Argument strength – an engineering perspective

Prof Robin Bloomfield FREng
Dr Kate Netkachova

Bochum, Germany
01 December 2016
Adelard

- Adelard is a specialized, influential product and services company working on safety, security and resilience since 1987
- Wide-ranging experience of assessing computer-based systems and components
- Work across a range of different industrial sectors, including defence, nuclear, rail, aviation, financial, medical
  - Policy, methodology, technology
  - Product for managing safety and assurance cases (ASCE)
  - Security-informed safety and dependability
- Consultants PhD level, international team from
  - England, Scotland, Portugal, Italy, Ukraine, Australia, Germany, Greece, Ireland, Hungary, Romania
- Partner in UK Research Institute on Trustworthy ICS (RiTICS)
Safety and security
Research Institute in Trustworthy Industrial Control Systems

£2.4M programme, 5 coordinated projects.
Phase 1 (Directorship) awarded 01/01/14, Chris Hankin, Imperial College London.
Phase 2 awarded 01/10/14.

MUMBA: Multifaceted metrics for ICS business risk analysis
CAPRICA: Converged approach towards resilient industrial control systems and cyber assurance
CEDRICS: Communicating and evaluating cyber risk and dependencies in ICS
SCEPTICS: A systematic evaluation process for threats to ICS (incl. national grid and rail networks)
RITICS: Novel, effective and efficient interventions
Health Foundation Review

Health Foundation Report
An assurance and decision analysis framework

Reasoning and communicating with assurance cases
Developing assurance

Influence diagram

CAE structure

Mental models

Engineering models
Assurance principles

Understand the system and environment

Assurance process

Case itself

• Effective understanding of the hazards and their control should be demonstrated
  – Intended and unintended behaviour of the technology should be understood
  – Multiple and complex interactions between the technical and human systems to create adverse consequences should be recognised.

• Active challenge should be part of decision making throughout the organisation.

• Lessons learned from internal and external sources should be incorporated.

• Justification should be logical, coherent, traceable, accessible, repeatable with a rigour commensurate with the degree of trust required of the system.
CAE - concepts

- **Claims**, which are assertions put forward for general acceptance
  - They are typically statements about a property of the system or some subsystem. Claims that are asserted as true without justification become assumptions and claims supporting an argument are called sub-claims.

- **Evidence** that is used as the basis of the justification of the claim
  - Sources of evidence may include the design, the development process, prior field experience, testing (including statistical testing), source code analysis or formal analysis.

- **Arguments** link the evidence or sub-claim to the claim
  - They are the “statements indicating the general ways of arguing being applied in a particular case and implicitly relied on and whose trustworthiness is well established”, together with the validation for the scientific and engineering laws used.
Concept: Assurance case

Assurance Case “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”
In practice … the engineering and the tools
In practice ...

The importance of narrative
Reaching back – avoiding ppt of ppt dilution
Communication and reasoning

- Structured justification has two roles:
  - Communication is essential, from this we can build confidence and consensus
    - boundary objects that record the shared understanding between the different stakeholders
  - A method for recording our understanding and reasoning about dependability
- Both are required to have systems that are trusted and trustworthy
Standards and guidelines

- IEC/ISO
  - ISO/IEC 15026-2:2011 IS Systems and software assurance assurance cases
  - IEC 62741 Ed. 1.0 (WD) Reliability of systems, equipment and components, guide to the demonstration of dependability requirements. The dependability case
  - IEC 62853/Ed1: Open Systems Dependability
- OMG Object Management Group
  - Structured Assurance Case Meta-Model (SACM)
  - RFI on Machine-checkable Assurance Case Language (MACL)
- Opengroup
  - Real-Time and Embedded Systems: Dependability through Assuredness Framework
Strength or confidence in an “argument”

• How do we describe how confident we are or need to be?
  – Linguistic, probabilistic, implicit

• How do we aggregate doubts/confidence into the overall judgment in a way that is conservative but useful?
  – Bayesian frameworks (BBNs) not feasible, look for conservative, rigorous yet useful approaches. Chain of confidence.

