ASSC 2018

Australian System Safety Conference 2018

May 23 to 25, 2018
in Melbourne
Australia

Conference Theme

Strengthening and Integrating System Safety Engineering for Australia's future

BACK TO THE FUTURE – POLLOCK VERSUS TOULMIN

Arguing about arguing

ASSC 2018

Australian System Safety Conference 2018

May 23 to 25, 2018
in Melbourne
Australia

Conference Theme

Strengthening and Integrating System Safety Engineering for Australia's future

2

PREAMBLE

DISCLAIMER

- The approach discussed in this presentation is not part of Raytheon Australia PTY LTD Policy, Process, Procedure or Practice

DISCLAIMER

- I am an Engineer, though I originally studied Industrial Design, that included subjects from education towards a DIP ED, which drew me into Cognitive Science both where it went towards learning and then also where it went towards the problem of design.
- I then looked at Cognitive Science where it went towards system comprehension which drew me towards the notations to capture rationale.
- I eventually fell head first into a Masters in Safety, Risk and Reliability Engineering to find that the search for rationale was to no avail, or so some would have me believe.

CURRENT HOBBY INTERESTS

- Walking problem reduction over URN and into Event-B to capture reasoning over model refinements to gain epistemic assurance as a side effect of logic design.
- Modelling FRAM in backward chaining expert system shells.
- Modelling FRAM/STPA in stateful actor based dataflow languages that include non-determinism.
- Promoting a call for the development of an Agile Assurance Adoption Framework.
- Using QUASAR as a heuristic when modelling in URN.
- Agent Oriented Assurance Cases (the goal of this story).
  - Within the design notations and embeddable within architectural viewpoints.

But surely you can get by with FTA, FMECA and GSN?

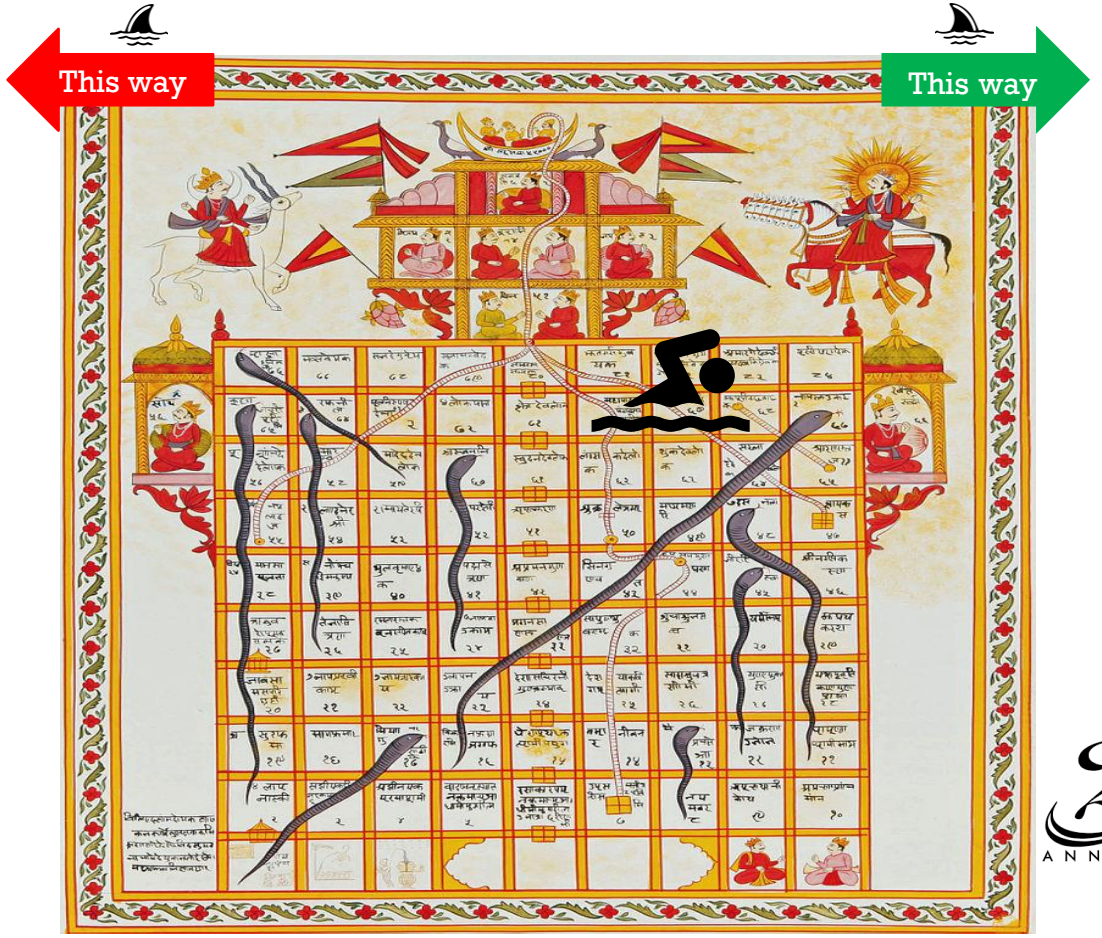
CONTEXT

In the context of large defence projects with by contract, MIL-STD 882 (an archetype of safety case models), UK "style" Safety Cases (MIT disagree and despite 882 being an archetype of safety case models`), Defense Force driven Weapon System Certification, Work Health and Safety (WHS) and generally poor harmonisation between the streams to argue $afety thrice and more.

