ADELARD

What is a case?

From "What is.." to "What should it be ..."

Assurance cases as modern art

Robin E Bloomfield
Kate Netkachova, Xingyu Zhao and Bev Littlewood
reb@adelard.com

VerisureWorkshop

July 2015

PT/2ab/3017/11

Exmouth House 3–11 Pine Street London EC1R 0JH
T +44 20 7832 5850 F +44 20 7832 5853 E office@adelard.com W www.adelard.com

CSR Building confidence in a computerised world
www.csr.city.ac.uk

Overview

- Pseudo ethnographic approach
  - What is a case
  - What do users do
- Factoring inductive and deductive
  - Interpretation of CAE Blocks
- An example
  - pnp and confidence
- Discussion and conclusions
  - From “What is..” to “What should it be ...”

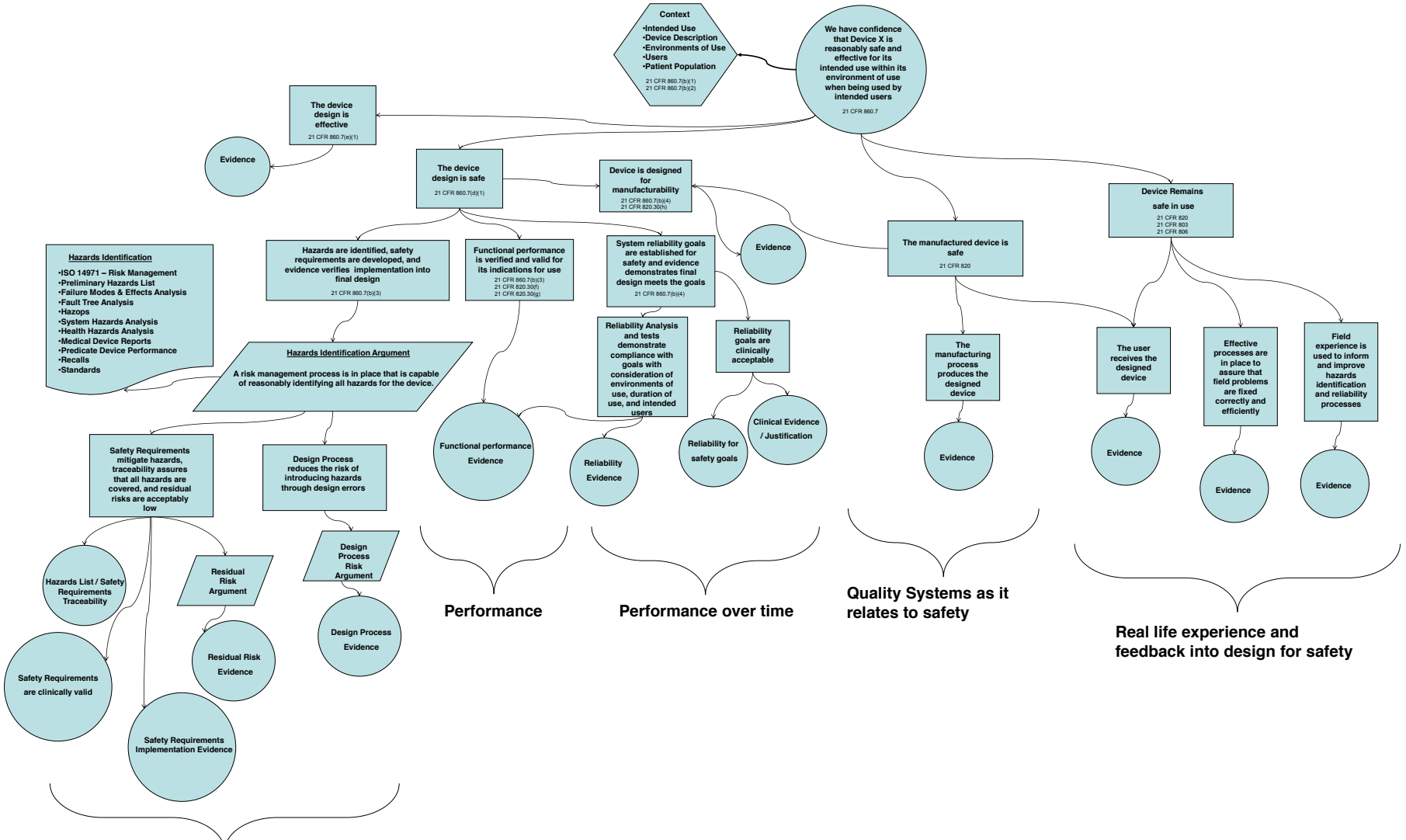
Definitions

- Standards
  - terminological, referential, denotational
- Operational
  - How is it constructed
- Empirical
  - Investigate artifacts that are defined as cases by users
- Sociological
  - What it is used for
    - Decision making, getting past regulator, commodity, recoding personal understanding
- Emotions
  - Belief
- Analogical and metaphorical
  - What is it like, how do people describe them?
- Normative
  - What should it be

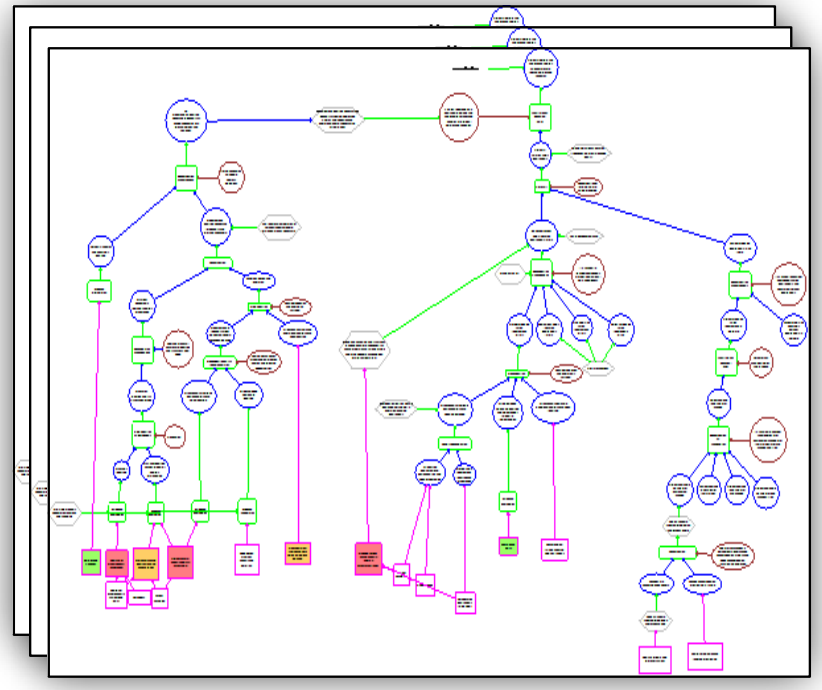
Ethnographic and empirical approach

- Supports decision making
  - Important ones
  - Persuasive - documenting reasoning
  - Assist in understanding or in compliance
- Public and private
  - Many stakeholders
- Content
  - Word and pictures
  - Many variants
  - Tool large cases… HC
- Process
  - Engineering process – journey matters
  - Decision making process

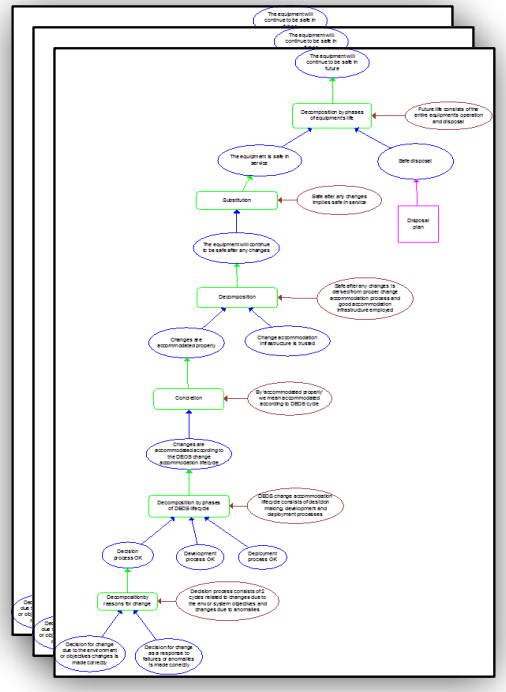
FDA example


Context
•Intended Use
•Device Description
•Environments of Use
•Users
•Patient Population
21 CFR 860.7(b)(1)
21 CFR 860.7(b)(2)
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
21 CFR 860.7
The device design is effective
21 CFR 860.7(e)(1)
Evidence
The device design is safe
21 CFR 860.7(d)(1)
Device is designed for manufacturability
21 CFR 860.7(b)(4)
21 CFR 820.30(h)
Evidence
The manufactured device is safe
21 CFR 820
Device Remains safe in use
21 CFR 820
21 CFR 803
21 CFR 806
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
Hazards are identified, safety requirements are developed, and evidence verifies implementation into final design
21 CFR 860.7(b)(3)
Functional performance is verified and valid for its indications for use
21 CFR 860.7(b)(3)
21 CFR 820.30(f)
21 CFR 820.30(g)
System reliability goals are established for safety and evidence demonstrates final design meets the goals
21 CFR 860.7(b)(4)
Hazards Identification Argument
A risk management process is in place that is capable of reasonably identifying all hazards for the device.
Reliability Analysis and tests demonstrate compliance with goals with consideration of environments of use, duration of use, and intended users
Reliability goals are clinically acceptable
The manufacturing process produces the designed device
The user receives the designed device
Effective processes are in place to assure that field problems are fixed correctly and efficiently
Field experience is used to inform and improve hazards identification and reliability processes
Safety Requirements mitigate hazards, traceability assures that all hazards are covered, and residual risks are acceptably low
Design Process reduces the risk of introducing hazards through design errors
Functional performance Evidence
Reliability Evidence
Reliability for safety goals
Clinical Evidence / Justification
Evidence
Evidence
Evidence
Evidence
Hazards List / Safety Requirements Traceability
Residual Risk Argument
Design Process Risk Argument
Safety Requirements are clinically valid
Residual Risk Evidence
Design Process Evidence
Safety Requirements Implementation Evidence
Performance
Performance over time
Quality Systems as it relates to safety
Real life experience and feedback into design for safety

