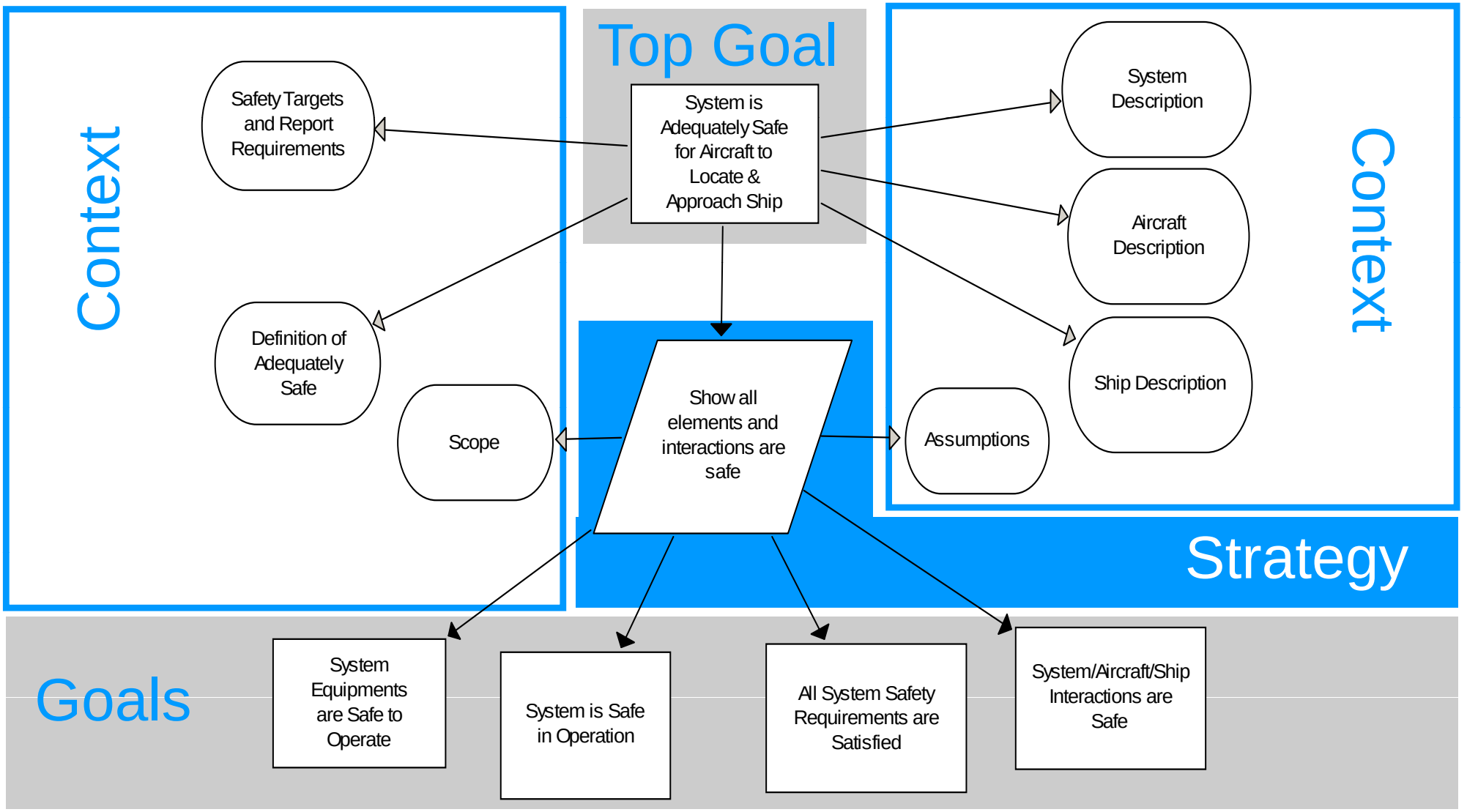


(N.B. We do not sell any of the tools mentioned in this presentation.)