Safety Cases versus Intent Specifications amongst an intercontinental agonistic if not antagonistic debate

Should our safety claims be of a fashion tectonically and philosophically somewhere between MIT and York University?

SO, LIKE A RIP OFF BONDI BEACH, ONE CAN GET DRAGGED INTO A MEME



meme
mi:m/
Noun
an element of a culture or system of behaviour passed from one individual to another by imitation or other non-genetic means.

What, do you mean its Graphical Intent Specifications versus Graphical Safety Cases and not just about notations?

Intent Specifications are supposedly based upon goal-oriented rationale but they don't use a graphical notation (yet)

Not to mention the argument between Argument notations versus Goal Oriented Requirements Engineering notations

Is it really true that Rationale does not equal Argument?

INTERNAL OR EXTERNAL SAFETY CASES?

- **A range of fallacies** are detectable in the debate between design rationale versus argument notations such that a harmonization of memes, sourced in both UK and US safety cliques, is being forestalled.
- **Harmonization is possible**, without stretching the case, through application of notations from Goal-Oriented Requirements Engineering.
- This talk proposes that User Requirements Notation (URN), an Goal-Oriented analysis and requirement notation, can span the memes between safety cliques to **provide a unified design-rationale-cum-assurance notation**.

> For economy, assurance argumentation should be integral to requirements and design notation semantics

ASSC 2018

Australian System Safety Conference 2018

May 23 to 25, 2018
in Melbourne
Australia

Conference Theme

Strengthening and Integrating System Safety Engineering for Australia's future

9 ARGUMENT BY SUBSTITUTION

If the notation fits …

AIM

ITU is the United Nations specialized agency for information and communication technologies

International Telecommunication Union

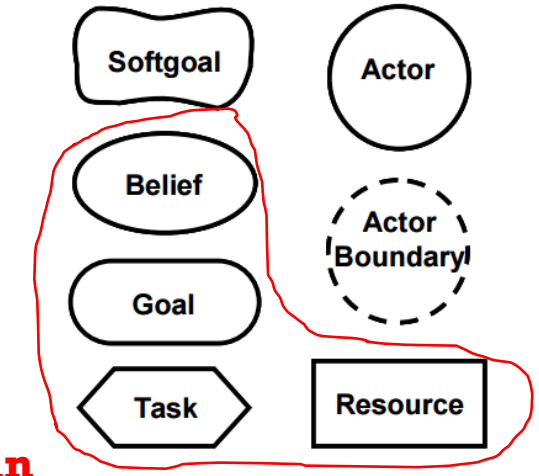
ITU-T Z.151

- Direct attention to User Requirements Notation (URN):
  - URN is a semi-formal, lightweight graphical language.
  - Used for modelling and analysing requirements in the form of goals and scenarios.
  - Used to specify and analyse various types of reactive systems, business processes and enterprise goals of organizations.
  - Can be used to model systems preliminary and architecture level for: **system quality trade-offs, qualitative risk modelling, FTPN, STPA and FRAM.**
  - Exports requirements and supporting reasoning into DOORS to translate into System Engineering outcomes.
- Comprises two notational styles:
  - Goal-oriented Requirement Language (GRL):
    - Supports 'weighted' reasoning and decision support.
    - Using stereotypes, it can act as a **typed argument framework**.
  - Use Case Maps (UCM)
    - See Wu and Kelly for **use in hazard analysis**.
      - See Sunday's description of Anticipatory Failure Determination Approach (AFDA) for a more methodological approach.
    - See Feodoroff for description of how to use UCM as **FPTN for systems and systems-of-systems.**

GSN, having been designed to be completely general, does not explicitly capture concepts that relate to the safety domain (such as system models).

URN provides at the design level, early work on argument-based design rationale to develop a set of abstract models of the design in terms of actors, goals, responsibilities, system qualities, positions/options, and arguments/criteria.

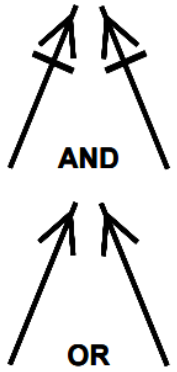
GSN IS A SUBSET OF GRL



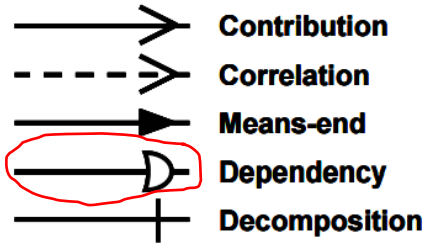
GSN in red

(a) GRL Elements

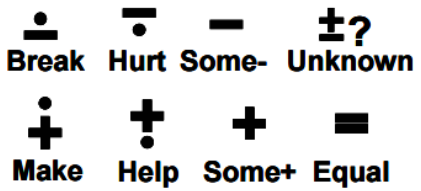
(b) GRL Satisfaction Levels



(c) Link Composition



(d) GRL Links



(e) GRL Contributions Types

Fig. A.1. Summary of the GRL Notation

But they aren't the same names?