Reasoning, communication, confidence



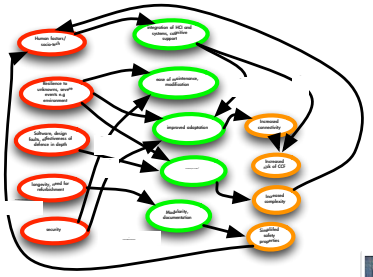
Case development and challenge



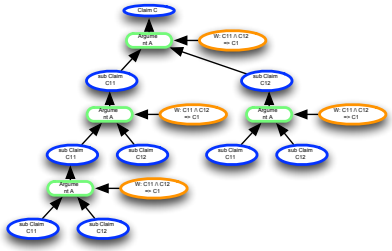
Meta-case
Case about the case

Development of assurance

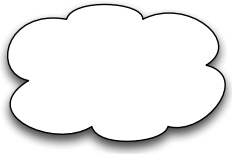
Influence diagram



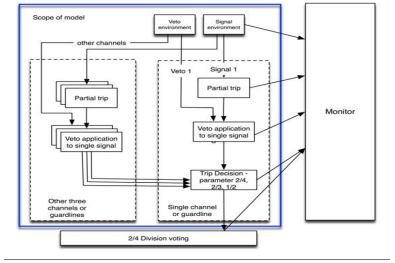
CAE structure



Mental models

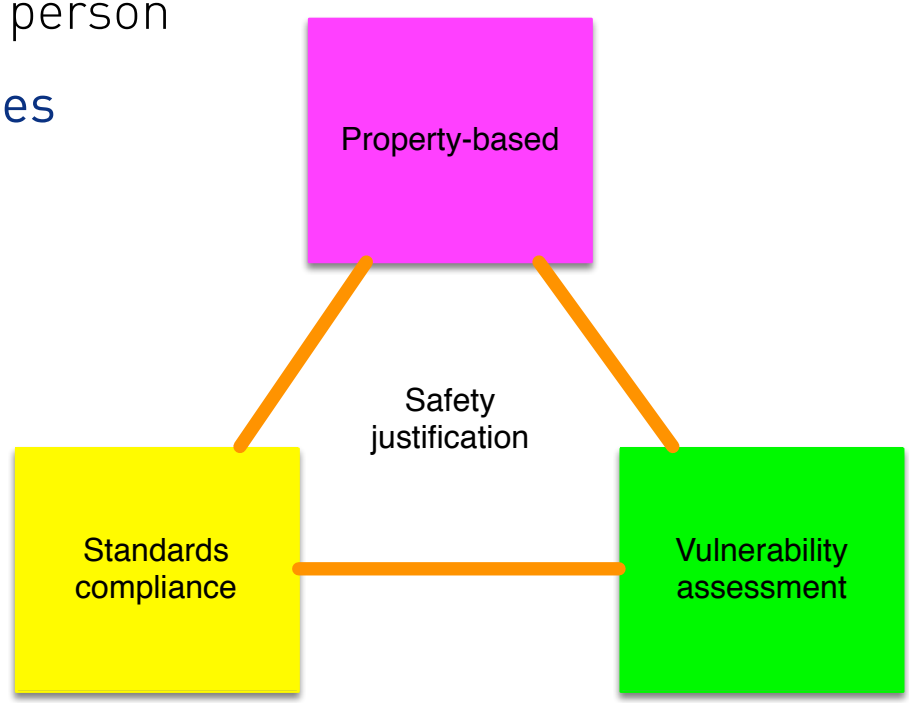


Engineeering models

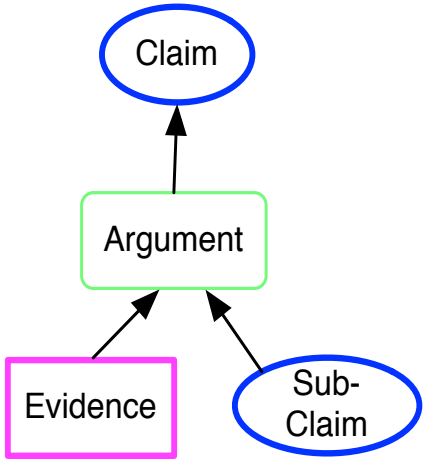


Different types of case

- Extreme behaviourist
  - Vs standards compliance person
- Modified with other principles
  - Good design
  - Defence in depth
  - Quality components

