ADELARD

Assure 2018

Assurance Cases: methodologies, mindsets and convergence?

Robin E Bloomfield FREng

Adelard LLP
City, University of London

reb@adelard.com
18th September 2018

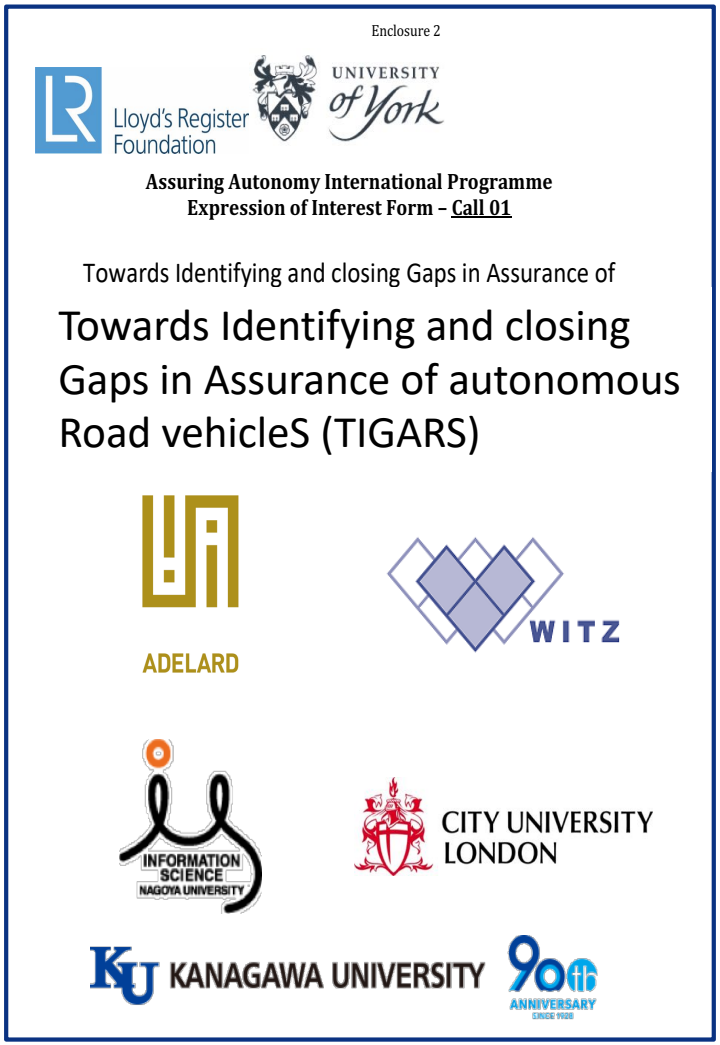
PT/550/171001/1

Adelard LLP, 24 Waterside, 44-48 Wharf Road, London N1 7UZ
T +44 20 7832 5850 E office@adelard.com W www.adelard.com

Assurance

- trust and trustworthiness are of enormous societal value
- is an enabler of innovation

Drivers



Enclosure 2

Lloyd's Register Foundation

University of York

Assuring Autonomy International Programme
Expression of Interest Form – Call 01

Towards Identifying and closing Gaps in Assurance of

Towards Identifying and closing Gaps in Assurance of autonomous Road vehicleS (TIGARS)

ADELARD

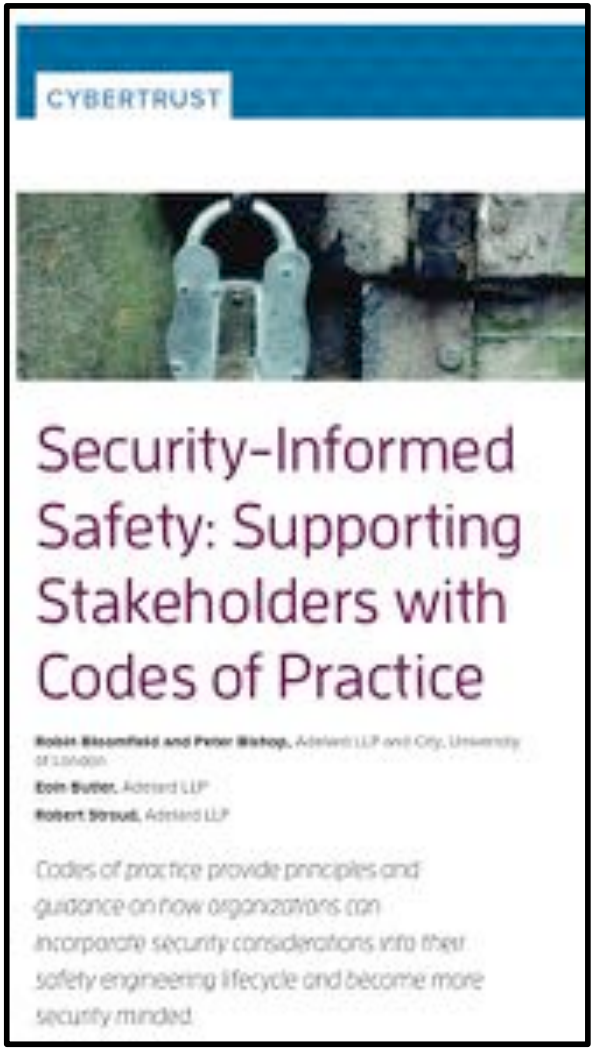
WITZ

INFORMATION SCIENCE NAGOYA UNIVERSITY

CITY UNIVERSITY LONDON

KANAGAWA UNIVERSITY

90th ANNIVERSARY



CYBERTRUST

Security-Informed Safety: Supporting Stakeholders with Codes of Practice

Robin Bloomfield and Peter Bishop, Adelard LLP and City University of London

Eoin Butler, Adelard LLP

Robert Stroud, Adelard LLP

Codes of practice provide principles and guidance on how organizations can incorporate security considerations into their safety engineering lifecycle and become more security minded.

Fundamentals of Effective Assurance Cases

- **Software Certification Consortium Meeting #19**
  Fundamentals of Effective Assurance Cases
  May 11-12, 2017 | Annapolis, Maryland | Co-located with HCSS 2018
- **Conference Archives:** https://cps-vo.org/group/scc/meetings
- Michael Holloway, Robin Bloomfield, Tim Kelly, John Rushby, Patrick Graydon , Kim Wasson, Fubin Wu, Tom Maibaum, Bill Scherlis, Edward Lee, John Goodenough, Paul Jones, Robert Martin,
- Remembering John Knight

Aims

- Assurance case practice and research
  - Improve practice
  - What does good look like?
- Challenges
  - Scale, tempo
  - Security and threats
  - AI and machine learning
  - Big data
  - Normal business
- Address challenges
  - Understand landscape
  - Develop methodology
  - Framework to support convergence, encourage innovation

Outline

- Engineering argumentation
  - Context and problem statement
- CAE Methodology
  - Summary of approach and understanding
    - Inductive, deductive, defeaters
  - Application and mindset
- Convergence
  - Outline framework
    - Divergence or convergence?
- Discussion and conclusions

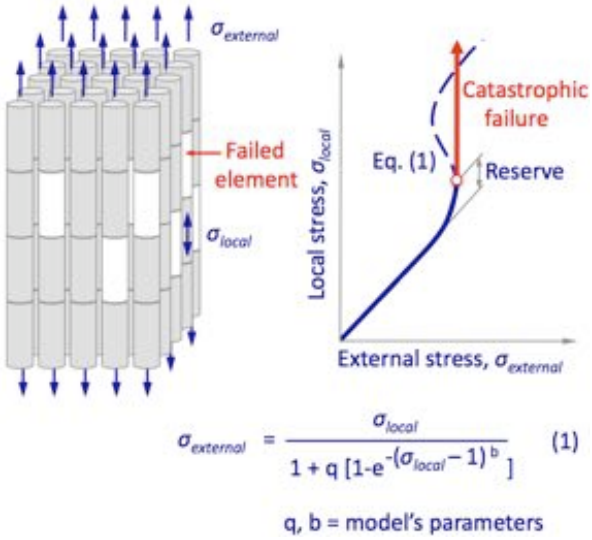
Engineering reasoning and assurance

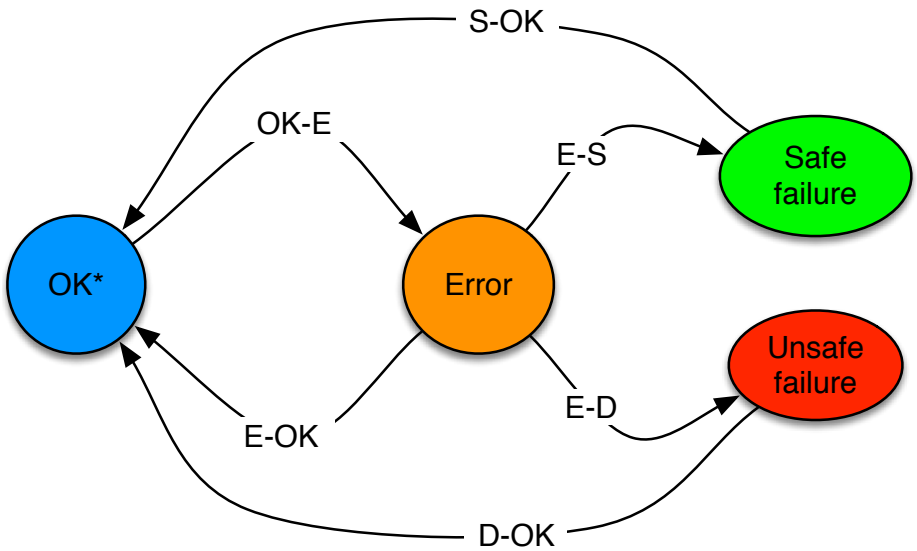
Success of dependability engineering

Success of dependability engineering

- Automotive engineering
  - Yet Toyota, VW
- Air and rail transportation
  - Yet Spanish crash, Nimrod
- Finance system
  - Yet crashes, $400M bug
- Nuclear power
  - Yet Fukushima, QA fraud
- Consumer products
  - Yet recalls and data loss
- Medical systems
  - Yet avoidable deaths

Potential Catastrophic failures





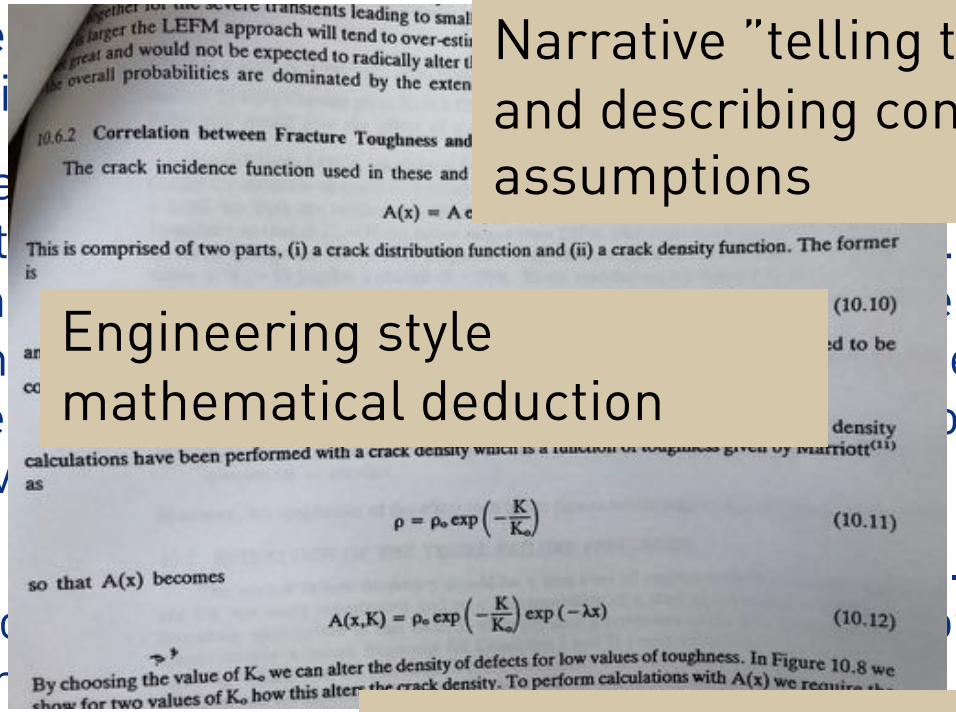
https://upload.wikimedia.org/wikipedia/commons/2/2b/CatastropheFailureModel.png

Engineering - probabilistic fracture mechanics

- Extract from supporting documentation
  - The variability generally treated by PFM is that arising from random variation due to the manufacturing process or method of operation. This type of behavior is ideally treated probabilistically because information is usually available.
  - In PFM analysis we consider whether failure might occur with an unacceptable frequency due to random deviations …..However, gross deviations from design parameters *are not modelled* (because of the lack of information on their form) and *these can often be a major cause of failure*, as seen from examination of the causes of failure of non-nuclear vessels. …..
  - … These may be caused by design or human errors. *Such deviations should not, of course occur* with modern methods of manufacture and operation. *Thus* the failure frequency calculated ….

Example - Engineering - probabilistic fracture mechanics

- The variability generally treated by PFM is that arising from random variation due to the manufacturing process or method of operation. This type
- In PFM a ....However, gross unaccept deviation ed (because of the lack of in en be a major cause of failure of failure of non-nuclear v
- ... These . Such deviations should n f manufacture and operation



larger the LEFM approach will tend to over-esti
great and would not be expected to radically alter t
overall probabilities are dominated by the exten

10.6.2 Correlation between Fracture Toughness and

The crack incidence function used in these and

$A(x) = A e$

This is comprised of two parts, (i) a crack distribution function and (ii) a crack density function. The former is

(10.10)

ed to be

density

calculations have been performed with a crack density which is a function of toughness given by Marriott[11] as

$$\rho = \rho_o \exp\left(-\frac{K}{K_o}\right) \qquad (10.11)$$

so that A(x) becomes

$$A(x,K) = \rho_o \exp\left(-\frac{K}{K_o}\right) \exp(-\lambda x) \qquad (10.12)$$

By choosing the value of K_o we can alter the density of defects for low values of toughness. In Figure 10.8 we show for two values of K_o how this alter the crack density. To perform calculations with A(x) we require

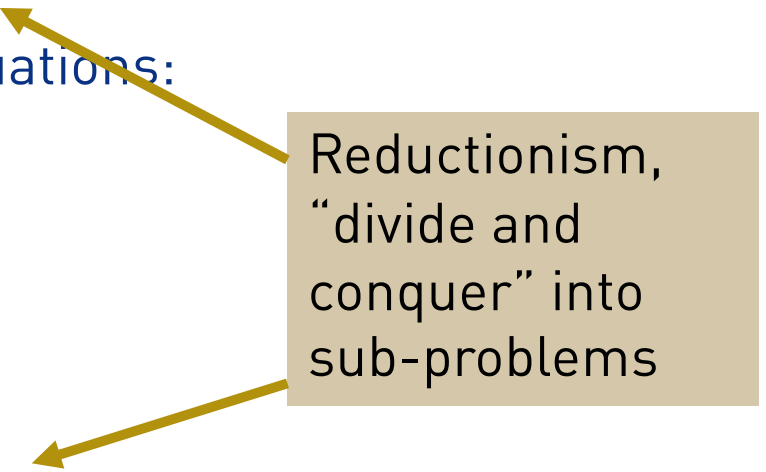
Narrative "telling the story" and describing context and assumptions

Engineering style mathematical deduction

References supporting papers

Medical infusion pumps

- FDA recommends that the hazard analysis include a process for identifying initiating events and sequences of events for each hazardous situation throughout all aspects of device use (e.g., drug loading, priming, programming, infusion).
- Sources of hazardous situations:
  - Operational (Table 3)
  - Environmental (Table 4)
  - Electrical (Table 5)
  - Hardware (Table 6)
  - Software (Table 7)
  - Mechanical (Table 8)
  - Biological and Chemical (Table 9)
  - Use (Table 10)



Software testing - IAEA

Narrative "telling the story" and describing context and assumptions

There is a limit to the reliability figures that can be [illegible] statistical testing. In part these are practical issue[illegible] done in a reasonable time that might be amenable to test acceleration in some form. Other considerations are more limiting, and arise when the assumption doubts dominate the reliability figure.

