Certification and evaluation - current methods and future prospects

Aviation Software Systems: Design for Certifiably Dependable Systems, on October 5-6 in Alexandria VA

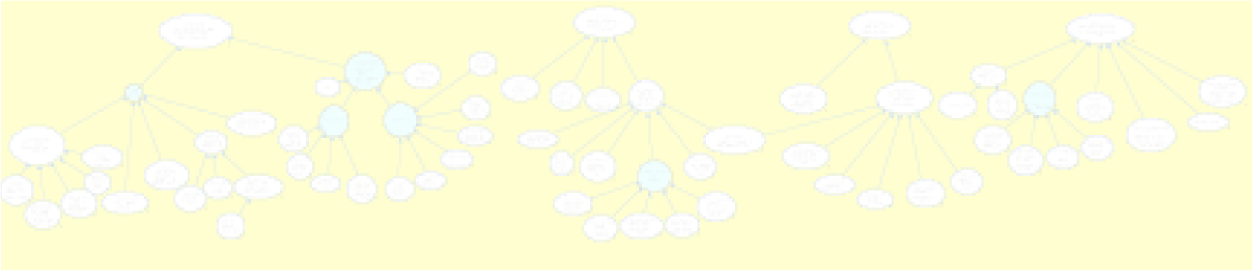
Robin E Bloomfield (reb@csr.city.ac.uk)
Professor of System and Software Dependability
Director, Centre for Software Reliability, City University, London
Founder, Adelard LLP

Challenges

- *To "stand still" or maintain balance* - so that there are no disasters. The demands of current systems, complexity of new systems, time to market, pressures, the structure of the supply chain, competence, the scale of reuse, unvalidated (unvalidatable?) standards, evolving threats all make this non-trivial and uncertain.

- *Flexible doctrine* To allow a choice of doctrine between conservative approaches to technology adoption and an ability to make informed decisions to exploit the benefits of using computer based systems. To effectively describe and communicate the levels of trustworthiness.

Assurance cases



- “a documented body of evidence that provides a convincing and valid argument that a system is adequately dependable for a given application in a given environment”

- goal-based “claims-argent-evidence” safety case approach has widespread use

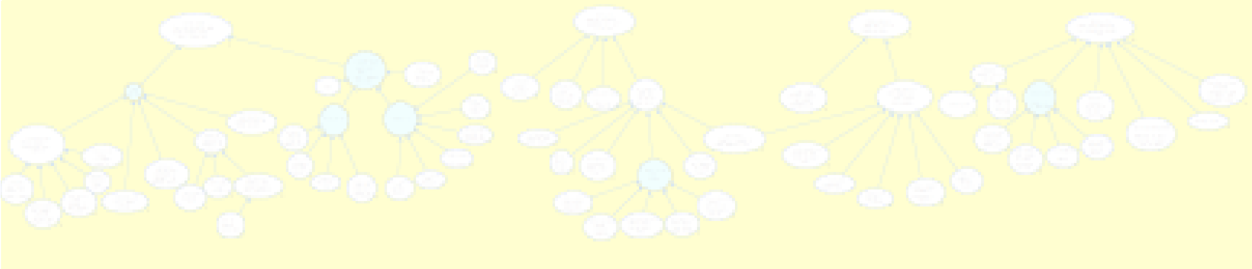
  - UK Defence procurement and supply chain
  - Recent critical UK financial system
  - Civil ATM regulations; Goal based emerging in nuclear
  - Railways

- at its best promotes clarity, phased requirements, reduces project risks, promotes dialogues, provides a rationale, addresses non-compliance, increases confidence