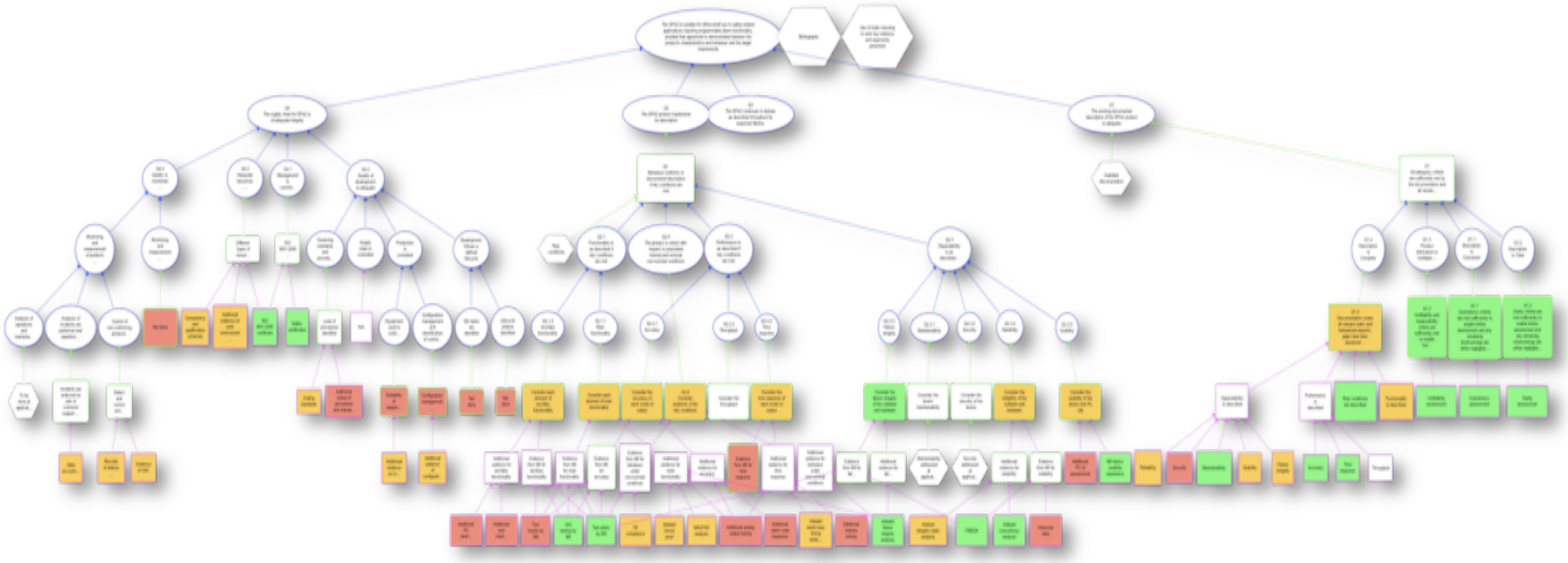


Structured Safety or Assurance Case

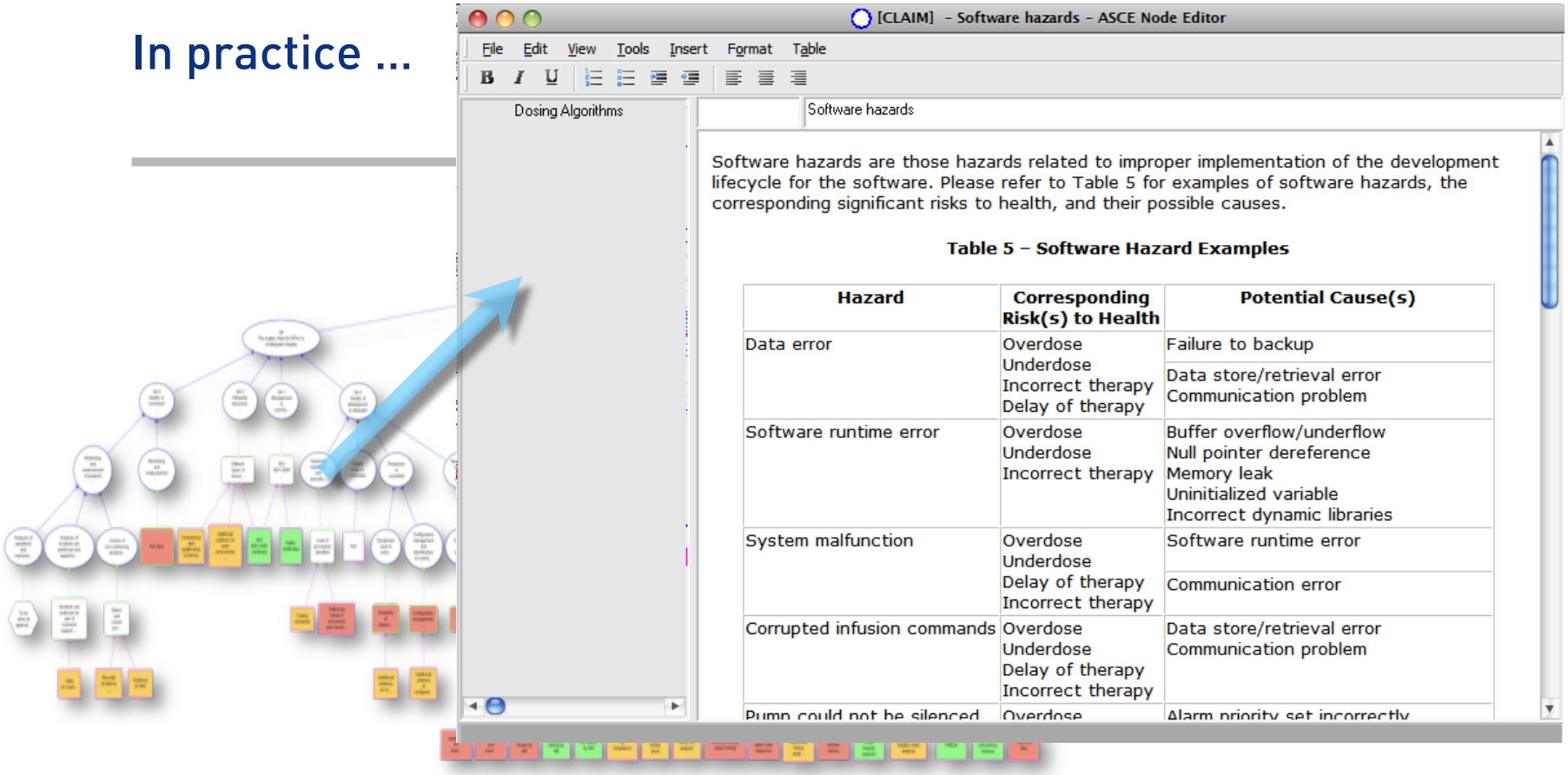


- “a documented body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment”

In practice … the engineering

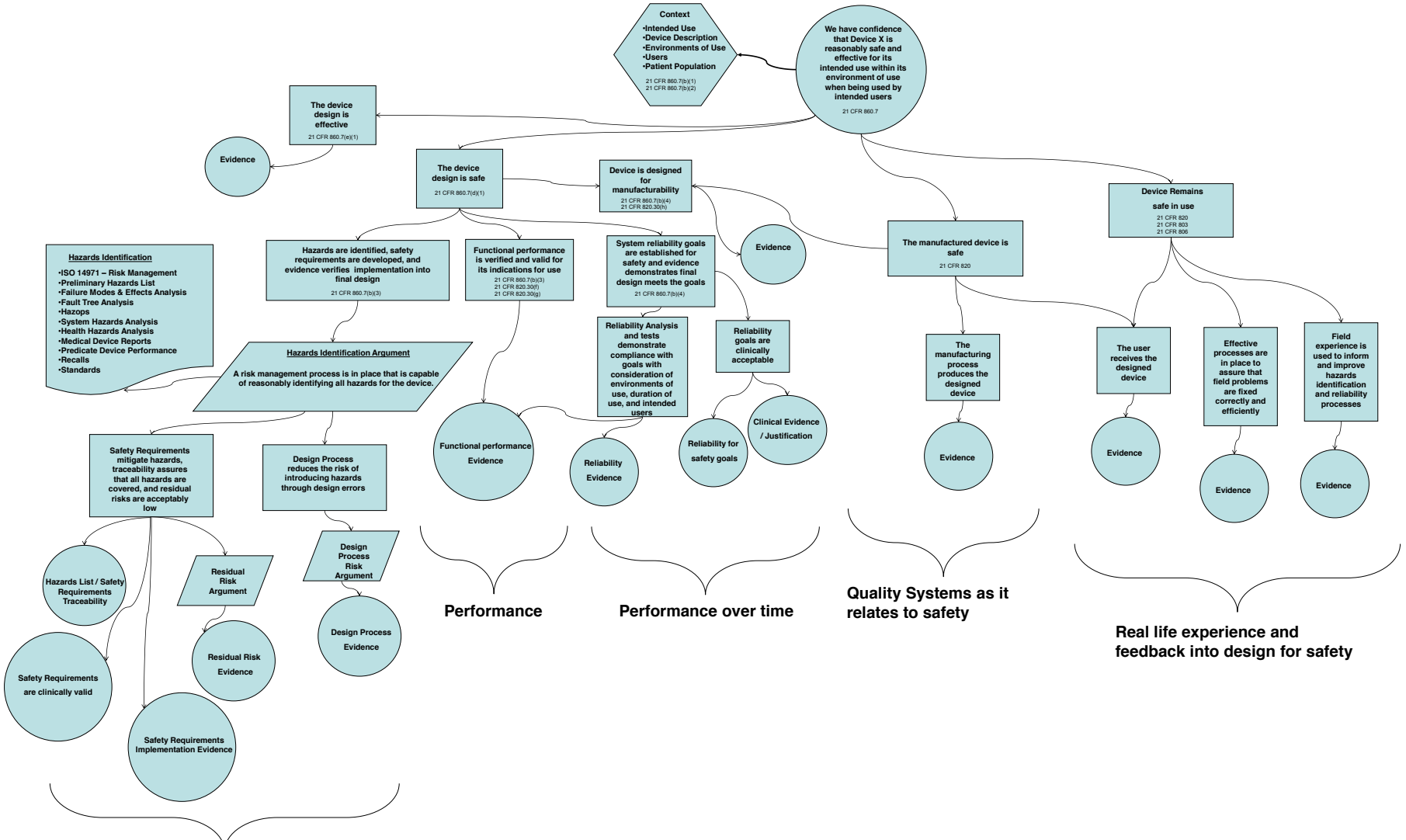


In practice …



Main notations GSN and CAE

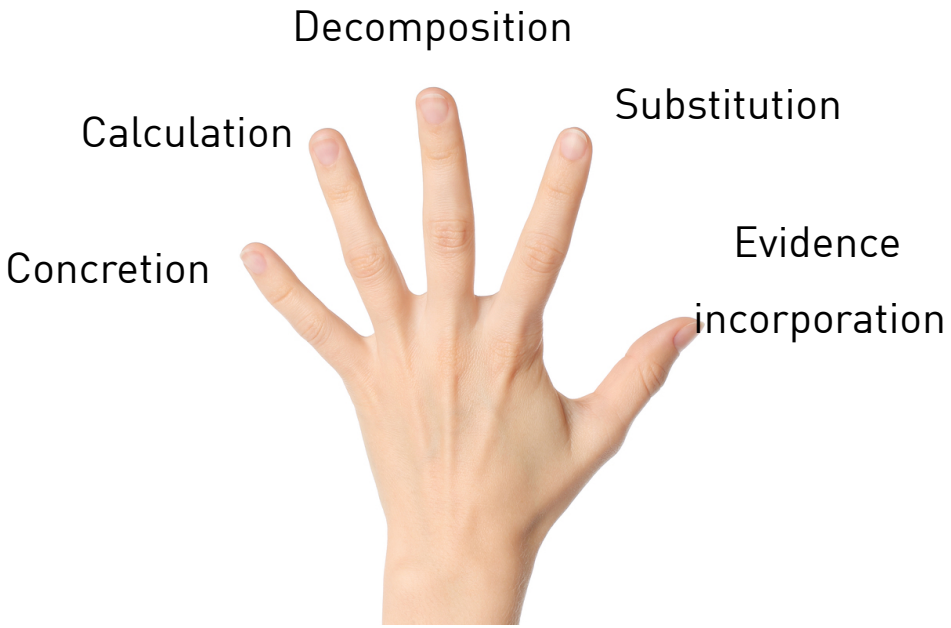
FDA example


Context
•Intended Use
•Device Description
•Environments of Use
•Users
•Patient Population
21 CFR 860.7(b)(1)
21 CFR 860.7(b)(2)
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
21 CFR 860.7
The device design is effective
21 CFR 860.7(e)(1)
Evidence
The device design is safe
21 CFR 860.7(d)(1)
Device is designed for manufacturability
21 CFR 860.7(b)(4)
21 CFR 820.30(h)
Evidence
The manufactured device is safe
21 CFR 820
Device Remains safe in use
21 CFR 820
21 CFR 803
21 CFR 806
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
Hazards are identified, safety requirements are developed, and evidence verifies implementation into final design
21 CFR 860.7(b)(3)
Functional performance is verified and valid for its indications for use
21 CFR 860.7(b)(3)
21 CFR 820.30(f)
21 CFR 820.30(g)
System reliability goals are established for safety and evidence demonstrates final design meets the goals
21 CFR 860.7(b)(4)
Hazards Identification Argument
A risk management process is in place that is capable of reasonably identifying all hazards for the device.
Reliability Analysis and tests demonstrate compliance with goals with consideration of environments of use, duration of use, and intended users
Reliability goals are clinically acceptable
The manufacturing process produces the designed device
The user receives the designed device
Effective processes are in place to assure that field problems are fixed correctly and efficiently
Field experience is used to inform and improve hazards identification and reliability processes
Safety Requirements mitigate hazards, traceability assures that all hazards are covered, and residual risks are acceptably low
Design Process reduces the risk of introducing hazards through design errors
Functional performance Evidence
Reliability Evidence
Reliability for safety goals
Clinical Evidence / Justification
Evidence
Evidence
Evidence
Evidence
Hazards List / Safety Requirements Traceability
Residual Risk Argument
Design Process Risk Argument
Safety Requirements are clinically valid
Residual Risk Evidence
Design Process Evidence
Safety Requirements Implementation Evidence
Performance
Performance over time
Quality Systems as it relates to safety
Real life experience and feedback into design for safety