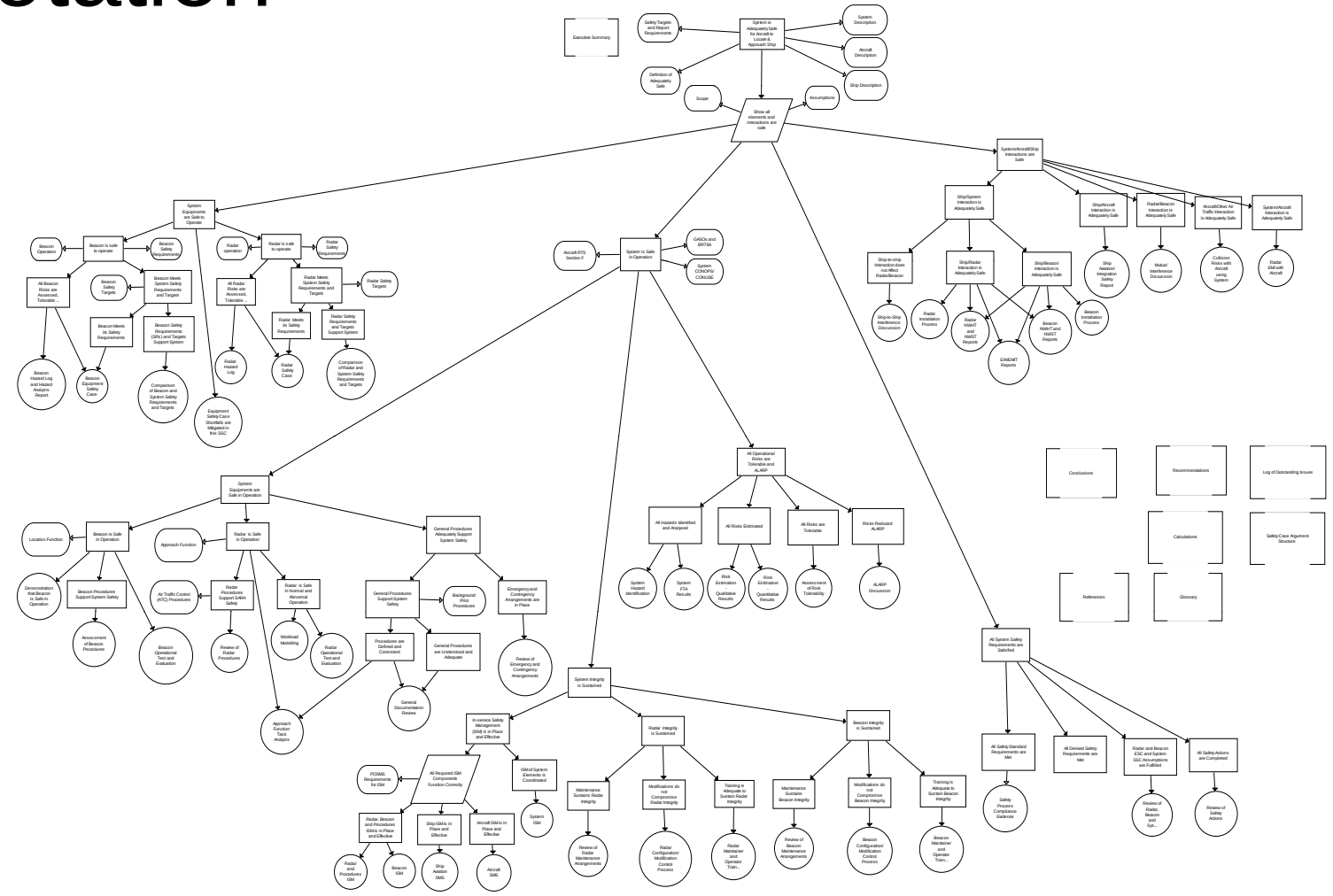
05 Approach - Scope of the OSC



05 Approach - OSC Safety Strategy

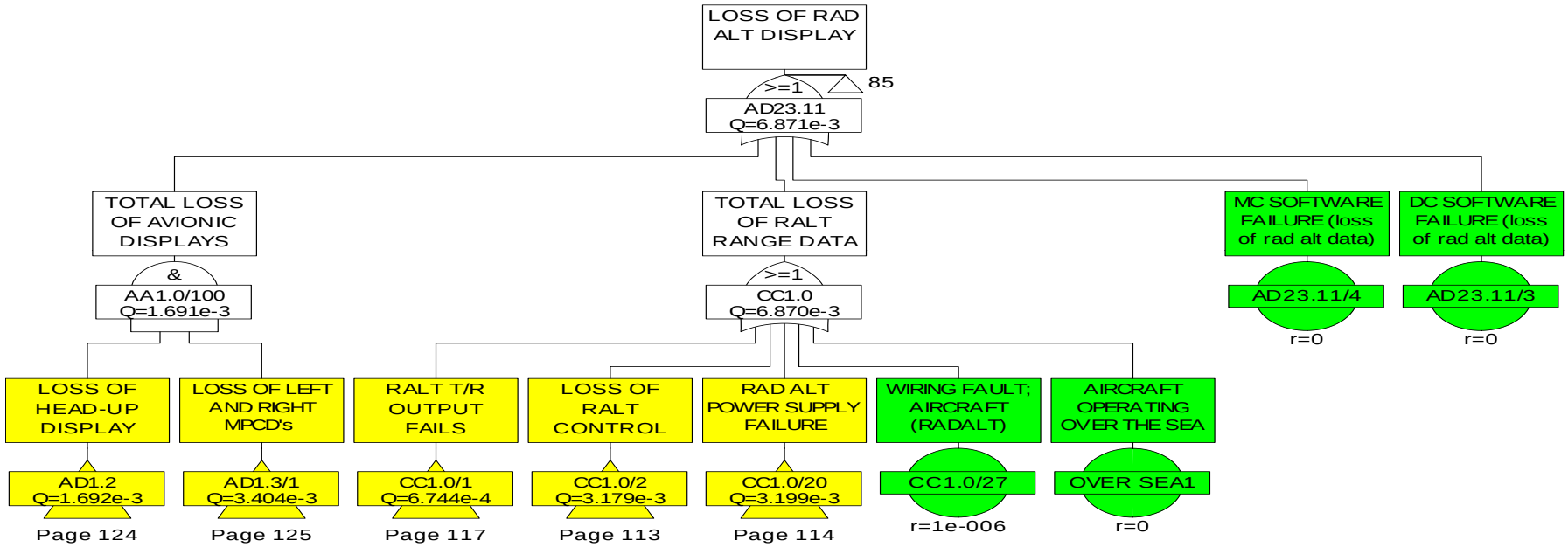


05 Approach – Goal Structuring Notation



05 Approach – Fault Tree Analysis

- Common technique in system safety engineering.
- Used to show how failures contribute to safety hazards and thence to accidents (a 'loss model').
- Equipment, documentation and human failures included.



