Introduction to Safety Cases

Tim Kelly

E-mail: **tim.kelly@cs.york.ac.uk**

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

Overview

- Historical Context
- Definitions
- Role of Argument & Evidence
- Safety Case Reports
- Safety Arguments

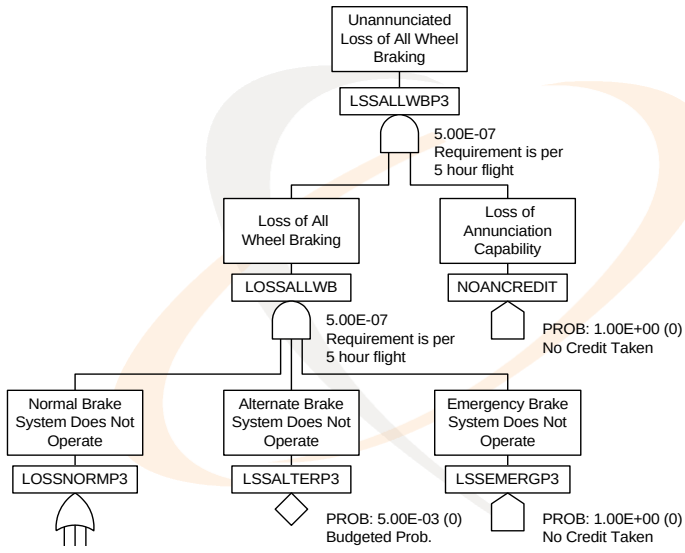
A Brief History of Safety Cases

- 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
- Prescription
  - Designers / operators claim safety through satisfaction of the ***regulator's*** requirements
- 'Goal-based' standards
  - Up to the ***designers / operators*** 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
- **Knowledge Imbalance** – *developers* know more about their products than the *regulators*
- Some existing forms of assurance are increasingly considered too **indirect** (e.g. software)

Fault Tree Analysis Example 1

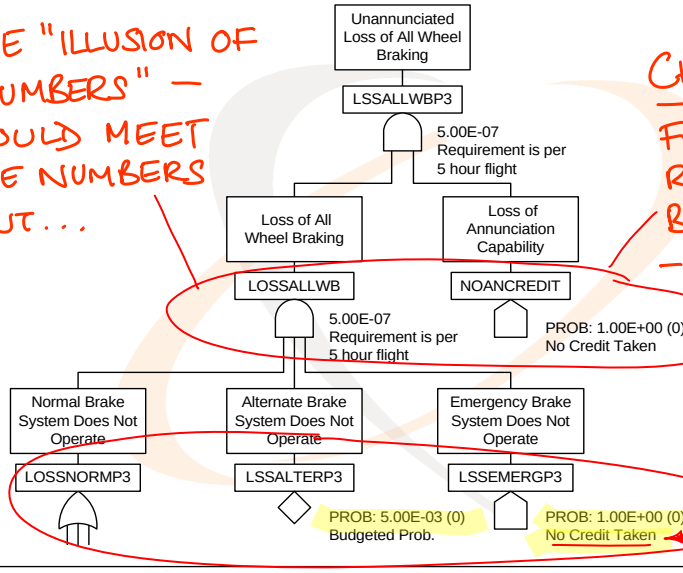


Fault Tree Analysis Example 1

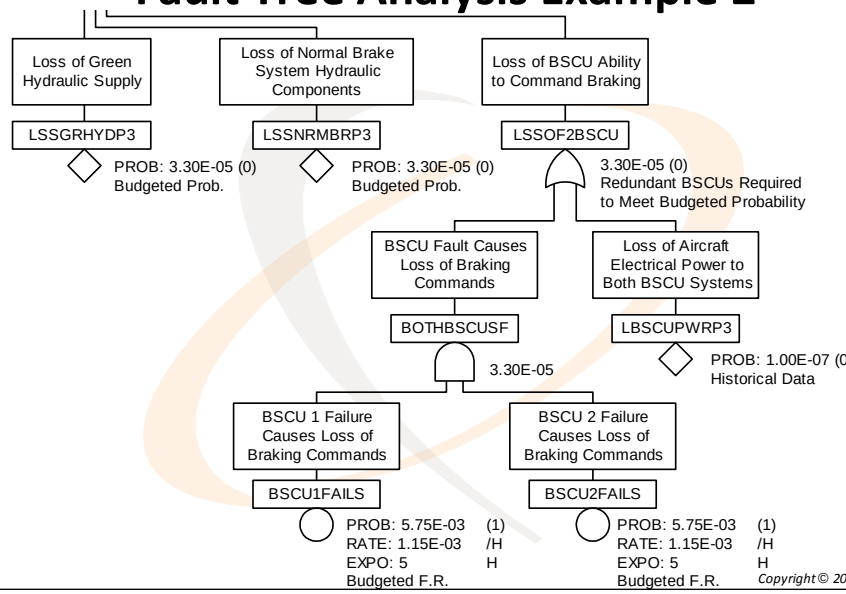
THE "ILLUSION OF NUMBERS" — COULD MEET THE NUMBERS BUT...