CAE Blocks – generic fragments

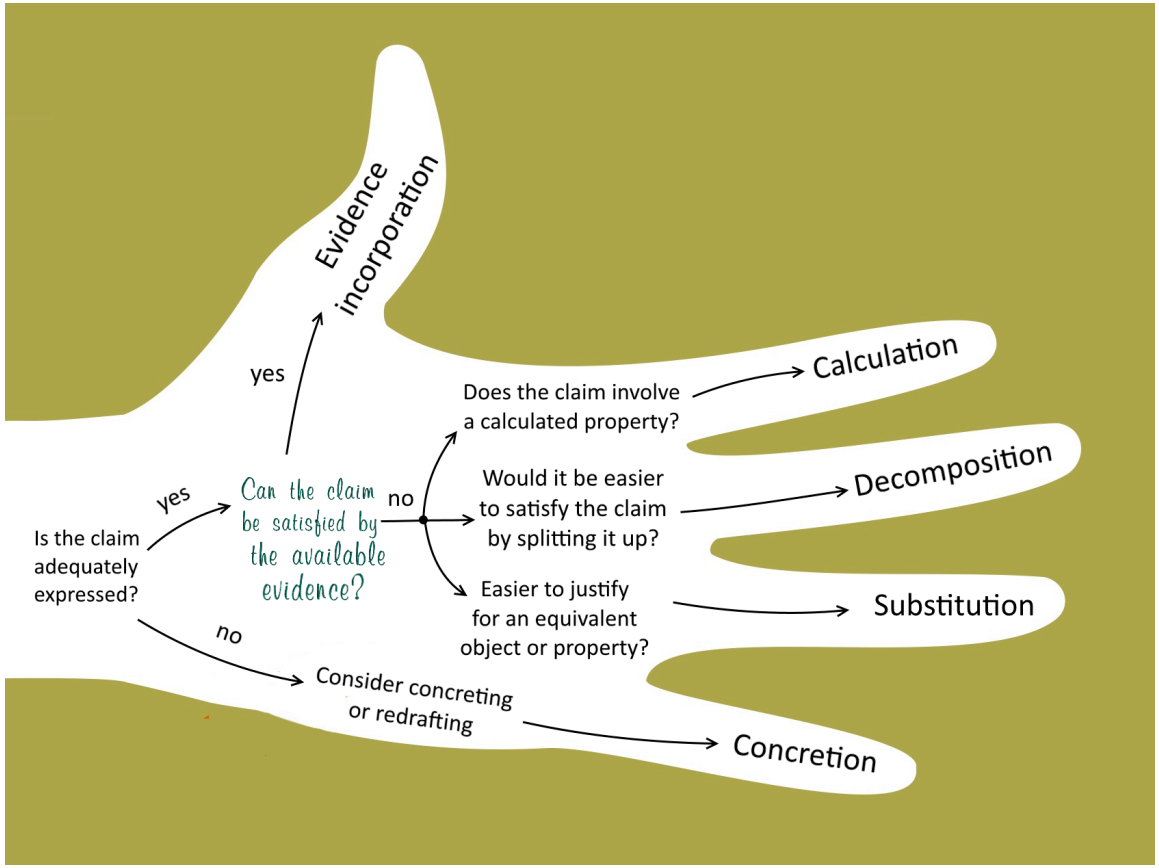
- Design goal
  - Empirically based – sufficiently expressive
  - Technically sound and able to link to more formal approaches
- Support structuring
  - Useful as restrict choice
  - In practice cases might combine blocks, use understood and problem specific approaches
    - Many different styles
- Maturity
  - Ideas around ~5 yrs
  - Used in nuclear industry case studies and R&D and part of our thinking
  - Technical paper available and draft guidance

5 Building Blocks

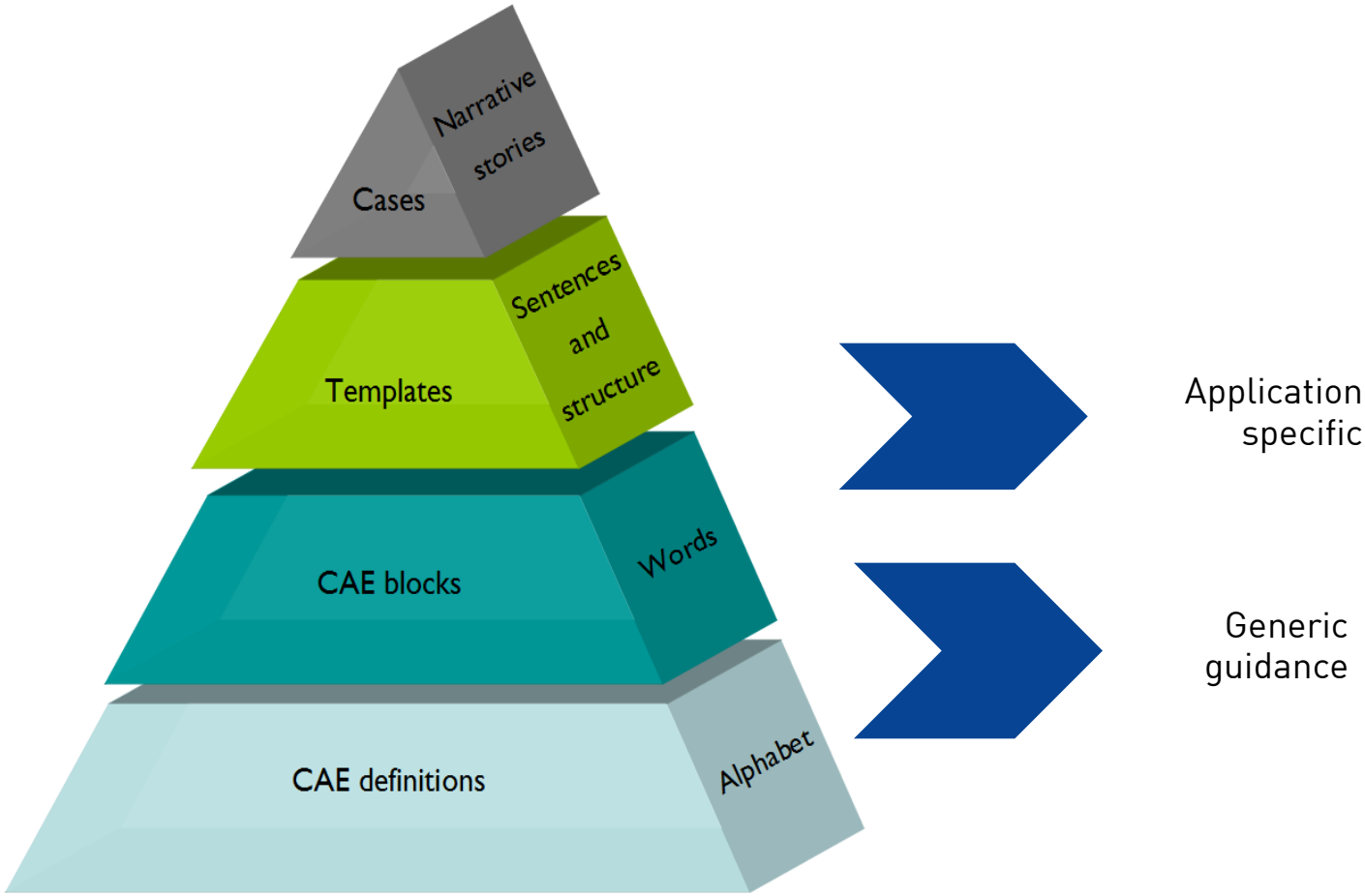


- **Decomposition**
  Partition some aspect of the claim
- **Substitution**
  Refine a claim about an object into claim about an equivalent object
- **Evidence incorporation**
  Evidence supports the claim
- **Concretion**
  Some aspect of the claim is given a more precise definition
- **Calculation or proof**
  Some value of the claim can be computed or proved
- **Also composite blocks**

A helping hand with CAE

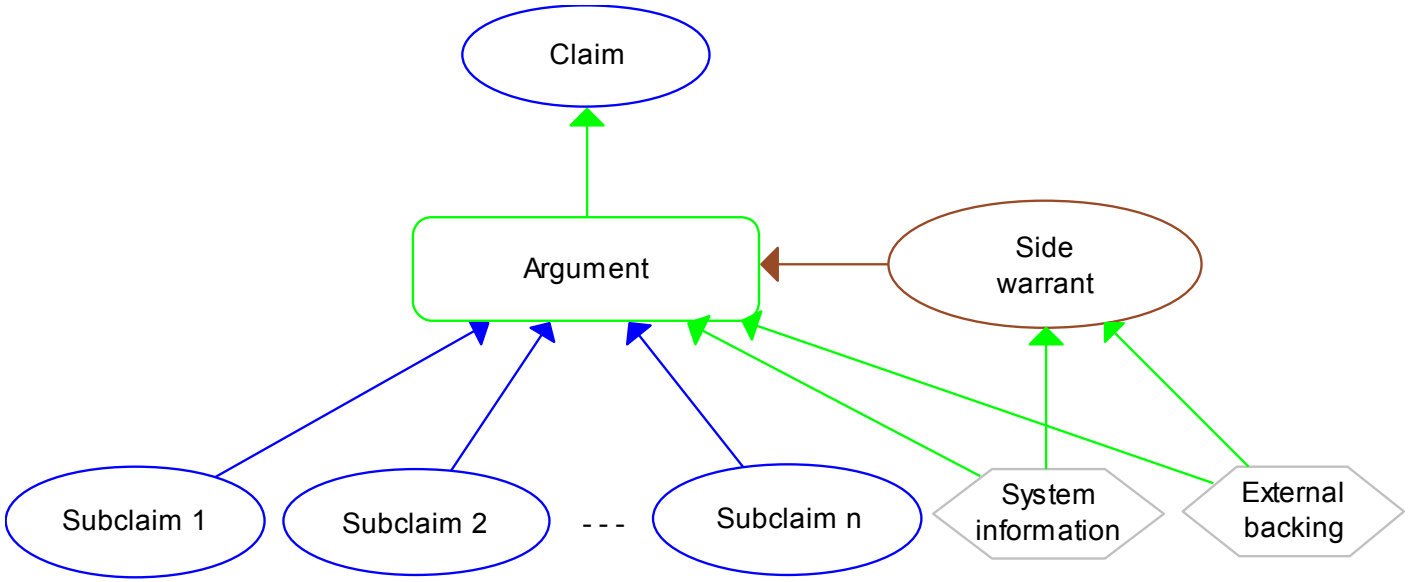


CAE stack



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.



