Requirements and Safety Cases

Prof. Chris Johnson,
School of Computing Science, University of Glasgow.
johnson@dcs.gla.ac.uk
http://www.dcs.gla.ac.uk/~johnson

University of Glasgow

Introduction

- Safety Requirements:
  - Functional and non-functional requirements.
- Safety Cases:
  - Arguments about acceptable safety;
  - Experience from NASA contractors work.
- The Haddon Cave Report:
  - Questioning culture of tick-box exercises.

University of Glasgow

Requirements Engineering

- See software engineering courses.
- Stage 1: Functional requirements analysis:
  - What a system should do not how;
  - What functions must it computer/perform?
- Stage 2: Non-functional analysis:
  - Safety requirements analysis (eg 61508);
  - Usability engineering;
  - Security assessment.

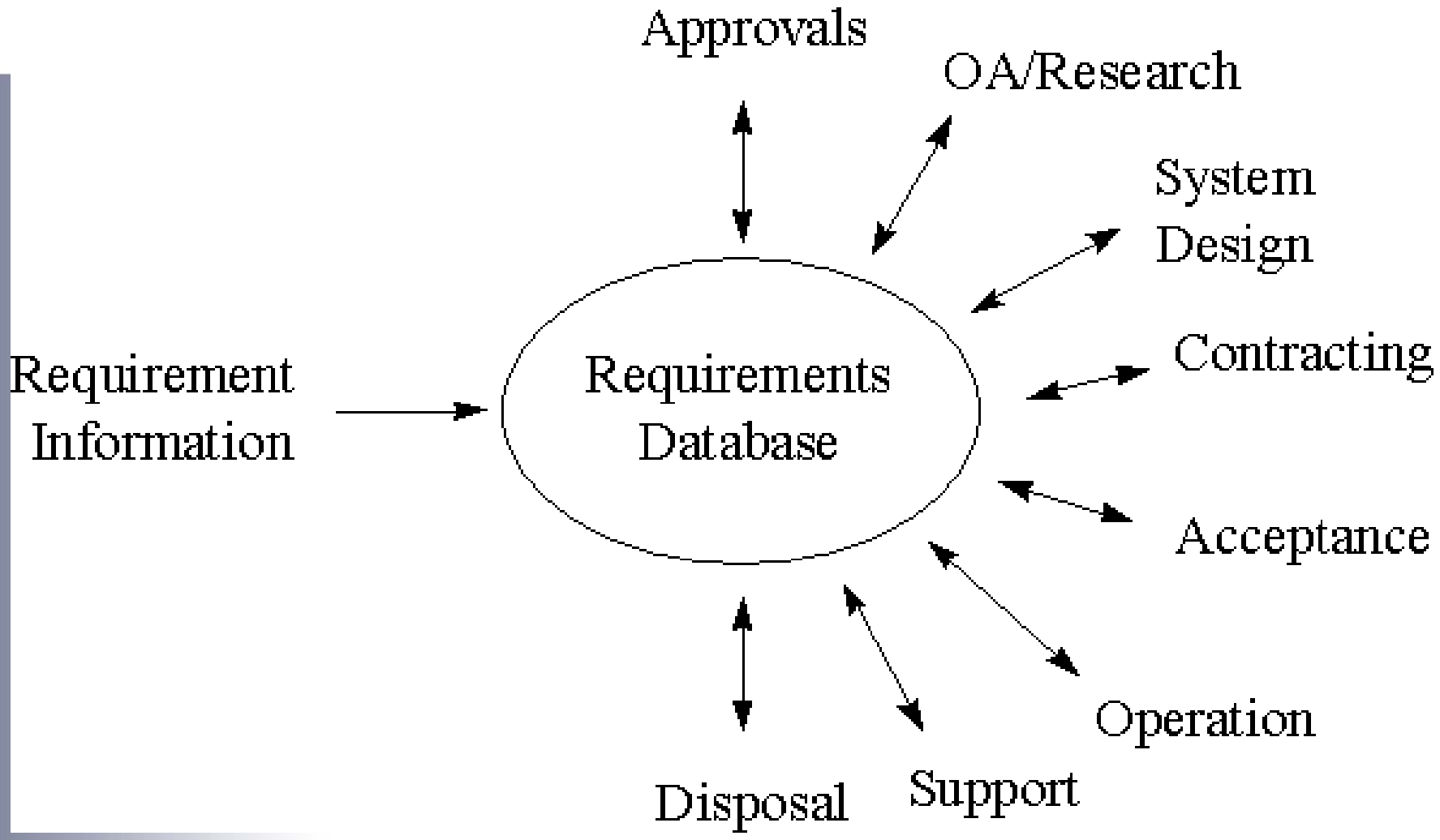
University of Glasgow

Requirements Analysis

- Requirements written in a specification.
  - Informal, semi-formal, formal?
- Verification:
  - does system meet requirements?
- Validation:
  - are requirements appropriate?
- Please remember the difference for exam.

University of Glasgow

MOD ‘Smart’ Procurement Initiative



University of Glasgow

MOD ‘Smart’ Procurement Initiative

Specify Non-Functional Requirements.

Non functional requirements are constraints on the system design. They may arise from user requirements, technical disciplines or the external environment:

- reliability
- maintainability
- operability
- safety
- security
- engineering standards
- environment
- support

University of Glasgow

MOD ‘Smart’ Procurement Initiative

Non-functional requirements are often expensive but add quality.

Early identification will avoid costly changes and facilitate the trade-off process leading to a cost-effective solution.

Blanket application of individual non-functional requirements will be unnecessarily costly and should be avoided.

They should be identified against and linked to the lowest level function in the decomposition to which they specifically apply.

Non-functional requirements should also be expressed as unique statements of requirement with the same attributes as system functions.