05 Approach – Human Performance Modelling

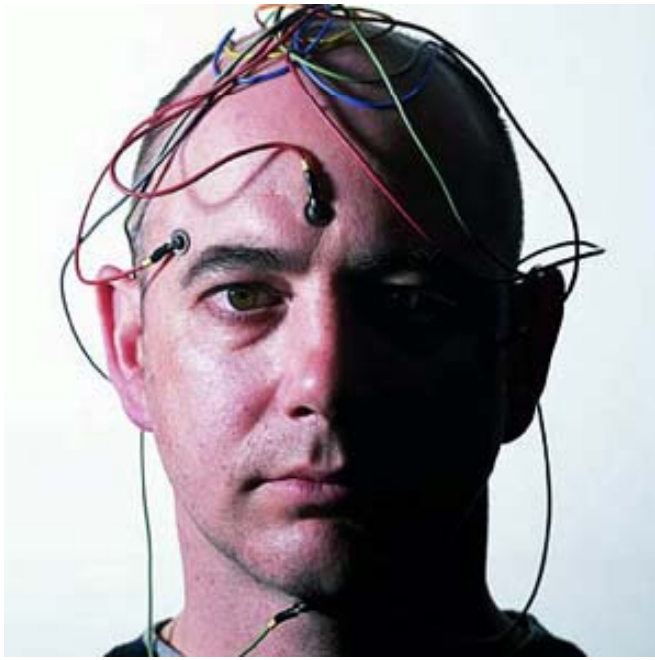
The Pilot and Talk Down Controller tasks were captured in Task Analysis diagrams.

An Integrated Performance Modelling Environment was used to combine, for each TA element:

- A UK MOD ‘Workload Scale’ or rating system.
- A predictive algorithm using the WS ratings.

Then 1000 runs of each complete TA were performed to generate the results.