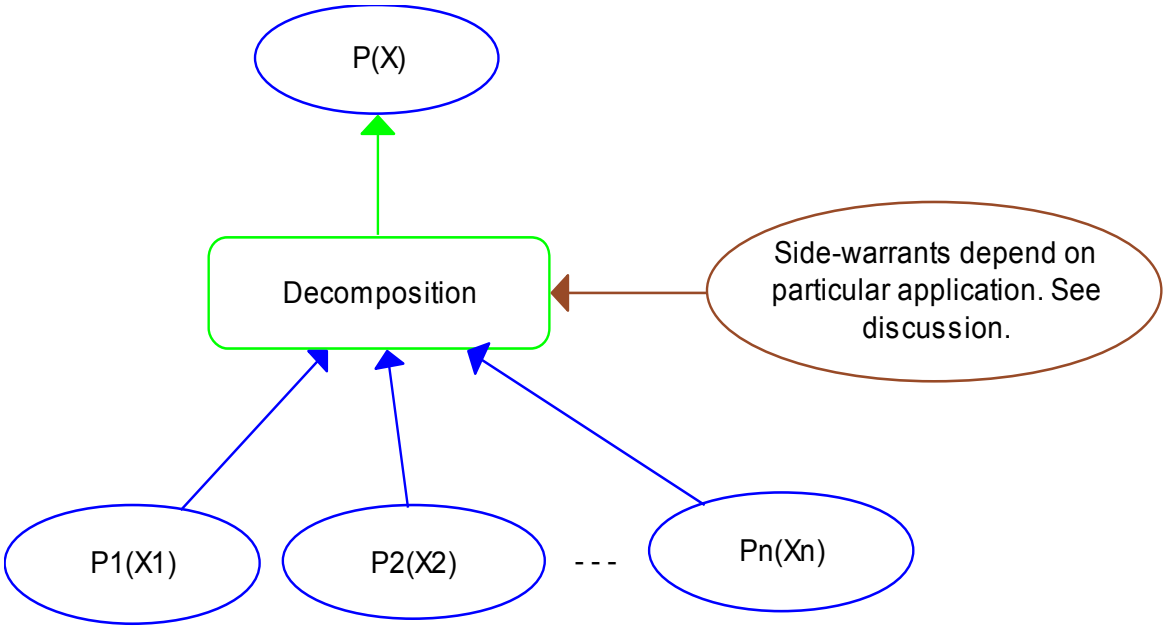
General block structure

Side warrants

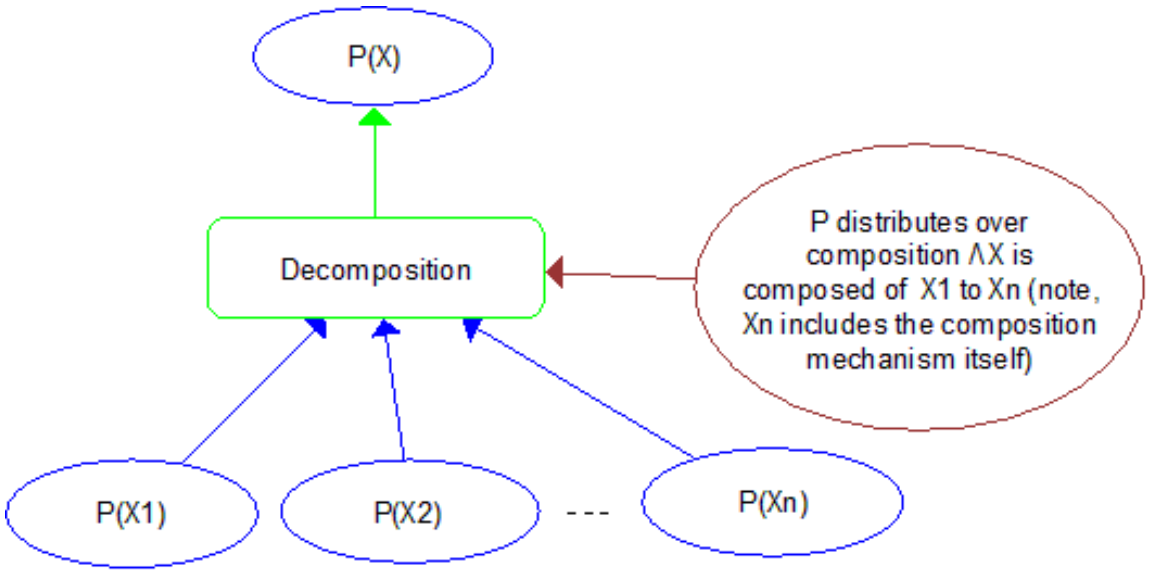
- The argument node can be descriptive
- The side warrant helps make the argument and can be supported with backing
- It address the “because ..?” questions in more detail
  - Simple semantics is
  - C11 /\ C12 /\ W => C1
- When we use a block we need to show:
  - Verification of the block
  - Validity with respect to the real world e.g. whether“1+1 = 2”

Decomposition block

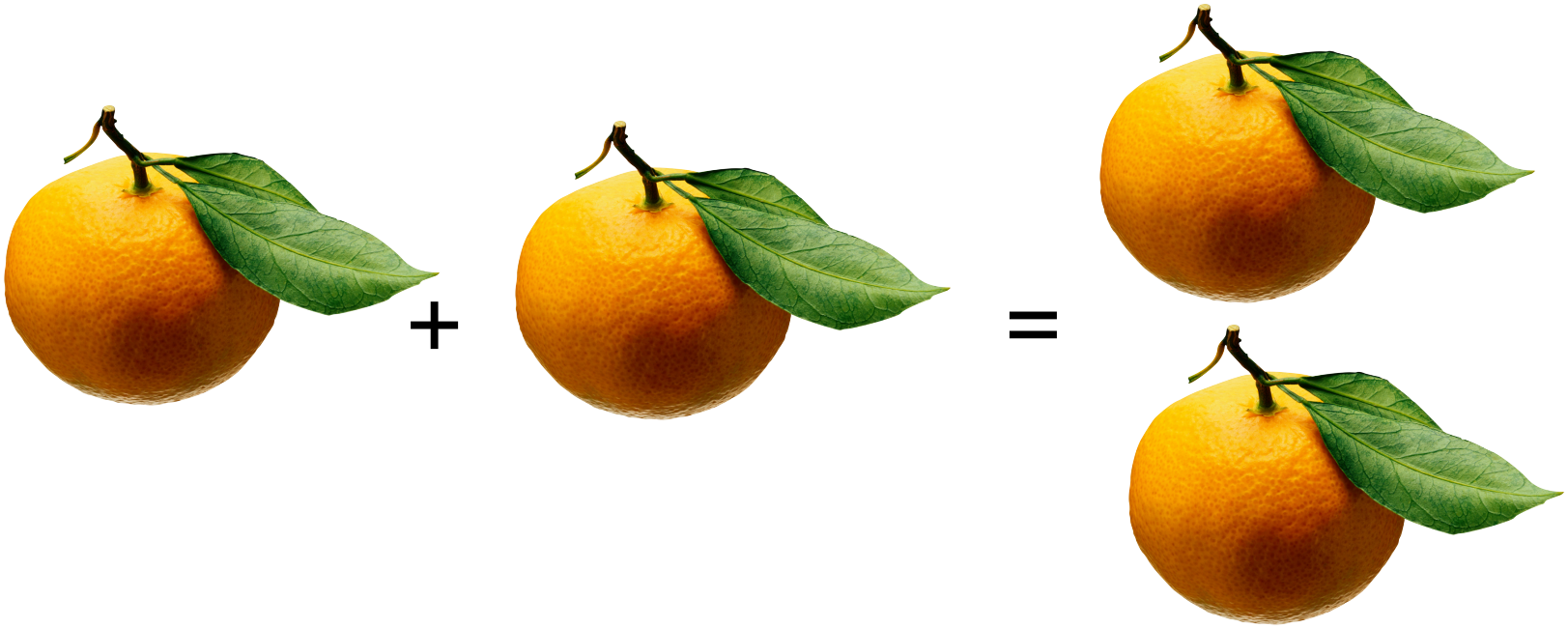
- A claim that an object X has property P is justified from claims about other objects and properties



