The Benefits of Assurance Cases

Richard Hawkins

E-mail: **richard.hawkins@cs.york.ac.uk**

High Integrity Systems Engineering Group
Department of Computer Science
THE UNIVERSITY of York

A Brief History of (UK) Safety Cases

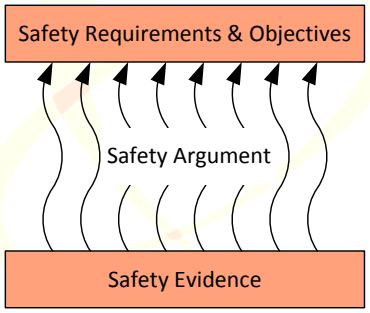
- Number of serious accidents, e.g.
  - Windscale Nuclear Accident (late 1950s)
  - Piper Alpha Off-shore Oil and Gas Platform Disaster (1990s)
  - Clapham Rail Disaster (1990s)
- Prompted reconsideration of how safety is managed in the safety-critical sector
  - Industries were **not** ignorant of safety
  - Safety standards **existed** – but often based on **prescriptive** codes
  - **What Was Missing:** Systematic and thorough consideration of safety, and communication of this to a regulator
    - Completeness
- Prescription
  - Designers / operators claim safety through satisfaction of the ***regulator's*** requirements
- 'Goal-based' standards
  - Up to the ***designers*** to demonstrate that they have an adequate argument of safety in support of high level objectives (e.g. ALARP)

Motivation for Safety Cases

- **Completeness** – hard to judge …
  - … when evidence is *distributed* and *diverse*
  - … when arguments are *implicit*
- **Rationale** behind prescriptive requirements missing
  - Prescribed processes do not necessarily lead to achievement of a specific level of integrity
- **Knowledge Imbalance** – developers know more about their products than the regulators
- Prescription in safety standards hinders the adoption of new process approaches that could improve flexibility and predictability of system development
  - e.g. Model Driven Development

The Purpose of a Safety Case

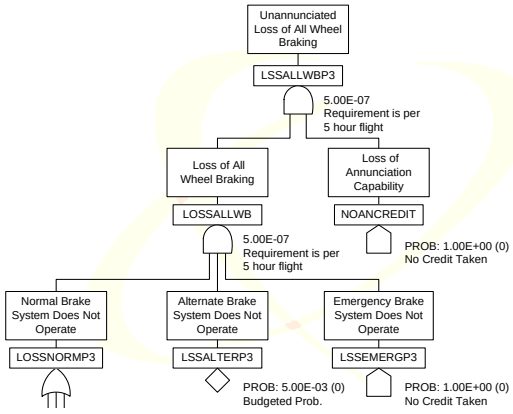
- **A safety case presents the argument that a system will be acceptably safe in a given operating context**



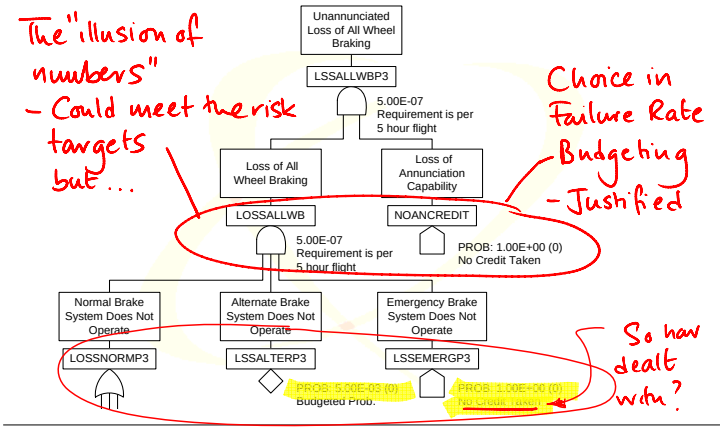
Argument & Evidence

- ***Supporting Evidence***
  Results of observing, analysing, testing, simulating and estimating the properties of a system that provide the *fundamental* information from which safety can be inferred
- ***High Level Argument***
  *E*xplanation of how the available evidence can be reasonably interpreted as indicating acceptable safety – usually by demonstrating compliance with requirements, sufficient mitigation / avoidance of hazards etc
- Argument without Evidence is **unfounded**
- Evidence without Argument is **unexplained**