We need to take these into account in the justification of the quantified reliability and one way we can do this is to use the so-called chain rule. This rule is often used to deal with uncertainty (e.g. whether two channels are independent or not). So if P_{assump_OK} is the confidence that the assumptions underlying some *pfd* estimation rule are applicable, then:

$$E(pfd) = P_{assump\_OK} * (pfd1 | assump\_OK) + (1 - P_{assump\_OK}) * pfd2 \quad \text{- (st1)}$$

where $pfd1|assump\_OK$ is the estimated value if the assumptions underpinning the rule1 are valid. For the case where the rule assum[illegible] some alternative *pfd* estimation method.

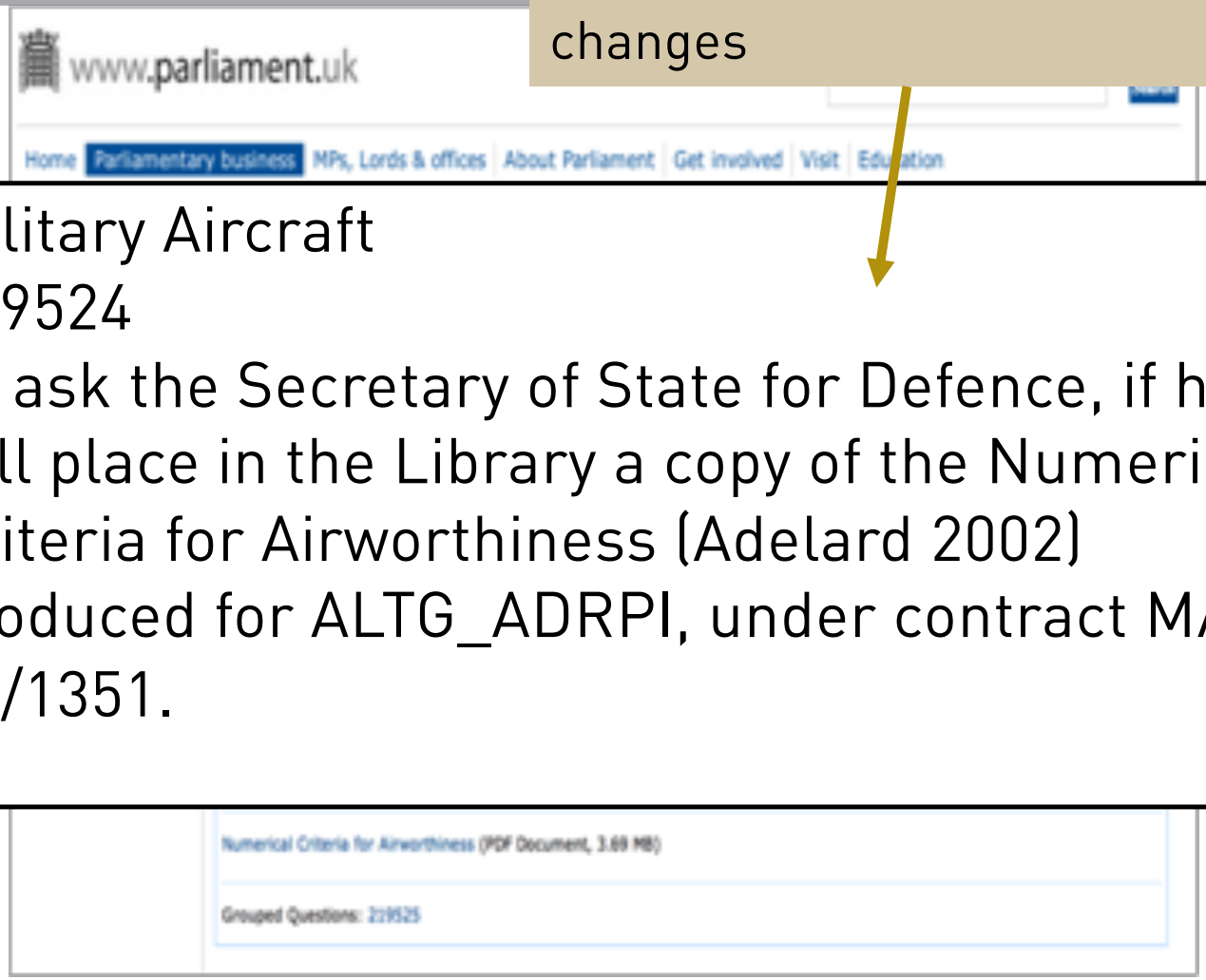
Engineering style mathematical deduction

(st1) can be approximated as:

$$E(pfd) < (pfd1 | assump\_OK) + P_{assump\_not\_OK} * pfd2$$

Airworthiness

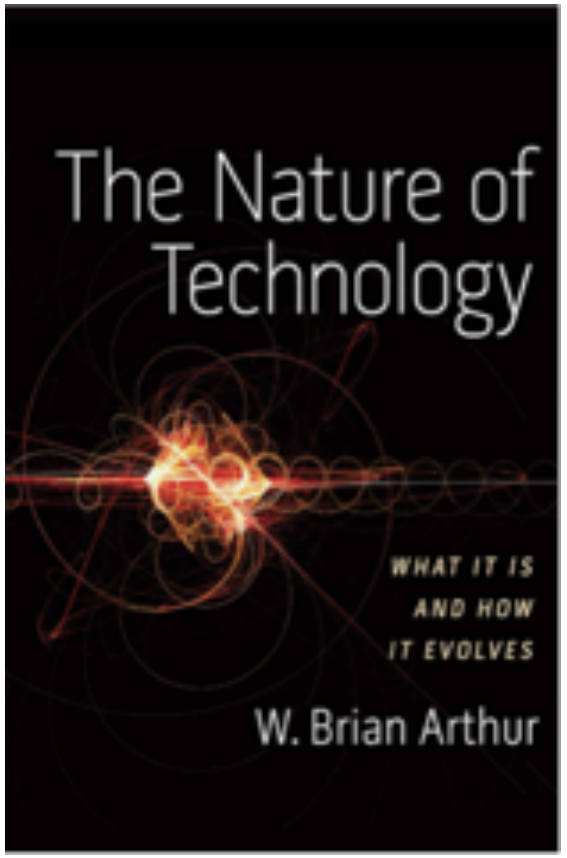
Longevity
Stakeholder and audience changes



Military Aircraft
219524
To ask the Secretary of State for Defence, if he will place in the Library a copy of the Numerical Criteria for Airworthiness (Adelard 2002) produced for ALTG_ADRPI, under contract MAP 2b/1351.

Complexity

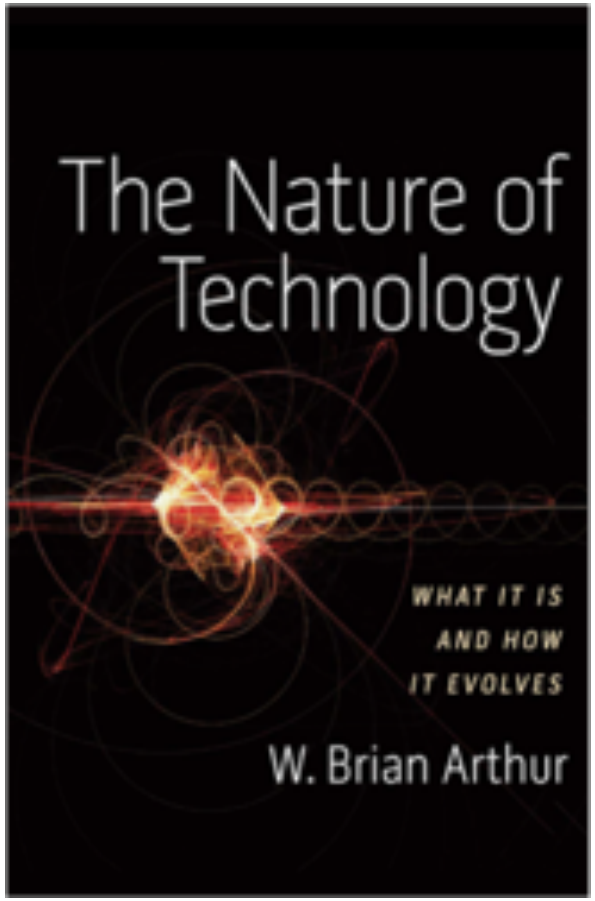
- Structural deepening - adaptations to remove obstacles, improve performance but
  - "Over time it becomes encrusted with systems and subassemblies hung onto it to make it work properly, handle exceptions, extend its range of application, and provide redundancy
- Adaptive stretch – for new applications or requirements
- Structural deepening, lock-in, and adaptive stretch—have a natural cycle.
- Eventually old principle is strained beyond limits and gives way to a new one.



Structural deepening - complexity

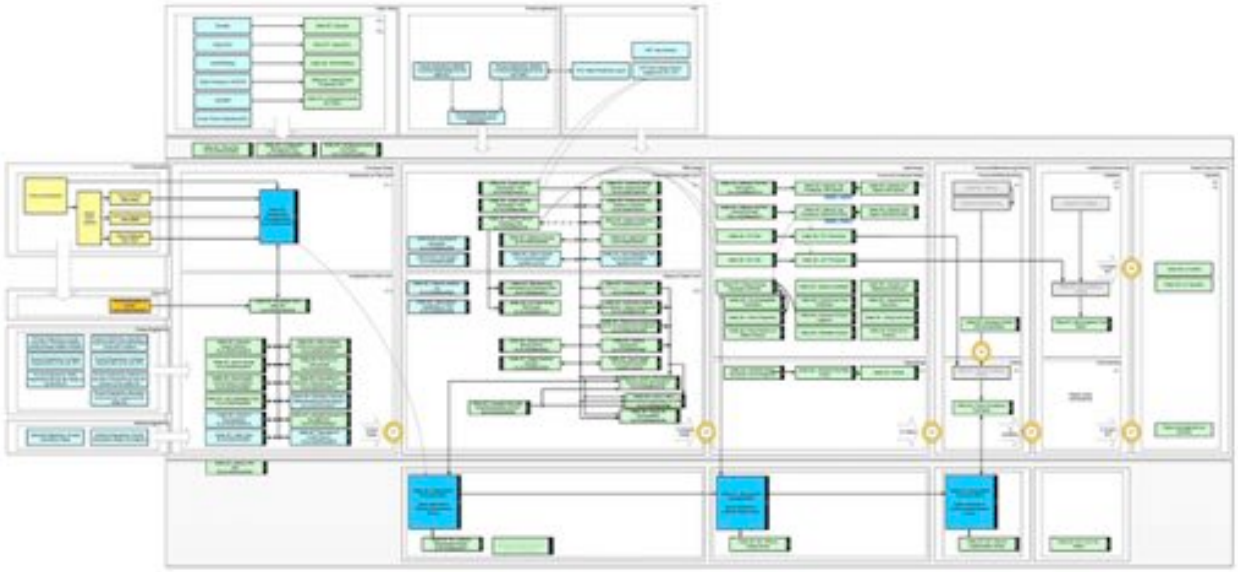
- Modern aircraft engines are 30 to 50 times more powerful than Whittle's original jet engine
- Whittle's turbojet prototype of 1936 and a few hundred parts; its modern equivalent has upwards of 22,000 parts.

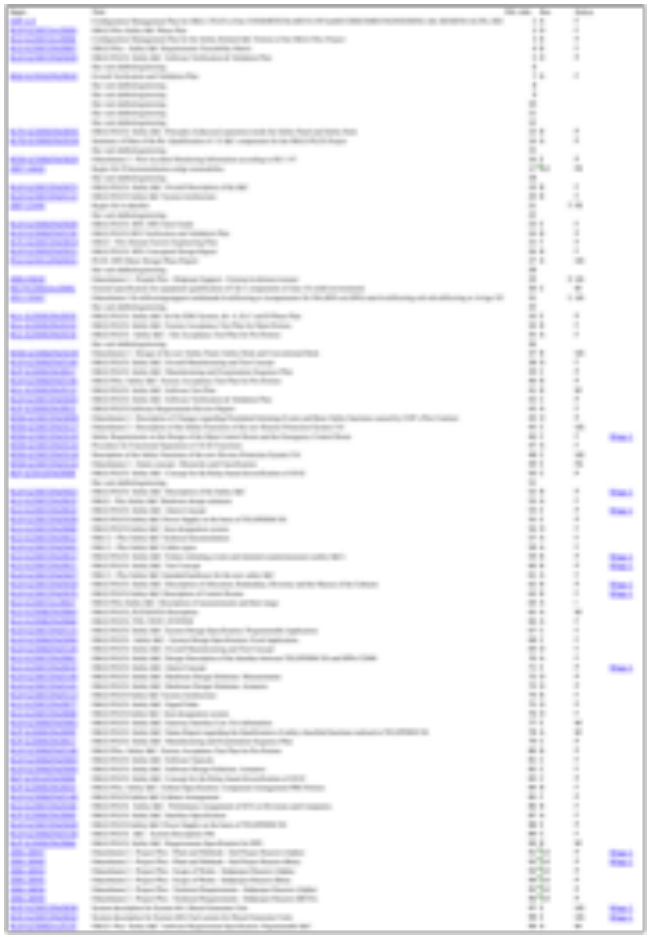
  - Arthur, W. Brian. The Nature of Technology: What It Is and How It Evolves (Kindle Locations 1958-1960). Penguin Books Ltd.