Goal Structured Notation (GSN) is simply a typed argument framework.

Goal-oriented Requirement Language (GRL) is one of two notational styles within User Requirement Notation (URN)

GSN ⊊ GRL

Is that legal?

TASK ≈ «STRATEGY»

- Vacillate over dictionary meanings:
  - Dictionary vagueness around definition of Strategy as it can either be a "plan of action" OR "the art of planning"
  - GSN adopts "plan of action" for Strategy, actually called Plan in HTA.
  - HTA also uses Goals which are likely descriptive accounts of "work to be undertaken", GSN Goals simply become "argument to be undertaken"
  - Task (the noun) is:
    - descriptive "work to be undertaken" (a.k.a. Goal) or
    - prescriptive "function to be performed" alluding to strategy by "plan of action"
  - GRL uses both Goals and Tasks dependent upon descriptive or prescriptive intention. HTA can be carried out in GRL.
- Semantic twists only. Vacillate for a suitable length of time. Change "meaning" of GRL Task to GSN "Strategy" using «stereotyping».

> Stereotyping is a legal mechanism in UML and SysML for weaselling semantics.

RESOURCE ≈ «SOLUTION»

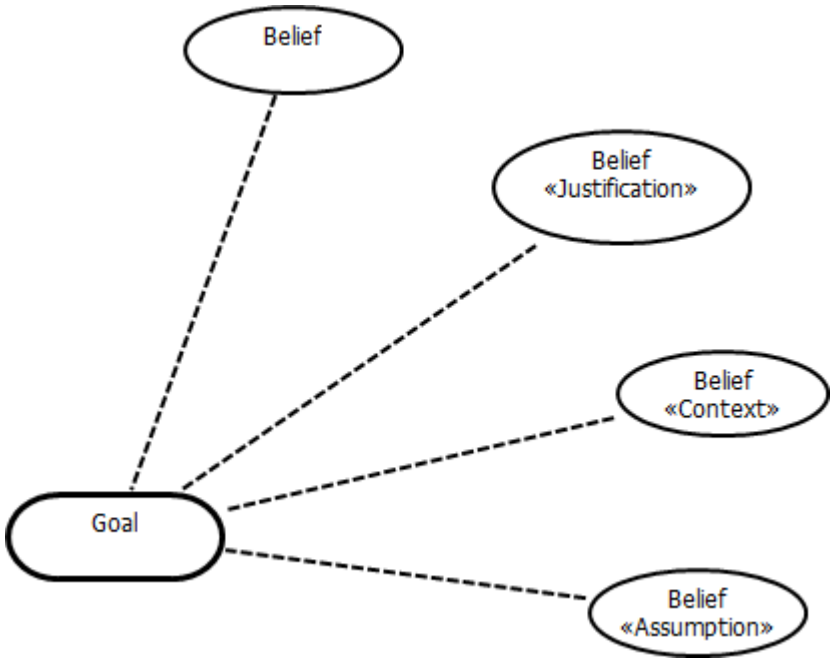
- Ditto, vacillate over semantics, use «stereotyping»

It's that easy?

BELIEF ≈ «JUSTIFICATION», «CONTEXT», «ASSUMPTION»

Would that beggar belief if I used Toulmin's «Warrant» here?

- Ditto, vacillate over semantics, use «stereotyping»



et Ditto

EXPLANATION

But there was no mention of epistemology back then!

Does that mean that the GSN design was epistemically lucky?

Belief as a Basis	Reasoning
Justification	Hintikka semantics captures knowledge as **true belief**. Justification logics supply the missing third component of Plato's characterization of knowledge as **justified true belief**.
Context	This is really the **Epistemological Frame Problem** as this is the **set of beliefs** that must be reassessed in the advent of change to the argument.
Assumption	Very likely relates here to the notion of **Epistemic Game Theory** sense as this acts as a **belief about the imperfection or incompleteness** of the context of the argument. Argument is otherwise a dialogue, or a game, between two agents.

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

$\therefore GRL \supsetneq \text{«}GSN\text{»}$

GRL	Goal Structured Notation (GSN)
Actor/«Agent»	-
Goal	Goal
Task	«Strategy»
Resource	«Solution»
Belief (along with Belief Link)	«Justification», «Context», «Assumption»
Dependency (link)	Solved-By (link)

http://www.goalstructuringnotation.info/gsn-metamodel
https://www.omg.org/spec/SACM

Is this irony? The institution founded on an act of Unification opting for a reasoning exchange mechanism?