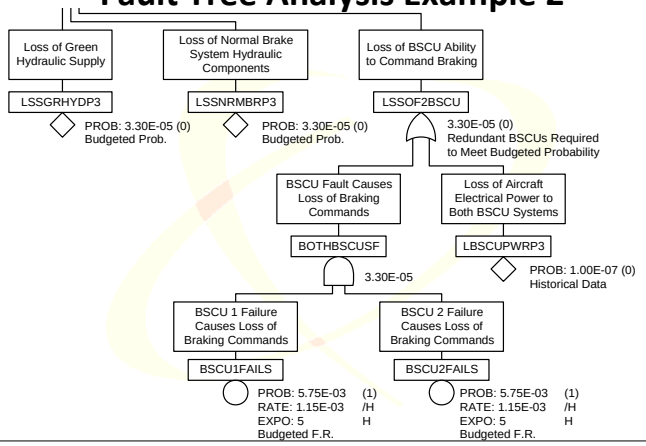
Fault Tree Analysis Example 1



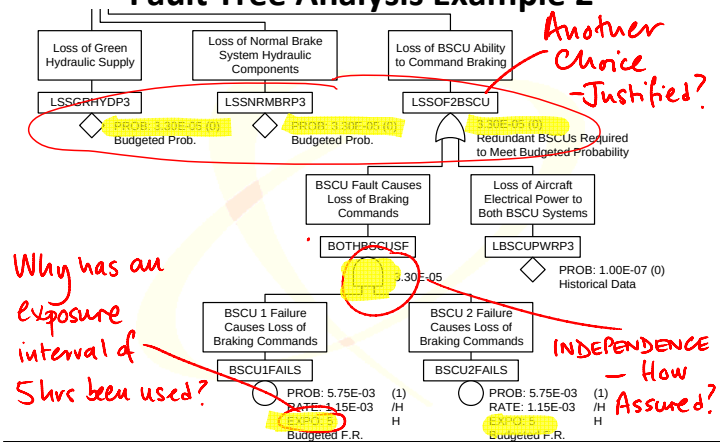
Fault Tree Analysis Example 1



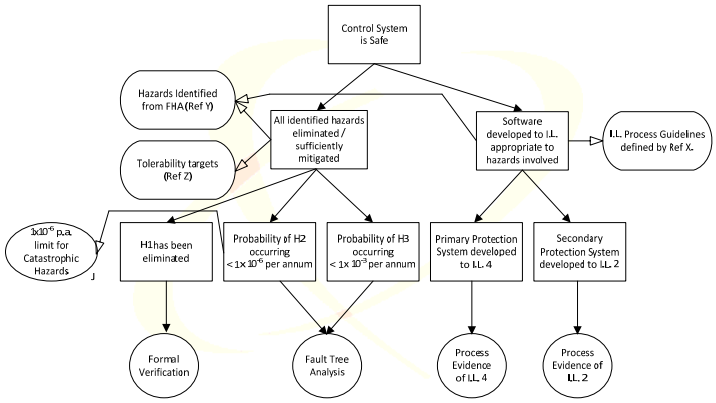
Fault Tree Analysis Example 2



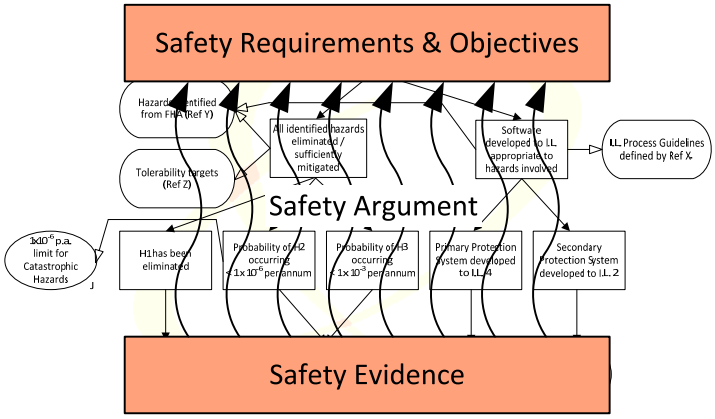
Fault Tree Analysis Example 2



A Simple Goal Structure



A Simple Goal Structure



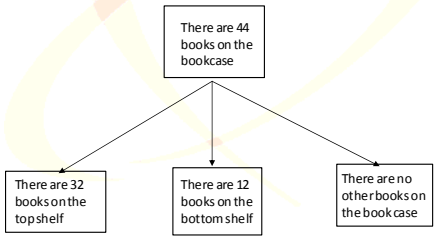
A Simple Goal Structure

Take away the argument & what are you left with? The "BAG of Evidence"

← Note – This is not a safety case!