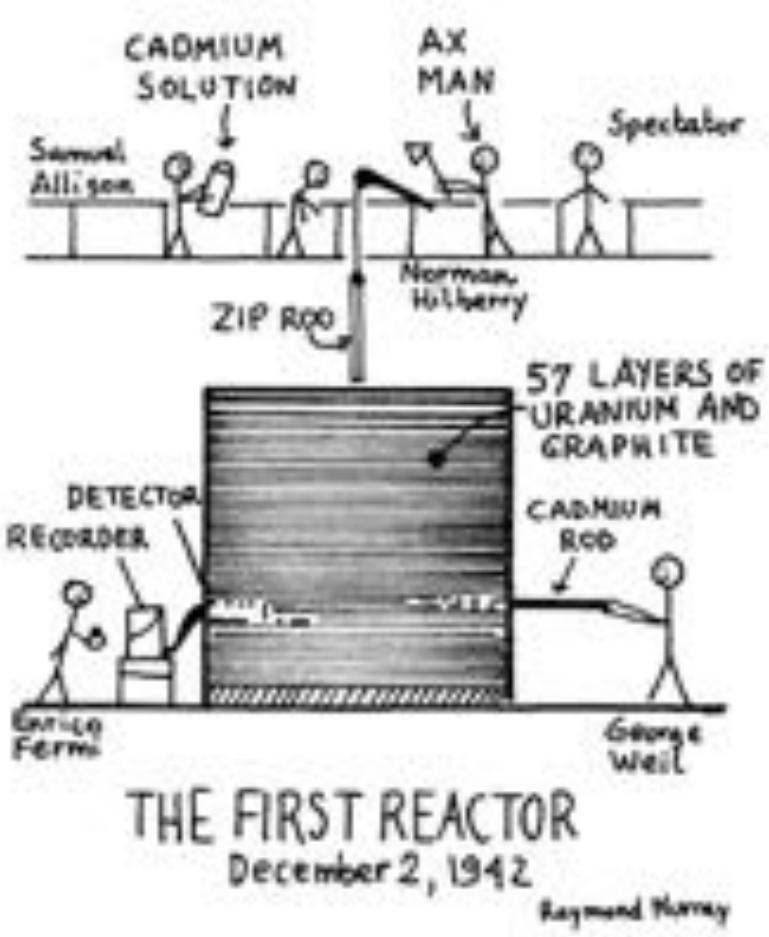
Scale – Multiple lifecycle processes

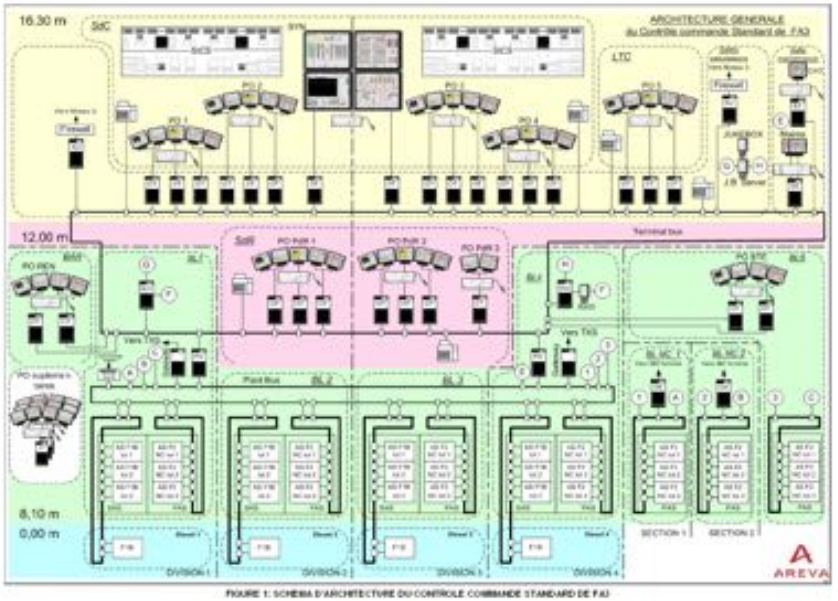
- Review of a project
  - 120 documents
  - Grouped according to phases and scope





Reactor protection systems





The new millennium

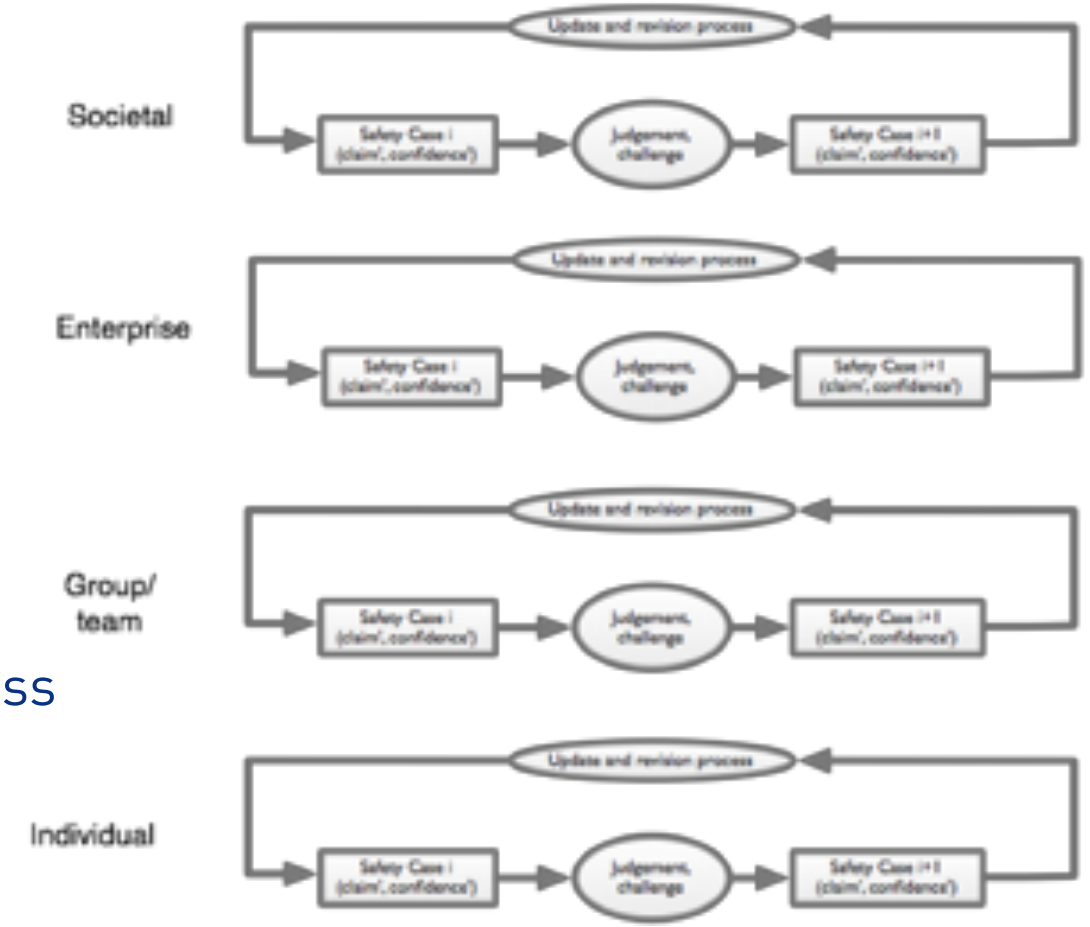
- Four challenges
  - Security-informed safety
  - Resilience
  - Autonomy and Machine Learning
  - Normal business
- If we were producing a comprehensive roadmap for achieving and evaluating safety and resilience exploit insights into the range of interlocking issues to be addressed
  - RAEng report on the connected world and cyber safety and resilience (RAEng 2015, 2018),
  - NAS study on 'Sufficient Evidence' (Jackson 2007)

Communication and reasoning

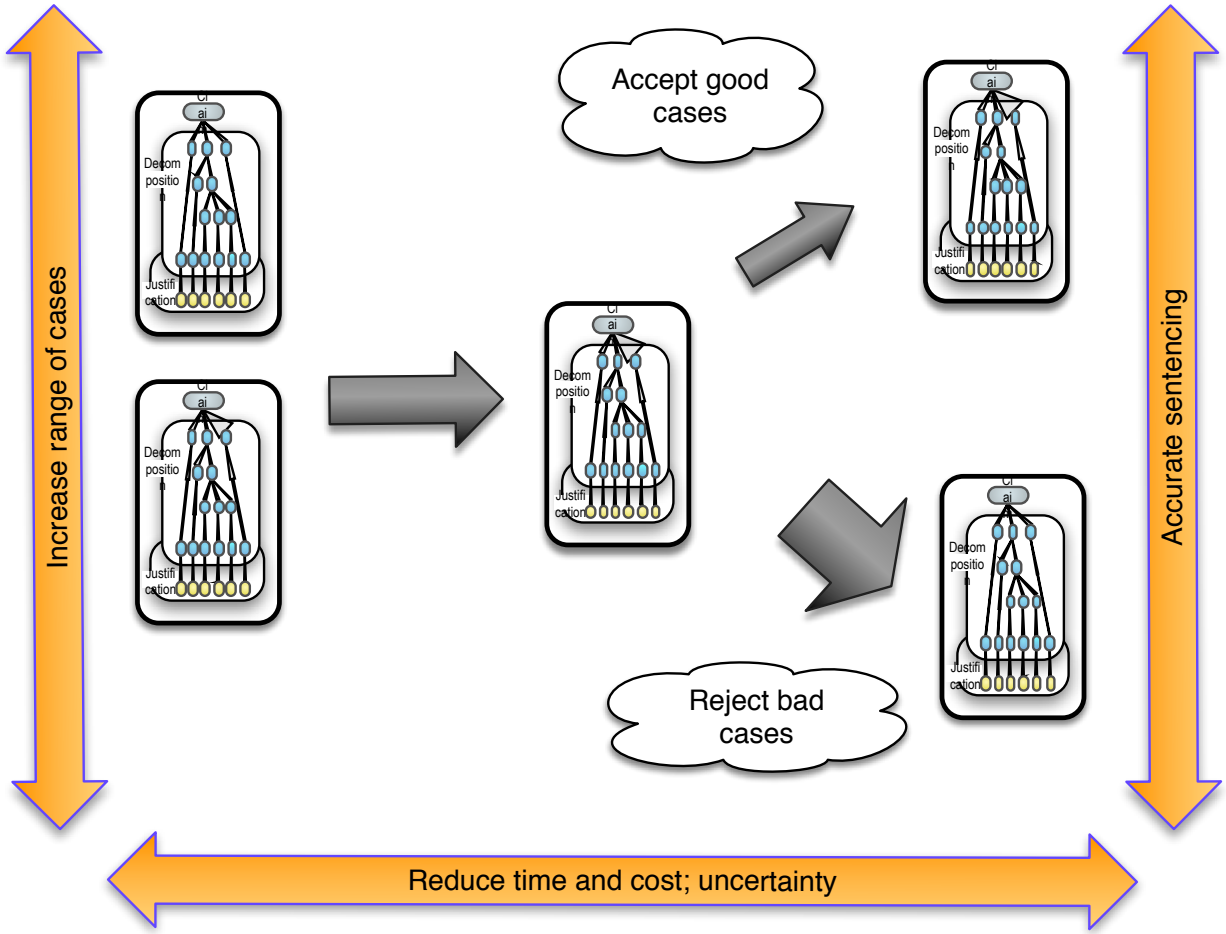
- Assurance case has two roles:
  - communication is essential, from this we can build confidence and consensus
    - boundary objects that record the shared understanding between the different stakeholders
  - a method for recording our understanding and reasoning about dependability
- Both are required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

Assurance process – building confidence, challenging assumptions

- Captured in a management system and in meta-case
- Challenge and response cycle essential
- Proof as a social, technical, adversarial process



Effectiveness



Nature of engineering justifications

- Descriptions
  - Narrative, specialized vocabularies
  - Notations and diagrams
  - Multi disciplines
- Models and reasoning
  - Mathematical as well as informal, computer based
  - Structure and behaviour
  - Assumptions and caveats
- Scale
  - Recursive – structural deepening
- Lifeycle processes
  - Complexity, longevity
- Proportionate and appropriate for the audience