What if a Unification was possible through a flexible light weight notation with stereotypes?

Voila!

Mapping GRL to OMG SACM(ARM) via GSN!

CAE IS A SUBSET OF GRL

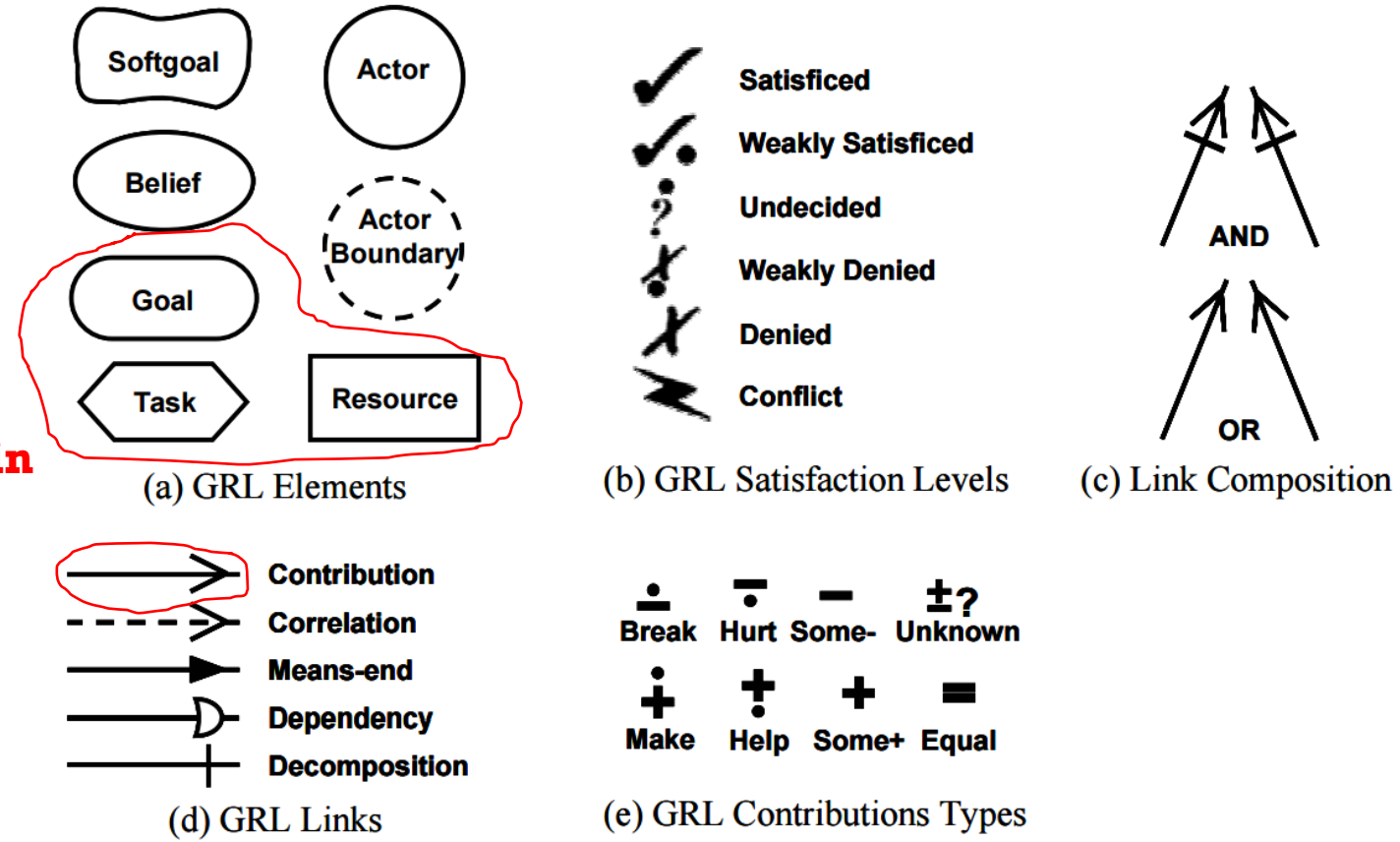


Fig. A.1. Summary of the GRL Notation

But they aren't the same names? Oh, you mean use «stereotypes» again?

Claim Argument Evidence (CAE) is simply a typed argument framework.