Decomposition block – single property



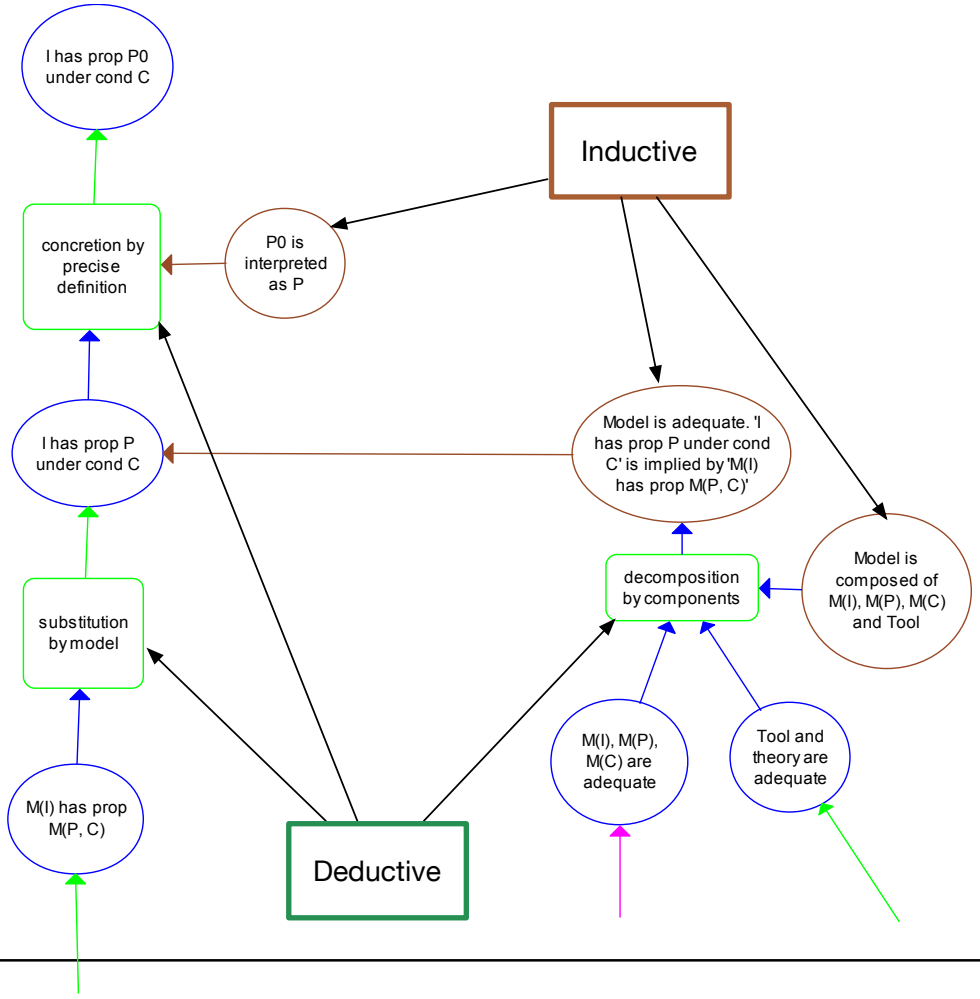
Example of a single object decomposition



Oranges – 1+ 1 =2

- Pressure, temperature
- Timescales
  - Rotting
- Hidden
  - Extra
- Fake
  - Explosive (looks like an orange …)
- Dropped, squashed
  - Process of combining
- What does “two” oranges mean
  - Juice, contents, dimensions as a whole fruit
- Claim(X, property, environment) + Block

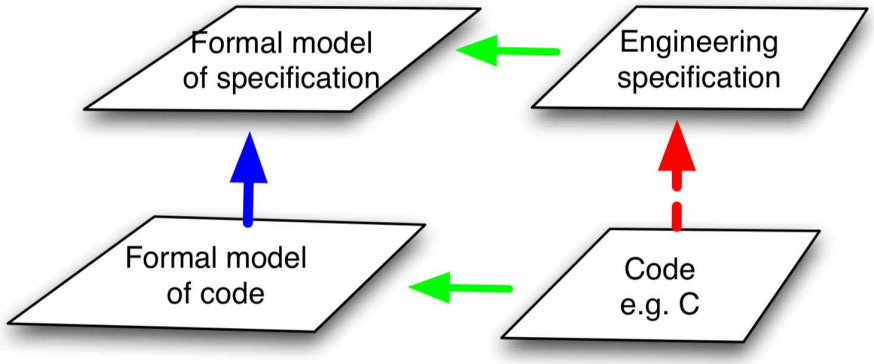
Inductive/deductive – Verify/validate

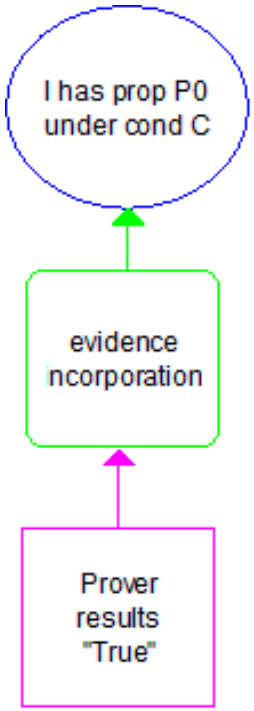


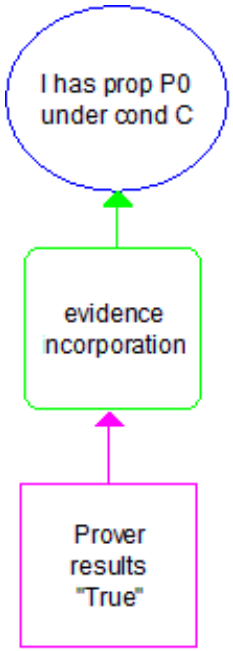
Application

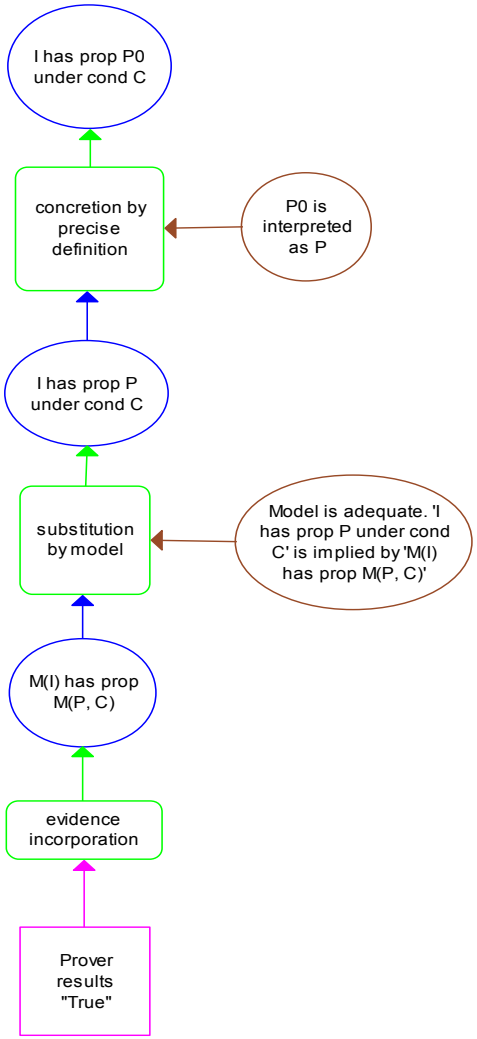
Simple example – smart device

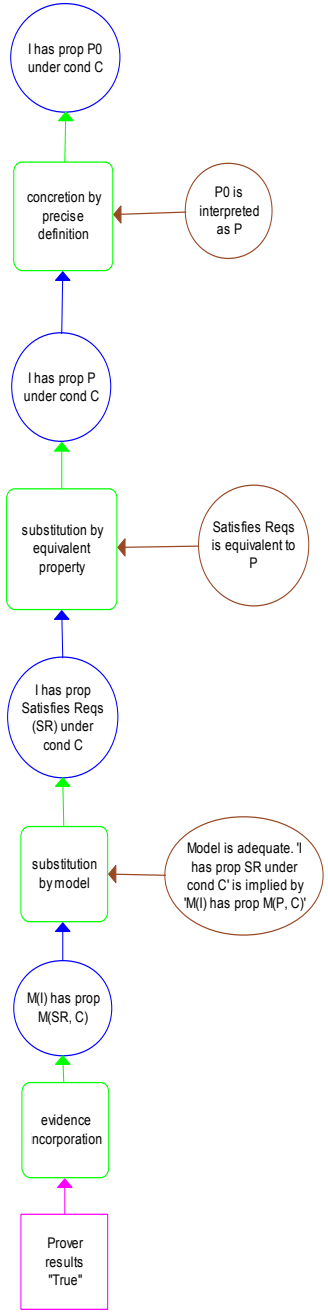
- Seek perfection, achieve high reliability – engineering
- Population of devices → very high reliability claims for 95% confidence no death from product line
- Equivalent claim – pnp < 5%
- Also John, Bev, Andrey Povyakalo's work on architectures