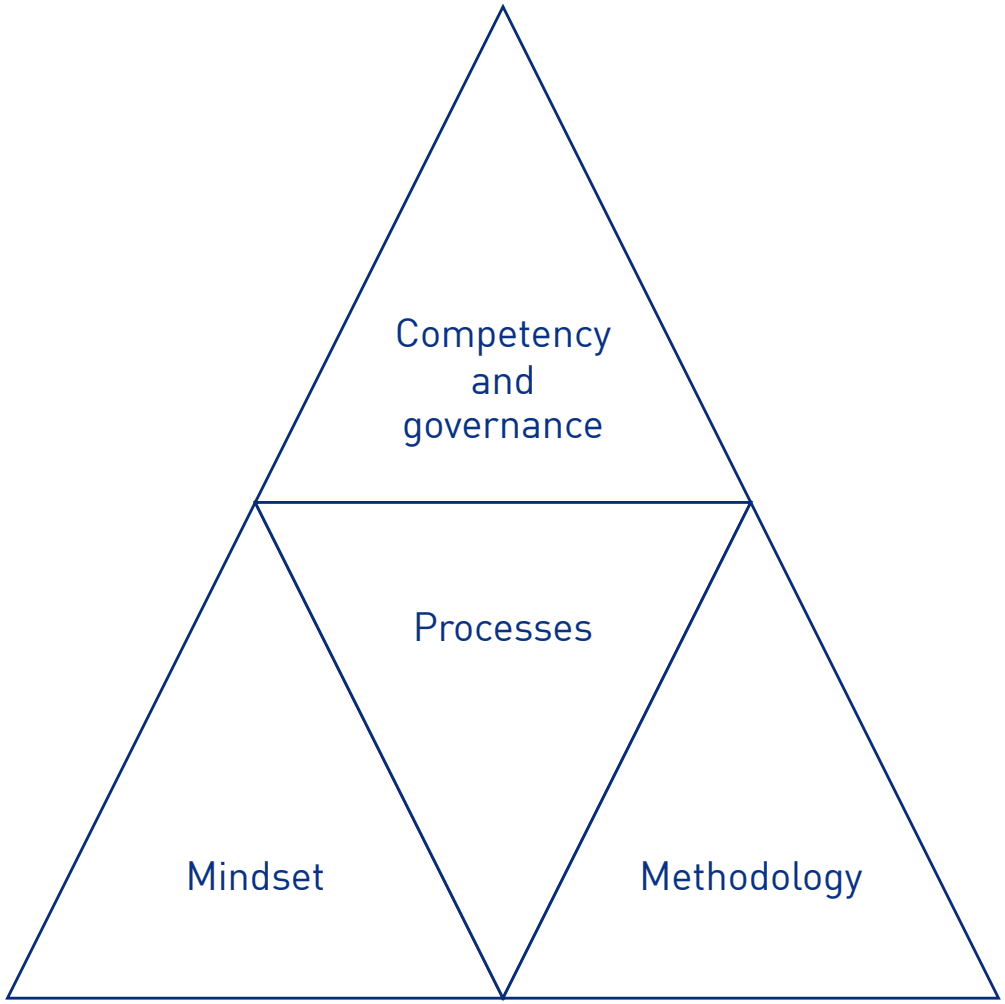
Methodology

Learning from experience

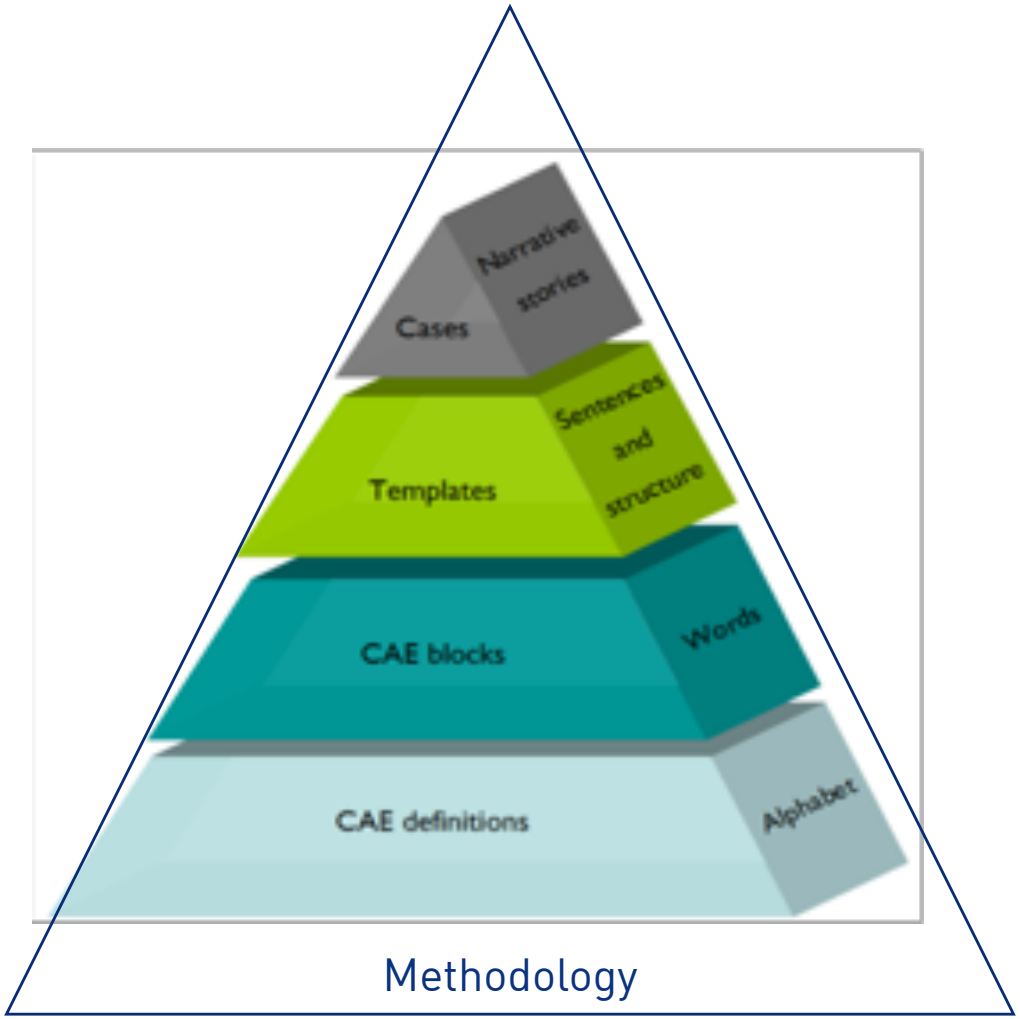
Evaluation and effectiveness

- Review use of cases across different applications
  - Understood their role better, what we thought was trying to be expressed
- Hazard analysis of case process
  - Convincing but invalid cases
- Masters courses
  - Compared final projects
- ASCE courses
  - 40 last year
- Case study application
  - Recast and analysed real cases
- Recently
  - Workshops and following industrial adoption

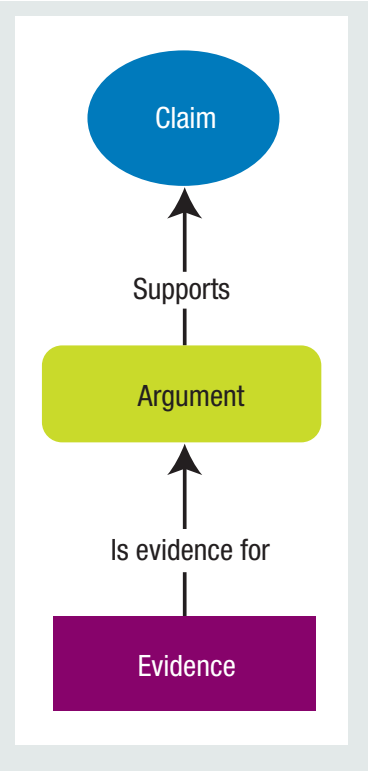
Effective cases



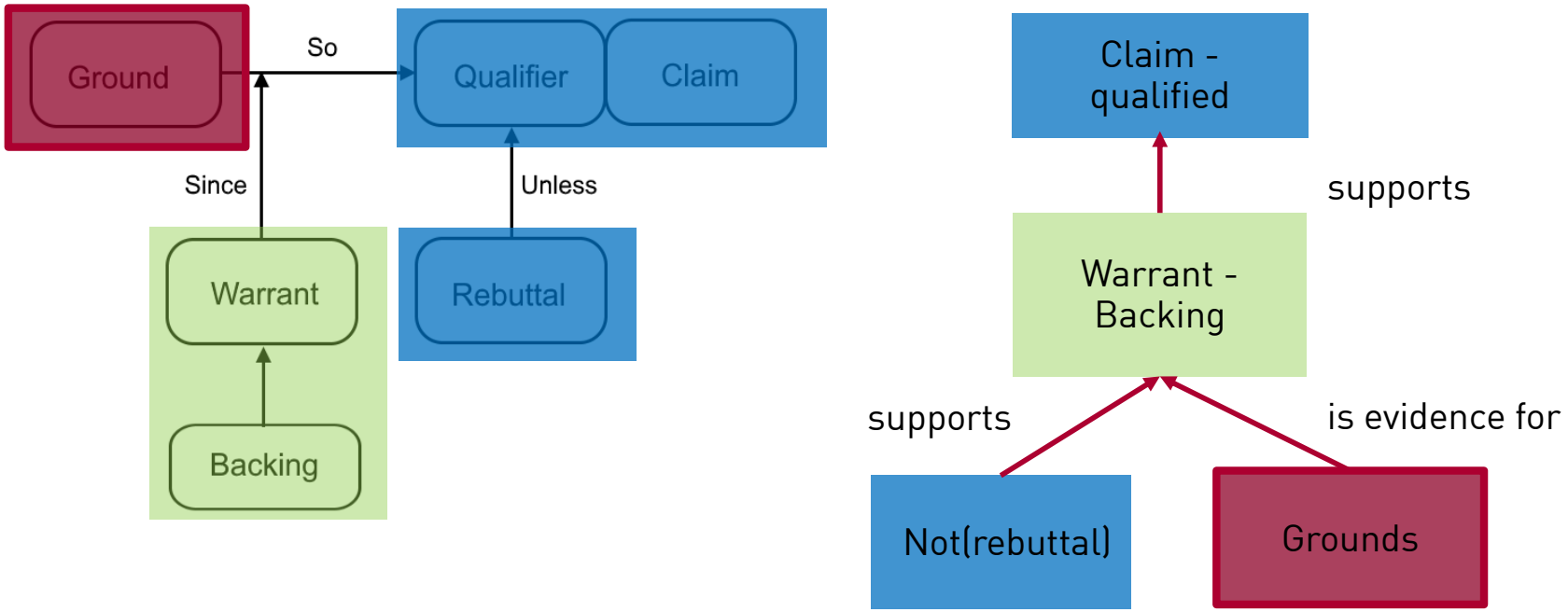
CAE Stack



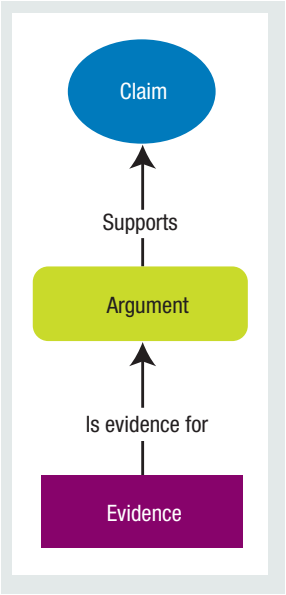
Claims, Arguments, Evidence

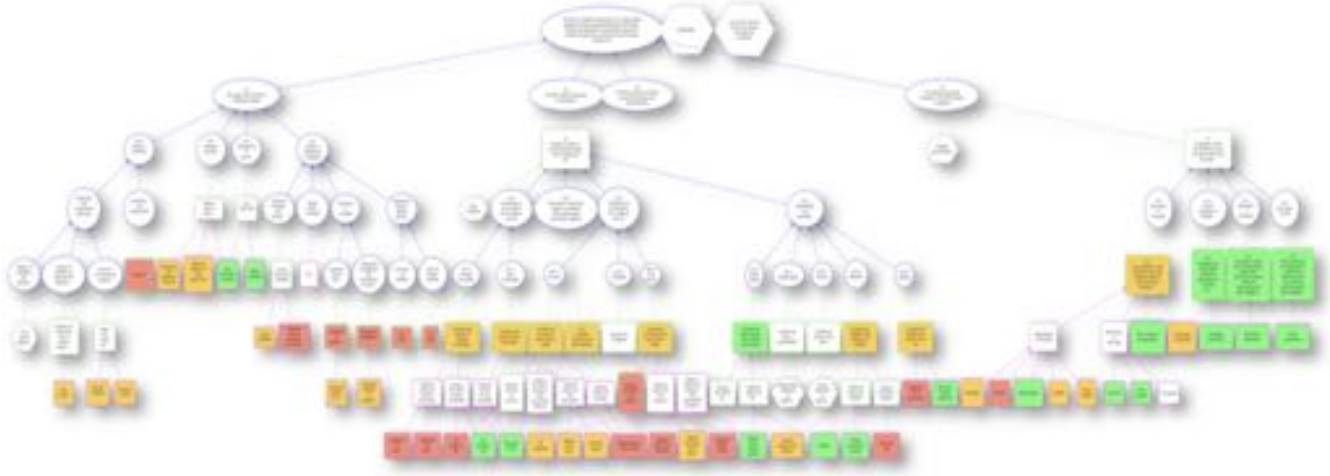


Toulmin notation and CAE



From concepts to engineering





CAE - concepts

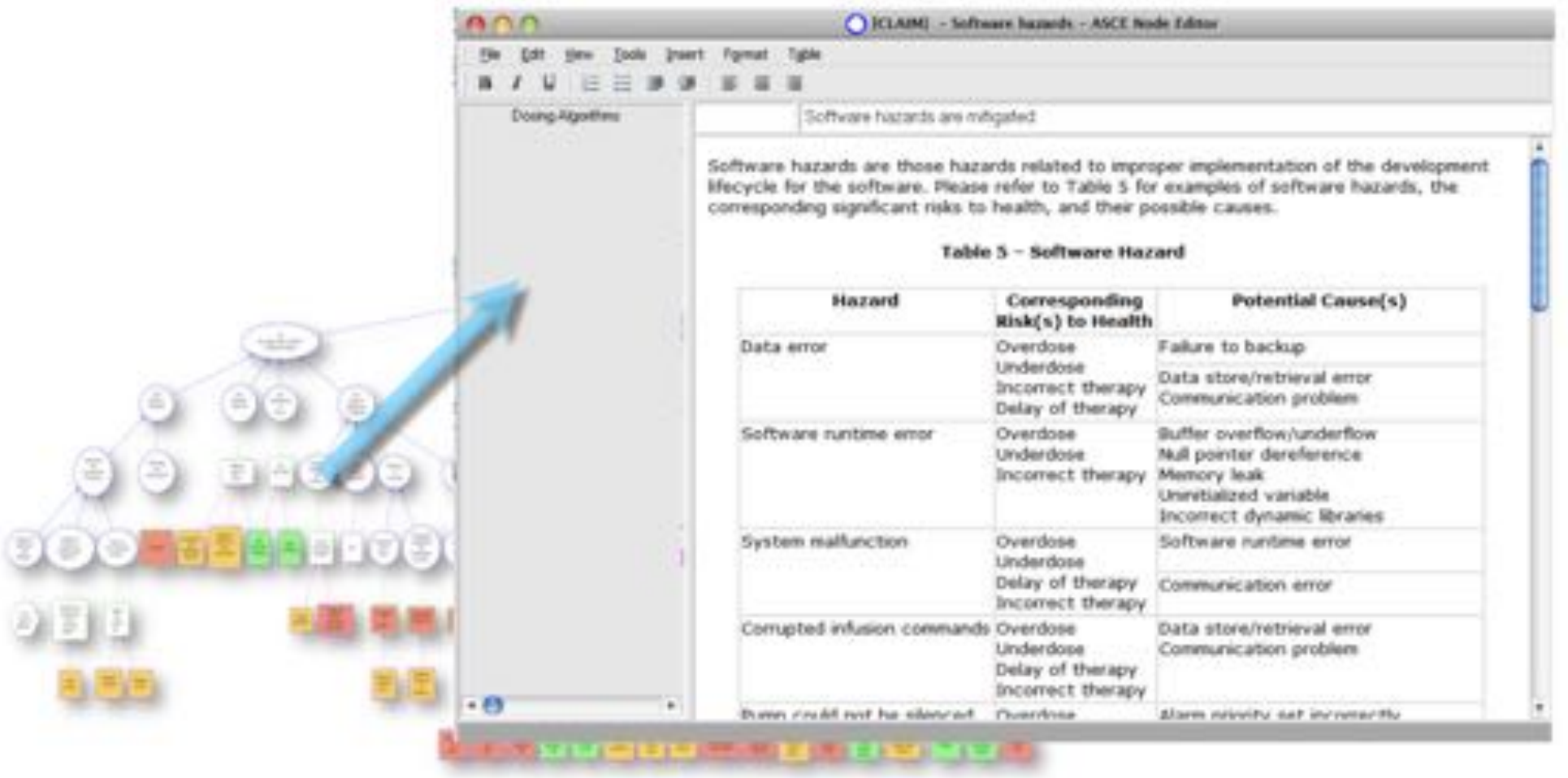
- ***Claims***, which are assertions put forward for general acceptance
  - They are typically statements about a property of the system or some subsystem. Claims that are asserted as true without justification become assumptions and claims supporting an argument are called sub-claims. Implicit and explicit confidence. Claims can propositionalise uncertainty.
- ***Arguments***, which link the evidence 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. i.e. Instantiated "Warrants" in Toulmin scheme
- ***Evidence***, which 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.