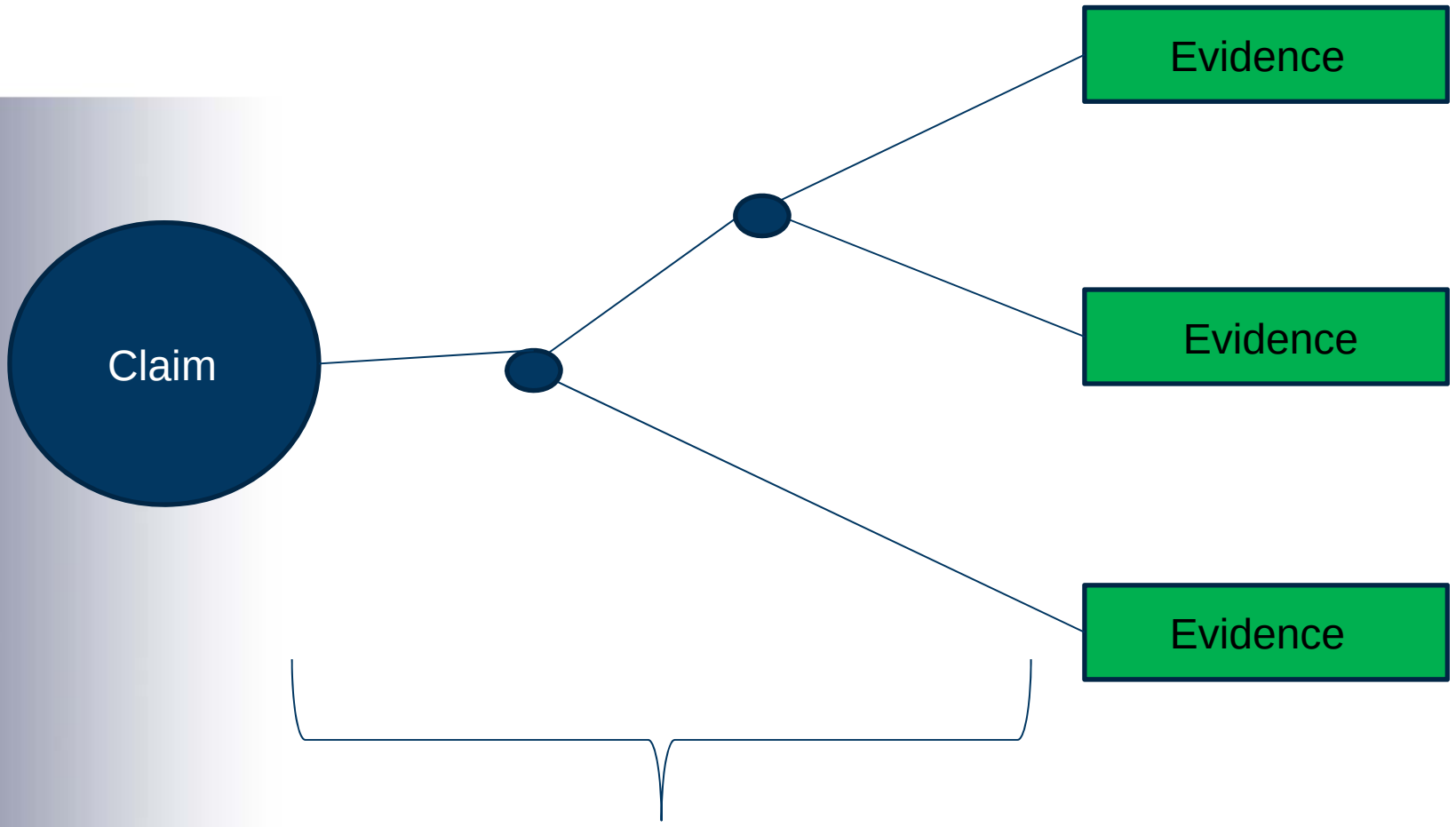
University of Glasgow

Requirements Analysis

- Requirements - what a system does.
- But regulators want more.
- Why is a system acceptable?
  - need for a SAFETY CASE.
- Based around an argument;
  - Cannot prove system is safe;
  - Testing will not do it;
  - Formal analysis also has limitations…

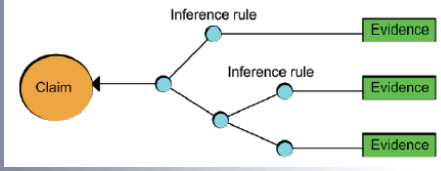
University of Glasgow

Overview of Safety Cases...



Making Arguments Explicit

- Key idea is to write down arguments.
- Safety as a dialogue:
  - Create an argument;
  - Expose it to adversarial challenge;
  - Revise the argument...
- Integration & Safety Management Systems
  - Revise evidence and arguments;
  - Based on incident and accident reporting;
  - Importance of maintaining safety case...



Definitions

- "A *documented body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment" ASCAD Manual, 1998*

