Safety Cases:
Challenges of Complexity and Traceability

George Cleland glc@adelard.com

Overview

- Who are we?
- Safety cases – issues and background
- Some example cases
- Issues of complexity
- Notations for safety argumentation
- Scenario
- Quality, Provenance and Traceability
- Conclusions

Adelard

Who are we?

- 20 years background in the safety industry
- safety cases and safety management systems
- independent safety assessment
- software assurance, including formal methods and static analysis
- human factors
- hazard analysis, hazard management
- development, interpretation and application of safety-related standards and guidelines
- applied research in safety and software reliability
- ASCE – the Assurance and Safety Case Environment

Adelard

Safety cases - issues

- Increasingly required by law/regulation/standards
- Emergence of goal-based standards
  - cf evidence based
  - encourages innovation, but requires more focus on achievement
  - safety case is the key assurance information repository
- Complexity
  - vast amount of data to be integrated - information overload
  - complexity of argument
- Comprehension
  - safety cases need to be independently audited
  - many stakeholders require different views of the safety case
- Supply chain
  - geographically and culturally diverse suppliers
- Range of risks associated with safety case 'failure'

Safety Case Requirements

- UK:
  - Defence
  - Offshore and on-shore process industries
  - Rail
  - Air
  - Nuclear
  - Even ‘exempt’ areas are choosing to deliver safety cases
- Other:
  - IEC 61508:
    - —Functional safety assessment
  - DO178:
    - —Software accomplishment summary
  - MilStd 882
    - —Technical data package

Overview

- Standards are moving from prescriptive approaches to *goal based*
- That is, it says *what* you must do, not *how* you must do it
- In a safety context you must not only achieve adequate safety, you must demonstrate your achievement

- The top-level goals are:

1. Identify the *safety requirements*
2. Show that the safety requirements are *met*

Adelard

Key requirements (1)

Safety Requirements:

- Identify all relevant safety legislation, regulations, standards and organisational/govt Policy
  - These are the source of the safety requirements
- All activities and products must comply with these
- Monitor & manage changes to the operational, technological, legislative and regulatory environment, and any other changes that may have an impact on safety

Key requirements (2)

Schedule:

- Safety should be considered from the *earliest stage* in a programme and used to *influence* all activities and products
  - Safety is a vital characteristic of systems or services - it often has a significant impact upon operational effectiveness

Key requirements (3)

Organisation:

- Safety tasks are carried out by demonstrably competent individuals and organisations
- Safety management is implemented as a key element of a harmonised, integrated *systems engineering* approach
- An auditable Safety Management System is implemented throughout the project lifecycle
- Interfaces between SMS, Safety Cases, systems and organisations are effectively managed and documented

Adelard

Key requirements (4)

Safety Culture:

- Standards explicitly mentions safety culture, e.g.

> Safety culture is the product of individual and group values, attitudes, perceptions, competencies and patterns of behaviour that determine the commitment to, and the style and proficiency of, safety management

  - The quality of safety management and the associated safety culture as exemplified by the Safety Management System is a factor in the confidence in the evidence
  - The effective dissemination and exchange of safety information underpins a successful safety culture

Key requirements (5)

Safety Case / Safety Case Reports:

- The Safety Case demonstrates how safety will be, is being and has been, achieved and maintained
- Safety Case Reports delivered at intervals to give
  - oversight of safety management
  - current state of safety analysis
  - gaps or weaknesses
  - plans

Key requirements (6)

Hazard/incident management:

- All credible hazards and accidents are identified, the associated accident sequences are defined and the risks associated with them are determined
- Hazards are managed and traced systematically
- All risks are managed to be broadly acceptable and/or ALARP
- Identified controls and mitigations implemented or traced as derived requirements
- Defect/failure reports and incident/accident/near-miss reports are monitored and remedial actions identified and implemented

Adelard

What exactly 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 environment
>
> DefStan 00-56/4

- The Safety Case contains a structured argument (rationale) demonstrating that the evidence contained therein is sufficient to show that the system is safe
- The argument should commensurate with the potential risk and the system's complexity
- To be compelling and comprehensible a safety case and its derived reports must 'tell a story'

Viewpoints

Stakeholder viewpoint - a key issue.