Deductive and inductive arguments

- For valid deductive arguments the premises *logically entail* the conclusion
  - The entailment means that the truth of the premises provides a *guarantee* of the truth of the conclusion.
- An inductive logic is a system of evidential support that extends deductive logic to less-than-certain inferences.
  - In a good inductive argument the premises should provide some *degree of support* for the conclusion, where such support means that the truth of the premises indicates with some *degree of strength* that the conclusion is true.
  - acceptability, relevance and sufficiency

Adapted from https://plato.stanford.edu/index.html

CAE in practice – narration



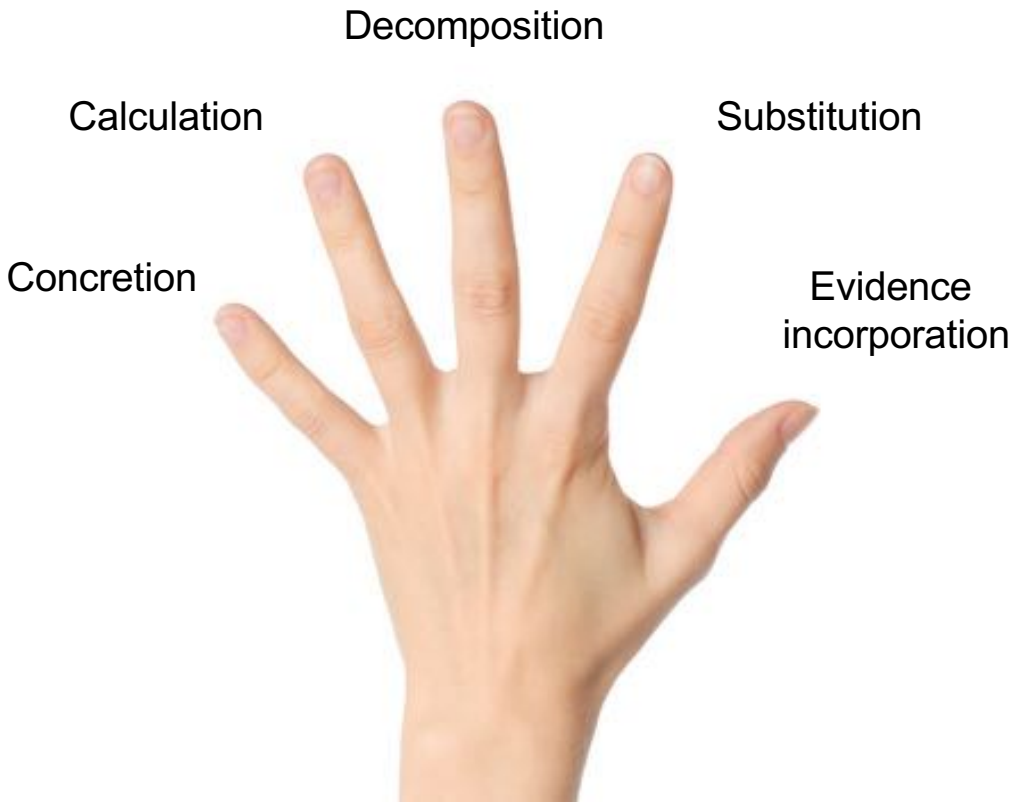
Cases reviewed – empirically based

- Smart sensor safety case for the nuclear industry
- CCF case from previous research 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

Language initially unconstrained CAE and GSN

Empirically found a small set of constructs expressive enough - CAE “Blocks”

Five Building Blocks



Decomposition

Partition some aspect of the claim

Divide and conquer

Substitution

Refine a claim about an object into claim about an equivalent object

Evidence incorporation

Evidence supports the claim

Emphasis on direct support

Concretion

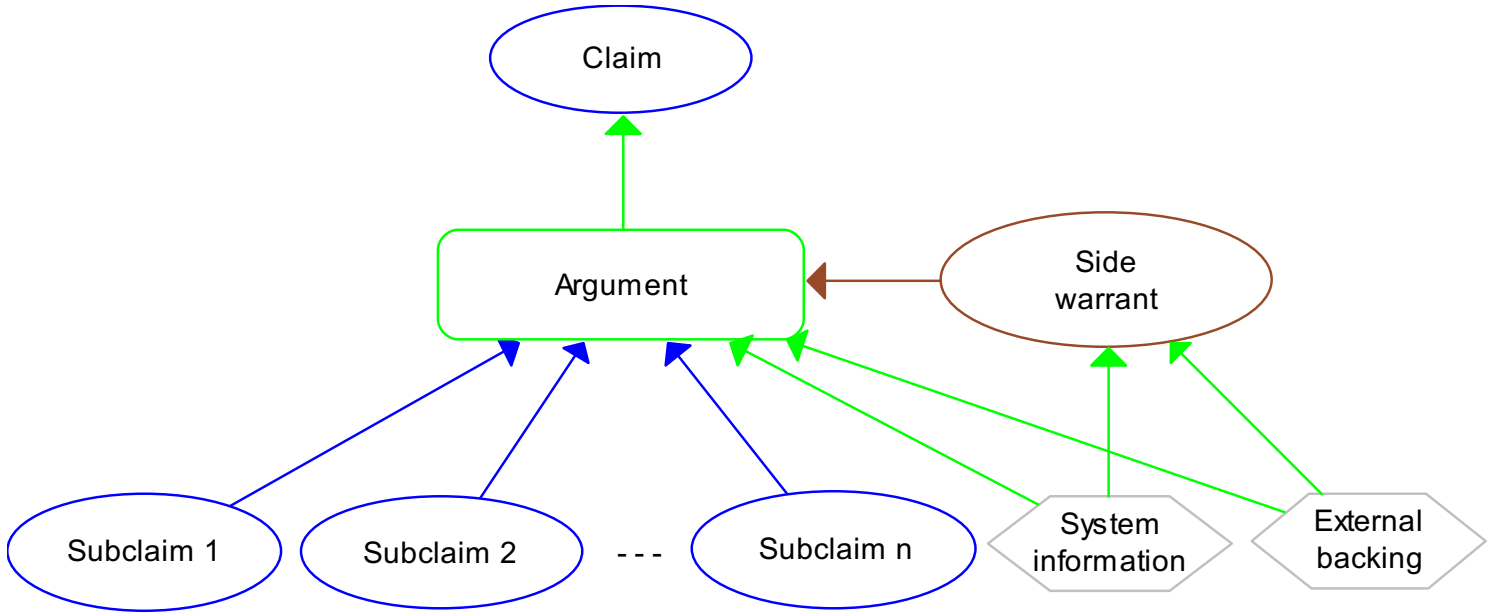
Some aspect of the claim is given a more precise definition

Calculation or proof

Some value of the claim can be computed or proved

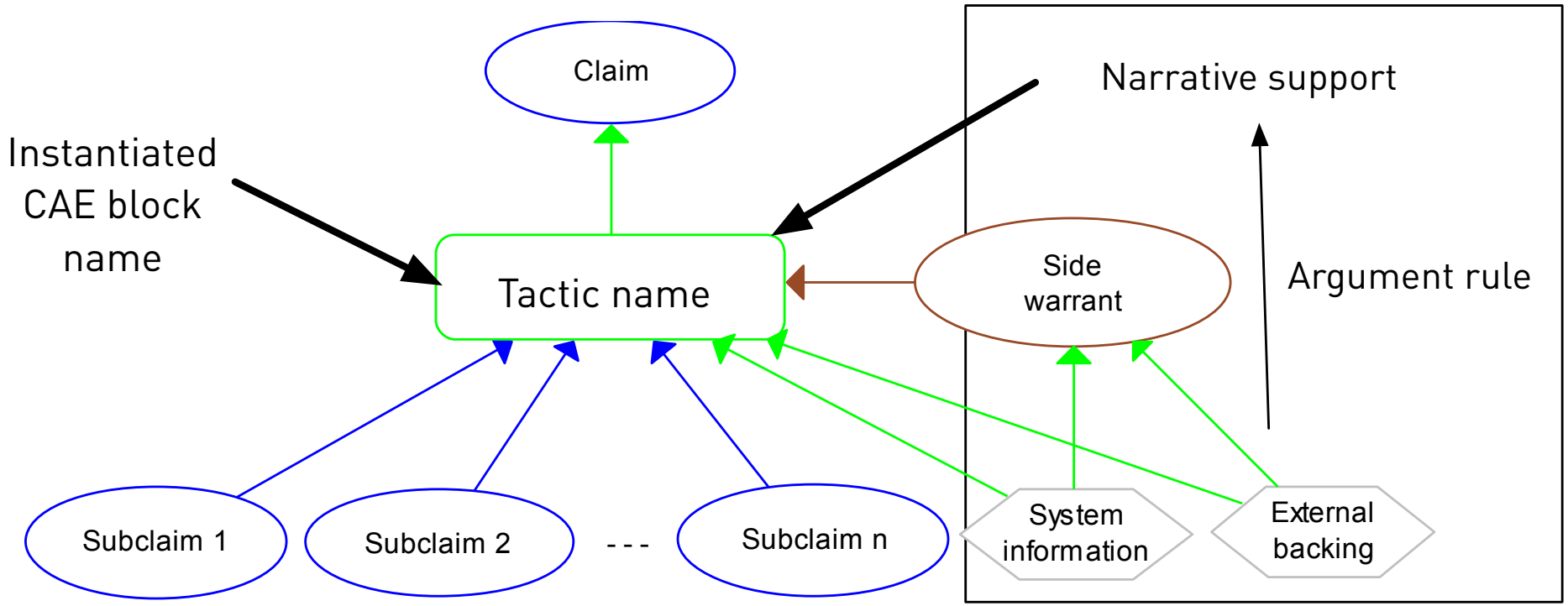
General structure of the block

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

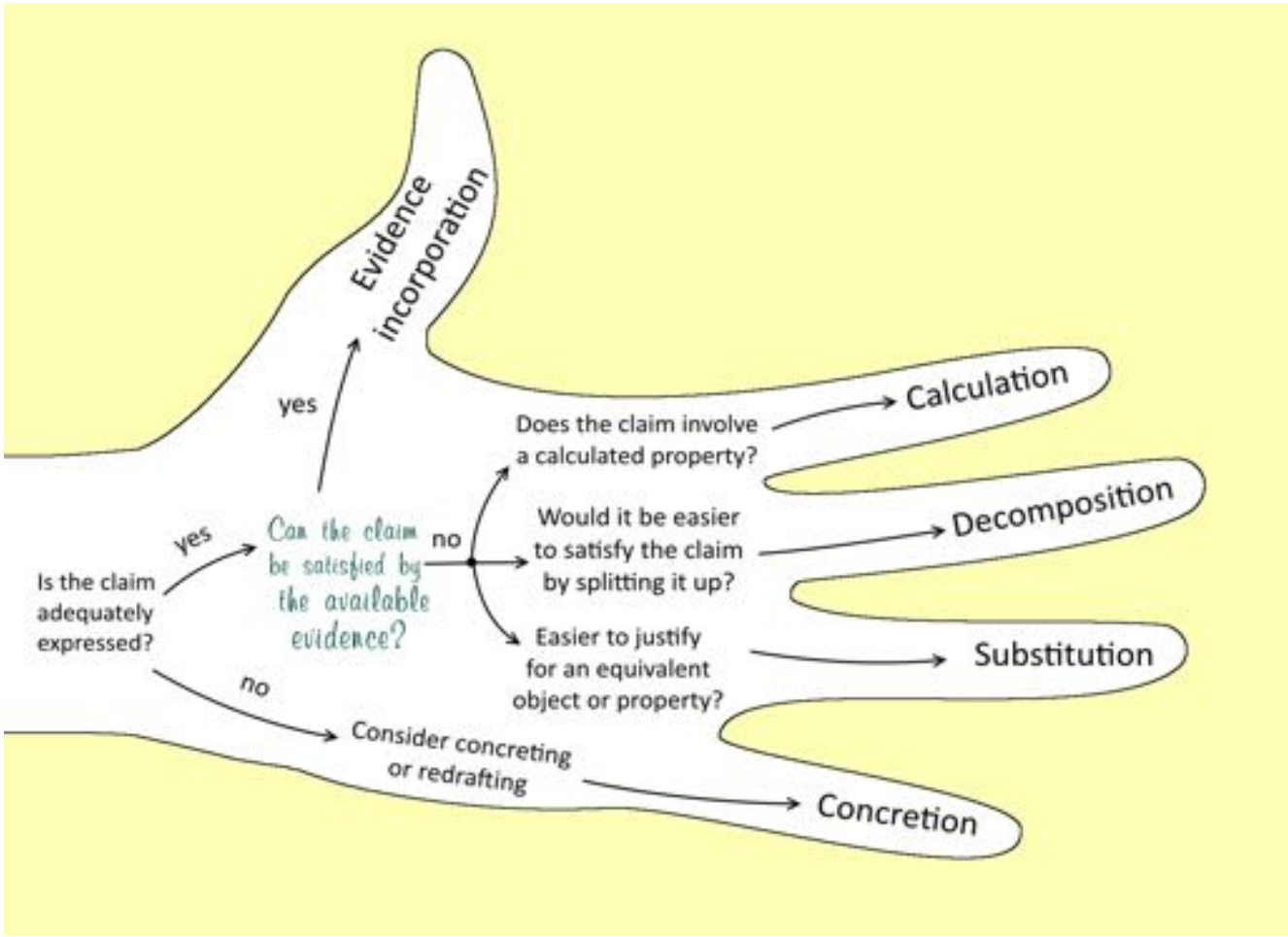


General block structure

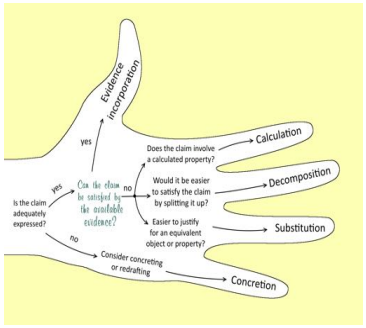
Notation - options

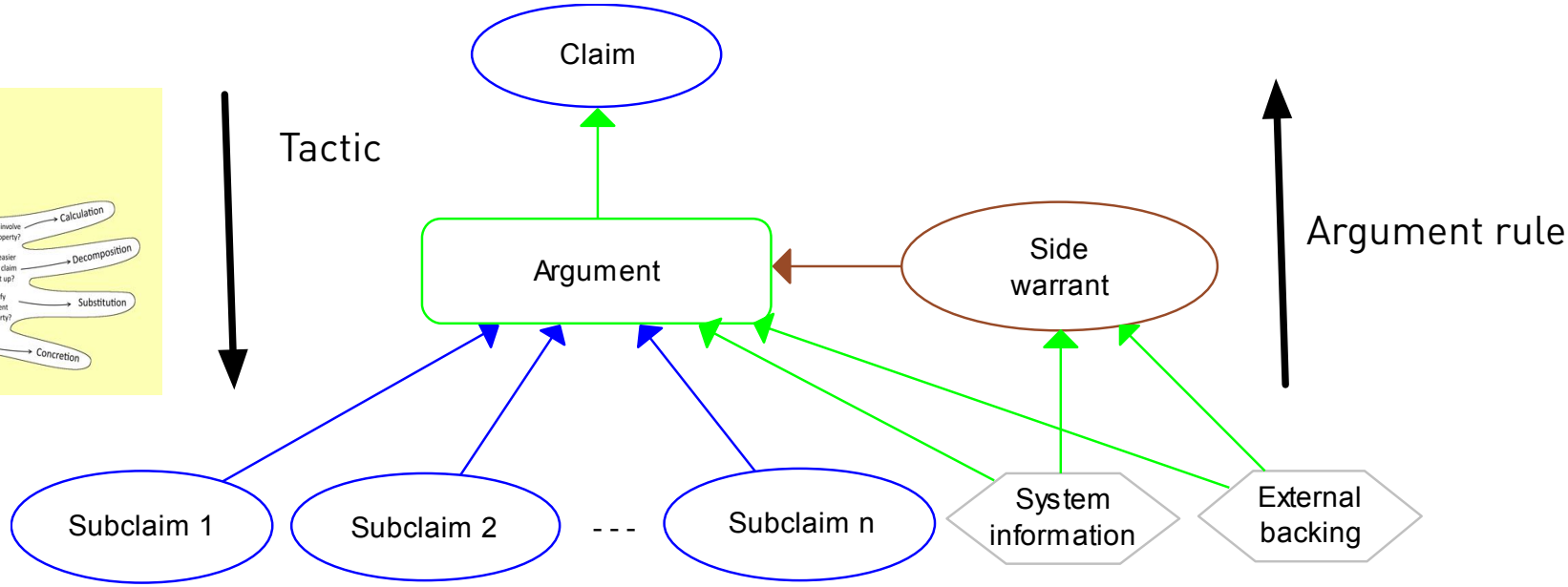


‘Helping hand’ - guidance on selecting Blocks



General structure of the block





General block structure

Science of security – importance of deductive/inductive

"We now detail security research failures to adopt accepted lessons from the history and philosophy of science.