CHOICE IN FAILURE RATE BUDGETING — JUSTIFIED?

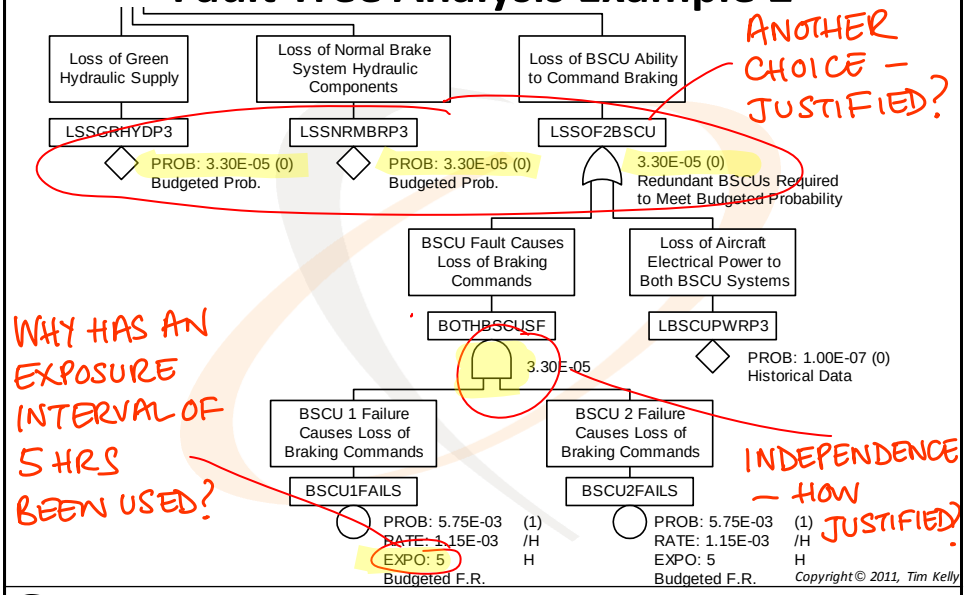
HOW IS THIS DEALT WITH?



Fault Tree Analysis Example 2



Fault Tree Analysis Example 2



(Further) Motivation for Safety Cases

- Completeness – hard to judge …
  - … when evidence is distributed and diverse
  - … when arguments are implicit
- Rationale behind prescriptive requirements missing
- Knowledge Imbalance – developers know more about their products than the regulators
- Some existing forms of assurance are too indirect
- The role of evidence can otherwise be unclear
- The assumptions and implicit judgements in evidence need to be presented explicitly and argued

The Purpose of a Safety Case

Principal Objective:

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

- 'system' could be ...
  - physical (e.g. aero-engines, reactor protection systems)
  - procedural (e.g. railway operations, off-shore)
  - Software (in a system context)

In practice:

- often series of safety cases produced — stages of development and/or operation
- safety cases are large, complex, technical and *political* documents

Some Safety Case Definitions

- *"A safety case is a comprehensive and structured set of safety documentation which is aimed to ensure that the safety of a specific vessel or equipment can be demonstrated by reference to:*
  - *safety arrangements and organisation*
  - *safety analyses*
  - *compliance with the standards and best practice*
  - *acceptance tests*
  - *audits*
  - *inspections*
  - *feedback*
  - *provision made for safe use including emergency arrangements"*

(JSP 430 Issue 1)

- *"A Safety Case is 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."*

(DS 00-56 Issue 4)

Argument & Evidence

A safety case requires two elements:

- *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

Safety Cases vs. Safety Case Reports

- The Safety Case is the totality of the safety justification + all the supporting material: testing reports, validation reports, relevant design information etc

- The Safety Case Report is the document that summarises all the key components of the Safety Case and *references* all supporting documentation in a clear and concise format

Safety Case Reports

- Exact contents depends on regulatory environment
- The following are key elements of most standards:
  - scope
  - system description
  - system hazards
  - safety requirements
  - risk assessment
  - hazard control / risk reduction measures
  - safety analysis / test
  - safety management system
  - development process justification
  - conclusions

Safety Arguments

- Safety Case is NOT just a collection of disparate pieces of information
- Safety Argument should form the 'spine' of the Safety Case showing how these elements are related and combined to provide assurance of safety
  - within the limits defined [*Scope*], the system [*System Description*] is SAFE because all identified hazards [*System Hazards*] and requirements [*Safety Requirements*] have been addressed. Hazards have been sufficiently controlled and mitigated [*Hazard Control / Risk Reduction Measures*] according to the safety risk posed [*Risk Assessment*]. Evidence [*Safety Analysis / Test*] is provided that demonstrates the effectiveness and sufficiency of these measures. Appropriate roles, responsibilities and methods were defined throughout the development of this system [*Development Process Justification*] [*Safety Management System*] and defined future operation