Goal-oriented Requirement Language (GRL) is one of two notational styles within User Requirement Notation (URN)

CAE ⊊ GRL

$$\therefore GRL \supsetneq \text{«}CAE\text{»}$$

GRL	Claim Argument Evidence (CAE)
Actor/«Agent»	-
Goal	«Claim»
Task	«Argument»
Resource	«Evidence»
Belief (along with Belief Link)	-
Contribution (link)** **note the change out	«Supports», «Is sub-claim of», «Is evidence for»

http://www.adelard.com/asce/choosing-asce/standardisation.html
https://www.omg.org/spec/SACM

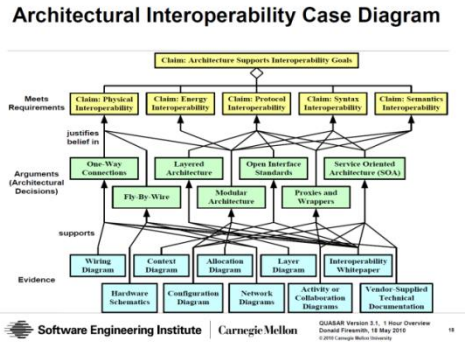
So GSN is a another reasoning approach and not just THE notation?

et Voila!

Mapping GRL to OMG SACM(ARM) via CAE!

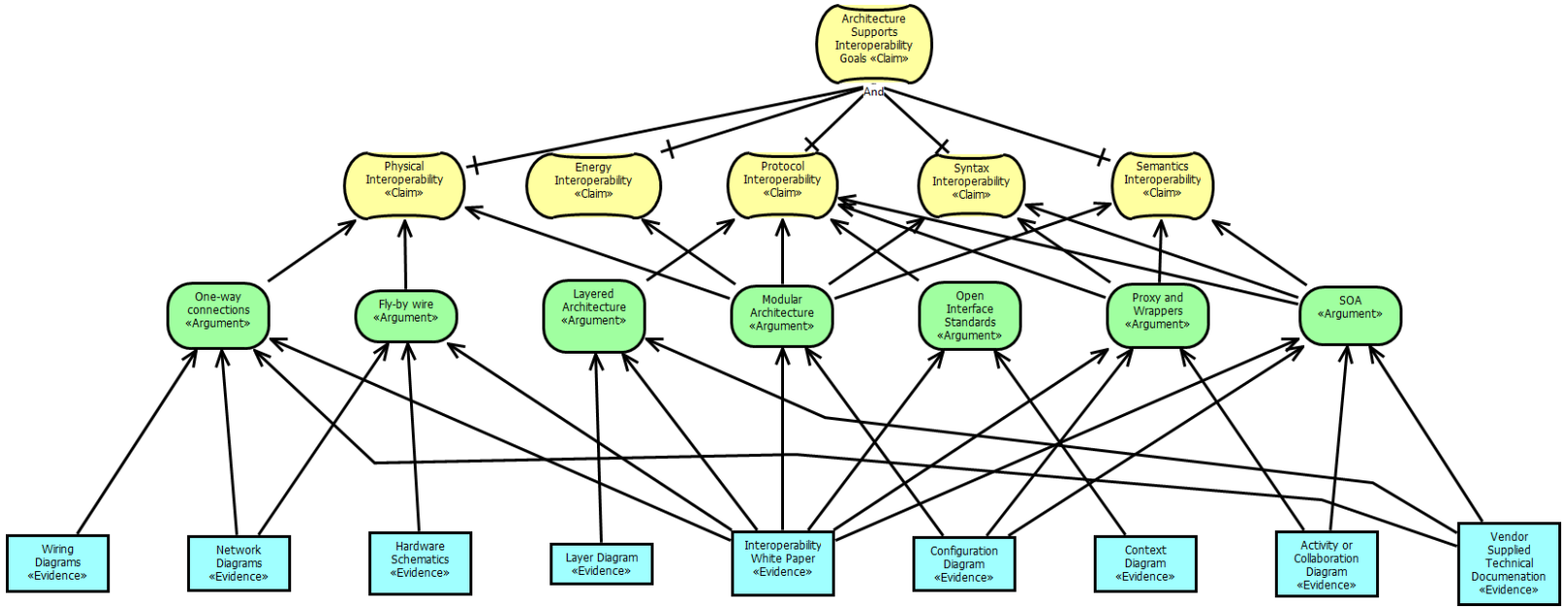
INTERPRETING CMU'S INTERPRETATION OF CAE

Abstraction Hierarchy



Need there be one Argument notation?

There certainly isn't only one Argumentation notation!?



But these structures do not express the concepts of strategy, solution, assumption and justification offered by GSN?

Is Claim Argument Evidence an Abstraction Hierarchy or is it a Notation?

CAE syntax is as different to GSN as that of GRL !!

$GSN > X \because X \neq GSN$ holds for both GRL and CAE

BIG ASSURANCE TOOLSET FOR BIG ASSURANCE PROBLEMS: NASA CERTWARE

This way

- ARGUE IN (a.k.a. Explain):
  - INTENT SPECIFICATIONS (Leveson claims these are goal-oriented)
  - * Semi-formal proof languages
  - Bayesian reasoning models

- ARGUE IN (a.k.a. Justify):
  - Goal Structured Notation
  - Claim Argument Evidence
  - Eurocontrol
  - Textual outlines or "trees" of fractal argumentation in SACM meta-model
  - Argument Mark-up Language