A. Failure to observe inductive-deductive split

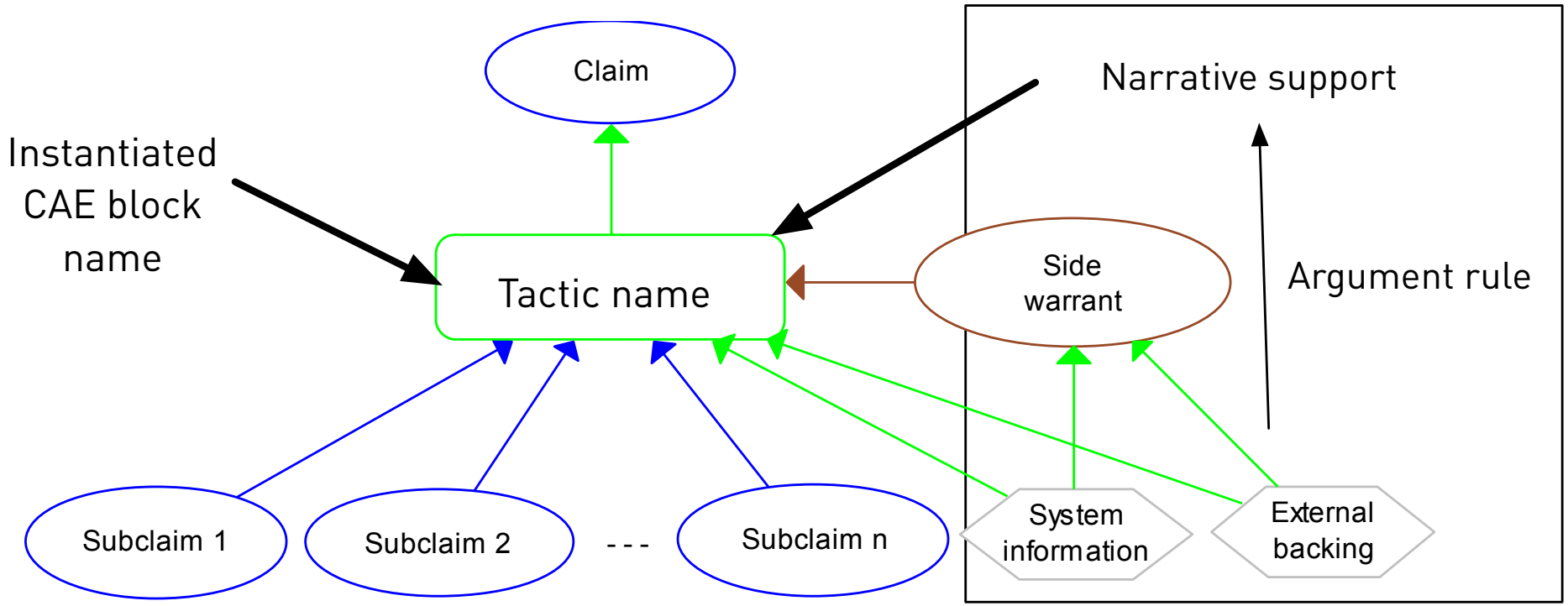
Despite broad consensus in the scientific community, in Security there is repeated failure to respect the separation of inductive and deductive statements "

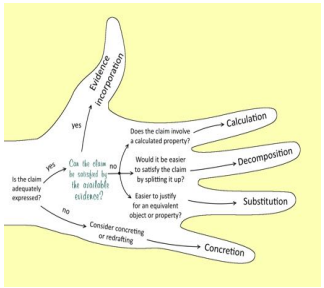
SoK: Science, Security, and the Elusive Goal of Security as a Scientific Pursuit

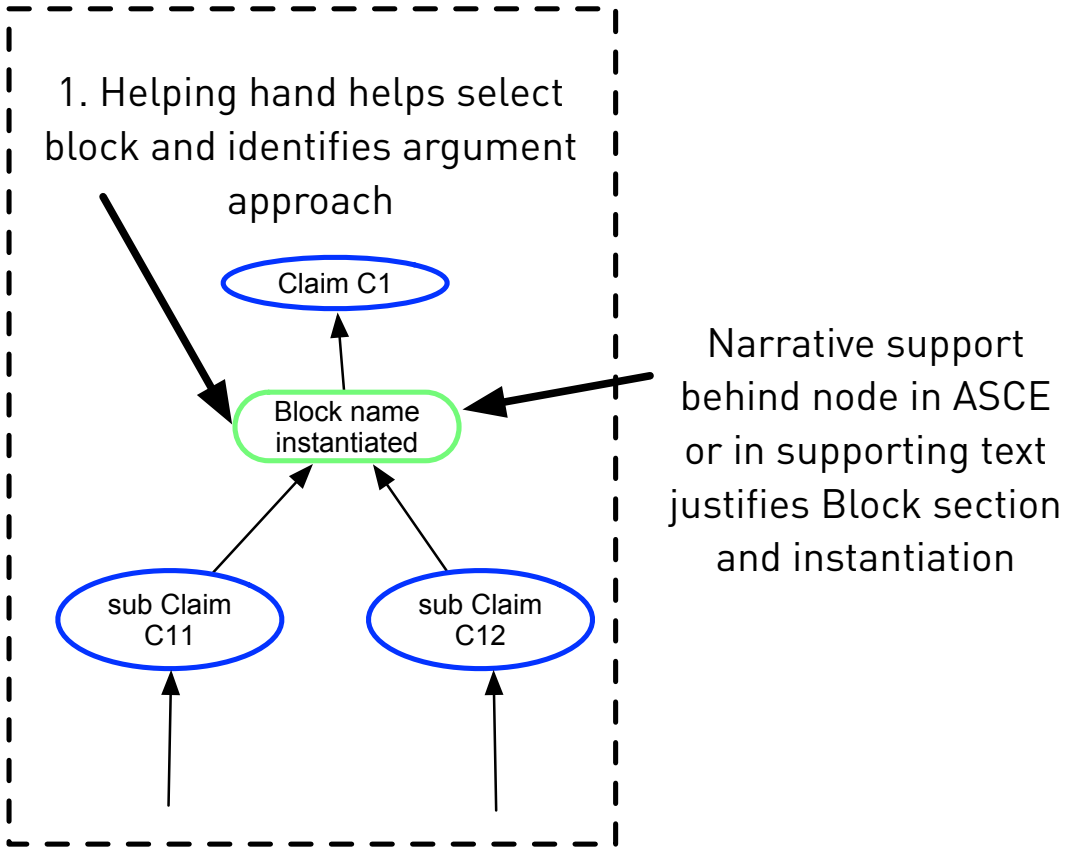
Cormac Herley
Microsoft Research, Redmond, WA, USA
cormac@microsoft.com

P.C. van Oorschot
Carleton University, Ottawa, ON, Canada
paulv@scs.carleton.ca

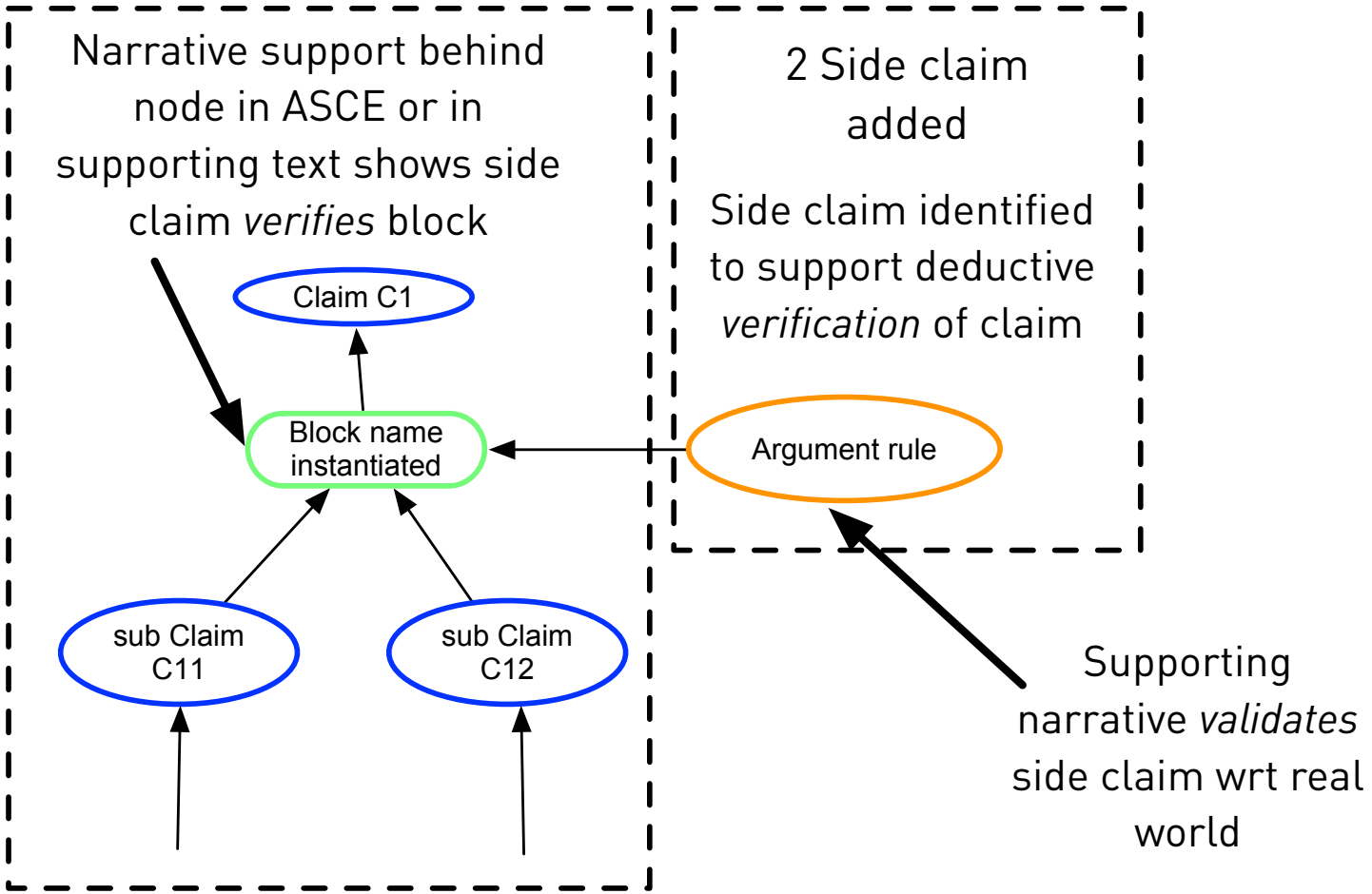
Notation - options

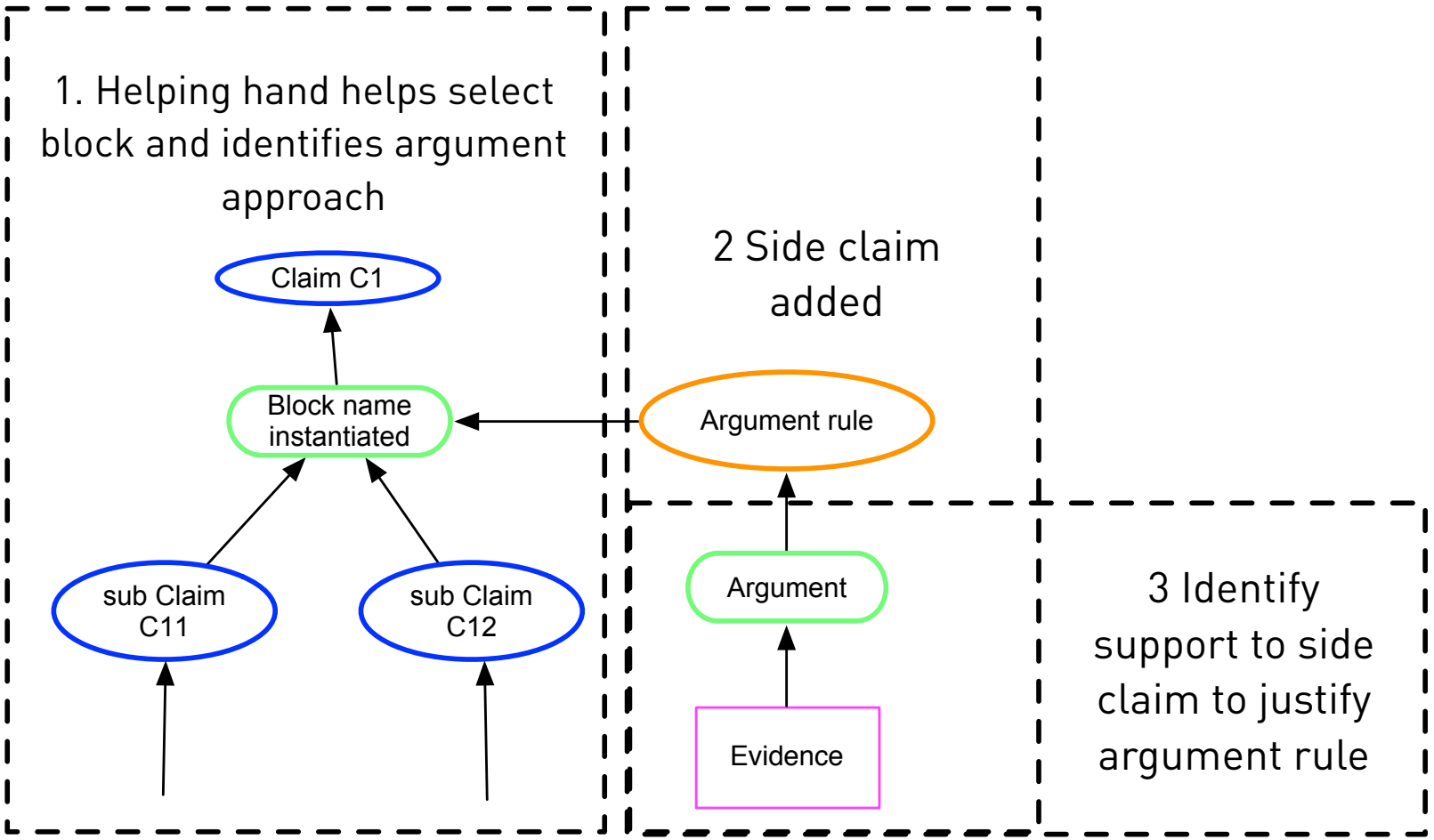




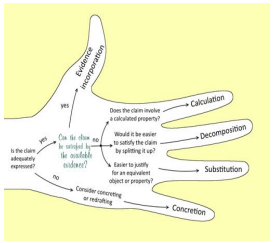


Narrative support behind node in ASCE or in supporting text justifies Block section and instantiation





Apply CAE Blocks in stages



1. Identify CAE Block

1 Block identifies argument approach

2 Side claim supports deductive argument

Claim C1

Argument A

W: C11 /\ C12 => C1

sub Claim C11

sub Claim C12

2 Add side claim

3 Develop side claim

Argument

Evidence

3 Justification of side claim validates wrt real world

Summary

- Approach informed by empirical study of CAE and GSN use
- Restricted set of CAE Blocks:
  - "What to do next?" vs "Which block is best to use?"
- Structured and narrative argument
- Explicit development of argument/side-warrant
  - Deductive/inductive distinction
- Consistent topologies (via normal form)
- Supports varying degrees of rigour
- Lacks
  - Formal template
  - Modularity and composition mechanism
- Tool support