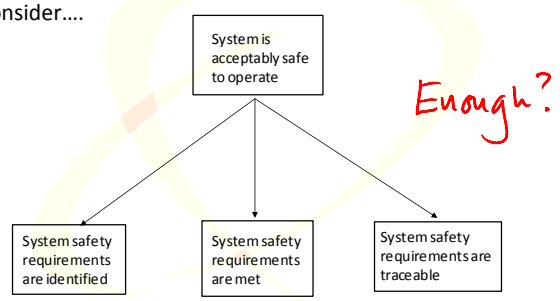
Sufficiency of Assurance Arguments

- Assurance Arguments can be split into two types
  - Deductive arguments
  - Inductive arguments
- Deductive arguments
  - If premises are true, then the conclusion must also be true.



Sufficiency of Assurance Arguments

- It is more common to see safety arguments which are inductive in nature
  - Consider….



  - The premises give us ***confidence*** in the truth of the conclusion

Safety Evidence Assurance

- **Relevance**
  - How relevant is a piece of evidence or argument to the conclusion being sought
  - How strongly does argument/evidence support the claim
- **Coverage**
  - To what extent does the argument / evidence presented 'cover' the conclusion
  - e.g. limited testing
- **Trustworthiness**
  - Thoroughness of evidence generation
  - e.g. staff competency & tool qualification

Trustworthiness of Evidence

Number of possible factors to consider:

Thoroughness – related terms: depth / rigour of analysis

- "Buggy-ness" – how many "faults" are there in the evidence presented
  - High faults (related to safety case "intent") = loss of confidence
- Level of Review
- In case of hand-generated evidence:
  - Experience of Personnel
  - Competency of Personnel
- In case of tool-derived evidence
  - Tool Qualification and Assurance
  - NB – Importance distinction between tools where output forms part of product vs. those with ancillary role

When to Articulate the Assurance Argument?

- Q: At what stage in a project is it worth attempting to articulate the assurance argument?
- Answers:
  - Early on (high level) to get a clear picture (and gain agreement) of argument structure
    - Useful as a scoping exercise and effort allocation
  - As project is progressing, in order to monitor status towards completion of an acceptable argument
  - At end of project in order to present the final argument and evidence that exists

Assurance Case Benefits

- *Mitigation for the following project risks*
  - Excessive iterations involved in reaching agreement on the sufficiency of the evidence
    - Poor comprehension
  - Effort spent on project (e.g. in performing analyses) that do not really provide appropriate assurance
  - Disproportionate effort allocated across safety development and assurance activity (rabbit holes!)
    - also needs understanding of ALARP
  - Duplication of effort (inefficient) when apportioning responsibility
  - Assurance objectives 'falling down the cracks' when apportioning responsibility

Assurance Case Problems?

- Prescription had many flaws but "people knew what they were supposed to do"
  - Helps project predictability (cost and timescales)
- Subjective assurance arguments, including explicit arguments of "good enough" could be the subject of debate with multiple stakeholders
  - Aim is mutual acceptance of a subjective position
  - Counter-argument: the assumptions are always there!
- Assurance arguments, by putting all of your arguments clearly and transparently in one place, will be open to (legal) attack
  - Counter-argument: to not have 'pulled it all together' could be seen as negligent; Assurance cases increasingly recognised as best-practice

Summary

- Safety cases introduced because although safety was being considered, evidence generated, codes followed etc. it was often hard to see an overall (systematic, defensible) assurance argument
  - Exploiting reality that developers have more knowledge about what makes their product safe than the regulators
- Safety cases require clearly articulated **argument**, supported by references to **evidence**
- Arguments must be judged for **sufficiency**
- Incremental assurance case development can be effective feedback for design, focus evidence production effort, and for **project risk-reduction**
  - Good idea even when approach not mandated

Key Questions for Medical Devices

- Is there enough competency in the food-chain (development, review and acceptance) to judge the sufficiency of assurance cases?
- With more integration of highly complex devices, can assurance case cope?
  - Complex interactions
  - Emergent hazards

Existing GSN Applications

- MoD: Site Safety Justifications (Complex Multi-facility, Multi-role safety case)
- BAE SYSTEMS: Eurofighter Avionics Safety Justifications
- Railtrack / Siemens: Dorset Coast Re-signalling Project
- BAE SYSTEMS: Nimrod MRA4 Enterprise Safety Case
- BAE SYSTEMS: Hawk
- MoD: Tornado Operational Safety Case
- BAE SYSTEMS: Harrier
- RR: Various Submarine Propulsion Justifications
- RAF: UK ASACS – Military Air Traffic Management
- Westinghouse: Underground Jubilee Line Extension
- NATS Unit Safety Case for NERC at Swanwick
- Swedish Air Traffic Control Applications
- Rolls-Royce Trent Engine Control Systems Safety Arguments
- ...