- 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. Def Stan 00-56 issue 4

University of Glasgow

Definitions

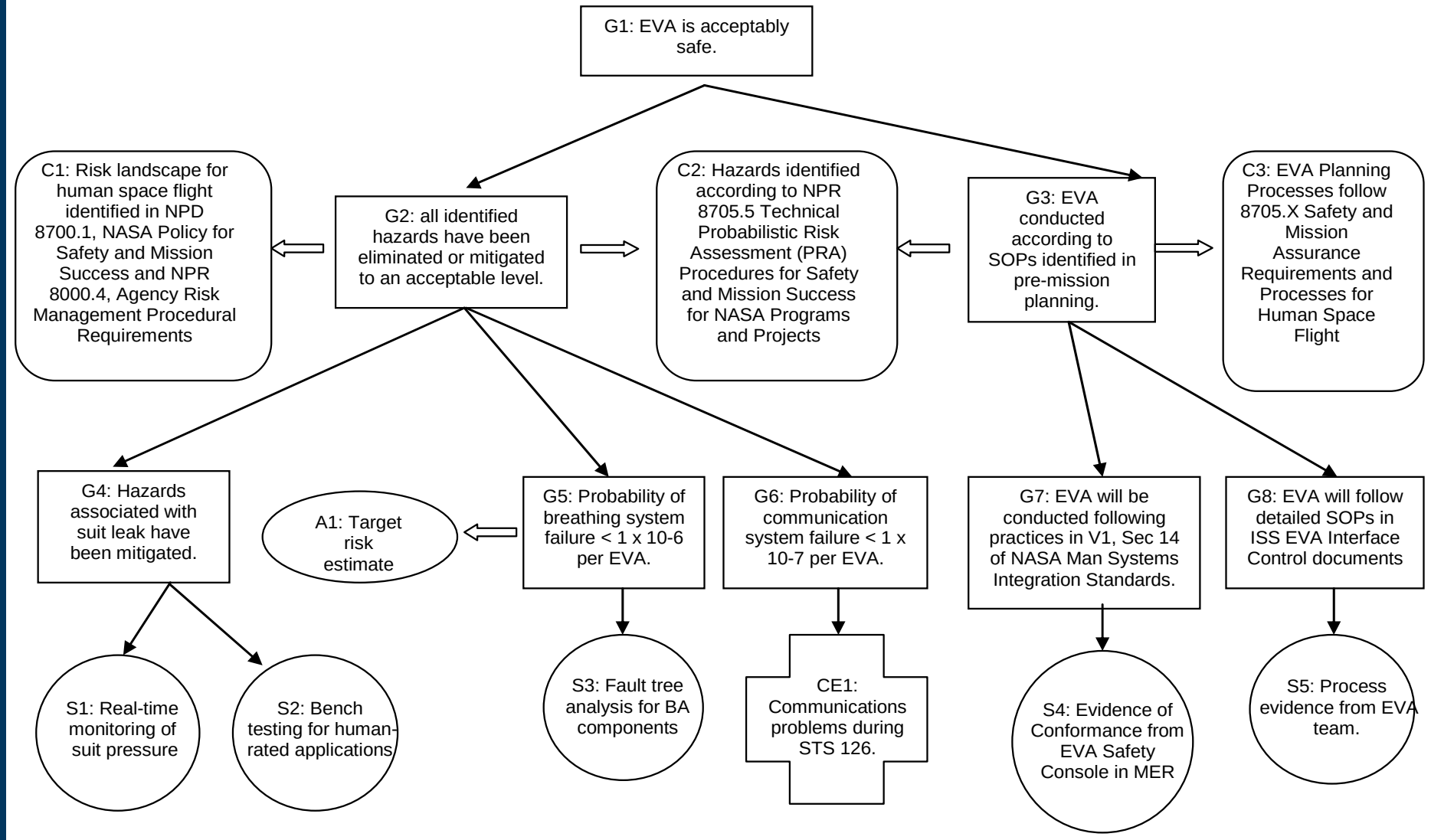
- A security assurance case uses a structured set of arguments and a corresponding body of evidence to demonstrate that a system satisfies specific claims with respect to its security properties. ISO 15026

- A formal presentation of evidence, arguments and assumptions aimed at providing assurance that a system, product or other change to the railway has met its safety requirements … Yellow Book

US Influences… Derek: SAIC/NASA-> Oil

- The U.S. Department of the Interior's recent recommendations to improve deepwater drilling in the Gulf of Mexico included instituting a safety case regime

International Space Station EVA Example



Medium Term Influences on Space Industry

- Financial stringency:
  - Cancellation of NASA Constellation;
  - Reduce commercial space subsidies $6b to $3b
