CAE Building Blocks
ASCE User Forum

Professor Robin E Bloomfield FREng
Dr Kateryna Netkachova
December 2014

PT/275/3017/11
Background
Background - drivers

- Nuclear industry
  - CAE New build, ONR
  - Licensees
  - UK and Swedish R&D
  - EU Harmonics project
  - IAEA

- Security informed safety
  - Adelard
  - City University London
Development of assurance

Influence diagram

CAE structure

Mental models

Engineering models

© ADELARD
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
Concept: Claims-Arguments-Evidence

Toulmin’s formulation of a claim

Example of a typical CAE structure
In practice ... the engineering
Building a Case

Technical strategies and solutions

- Property-based approach
- Safety justification
- Standards compliance
- Vulnerability assessment

MTTF_T > e.T / N.d

Principles and framework

Terminology and concepts

- Dependability
  - Availability
  - Reliability
  - Security
  - Confidentiality
  - Integrity
  - Maintainability

- Authorized actions

© ADELARD
Deployment of CAE

- Safety justification framework
  - Principles
  - Standards
  - Strategies
    - Strategy triangle
    - 4-state model
    - M0, M1, M2 layers
    - Standards
    - Evidence – attribute mappings
    - Information management
- Tools!
- CAE stack
Summary of principles

1. Effective understanding of the hazards and their control should be demonstrated
2. Intended and unintended behaviour of the technology should be understood
3. Multiple and complex interactions between the technical and human systems to create adverse consequences should be recognised.
4. Active challenge should be part of decision making throughout the organisation.
5. Lessons learned from internal and external sources should be incorporated
6. Justification should be logical, coherent, traceable, accessible, repeatable with a rigour commensurate with the degree of trust required of the system

*Derived from IAEA, UK Principles – EU Harmonics project*
Safety case strategy and system model

- Property-based approach
- Standards compliance
- Vulnerability assessment
- Safety justification
- Trusted
- Untrusted
- OK
- Error

Standards compliance
Vulnerability assessment
Safety justification
Layered analysis

- **M0 Policy and requirements**
  - the highest level where we analyse system requirements, safety and security policies

- **M1 Architectural level**
  - the intermediate level where we analyse the abstract system components combined according to the abstract architecture

- **M2 Implementation level**
  - the detailed level where we analyse the implementation of specific components and their integration within the specific architecture

- **Used for assessing policy interaction (M0), link to lifecycle processes**
Link to lifecycle processes

- The three layers provide a link between four important and interrelated processes:
  - The design and development lifecycle, typically some type of V
  - The risk management process
  - The safety lifecycle
  - The security lifecycle

- The development of M0-M1-M2 will draw on the products of these processes.
Mapping to development lifecycle
Standards and guidelines

• **IEC/ISO**
  – 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**
In practice ... the engineering
Why do we want to structure a Case?

The claim we want to investigate does not directly follow from the evidence:

- Does not easily relate to the property we want
  - Compliance vs reliability
  - Correctness not timing
- Derived from a slightly different system or device
- Not enough evidence
  - too few tests
- Evidence too “grey”
  - Superficially compelling but lacks rigour e.g. field experience
- Assumptions not addressed
  - Disparate evidence needed to build confidence
- To deal with scale of real cases
CAE stack

- Alphabet
- CAE definitions
- CAE blocks
- Templates
- Sentences and structure
- Narrative stories
- Cases

Application specific

Generic guidance
CAE Blocks – generic fragments

• **Design goal**
  • Empirically based – sufficiently expressive
  • Technically sound and able to link to more formal approaches

• **Support structuring**
  • Useful as restrict choice
  • In practice cases might combine blocks, use understood and problem specific approaches
    – Many different styles

• **Maturity**
  • Ideas around ~5 yrs
  • Used in nuclear industry case studies and R&D and part of our thinking
  • Technical paper available and draft guidance
Cases reviewed – empirically based

- Smart sensor safety case for the nuclear industry
- CCF case from previous FOG results
- The safety of a computer based medical device
- Generic medical device safety case
- The dependability of an electronic funds transfer system
- Changes to a payments system
- A defence training system
- Safety of changes to a command and control system
- An approach to assessing safety of ordnance
- A weapons safety case
- A case supporting vulnerability testing of an eVoting machine
5 Building Blocks

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

- **Substitution**
  Refine a claim about an object into a 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
The collection of blocks

5 basic blocks:
1. Decomposition
2. Substitution
3. Evidence incorporation
4. Concretion
5. Calculation

Composite blocks:
- Substitution + Decomposition
- Concretion + Decomposition
- Any basic block + Evidence incorporation
General structure of a block