This way

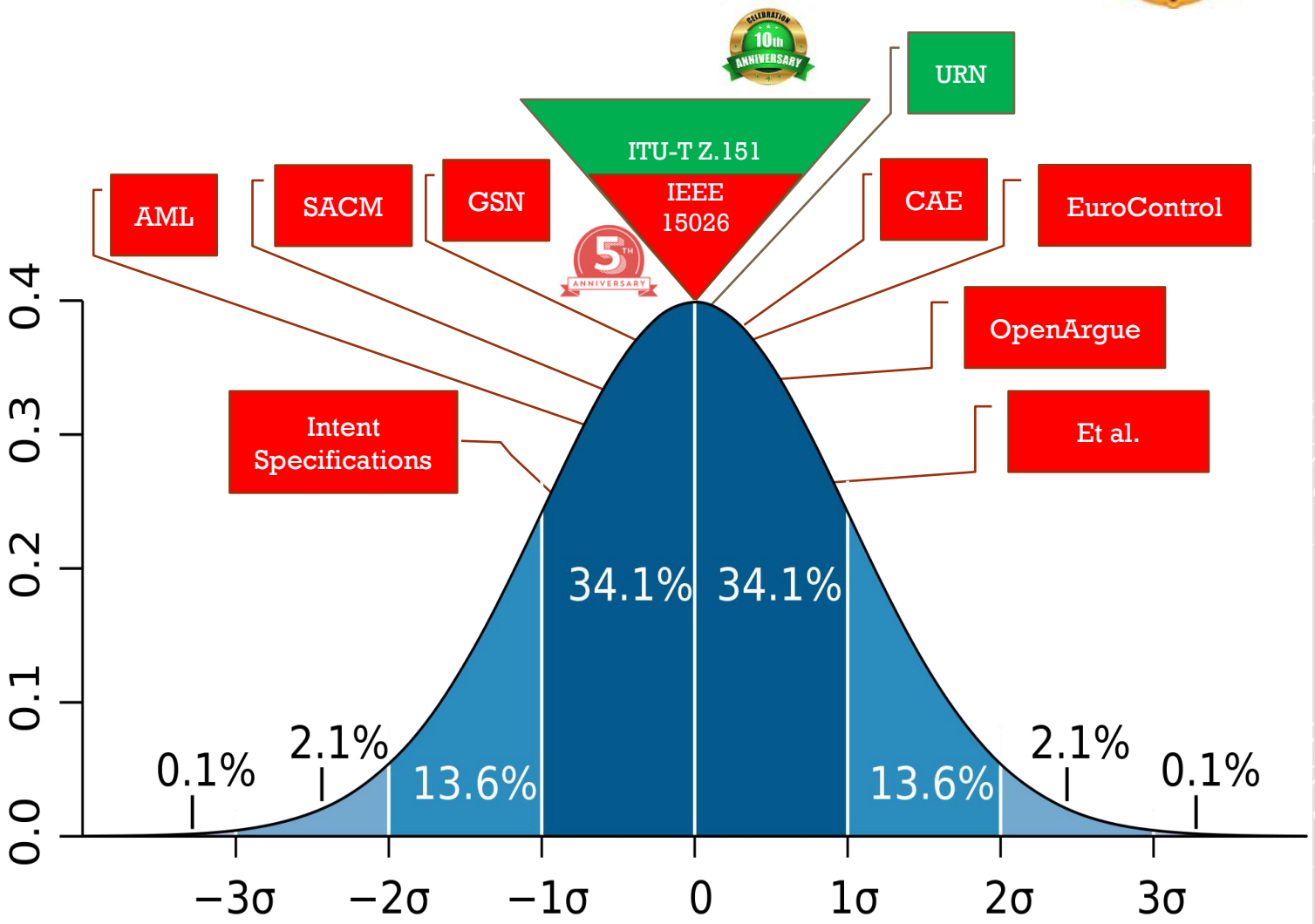
Would you believe interpretable in URN to draw this all into a single graphical requirements and architectural design decision rationale.

* Argument community is split down the middle as to whether proofs are argument or just evidence. So semi-formal proofs? Wow! That leads us to semi-formal notations such as URN. Why? Semi-formal proofs are over open not closed sentences. Problem Frames is also a semi-formal expression of Gentzen Sequent Calculus (a.k.a. proof). PF is a great heuristic for modelling in URN, especially when also seeded by control-theoretics concerns, all to be captured using a graphical interpretation of a semi-formal causal calculus. So, what if Intent Specifications were expressed as a bag of graphical semi-formal proofs?

Don't take sides in the debate between Rationale and Argument.

Reason/Argue in as many dialects or forms as you can muster because $GSN \approx X \because X \approx GSN$

IEEE 15026 ⊊ ITU-T Z.151



What on earth are we arguing about again?

Think of IEEE 15026 as ITU-T Z.151 minus agency, defeasible reasoning and causal thread formalisms.

Certware and other evidence tells us that variation in notational lexicon and syntax is legal.

So, if all argumentation notations and their semantics sit within a standard deviation of IEEE 15026 then …

Will I get sued if I don't use GSN?