  - ESA spending frozen €3.7 billion p.a.
- Impact on safety management systems…
- Safety cases have many benefits:
  - Map safety over commercial and govt bodies;
  - ** Map impact of cuts eg on evidence from testing.

Myths about the Use of Safety Cases 1

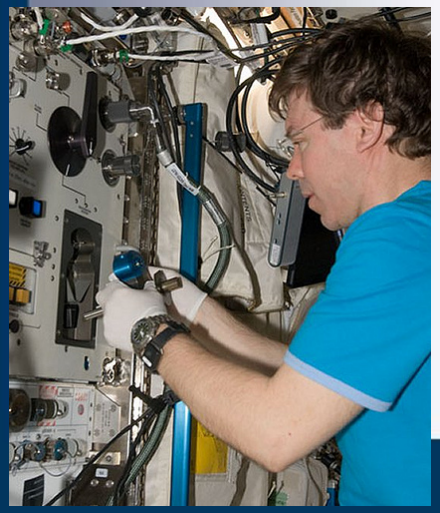
- ‘They are going to become obligatory?’
  - Reflects concerns over existing techniques;
  - Reflects concerns over NASA/ESA financial cuts.
- How can we explain this?
  - Engineers expecting new tools to be imposed!!!
  - Problems of communication;
  - Between management and safety teams;
  - Uncertainty at time of organisation change…

Myths about the Use of Safety Cases 2

- ‘We can save money across SMS?’
  - Safety budgets hard to defend…
- How can we explain this?
  - Hard to see how the idea grew up…
  - Could help reduce documentation overheads?
  - Safety case management can add high costs;
  - They can act as a barrier to innovation?