Stakeholders include:

- Supplier
  - safety manager
  - safety specialists
  - project manager
  - design team
- Customer
  - Duty Holder
  - Safety Manager
  - Safety specialists
- Sub-contractors
- Users, operators and managers
- Passengers, public
- ISA/Regulator
- And if things go wrong ... Lawyers

The buck stops here

- The Duty Holder
  - Under U.K. legislation the *duty holder* is a person with specific responsibilities for the safety management of the system and who has legal liability for ensuring the adequacy of such safety management.

Example cases

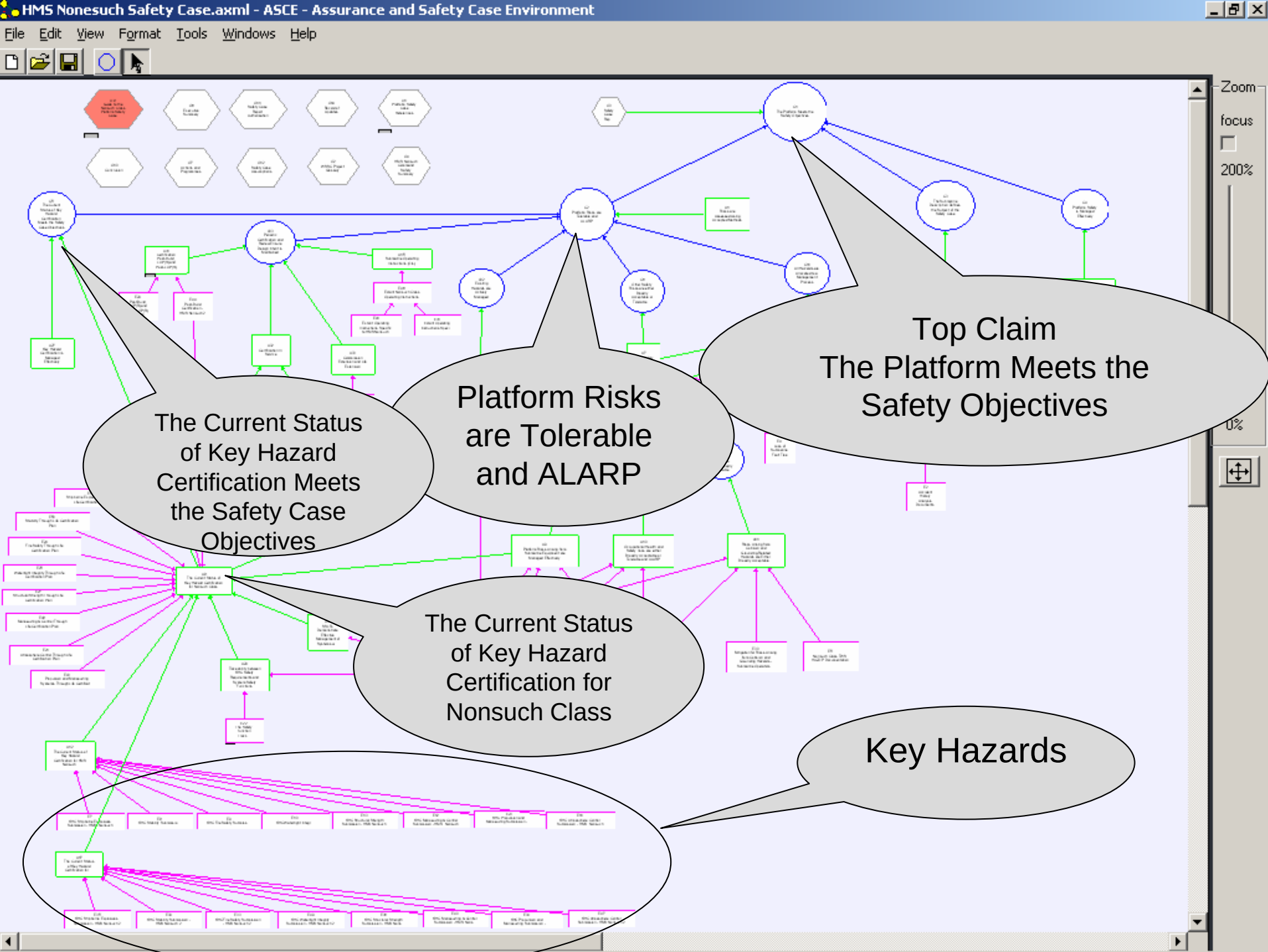
- Whole base safety case
- HMS Buckfast
  - 27 ‘shelf-feet’ of level arch files
    - —Incomprehensible
    - —Unmaintainable
    - —Useless
    - —But necessary for the base to have permission to operate
    - —“Shelfware”