Industrial adoption

Industrial adoption

- Project in its 4th year
- Analysed approach in two large organisations
- Detailed support and interaction with a large hazardous site
  - Safety case specialists
  - Engineering justification
- Workshops, guidance, observation

Adoption drivers + innovation defines effective

Drivers

- Infeasible or hard to justify claims
- Unconvincing or weak arguments
- Expensive or infeasible evidence needed
- Unacceptable impact on system design or operation
- Impractical timescales
- Peer and regulatory pressure

Innovation

- Explore the reuse of evidence
- Explore accepted terms
- Embrace the detail
- Clarify the differences
- Exploit organisational expertise and implicit arguments
- Push the boundaries - exploring the top-level claims further

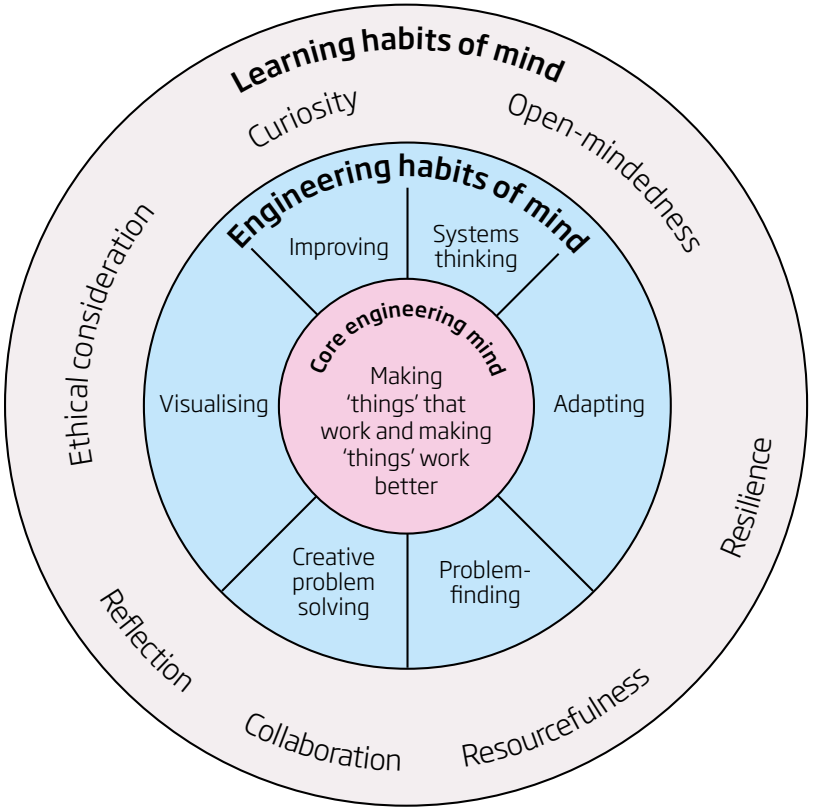
Technical and cultural - behaviour

ROYAL ACADEMY OF ENGINEERING

Centre for Real-World Learning at the University of Winchester

Thinking like an engineer
Implications for the education system

Summary report, May 2014



http://www.raeng.org.uk/news/news-releases/2014/may/do-you-think-like-an-engineer

Mindset

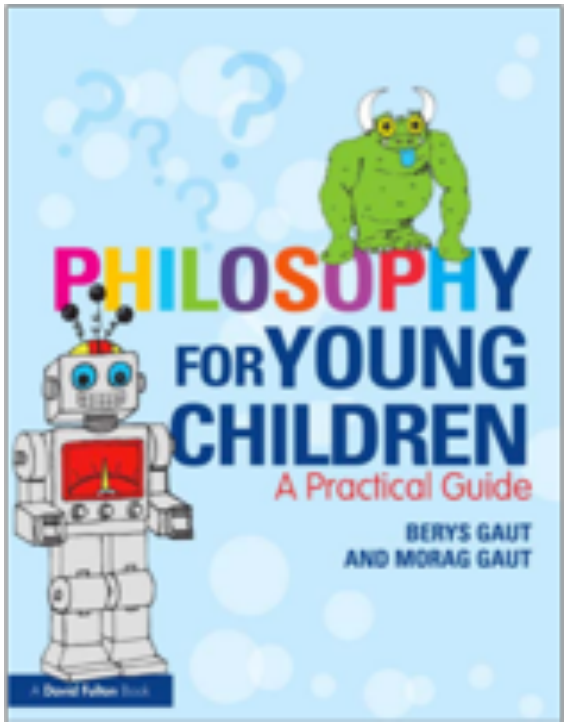
- In cognitive psychology, a mindset represents the cognitive processes activated in response to a given task
  https://en.wikipedia.org/wiki/Mindset
- The skills, aptitude, concepts and habits of mind that allow us to make effective cases
- Fostered by, and develops, methodology
- (also need organisational culture as well)

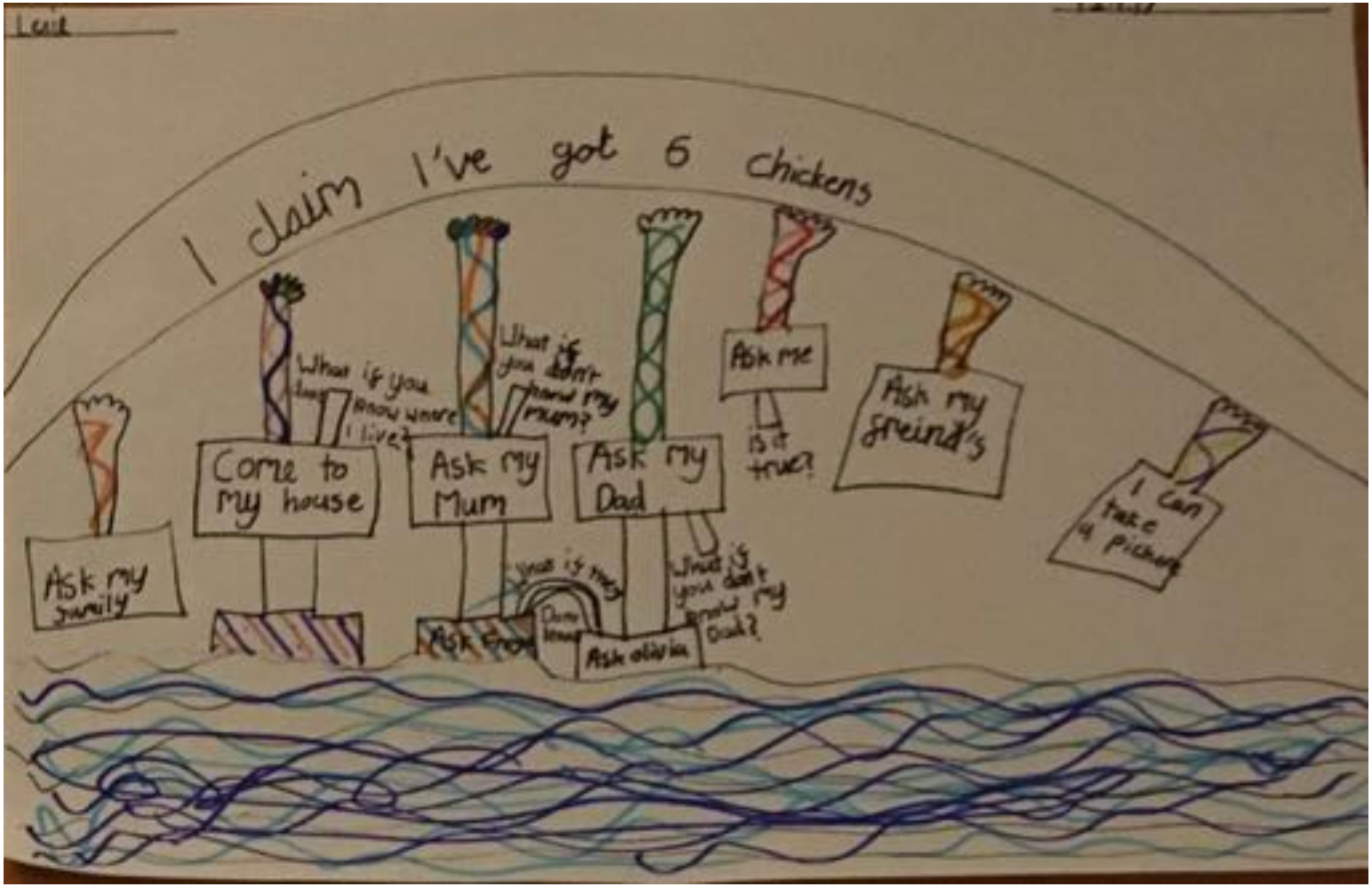
Indicators of importance

- Superficial but detailed safety cases
  - Vs understanding of hazards and their mitigation
- Experience of courses and workshops
  - Variability in people getting it
- Challenge from broadening approach to security and engineering justifications
  - The "non case" world using CAE
- NCSC withdrawal of risk assessment guidance IS1 and IS2
  - https://www.ncsc.gov.uk/guidance/critical-appraisal-risk-methods-and-frameworks

Exploring mindset – child's play?

- Philosophy in primary schools
- 8-9 year olds taught some CAE aspects





Chocolate and TV

Creating CAE structures

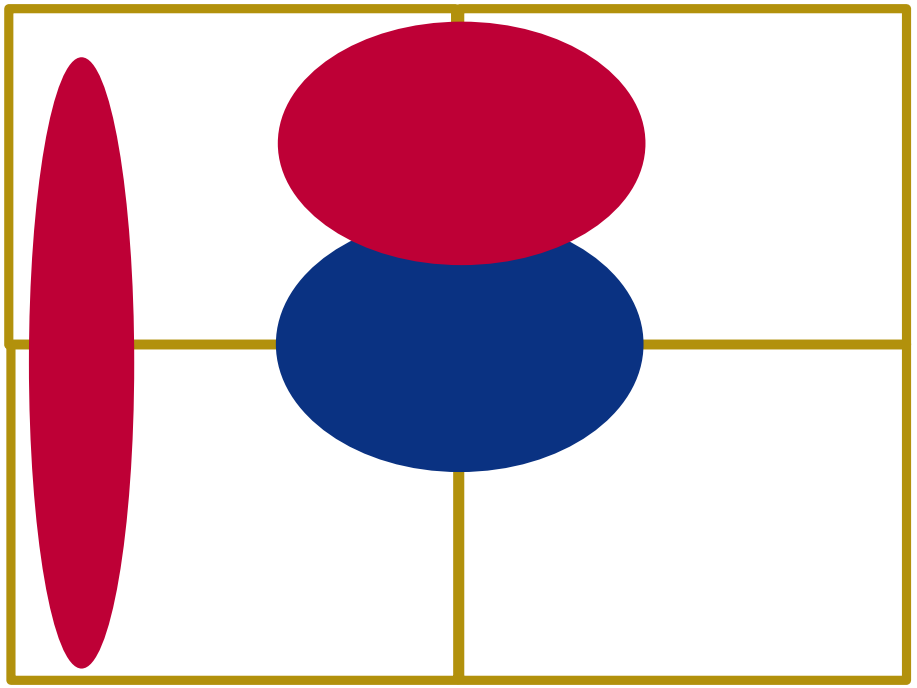
Group #1	Group #2
• Chocolate is good for you	• Chocolate is bad for you

Scope

Bad for you

Good for you

Amount



People

Safe/not safe

Just sufficient/over engineered

Convergence?

A framework for discussing convergence and

What good looks like

Starting point

- An assurance case is
  - "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"
  - i.e. system safe and effective
- Need to understand role of case to assess effectiveness
  - A "good case" depends on the decision being made, the system, the domain, the criticality, social distance, tempo, organisational and individual competence, the audience and authors

  - What is it for?
  - What is it about?

Concepts

- Claims, Arguments, Evidence
  - Claims can propositionalise uncertainty
    - Highly confident reliability is better than X
  - Arguments
- Deductive/inductive
  - Defeaters
  - Use of Blocks to make difference clear
- Technical frameworks
  - Deductive logics, Bayesian, confirmation theory

Convergence?

- Methodology
- Mindset
- Rigour and reasoning
- Communication
- Creativity and novelty
- Commodity

- Multidisciplinarity and values

Tension

- Rigour vs Communication
- Methodology vs mindset
- Creativity vs commodity

Communication and rigour

Communication	High	+ reviewable (but might lack depth) - convincing but may be invalid -rejection eventually	++ convincing, valid
	Low		- incorrect focus - unnecessary detail - not convincing + compelling
		Low	High
		Rigour	