Myths about the Use of Safety Cases 3

- ‘We can spend less on risk assessments?’
  - See lectures on 61508 and later on FMECA etc
- How can we explain this?
  - Could use safety cases to find replication/waste…
  - Could use safety cases to prioritise spending…
  - Or recognition that risk assessment not working?
  - Software and human reliability key to space future



Myths about the Use of Safety Cases 3

- "We do not have to provide other deliverables if we provide you with the safety case...."
- Partly true...
- They link evidence to arguments:
  - You can see the need for evidence;
  - But you also need to check evidence exists...

Myths about the Use of Safety Cases 4

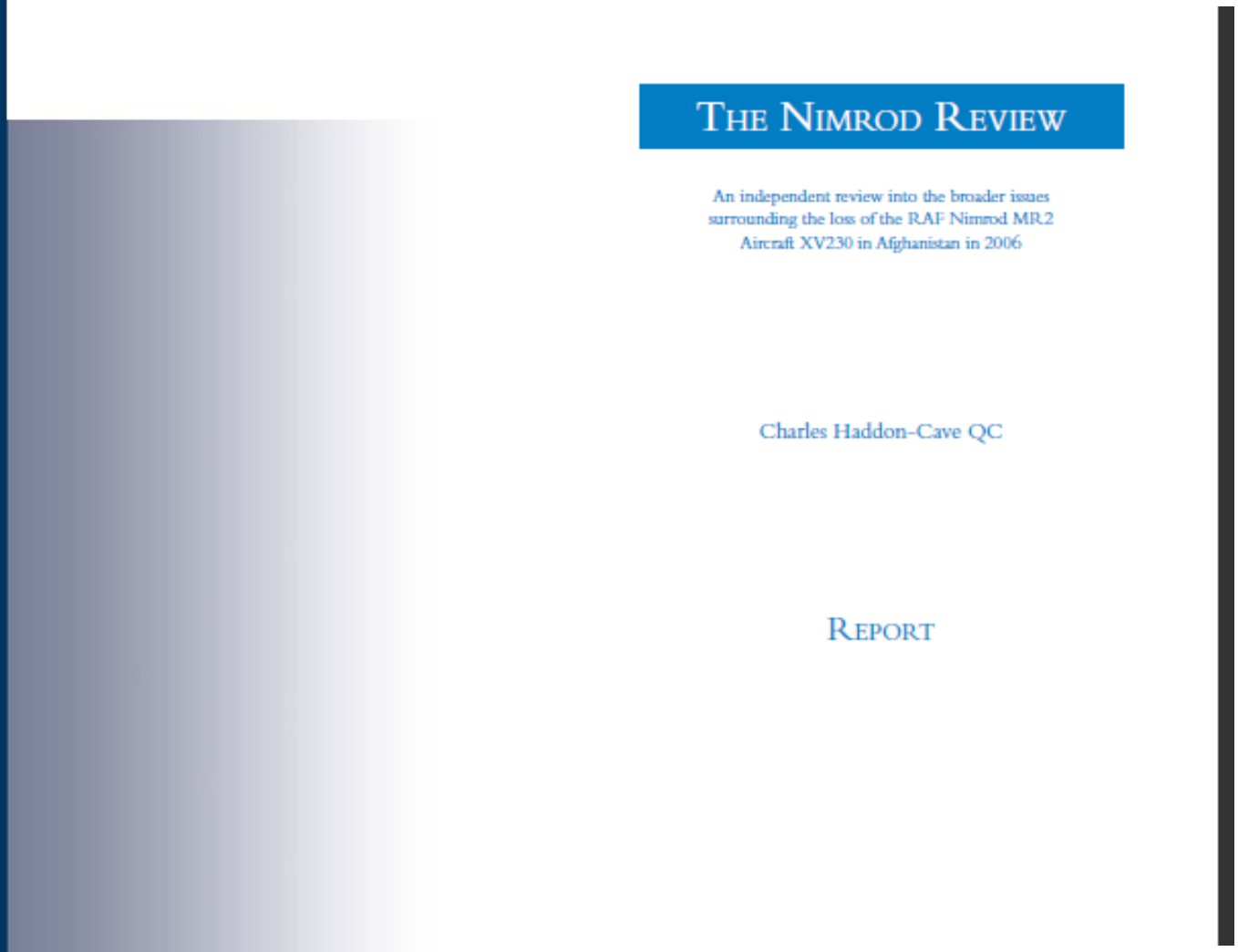
- ‘They help implement skill reductions?’
  - ‘Even an idiot could manage with these…’
- How can we explain this?
  - Safety cases map ideas in safety managers head;
  - They often seem deceptively simple…
  - Safety cases ‘support’ existing skills;
  - You must understand the underlying techniques.