- Whole submarine safety case
- HMS Nonesuch
- Safety case for current UK nuclear fleet
  - 1 DVD of data
    - —Constructed using structured argumentation (CAE/GSN)
    - —Hyperlink to supporting evidence
  - Easily navigable/reviewable
  - Useful in operations
  - Simple(r) to maintain

Adelard

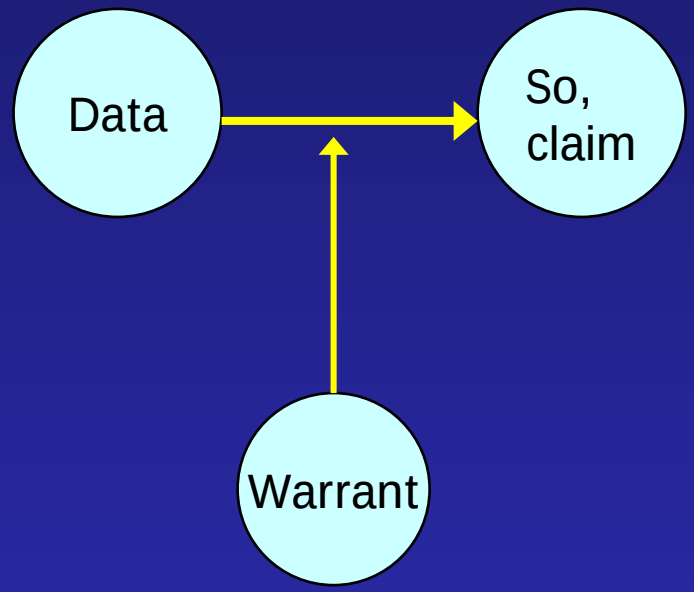
Whole Submarine Safety Case Example

- Developed for the MOD by SSMG
- Vanguard Class example
- Uses Claims-Argument-Evidence notation


HMS Nonesuch Safety Case.axml - ASCE - Assurance and Safety Case Environment
File Edit View Format Tools Windows Help
Zoom
focus
200%
0%
Top Claim
The Platform Meets the Safety Objectives
Platform Risks are Tolerable and ALARP
The Current Status of Key Hazard Certification Meets the Safety Case Objectives
The Current Status of Key Hazard Certification for Nonsuch Class
Key Hazards

Notations for arguments

- A conceptual framework and graphical notation for representing the structure of an argument can be traced back to Toulmin*.
- Toulmin makes a distinction between "*claim or conclusion whose merits we are seeking to establish*" and "*the facts we appeal to as a foundation for the claim*".