• Can we build confidence by addressing inherent sources of doubt in the informal notations?
  – Development of CAE Blocks
  – Interplay of deductive and inductive
Development of the Blocks approach
5 Building Blocks

- **Decomposition**
  Partition some aspect of the claim

- **Substitution**
  Refine a claim about an object into claim about an equivalent object

- **Evidence incorporation**
  Evidence supports the claim

- **Concretion**
  Some aspect of the claim is given a more precise definition

- **Calculation or proof**
  Some value of the claim can be computed or proved
**General structure of the block**

CAE blocks are a series of archetypal argument fragments. They are based on the CAE normal form with further simplification and enhancements.
Decomposition block

This block is used to claim that a conclusion about the whole object, process, property or function can be deduced from the claims or facts about constituent parts.

\[ P_1(X_1) \land P_2(X_2) \land \ldots \land P_i(X_n) \Rightarrow P(X) \]

Example of a single object decomposition
Examples of single decomposition

- Architectural decomposition
  - Subsystem 1 hazards are mitigated
  - Subsystem 2 hazards are mitigated
  - System is composed of Subsystem 1, Subsystem 2 and interaction
  - Interaction hazards are mitigated
  - System hazards are mitigated
Substitution block

This block is used to claim that if a property holds for one object, then it holds for an equivalent object. The nature of this ‘equivalence’ will vary with the object and property and will need to be defined.

Object substitution

Property substitution
Examples of substitution

Product X is reliable

Object substitution

Product Y is reliable

Product X and product Y are equivalent

All devices of type X are equivalent

Devices of type X are safe

Object substitution

The device analysed, being of type X, was safe

Product substitution

Generalised: product type substitution
Evidence incorporation

This block is used to incorporate evidence elements into the case. A typical application of this block is at the edge of a case tree where a claim is shown to be directly satisfied by its supporting evidence.
Example of evidence incorporation

There are 25 successful tests

Test report directly shows that there are 25 successful tests
Concretion

This block is used when a claim needs to be given a more precise definition or interpretation. The top claim $P(X, Cn, En)$ can be replaced with a more precise or defined claim $P1(X1, Cn, En)$.
Example of concretion

Risks due to CCF are tolerable in the deployed system

Property concretion

Pfd due to CCF < target

The risks due to CCF are considered tolerable if they are < target

Environment concretion

The operational environment is a locked room

A locked room is a safe operating environment

The operational environment is safe
Calculation

This block is used to claim that the value of a property of a system can be computed from the values of related properties of other objects. Show that the value $b$ of property $P(X, b, E, C)$ of system $X$ in env $E$ and conf $C$ can be calculated from values $Q_1(X_1, a_1, E, C), Q_2(X_2, a_2, E, C), ..., Q_n(X_n, a_n, E, C)$.

$$b = F(a_1, a_2, ..., a_i)$$
Example of calculation

Availability of the system is $a$

Failure rate of the system is $fr$

Recovery time of the system is $rt$

Calculation:

$$a = 1 - fr \times rt / 2$$
‘Helping hand’ - guidance on selecting Blocks

- Evidence incorporation
  - Calculation
  - Decomposition
  - Substitution

1. Does the claim involve a calculated property?
2. Would it be easier to satisfy the claim by splitting it up?
3. Easier to justify for an equivalent object or property?
4. Consider concretising or redrafting

- Is the claim adequately expressed?
  - yes
    - Concretion
  - no
    - Can the claim be satisfied by the available evidence?
      - yes
        - Calculation
      - no
        - Consider concretising or redrafting
Schematic of the CAE stack
Fragments

Nordic 32 example

Use of blocks:

1. Concretion
2. Substitution
   - Decompositions
   - Evidence incorporations
3. Decomposition
   - Evidence incorporations
Tool support – ASCE


(free for non-commercial educational use)
Summary

• Claims Argument Evidence
  – Use of terminology
  – Trusted evidence required
• Key roles for Case
  – Communication and reasoning
• Importance of both narrative and graphical structure
• Mature tools, methodology, guidance
• Illustrated some aspects of how deal with confidence
• Keen to learn from this community
  – Methodology and theoretical basis
  – Experience from other application areas
  – Comments and suggestions welcome