WHAT TYPE OF FALLACY IS THIS?

Safety Cases are "different" to Security and Dependability Assurance Cases because there is a legal requirement for Safety Cases

Safety Cases are structured Arguments

You can present a structured argument using GSN notation

There is therefore a legal requirement for using GSN notation

Now substitute GRL into that fallacy

OVERARCHING RULE:
THERE ARE NO SILVER BULLETS !!!

ASSC 2018

Australian System Safety Conference 2018

May 23 to 25, 2018
in Melbourne
Australia

Conference Theme

Strengthening and Integrating System Safety Engineering for Australia's future

24

THEMES FROM SAFETY CASE LITERATURE

What I believe I know about argument. I think.

EPISTEMOLOGICAL QUESTIONS

- Defined narrowly, epistemology is **the study of knowledge and justified belief**. The real epistemic questions are the following:
  - What are the **necessary and sufficient conditions** of knowledge?
  - What makes justified beliefs justified?
  - Is justification internal or external?
- So, where does Epistemology sit within Safety Cases?

What now? An epidemic of nomenclature?

Various safety case practitioners cum philosophers have postulated about the application of epistemology in that art.

LOGIC VERSUS EPISTEMOLOGY

- Rushby, post introduction of DO178C, sees **safety cases split into**:
  - **Logic** (and thereby calculi and, say, Argument®)
  - **Epistemology** (say, for the sake of argument, Argument™)
- Argues defeasible reasoning should be done outside of "case".
- Likens defeasible reasoning to hazard analysis.
- Hazards analysis is, in any event, a non-monotonic process.
  - Rushby is arguing that we should use non-monotonic reasoning integral to the development of architectural requirements and design decisions, just not in the "case".
  - Non-monotonic reasoning is likely then the semantic for embedded preliminary and architectural justifications.
- What if rationale for requirements and architectural decisions used a semi-formal calculus?

Argument™ > Argument® because Argument® ≠ Argument™ (v.v.)

But originally rationale was goals decomposed by AND/OR, now it's non-monotonic reasoning?

Rushby was selling Satisfiability Modulo Theories (SMT) which is over first order logics.

Rusby felt rationale is not Argument because Argument (or "case") is not to expose its background non-monotonic processes.

Fine because GRL has a dual "case" and rationale semantics together in the one notation!

HOARE'S QUESTION

- Hoare was musing over the relative success, at the time, of Boeing 777 aircraft, when he asked:

  How did software get so reliable without proof?

- **That is, we can get very close to Nirvana without logic.**
- But if not logic what? Rationale?
- Is rationale epistemic when it is the methodological explanation, albeit undocumented, of what we believe?
- What if we documented rationale with a semi-formal calculus?

Argument™ > Argument® because Argument® ≠ Argument™ (v.v.)

Proofs are too big to comprehend? Arguments are too big to comprehend? How can I believe what I can't comprehend?

There are arguments that large proofs are incomprehensible to humans.

If logic acts as the tractable aspect of design, it likely means the epistemic questions are left for the socio-technical aspects of safety.

TOULMIN BREAKPOINT

- Of note, when Toulmin (2003, p. 185) discusses the *'calculus'* of knock-out competitions he says:

  'What sign will indicate that the calculus of draws is being treated as mathematics and its propositions as mathematical propositions?'

  The answer is, roughly speaking, that the criteria by which it is decided to accept or reject propositions must no longer involve procedural or other extraneous considerations, but must lie entirely within the calculus.

- **That is, no need for epistemic reasoning over top of logic**.
- There may still be room for epistemic reasoning over other topics.
- There may still be room for epistemic reasoning over the selection of one or the other calculus.
- What if a calculus was applied to rationale capture?

Argument™ > Argument® because Argument® ≠ Argument™ (v.v.)

Does my rebuttal look too big in this argument?

One form of over argumentation is restating the logic in an epistemic form.

Cheap because it can be automated.

It can be automated because it is a lightweight M2M transform.

AGENT ORIENTEDNESS OF EPISTEMIC REASONING

- *Would you believe that an Agent C may think, believe or know A thus entailing A?*
  - $T_C A \vdash A$
  - $B_C A \vdash A$
  - $K_C A \vdash A$

Is that a reference to a slang term that is used in the American popular culture as a transitive verb to mean throw out or get rid of?

There are fuzzy edges here.

Sometimes we mean believe when we say know.

Sometimes we mean think when we say believe.

It never bodes well when we say know when we only think.

I WANT TO BELIEVE!

- For safety, of the three options:
  - Thinking A can be rejected because, as Toulmin contends, **an unbacked intuition is not an argument**. That is, it cannot stand on its own as a justified belief.
  - Knowing A can be rejected because the pessimism of safety is that there is a 50/50 chance the system will fail in its next hour of operation. **We cannot know unless we turn the key**. The models we use are also not the system.
  - Believing A is left to us.

I now know what to believe.

I think.

> Will safety be a justified belief or a justified true belief?