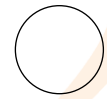
Presenting Clear Arguments

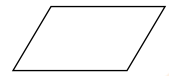
- Basic argument structure
  - claim – what we want to show
  - argument – why we believe the claim is met, based on
  - evidence – test results, analysis results, etc.
- In general, argument broken down hierarchically
  - claim, argument, sub-claims, sub-arguments, evidence
  - easy to show graphically, although can be done in document structure (sub-section numbering, etc.)
- In practice, other concepts useful
  - e.g. context to claims, assumptions

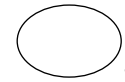
The Goal Structuring Notation

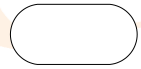
Purpose of a Goal Structure

To show how goals  are broken down into sub-goals,

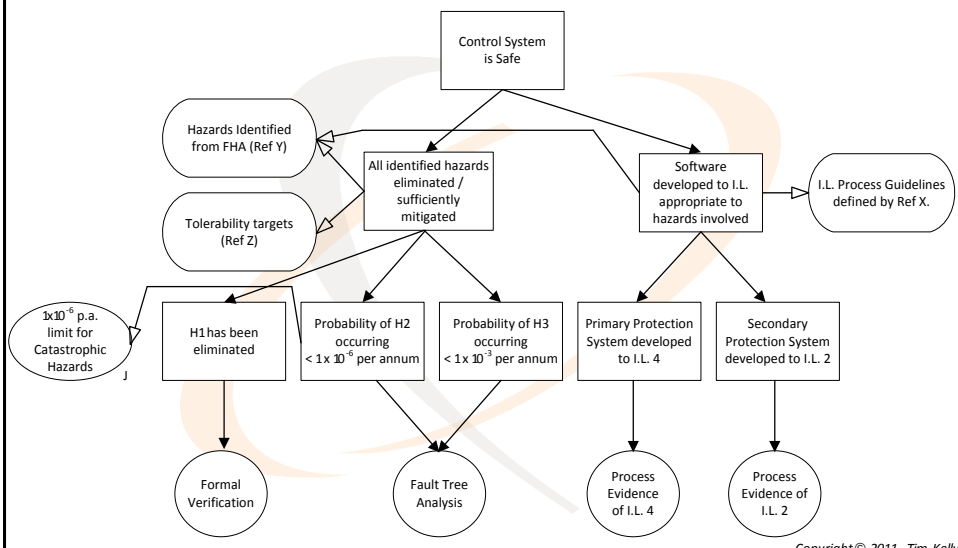
and eventually supported by evidence (solutions) 

whilst making clear the strategies  adopted,

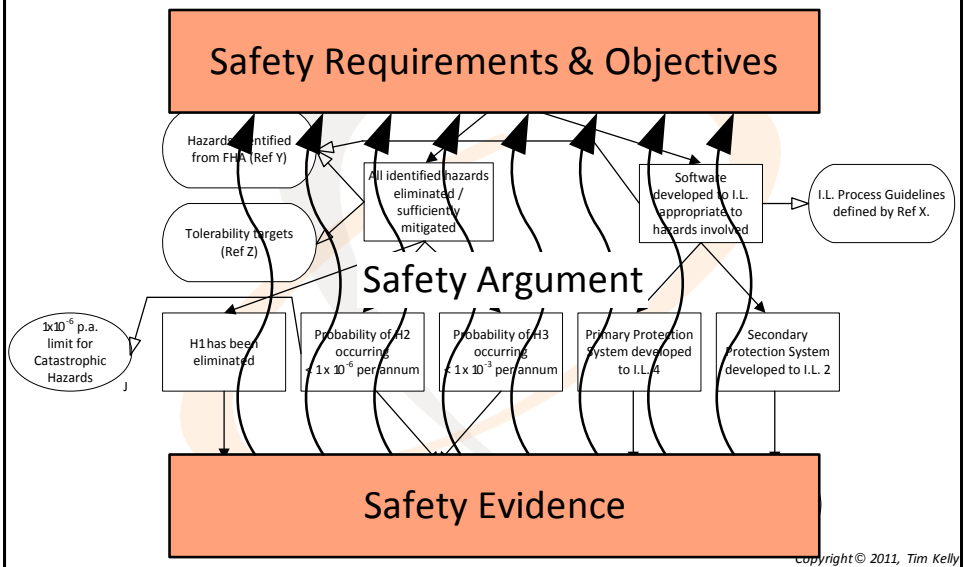
the rationale for the approach (assumptions, justifications) 

and the context  in which goals are stated

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!

Formal Verification
Fault Tree Analysis
Process Evidence of I.L. 4
Process Evidence of I.L. 2

Summary

- Production of a Safety Case is a key objective of all the safety lifecycle activities
- The objective of the Safety Case is to 'pull together' many forms of information and present a coherent argument of safety
- However, safety cases are not just documents
- Clear arguments *essential* for safety case approach