05
Results



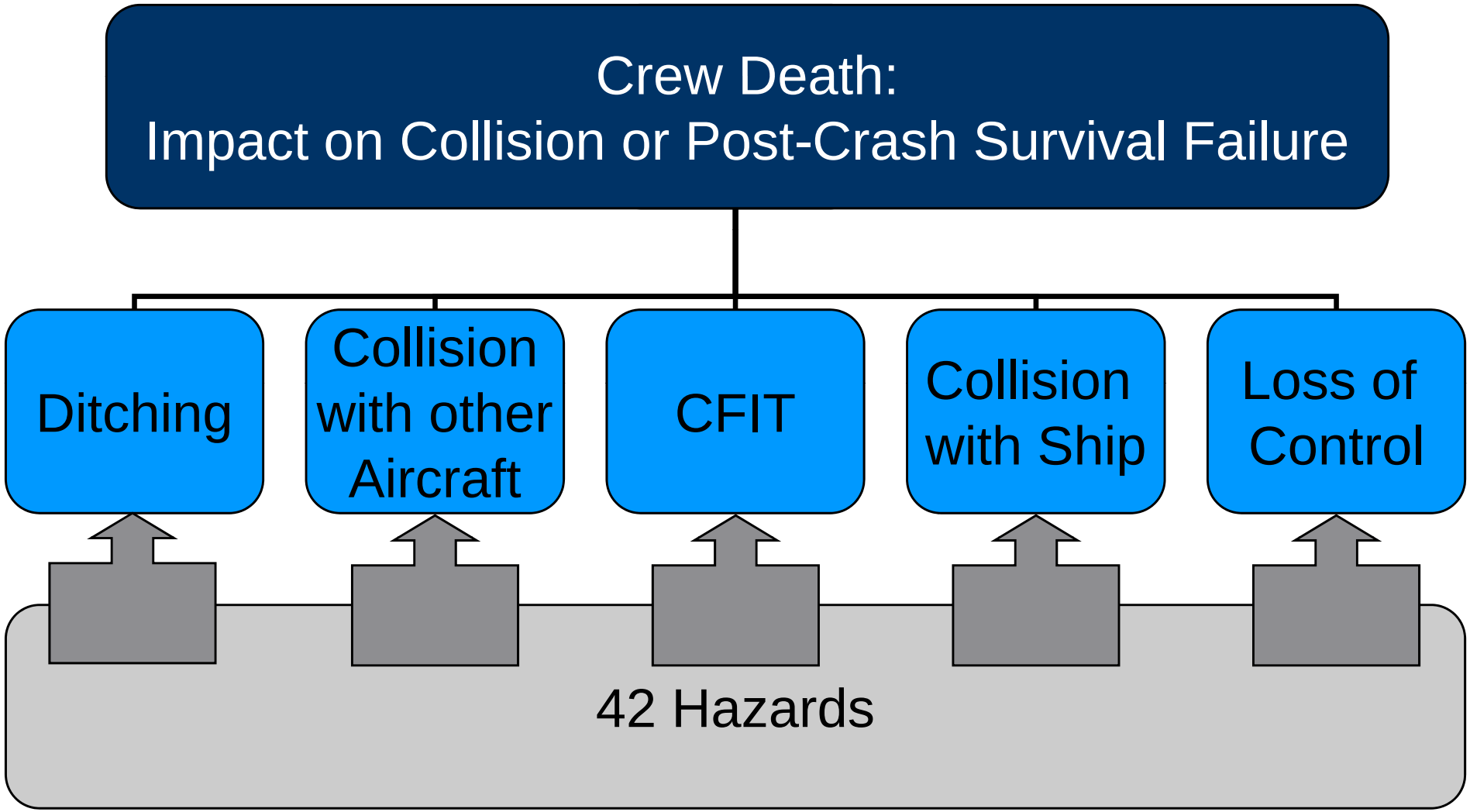
05 Results – Human Factors

Workload	Old Radar	New Radar	Increased workload?
Pilot	82%	75%	No
Controller	53%	33%	No

Pilot and Controller workload was also considered during abnormal operations, such as Radar, Beacon or Aircraft equipment failures.

There was no increase in workload with the new Radar for any abnormal operations.

05 Results – Risk Estimation



05 Results - Risks are Tolerable

Accident Description	Accident Rate and Assessment			
	Diversion Avail		No Diversion	
	Per Fleet FH	HRI	Per Fleet FH	HRI
Crew die in impact on collision	7.16E-08	D	1.28E-06	C
Crew drown or die of exposure due to survival failure	3.95E-11	D	1.67E-08	D

05 Results - Summary

Conclusions:

- The System of Systems (SoS) was safe, because:
  - Each element was safe to operate.
  - ***The whole SoS was safe in operation****.
  - All safety requirements were met.
  - All interactions between elements were safe.
- *** The Human Factors and other work confirmed the assumptions in the Fault Trees.
- *** The Radar software did not need to be of any particular Safety Integrity Level (SIL).

06
Lessons Learned

06 Lessons Learned – the Task

- The SoS application and operating environment needed to be better defined.
- An In-service Safety Management System (SMS) was needed for the SoS, especially coordination of elements.
- Maintenance, personnel and training were needed to ensure assumed availability of all elements achieved.
- Complete evidence for safe interactions of some elements should be provided (priority of testing at SoS level).

06 Lessons Learned – Wider

We could assess not just safety but any quality or attribute of a system in this way, provided that we:

- Have a definition of the quality or attribute (for Scope).
- Have defined targets (have we met them: ‘Yes’ or ‘No’?).
- Have logical arguments to support our claims.
- Have evidence to support our arguments.
- Have tools and techniques that allow us to communicate (the complexity of) all of the above.

Assuring Operational Systems – - a Safety Case Study

QinetiQ

The Global Defence and Security Experts

Any Questions?