Myths about the Use of Safety Cases 5

- “Safety cases help to redefine the way we do business....”
- True.
- In the past government bought systems;
  - Build to a spec and hand over ownership.
- In the future:
  - Sub-contractors sell a service or function;
  - Safety case explains how the function is safe...
  - Independent of the implementation?

University of Glasgow

Some More Pessimism



THE NIMROD REVIEW

An independent review into the broader issues surrounding the loss of the RAF Nimrod MR2 Aircraft XV230 in Afghanistan in 2006

Charles Haddon-Cave QC

REPORT

BAE SYSTEMS

STRATEGY FOR NIMROD BASELINE SAFETY CASE

- For the Nimrod, the Baseline Safety Case will take the form of a "top-down" safety argument.
- The argument will be structured to demonstrate that the aircraft is acceptably safe to operate within specified contexts and will be accomplished by the implementation of 2 Strategies:
  - Strategy 1 - Argument that all identified safety hazards have been appropriately identified and addressed.
  - Strategy 2 - Argument by compliance with the relevant certification/regulatory requirements and standards.

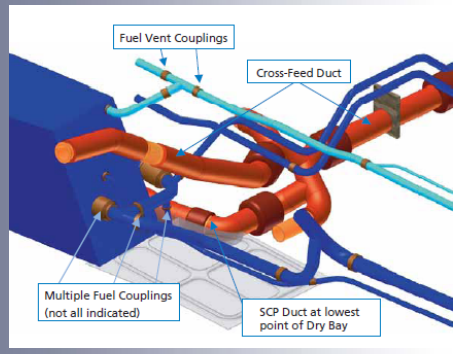
Loss of Nimrod XV230 in Afghanistan

- Mid air fire, 12 died.
  - (1) Escape of fuel during Air-to-Air Refuelling, or a leak from a fuel coupling.
  - (2) Ignition of that fuel by the Cross Feed duct.
- If Nimrod Safety Case had been drawn up with proper skill, care and attention, the catastrophic fire risks ... would have been identified and dealt with".
- Could safety cases achieve so much?

Nimrod Safety Case

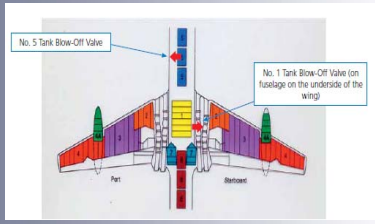
- Unfortunately, the Nimrod Safety Case:
  - was a lamentable job from start to finish;
  - riddled with errors;
  - story of incompetence, complacency & cynicism.

- Process undermined by general malaise:
  - widespread assumption Nimrod ‘safe anyway’
  - it had successfully flown for 30 years
  - Safety Case was a paperwork & tickbox exercise.



Nimrod Safety Case

- BAE hazards 40% open,30% unclassified.
- At handover meetings in 2004:
  - BAE did not disclose to customer the scale of *"Open/Unclassified"* hazards.
- So safety cases did not add much????
  - Did the customer understand safety arguments...
- Safety Case task delegated to junior person



University of Glasgow

Conclusions

- Safety Requirements:
  - Functional and non-functional requirements.
- Safety Cases:
  - Arguments about acceptable safety;
  - Experience from NASA contractors work.
- The Haddon Cave Report:
  - Questioning culture of tick-box exercises.

University of Glasgow

Any Questions…