CITY City University London

Adelard

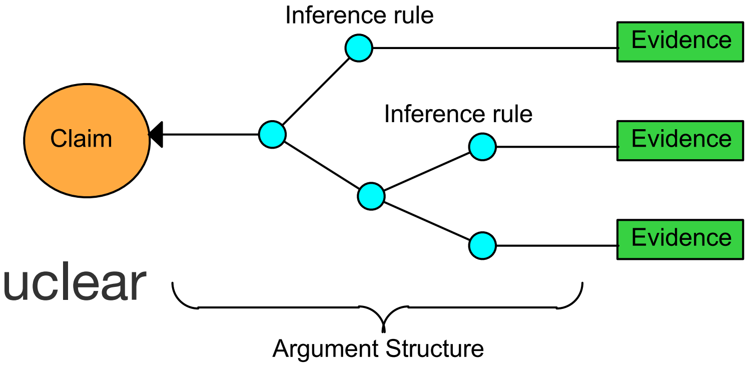
Assurance cases



- “a documented body of evidence that provides a convincing and valid argument that a system is adequately dependable for a given application in a given environment”

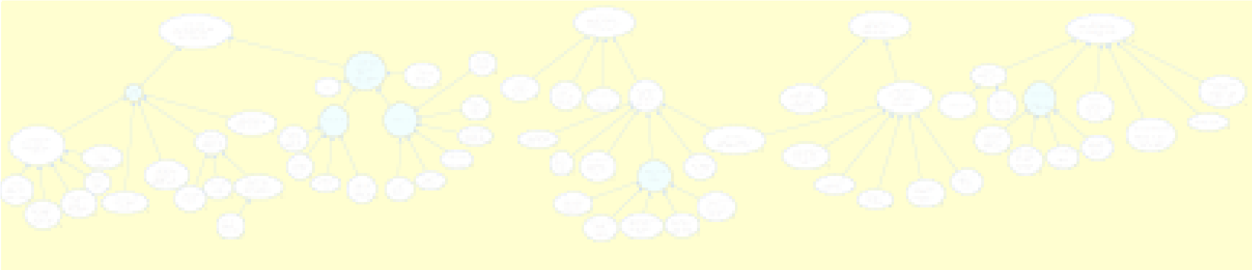
- goal-based “claims-argent-evidence” safety case approach has widespread use

  - UK Defence procurement and supply chain
  - Recent critical UK financial system
  - Civil ATM regulations; Goal based emerging in nuclear
  - Railways



- at its best promotes clarity, phased requirements, reduces project risks, promotes dialogues, provides a rationale, addresses non-compliance, increases confidence

Assurance cases



- “a documented body of evidence that provides a convincing and valid argument that a system is adequately dependable for a given application in a given environment”
- goal-based “claims-argent-evidence” safety case approach has widespread use
  - UK Defence procurement and supply chain
  - Recent critical UK financial system
  - Civil ATM regulations; Goal based emerging in nuclear
  - Railways
- at its best promotes clarity, phased requirements, reduces project risks, promotes dialogues, provides a rationale, addresses non-compliance, increases confidence

Challenges

“a documented body of evidence that provides a convincing and valid argument that a system is adequately dependable for a given application in a given environment”

- What is the system - *of systems (of systems))?*
- What is the environment - *organisational, physical, changes, threats*
- What is the application or service - *adaptation*,
- What is a convincing and valid argument - *defining and demonstrating safety properties, dealing with uncertainty, assumption doubt, correctness wrt properties*
- What is adequately safe, secure - *trade offs, not independent, composability*
- What will change, and how? -
    - ability to respond outside of design basis increasingly important, *resilience*?

Proposal

- To simplify .... propose a paradigm shift from compliance based certification to behaviour based cases that exploit analytical reasoning but also deal with unavoidable uncertainties. Maintain emphasis on systems, but consider socio-technical systems (socio, technical and socio-technical issues)

  (institutional issue for roadmapping?)

Directions - specific, immediate and long term

- Overall approach - assurance, safety and security, “cases” - how it behaves, not how hard you have tried
- Explicit analysis, evaluation and design of certification process
- Model(s) based assurance of socio-technical systems
  - service, system, environment, organisation
  - formal reasoning of models, assumption doubt and model validation
  - for critical systems, confidence in fault freeness vs reliability claim
  - exploit timebands as a structuring mechanism
- Confidence
- Responsibility mapping
- Dynamic of trust - how won, how lost, how recovered
- New approaches to common mode failure, beyond design basis, resilience, interdependency analysis
- Explore metaphors and - anthropomorphic, biological, complexity science

  by nature, multi-disciplinary, inter-disciplinary, new disciplines?