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

- The argument node can be descriptive
- The side warrant helps make the argument and can be supported with backing
- It address the “because ..?” questions in more detail
  - Simple semantics is
  - $C_{11} \land C_{12} \land W \implies C_1$
  - We need to demonstrate this
- When we use a block we need to show:
  - Verification of the block
  - Validity with respect to the real world
- Discussion
  - “1+1 = 2”
Divide and rule

- Compose and relax
Decomposition block

- A claim that an object X has property P is justified from claims about other objects and properties
Decomposition block – single property

Example of a single object decomposition
Examples of decomposition

Decomposition by architecture

- Architectural decomposition
  - Subsystem 1 hazards are mitigated
  - Subsystem 2 hazards are mitigated
  - Interaction hazards are mitigated

Decomposition by system functions

- Functional decomposition
  - System is composed of Subsystem 1, Subsystem 2 and interaction
  - Service 1 is safe
  - Service 2 is safe

- System provides safe service
  - System's services are composed of Service 1 and Service 2
Decomposition

• 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.

• For example,
  • System decomposed into a sub-systems (architectural decomposition)
  • Property decomposed into sub-properties (attribute expansion)
  • Environment decomposed into different parts (e.g. threat levels, pressure temperature)

• Double decomposition is also allowed. For example, the block can be used to claim that a property of an object can be deduced from the sub-properties of sub-objects.
Decomposition – application questions

• What is the property? What is the object? What are the sub-objects?
  • Why these and no others? Do these need to be a complete set?

• What about links between sub-objects, should these be sub-objects in their own right?
  • What else is in the object? What else is it connected to?

• Does the object explicitly include environment and configuration, if not is this justified?

• How can the object property be inferred from the component properties?
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 X and product Y are equivalent

Product Y is reliable

Product substitution

Devices of type X are safe

Object substitution

The device analysed, being of type X, was safe

All devices of type X are equivalent

Generalised: product type substitution. (Beware of reasoning from specific to general!)
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 $Q(X, Cn, En)$.
Example of concretion

- Risks due to CCF are tolerable in the deployed system
- The risks due to CCF are considered tolerable if they are < target
- Pfd due to CCF < target
- Property concretion

- The operational environment is safe
- Environment concretion
- A locked room is a safe operating environment
- The operational environment is a locked room

Property concretion
Environment concretion
The value of a property of a system can be computed from the values of related properties of other objects (e.g. its sub-systems) in that environment and configuration. Show that the value $b$ of property $P(X, b, E, C)$ of system $X$ in environment $E$ and configuration $C$ can be calculated from the values of:

\[
b = F(a_1, a_2, ..., a_i)\]

where $Q(X, b)$, $Q_1(X_1, a_1)$, $Q_2(X_2, a_2)$, ..., $Q_i(X_i, a_i)$, and:

\[
Q_1(X_1, a_1) \land Q_2(X_2, a_2) \land ... \land Q_i(X_i, a_i) \land (b = F(a_1, a_2, ..., a_i)) \Rightarrow Q(X, b)
\]
Example of evidence incorporation

There are 25 successful tests

Test report directly shows that there are 25 successful tests

evidence incorporation

Test report
Evidence incorporation – explicit trust

Evidence demonstrates X

Demonstration requires direct trustworthy evidence

decomposition by subproperty

Evidence is trustworthy

Evidence purports to demonstrate X

"Trustworthy" could be expanded into attributes such as relevant, traceable. However, evidence about evidence could get horribly recursive.

evidence incorporation

Report showing X
Example of calculation

Availability of the system is \( a \)

Failure rate of the system is \( fr \)

Recovery time of the system is \( rt \)

Calculation

\[ a = 1 - fr \times rt / 2 \]
Composite blocks
Example of composite block

Composite block and its expansion to the underlying basic blocks
Fragments/Templates

Work in progress

1 - Claim for system reliability
2 - Substitution of claim about real system by one with the test results
3 - Justifying test approach
4 - Sentencing of the results
CAE framework – assessment support

Substitution of claim about real system to one where we have results

Sentencing of results

Justification in validity of experiment or analyses
CAE normal form

- Claim nodes may only be connected to argument nodes
- Argument nodes may only be connected to claim and evidence nodes
- Each argument node may only have one outbound link to a claim node
- Each claim is to be supported by only one argument
- Argument nodes must be supported by at least one subclaim or evidence node
- Evidence nodes represent the bottom of the safety argument and are not supported
- A claim, subclaim or evidence may support more than one argument

Example of a claim structure before and after normal form
Deploying CAE Blocks
Scenarios of use