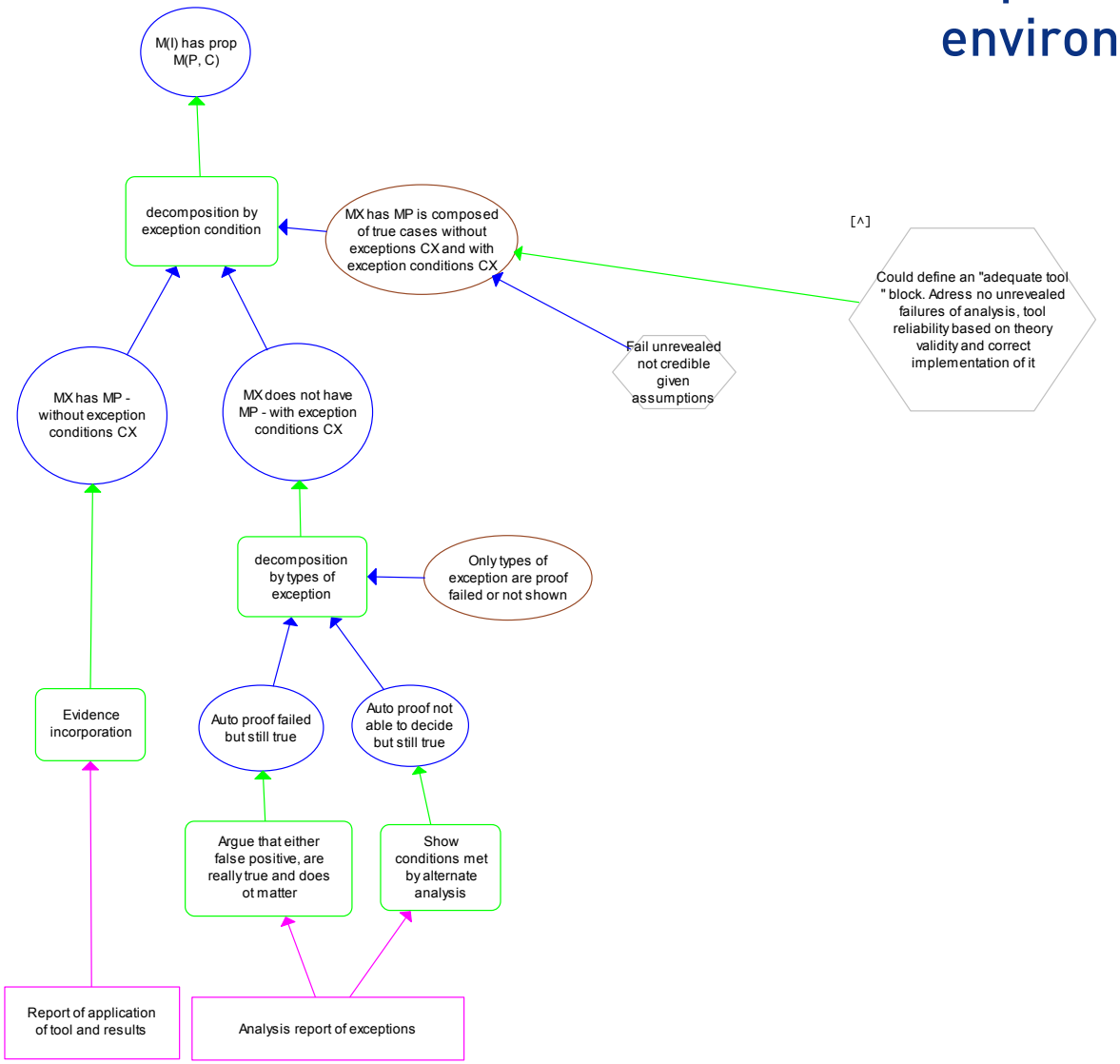

I has prop P0
under cond C
evidence
ncorporation
Prover
results
"True"


I has prop P0 under cond C
evidence ncorporation
Prover results "True"

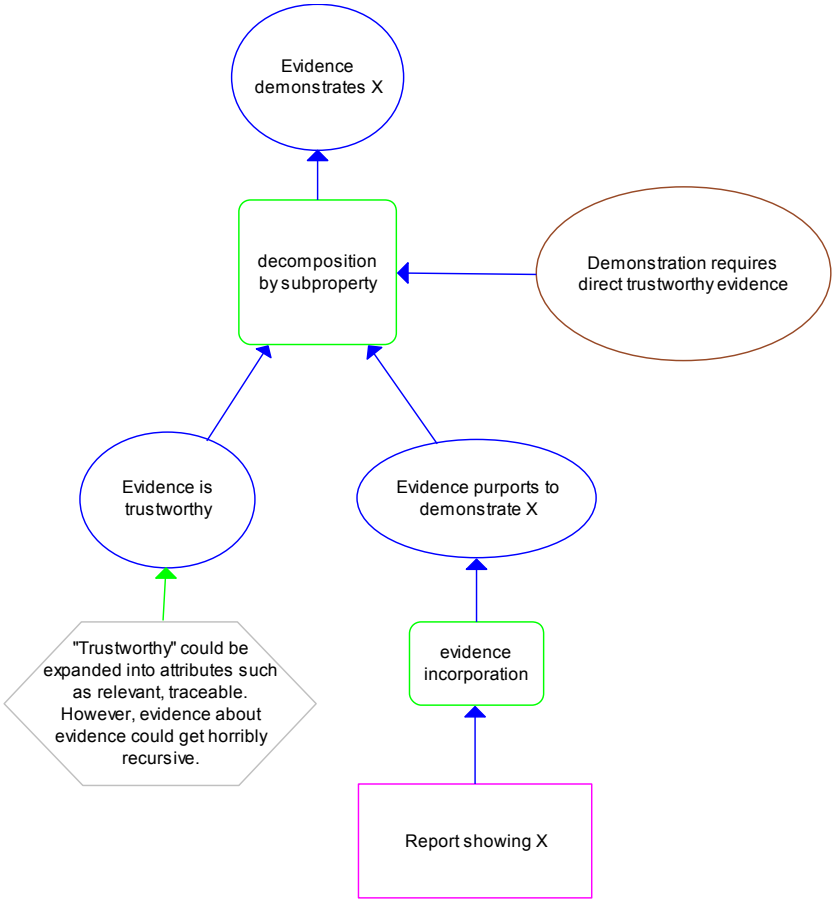

I has prop P0 under cond C
concretion by precise definition
P0 is interpreted as P
I has prop P under cond C
substitution by model
Model is adequate. 'I has prop P under cond C' is implied by 'M(I) has prop M(P, C)'
M(I) has prop M(P, C)
evidence incorporation
Prover results "True"


I has prop P0 under cond C
concretion by precise definition
P0 is interpreted as P
I has prop P under cond C
substitution by equivalent property
Satisfies Reqs is equivalent to P
I has prop Satisfies Reqs (SR) under cond C
substitution by model
Model is adequate. 'I has prop SR under cond C' is implied by 'M(I) has prop M(P, C)'
M(I) has prop M(SR, C)
evidence ncorporation
Prover results "True"