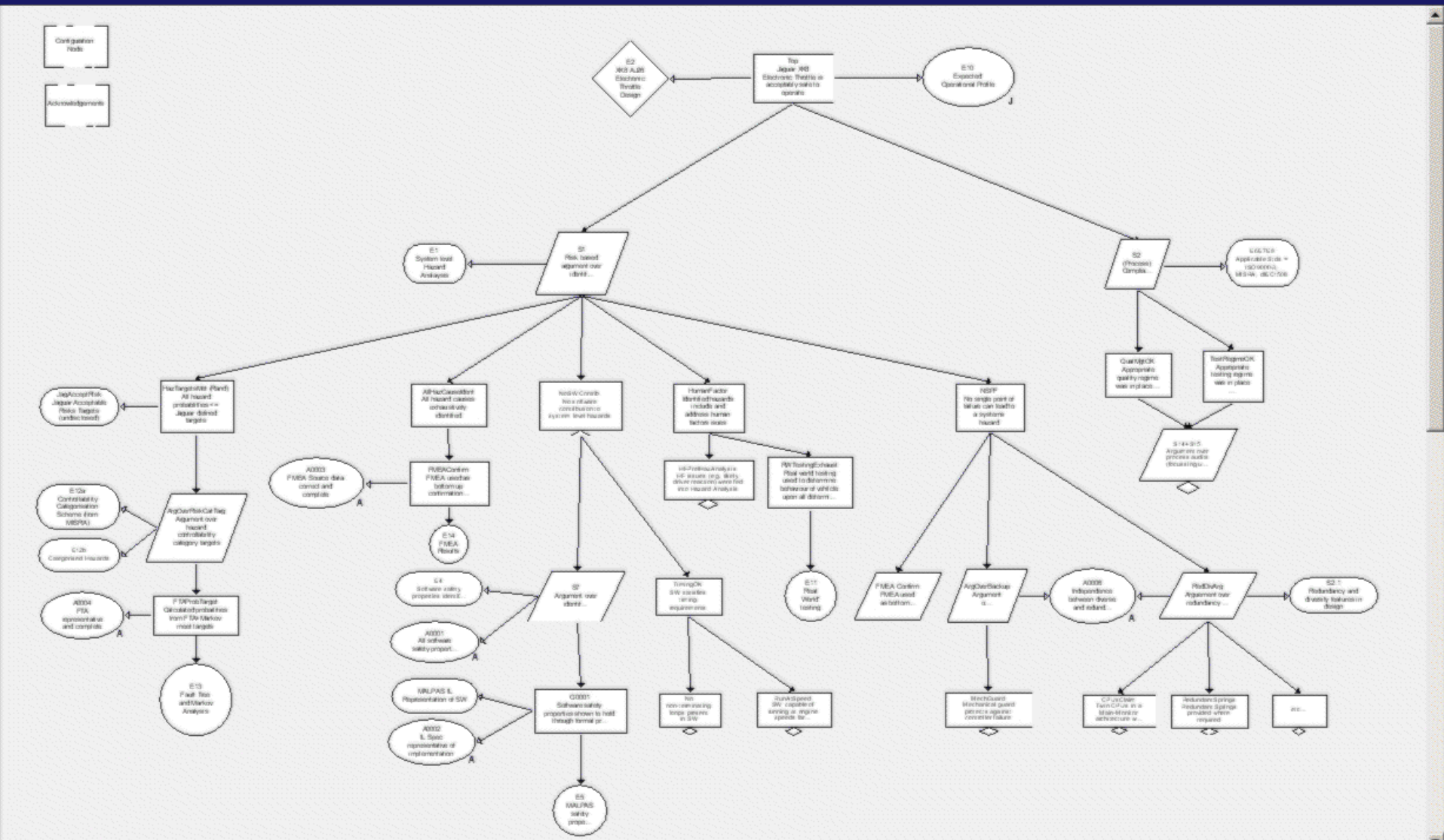
*Toulmin, Stephen. Uses of Argument (Cambridge: Cambridge University Press, 1958)