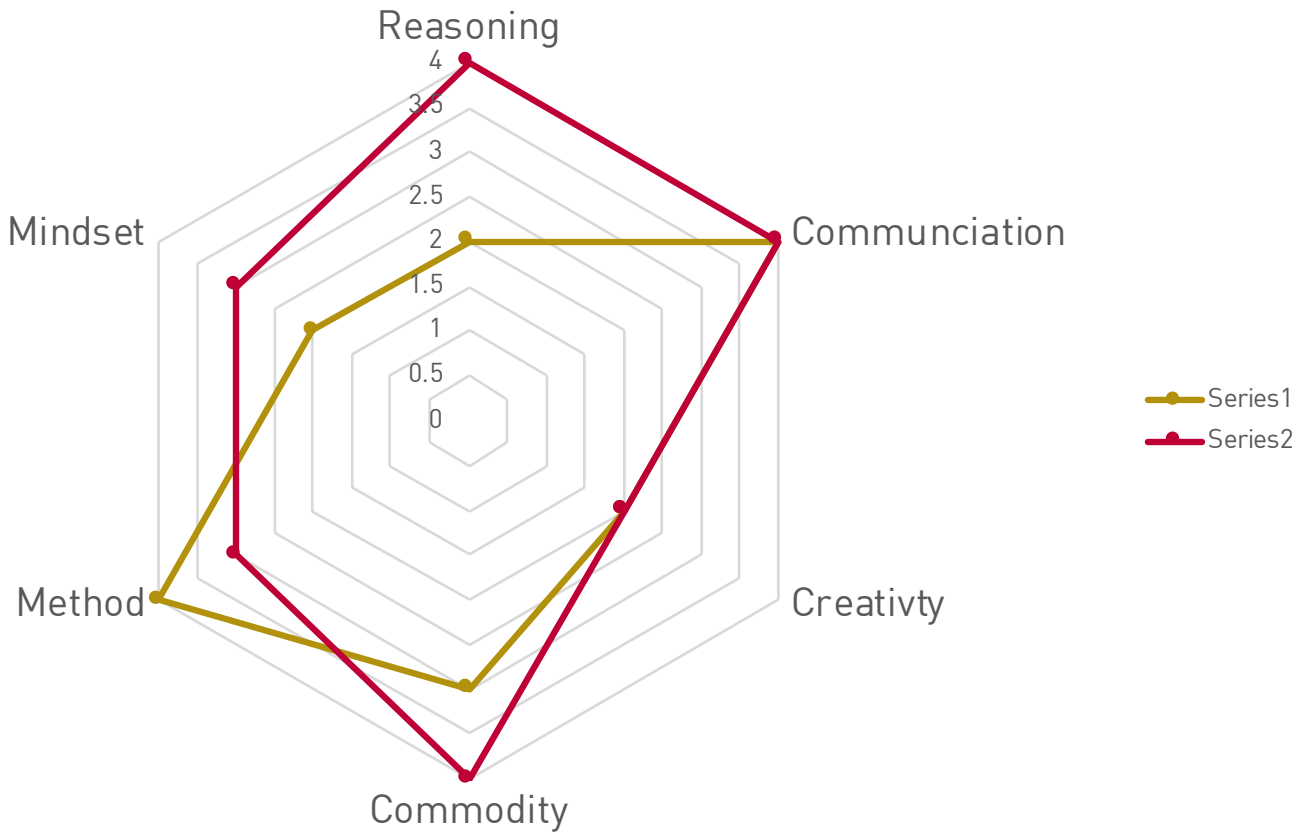
Mindset and methodology

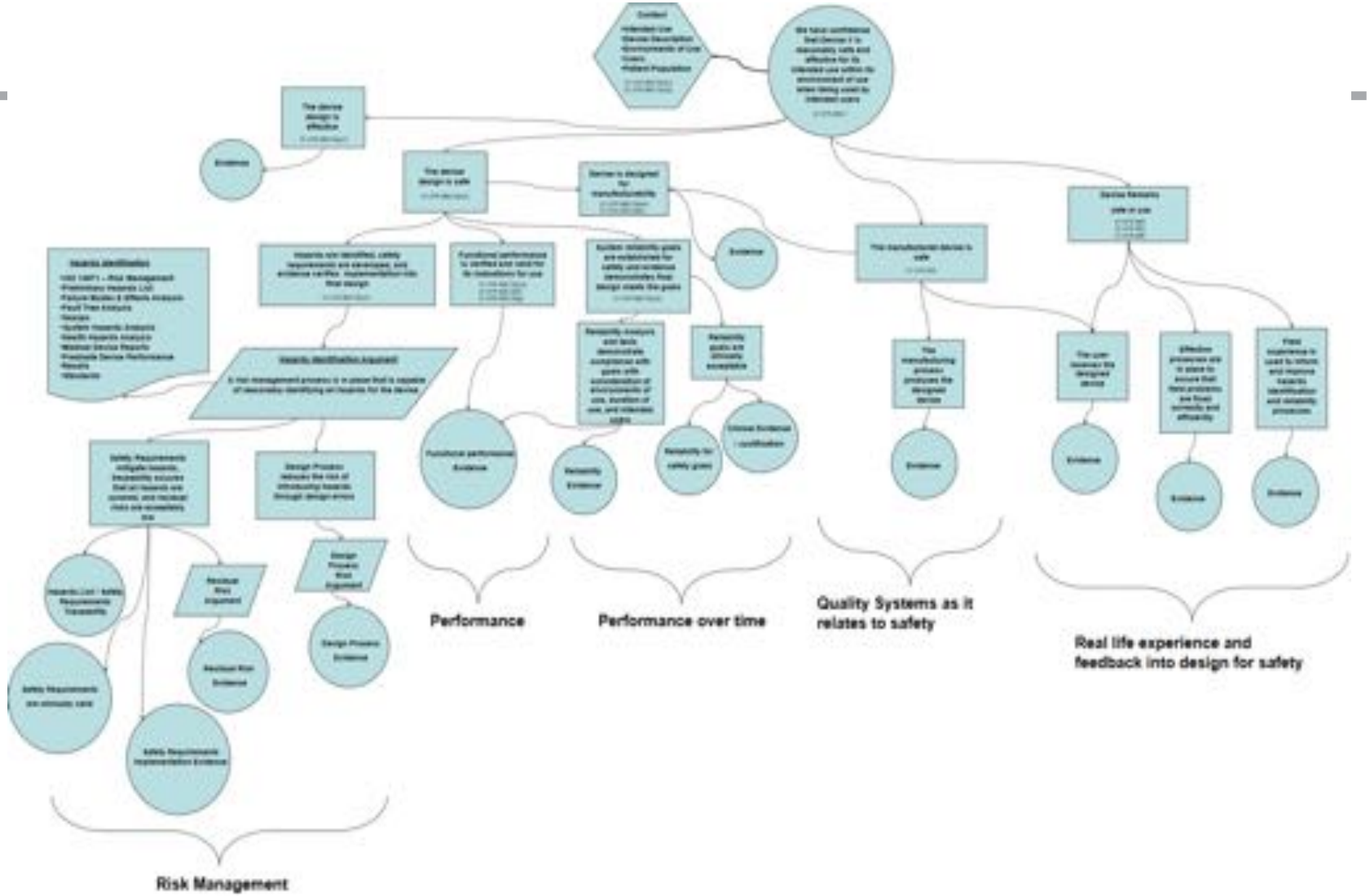
Mindset	High	+ creative challenging - unfocused chaotic, inefficient	++ creative efficient
	Low		- unthinking, irrelevant + disciplined
		Low	High
		Methodology	

Creativity and commoditisation

Creativity	High	+ problem solving but not efficient - inefficient, reinventing wheel	++ problem solving, optioneering ++ production efficiency, focused and ++ relevant reuse
	Low		- irrelevant, expensive solution - system boundaries + efficient production + good communication
		Low	High
		Commodity	

Characterising cases and research





State of practice

- Reasoning weak
  - Inductive/deductive not emphasised enough
- Communication
  - OK but let down by narrative
  - Or overly graphical
- Mindset and creativity
  - Not explicitly considered
- Commodity
  - Both unthinking reuse and not enough reuse
  - Body of knowledge

Discussion and conclusions

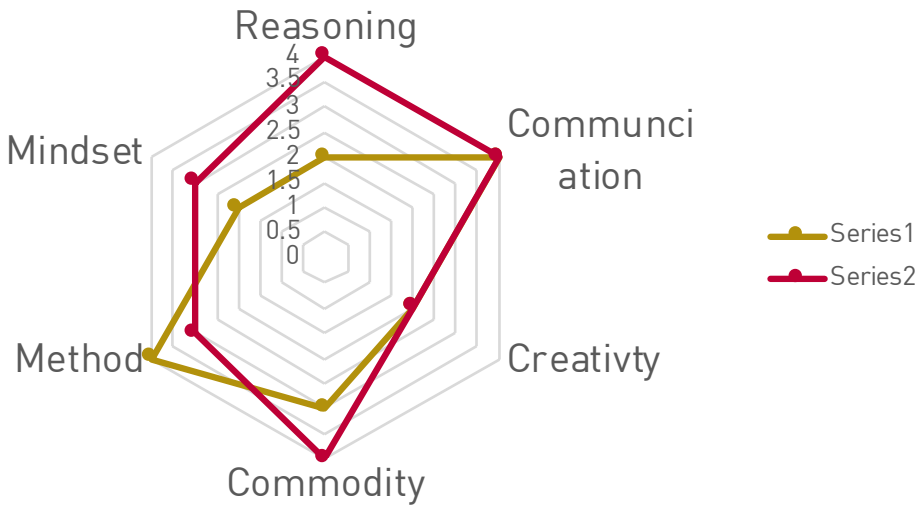
Can we address challenges?

- Challenges
  - Scale, tempo
  - Security and threats
  - AI and machine learning
  - Big data
  - Normal business
- Explore state of practice need to understand disparate nature and roles of cases
  - Are cases adequate but expensive, is research fragmented, incoherent, slow?
- What makes a ”good case” depends on the decision being made, the system, the domain, the criticality, social distance, tempo, audience and authors

In addition recognise tensions and interactions

Recognise interaction between

- Rigour vs Communication
- Methodology vs Mindset
- Creativity vs Commodity



Developing and deploying a methodology

- Core concepts and methodology to address landscape
  - CAE, role of arguments, inductive/deductive split. CAE Blocks and associated support
- Simple but rich enough
  - Can compare and contrast other approaches
  - Values and interdisciplinary work
- Framework to support convergence, encourage innovation
  - Potential for convergence
  - Differences understood and can critique

Support methodology and outreach

In terms of mindset and methodology

- More chocolate and TV with different groups
  - Safety, engineering, security
- Development of method to address different types of user
- Explore deployment of CAE Blocks
  - Investigate further the inductive/deductive split
- Continuing industrial study

Other activities

- CAE guidance and website on CAE ClaimsArgumentsEvidence.org
- Guidance and example of security informed safety case for transport, security workshops
- Tool enhancements, ASCE v5

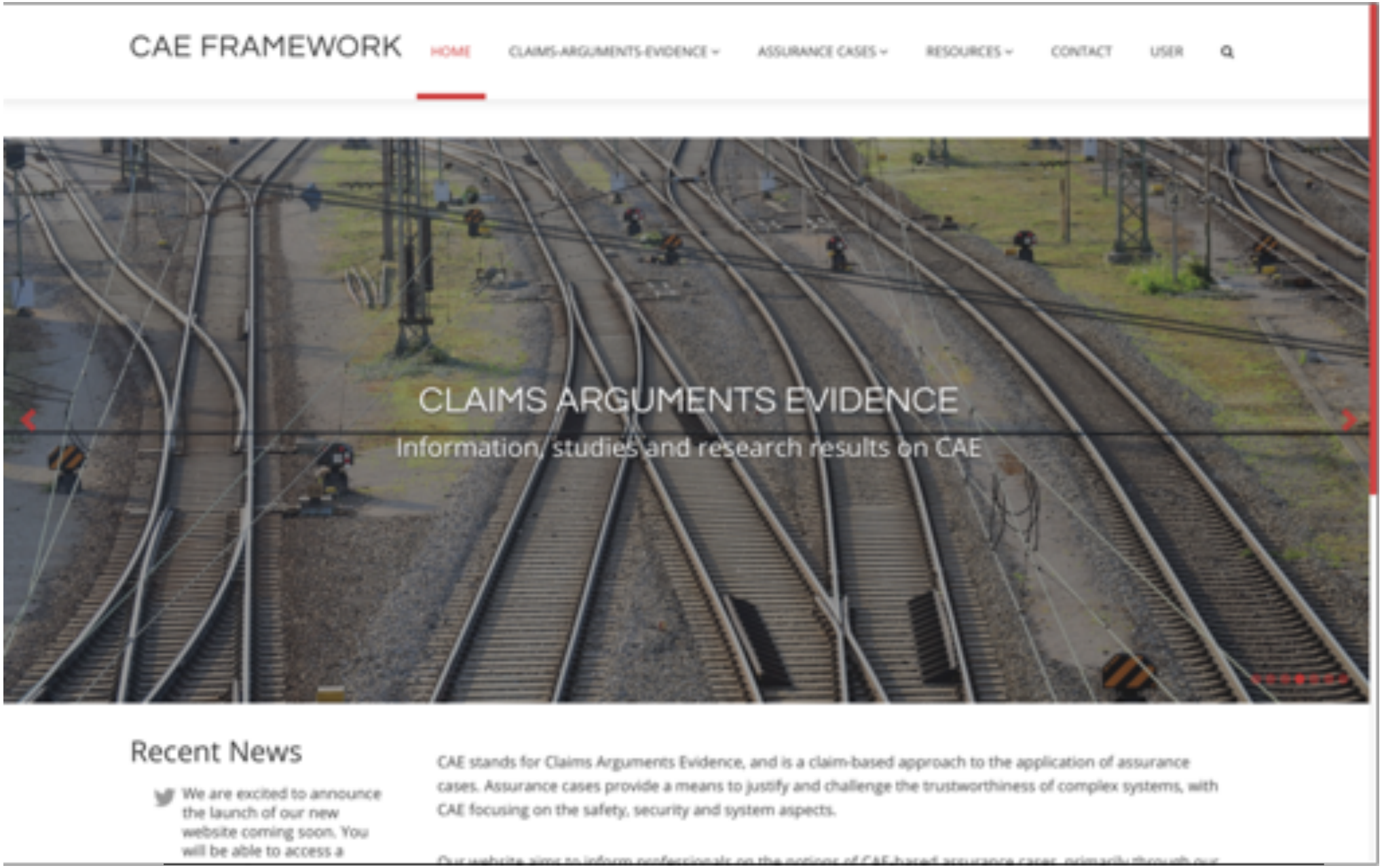
Support methodology and outreach

In terms of mindset and methodology

- More chocolate and TV with different groups mindset, creativity
  - Safety, engineering, security
- Development of method to address different types of user mindset
- Explore deployment of CAE Blocks
  - Investigate further the inductive/deductive split rigour
- Continuing industrial study

Other activities

- CAE guidance and website on CAE ClaimsArgumentsEvidence.org
- Guidance and example of security informed safety case for transport, security workshops, Code of practice commodity, mindset, method
- Tool enhancements, ASCE v5



Enclosure 2

Lloyd's Register Foundation

UNIVERSITY of York

Assuring Autonomy International Programme
Expression of Interest Form – Call 01

Towards Identifying and closing Gaps in Assurance of

Towards Identifying and closing Gaps in Assurance of autonomous Road vehicleS (TIGARS)

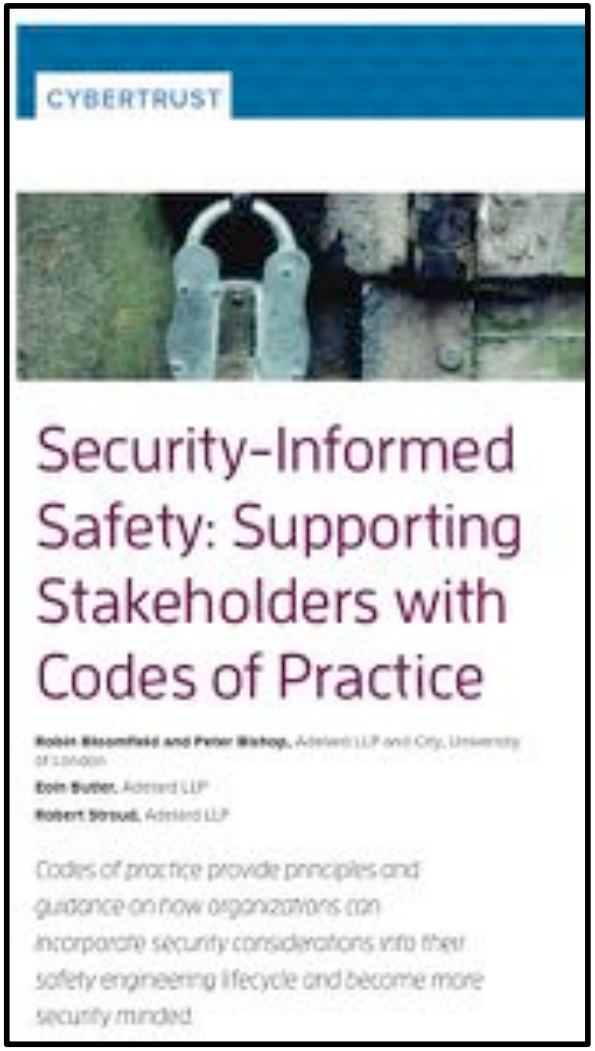
ADELARD

WITZ

INFORMATION SCIENCE NAGOYA UNIVERSITY

CITY UNIVERSITY LONDON

KU KANAGAWA UNIVERSITY 90th ANNIVERSARY



Future

- Will structural deepening, lock-in, and adaptive stretch run out steam?
- Will addressing autonomy and security lead to a significant shift in research and practice?
- We are recruiting please see our website and/or talk to me!

ADELARD