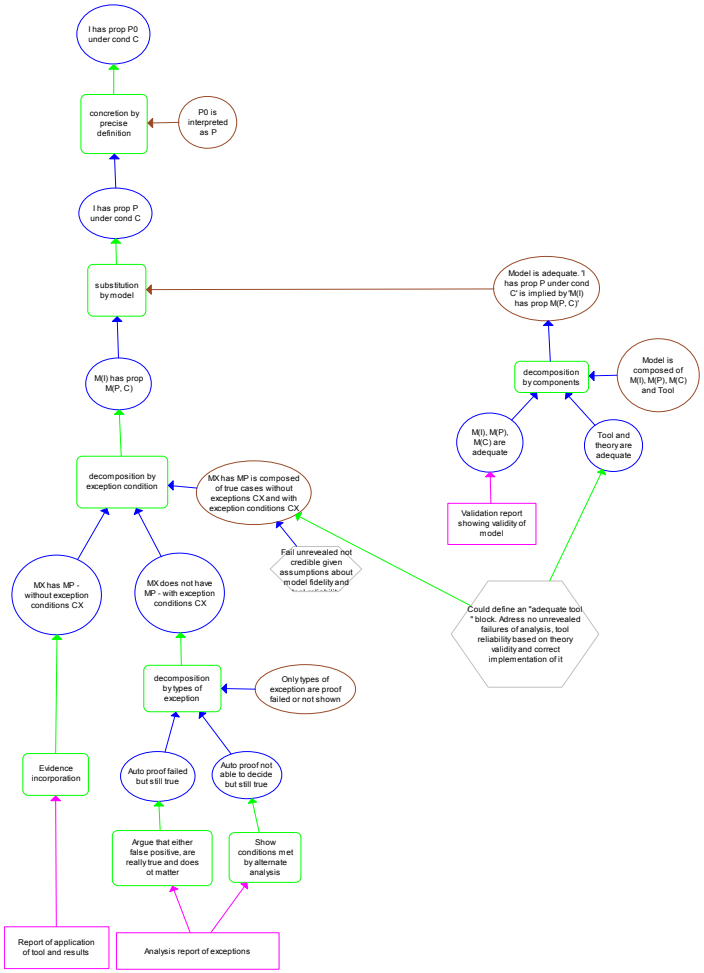
Experimental environment

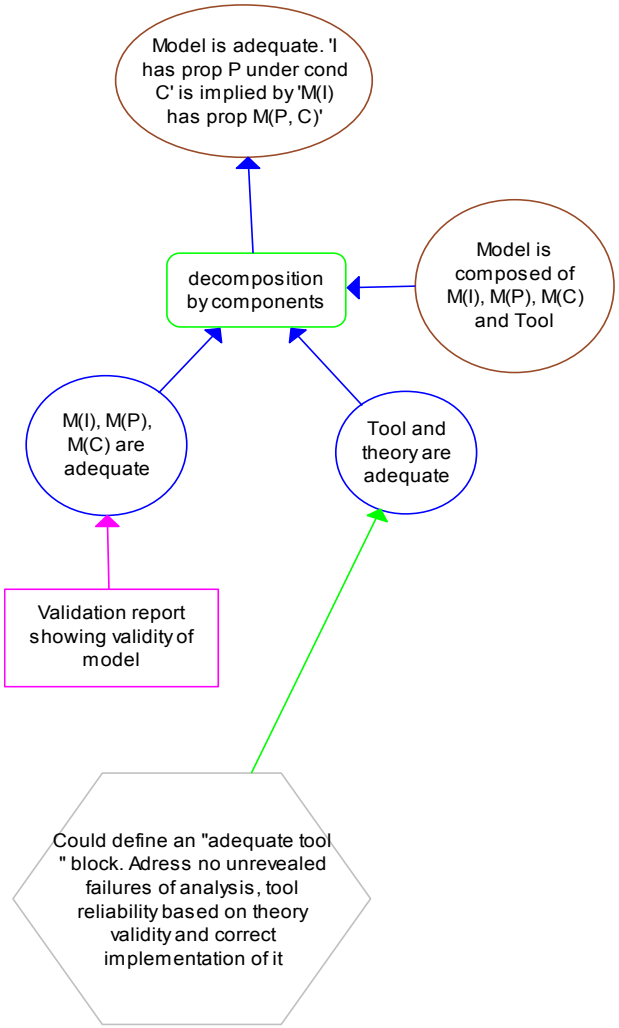


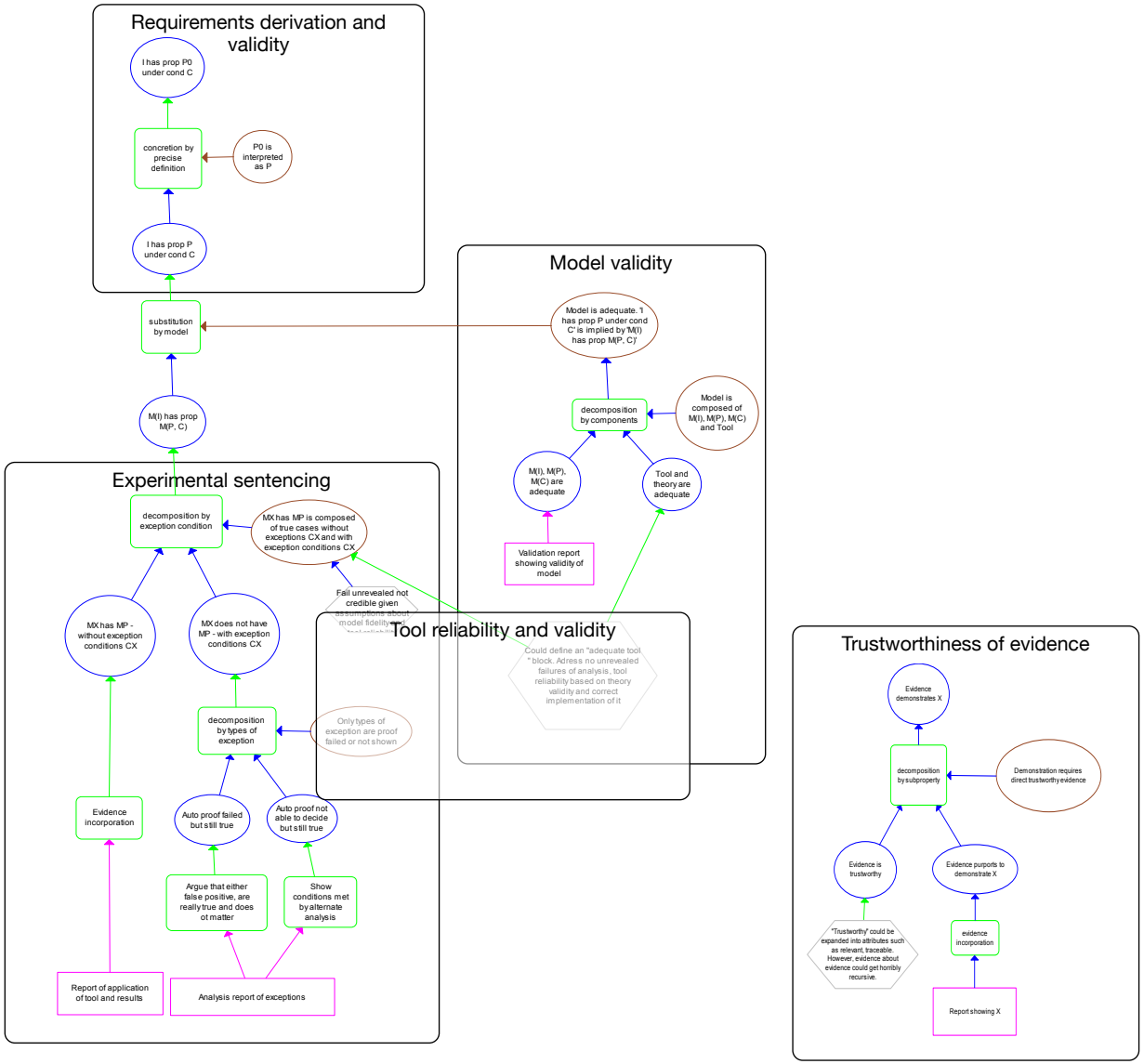
Evidence incorporation – explicit trust



Model fidelity






Requirements derivation and validity
I has prop P0 under cond C
concretion by precise definition
P0 is interpreted as P
I has prop P under cond C
substitution by model
M(I) has prop M(P, C)
Model validity
Model is adequate. 'I has prop P under cond C' is implied by 'M(I) has prop M(P, C)'
decomposition by components
Model is composed of M(I), M(P), M(C) and Tool
M(I), M(P), M(C) are adequate
Tool and theory are adequate
Validation report showing validity of model
Experimental sentencing
decomposition by exception condition
MX has MP is composed of true cases without exceptions CX and with exception conditions CX
Fail unrevealed not credible given assumptions about model fidelity
MX has MP - without exception conditions CX
MX does not have MP - with exception conditions CX
decomposition by types of exception
Only types of exception are proof failed or not shown
Evidence incorporation
Auto proof failed but still true
Auto proof not able to decide but still true
Argue that either false positive, are really true and does ot matter
Show conditions met by alternate analysis
Report of application of tool and results
Analysis report of exceptions
Tool reliability and validity
Could define an "adequate tool " block. Adress no unrevealed failures of analysis, tool reliability based on theory validity and correct implementation of it
Trustworthiness of evidence
Evidence demonstrates X
decomposition by subproperty
Demonstration requires direct trustworthy evidence
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

Doubts – epistemic uncertainties

- Drivers – real world risks and probabilistic requirements
  - Implicit or explicit
- What are these and how to combine
  - Irony of diversity
- Research on conservative approaches
  - Sum of doubts
  - Inclusion/exclusion principle
  - Sum of doubts not conservative
    - BBN – Littlewood Wright
  - Argument is not precise enough
    - So in CAE terms its nodes + argument
    - Lack of analysis and confusing abstract evidence for test reports
- Whatever approach need data or judgments on doubts

Applying safety analysis to cases

- Analysis of decision making
- Hazops
- Preliminary hazard list
  - Experience
  - Common vulnerabilities
  - Common fallacies
- Develop analysis approach

Avoiding the McNamara fallacy

"The first step is to measure whatever can be easily measured. This is OK as far as it goes. The second step is to disregard that which can't be easily measured or to give it an arbitrary quantitative value. This is artificial and misleading. The third step is to presume that what can't be measured easily really isn't important. This is blindness. The fourth step is to say that what can't be easily measured really doesn't exist. This is suicide."

- —Daniel Yankelovich "Corporate Priorities: A continuing study of the new demands on business." (1972)
- http://en.wikipedia.org/wiki/McNamara_fallacy

Types of doubt

Doubt categories	Description	Comment Are these ordered?
"Zero" - deductive	Accepted formal proof	Denote as ϕ Need to document "sun rising tomorrow"?
Incredible	Analytical justification why impossible but admit may be wrong	Claim limit Assumption – document if might change, for challenge
Small but not significant	Credible but can be ignored in quantification but not analysis	Only need to rank Show sum not significant Show non-linear or cascade effects absent
Significant	Need to quantify	...but how?

Example

- If case uses accepted blocks with high level of trust

Doubt categories	Example
"Zero" - deductive	Underlying logics, theories
Incredible	Theory basis tool Deductive CAE Blocks (generic)
Small but not significant	Instantiation of Blocks Dangerous failure prover Trustworthiness of evidence Derived results used by tool (libraries) Back end tool engineering issues
Significant	Requirements capture real-world properties Faults in formulating formal model of safety properties Code translation problems or things missed in code-model

Calculus of doubt/confidence

- Speculation …

Doubt categories	Operators
"Zero" - deductive	$\phi + \phi = \phi$
Incredible	Claim limit cl or unquantifiable symbol cl+cl= cl or 2cl?
Small but not significant	Show Small << Significant Sum(small) not significant Nonlinear effects 5 small = significant
Significant	Sum Evaluate – judgments and experiment

Discussion and conclusions

- From “What is..” to “What should it be ...”
  - Examined actual use of cases
- Develop structuring approach
  - Useful to see in deductive/inductive split
- Experimenting with conservative approach to doubts
  - Calculus options and when valid
  - Types of doubt
  - Evaluation – how?
- Next steps – more normative view
  - Modularity, templates
  - Beta application via courses, industry workshops
  - Tool support
  - Assess transition challenge and maturity

WOSD 2015

- Workshop at ISSRE 2015
- Fifth Workshop on Open Systems Dependability (WOSD 2015)