Use of structural approaches to safety case

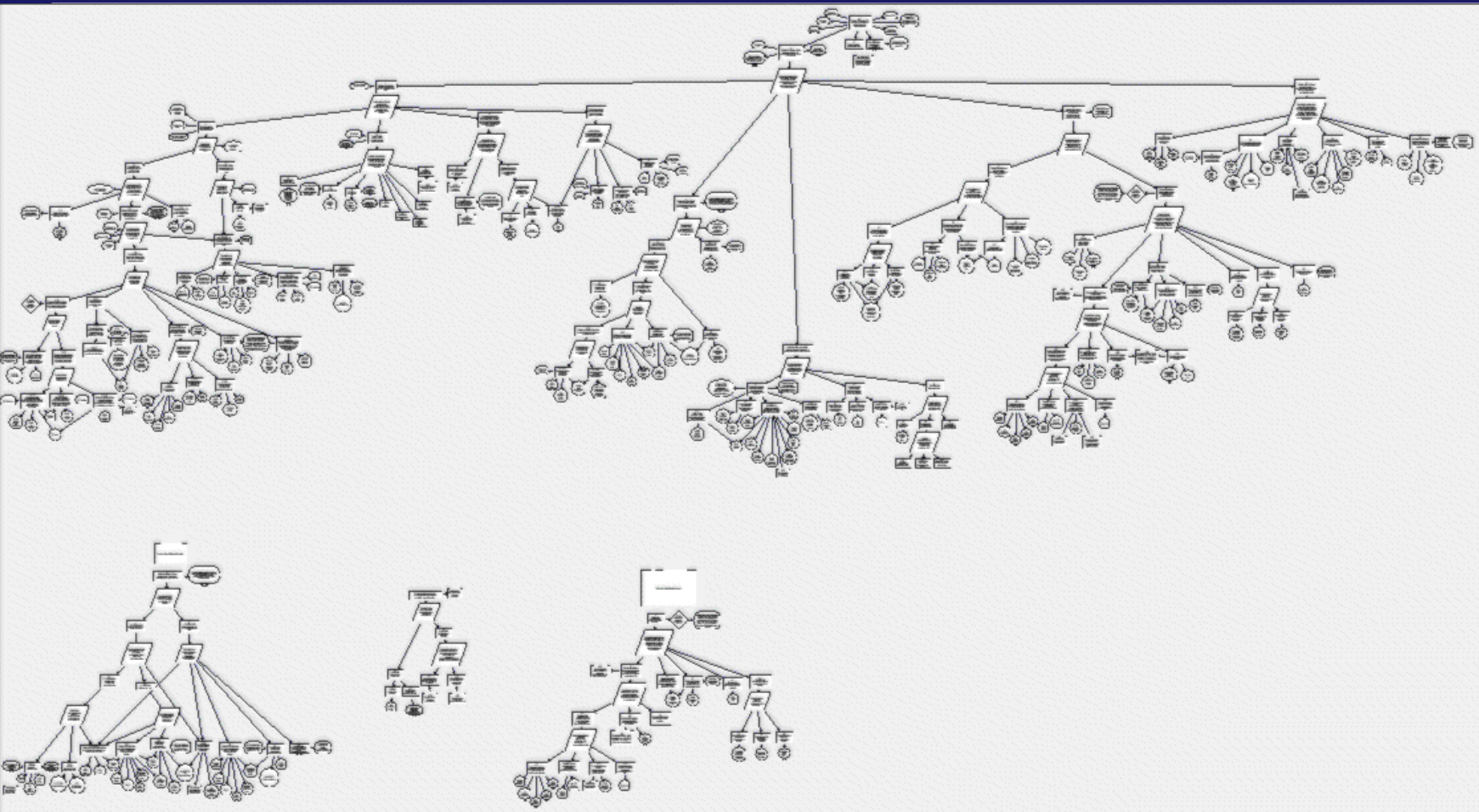
- Goal Structuring Notation (GSN)
- Claims Argument Evidence