- Internalise as lingua franca
- For reviewing cases and understanding intent
- For constructing cases
  - Top down
  - Bottom up
A helping hand with CAE
We have confidence that Device X is reasonably safe and effective for its intended use within its environment of use when being used by intended users. Device Remains safe in use. The manufactured device is safe. The device design is safe. Hazards are identified, safety requirements are developed, and evidence verifies implementation into final design. Hazards Identification Argument A risk management process is in place that is capable of reasonably identifying all hazards for the device. Hazards Identification (ISO 14971) – Risk Management
• Preliminary Hazards List
• Failure Modes & Effects Analysis
• Fault Tree Analysis
• Hazops
• System Hazards Analysis
• Health Hazards Analysis
• Medical Device Reports
• Predicate Device Performance
• Recalls
• Standards

Safety Requirements mitigate hazards that all hazards are covered, and residual risks are acceptably low.

Safety Requirements are clinically valid.

Design Process Risk Argument
Design Process Risk Evidence
Design Process Evidence

Functional performance is verified and valid for its indications for use. Functional performance Evidence

System reliability goals are established for the device. System reliability goals are clinically acceptable. Reliability Evidence

Reliability goals are clearly defined and traceable to all hazards.

Reliability Analysis and traceability with consideration of environments of use, duration of use, and intended users.

Clinical Evidence / Justification

Device is designed for manufacturability. Device is designed for manufacturability Evidence

The device design is effective. The device design is effective Evidence

The device design is safe. The device design is safe Evidence

The manufactured device is safe. The manufactured device is safe Evidence

The user receives the designed device. The user receives the designed device Evidence

Effective processes are in place to assure that field problems are fixed correctly and efficiently. Effective processes Evidence

Field experience is used to inform and improve hazards identification and reliability processes. Field experience Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Performance

Performance over time

Quality Systems as it relates to safety

Real life experience and feedback into design for safety
Development of assurance

Influence diagram

CAE structure

Mental models

Engineering models

© ADELARD
We have confidence that Device X is reasonably safe and effective for its intended use within its environment of use when being used by intended users.

Device Remains safe in use

The manufactured device is safe

The device design is safe

Safety Requirements are clinically valid

Safety Requirements Implementation Evidence

Residual Risk Evidence

Residual Risk/ Safety Requirements Traceability

Risk Management

Safety Requirements are clinically valid

Residual Risk/ Safety Requirements Traceability

Risk Management

Safety Requirements Implementation Evidence

Residual Risk Evidence

Residual Risk Risk Argument

Design Process Risk Argument

Design Process Evidence

Evidence

Functional performance Evidence

Reliability Evidence

Reliability Analysis and tests demonstrate compliance with applicable standards and environments of use, duration of use, and intended users

Reliability analysis and tests demonstrate that the device remains the same as designed

Clinical Evidence / Justification

Evidence

The manufactured device is safe

The user receives the designed device

Effective processes are in place to ensure that field problems are fixed efficiently

Field experience is used to refine and improve hazards identification and reliability processes

Real life experience and feedback into design for safety

Performance

Performance over time

Quality Systems as it relates to safety

Time split – now/future

Property decomposition/expansion

Under developed?

Concretion of all to most residual risks

Use of canvas – of the two dimensions

4-5 joins often need examining

© ADELARD
Summary

• **Empirically based, technically sound blocks**
  • Can be used at different levels of formality
  • CAE Normal form

• **5 basic blocks:**
  • Decomposition
  • Substitution
  • Evidence incorporation
  • Concretion
  • Calculation

• **Composite blocks:**
  • Substitution + Decomposition
  • Concretion + Decomposition
  • Any basic block + Evidence incorporation

• **Simple decision diagram for selecting block**
Positive outcome

- Standardised way of creating cases
- Simple patterns, easy to use
- Structured plus narrative argument
- Explicit Backing element
- Explicit links to system models, etc.
Methodology development

• Driven by markets
  – Explicit CAE in nuclear, medical
  – Security informed safety

• CAE support and more guidance
  – CAE Blocks
  – Challenge and review
  – Link to models
  – ASCE support via plugins, schema

• Prototypes and guidance trials
  – Beta-release to interested parties
  – Used on courses – Adelard, City University MSc
  – Nuclear industry workshops planned
    • UK, Sweden, France
  – Appetite for other workshops or consultations?
Generic guidance

• Draft developed
  • IPR can be used with acknowledgment

• Selective review July - Nov
  • Multi-domain
  • ONR, FDA, CAA
  • Nuclear licensees

• Workshops
  • Current practices

• Next version
  • Feb 2015
  • Include more extended examples
Future research

• Template meta-language
• Graduated formality
• Repository of examples
• Notation-independent
• Extended tool support