- GSN examples

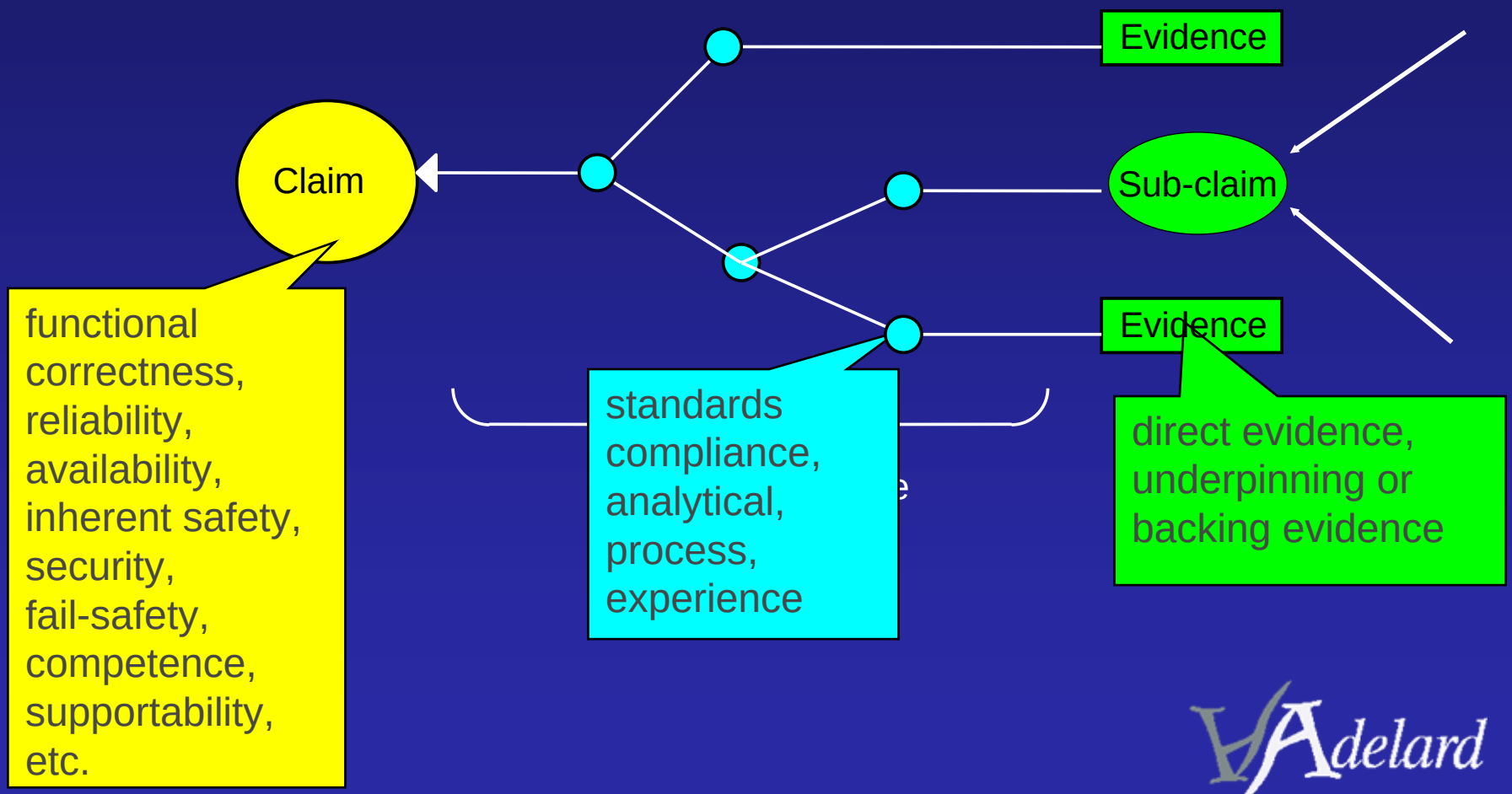
Jaguar Throttle Control Safety Argument



Fast Jet Safety Case



Structural Safety Cases



Safety Case / Safety Case Reports

- The Safety Case
  - A complex body of interdependent and evolving information
  - Not easily auditable or reviewable as a whole
  - Heterogeneous formats
    - PDF, Word, Access, Excel, DOORS, Wordperfect
    - even ASCE :-)
- Safety Case Reports
  - A ‘projection’ of the rationale and content of a safety case at an appropriate milestone, perhaps covering a specific component
  - Reviewable against the project expectation at the milestone
  - May need several reports for various stakeholders

Adelard

Scenario (simplified)

- UK MOD identifies a need to procure and operate a new platform
- IPT (Integrated Project Team) established to manage process through life
- IPT Leader is normally the Duty Holder
  - but…
- 'CADMID' process for through life procurement and support
- Other IPTs may be responsible for procuring and delivering equipment to be integrated onto the platform. e.g.
  - Weapons systems
  - Communications systems
  - Surveillance systems
  -
  -

Adelard

Scenario (2)

- Platform IPT contracts a prime to develop and deliver (and maybe operate) the platform
- Equipment IPT likewise
- Prime may sub contract (and sub-sub, and sub-sub-sub...)
- Often contracts cross geographic and cultural boundaries

Scenario (3)

- Safety Case
- Platform IPT responsible for overall platform safety case
  - The IPT could develop the case itself with support from the Prime and Sub-contractors.
  - The Prime contractor could develop the case and deliver it to the IPT which then would maintain the case.
  - The Prime contractor could develop the case and continue to maintain it through life on behalf of the IPT.
  - The IPT could contract out the development (and possibly maintenance) of the case to a consultant.
- Platform IPT responsible for integration of equipment cases on to platform

- Equipment cases.....

Issues of Quality, Provenance and Traceability

- Platform safety case is therefore composed of elements from diverse sources
- Safety (case) requirements need to be communicated out through the organisational hierarchy
  - Evidence requirements (nature and quality)
  - Safety case fragment requirements
- Contributed elements need to be integrated
  - Relevance, timeliness, quality
- Overall case needs to be reviewed
  - Coverage, consistency, completeness, comprehension...

Adelard

Nature of evidence

- Hazard Log or Risk Register
- Safety requirements documentation
- Description of the Safety Management System employed by the IPT or the Prime Contractor (or both)
- Results of various test activities or field trials
- Analysis of design
- Results of safety analysis activities e.g. FEMECAs, HAZOPs, etc
- Results of modelling or simulation, e.g. loss models, simulated weapons detonation
- Training and competency records
- Process documentation
- and so on...

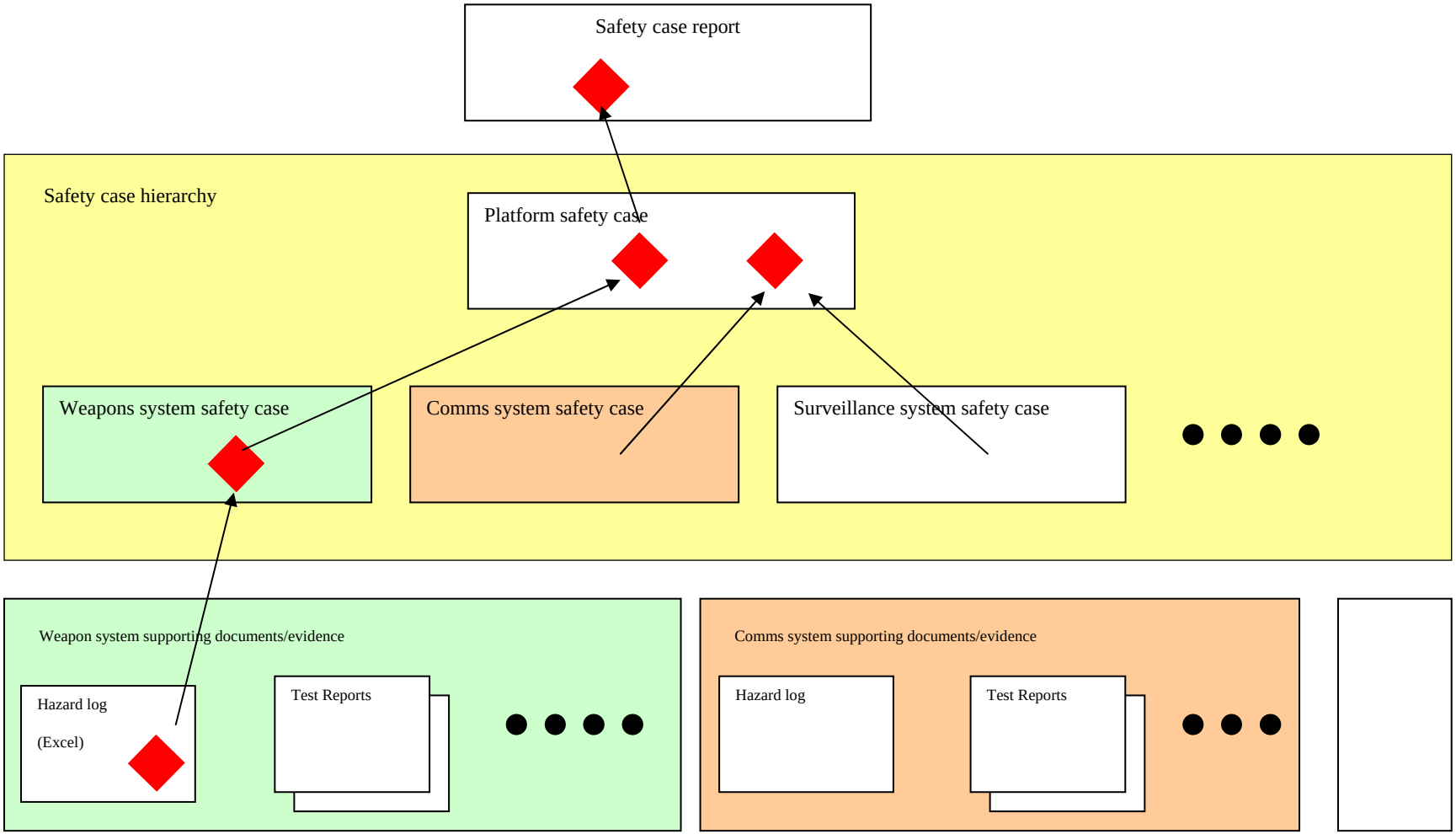
- All in multiple source formats

Adelard

Quality, Provenance and Traceability (2)

- Element of our case are developed by possibly many different organisations:
  - Management control, configuration management, safety culture, contract?
  - Diverse formats
- Provenence
  - Where did this come from?
- Traceability
  - What's changing? When?
  - By whom? With what authority?
  - What is the impact?

Safety case structure



Conclusions

- Safety case are complex bodies of interdependent and evolving information
  - elements of which are often developed under diverse management
  - and often poor (or no) explicit configuration control
- Structural approaches (GSN, CAE) improve our ability to construct robust cases and make them comprehensible
  - Hierarchical and modular approaches should increase this further
  - However any tool can be used poorly....
- Provenance and traceability is still a major problem

Adelard

The end

Questions?