> Epistemology holds that JTB is still short of knowledge !!

> Why is a duck?
>
> Because it may be epistemically lucky.

EPISTEMIC STANDARDS

- The notion of Epistemic Standards introduces the notion of **Scepticism and its role in Epistemic Reasoning**.
- Beliefs may not count as knowledge in some contexts because the epistemic standards are unusually high.
- Epistemic low standards are likely spaces were agreement prevails and there is unlikely to be contest or any contest is waning.
- This might relate to the Toulmin Breakpoint as scepticism will plague a calculus until it is fully established. The calculus is thereafter a shorthand.

So, sometimes I can ignore the sceptics?

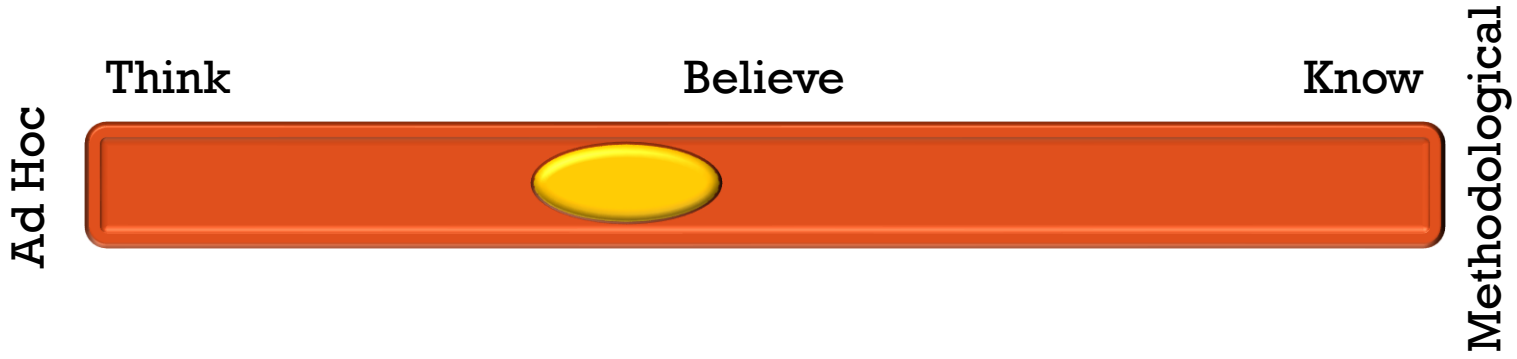
A belief can likely stand as a justified belief where it still holds after attack has subsided.

Where the attacking has subsided the assumption is that all significant scepticism has been overturned.

In reality, it might simply also be something holds for a time or under certain conditions or for a certain audience.

METHODOLOGICALLY OVERCOMING SCEPTICISM

- Whether something is a justifiable belief, or not, relates to the work that went into getting there.
- Everyone might apply a method to get to a belief but not everyone applies a methodology or acts methodologically.
- **Methodologies are thus an important tool**.
- The other problem is, of course, agreement on the methodologies.



So I need a mature organisation with repeatable processes?

Both technique and subjectivity biases plague us.

Known missing dimensions in one technique can be covered by other techniques.

PROBATIVE VALUE IS THE COURT APPLIED SCEPTICISM

- Occasionally, papers pop up that demand safety judgements by safety practitioners suffice even where approaches are somewhat less than methodological.
- When discussing probative value of expert witness testimony in court, however, Edmond contends that:

  Opinions produced using scientific, medical and technical procedures cannot be rationally assessed ***unless the procedures have been subjected to formal evaluation****.*

- Ergo, procedural practices must entail methodological approaches. Probative value entails validation of same.

Should I have evidence of conformity? Would normative heuristics help? Would a third party auditor help? Would audits by the regulator help?

Probative value leads us to jurisprudence.

Methods do not survive contact with industrial practices.

Validation may fail if one is too far from conformity with a normative heuristic.

PRACTICAL REASONING STYLES FOR DESIGNERS

The job application said I needed FTA, FMECA and GSN?

Demonstrable	Non-Demonstrable
Deductive	Inductive
	Probabilistic
	Statistical
	Abductive
	Defeasible

> Leveson has said that formal methods are not safety.

> Did Leveson mean that safety is a non-demonstrable quality?

> Non-demonstrable qualities require higher epistemic standards – that includes validated methodologies

WHICH ONE DO I CHOOSE?

- **Inductive Reasoning**. Ranging over **weak through strong claims**, to claim a **degree-of-support for a conclusion**.
- **Probabilistic reasoning** is **structured**, so think of Fault Tree Analysis or Bayesian Belief Networks for example.
- **Statistical reasoning** comes from trying to make sense of statistics.
- **Abductive reasoning** is taking your best shot. Working with incomplete information. Might actually be akin to the initial steps in clearing away the cloud that is that wicked design problem.
  - Conversely, one morning you enter the kitchen to find a plate and cup on the table, with breadcrumbs and a pat of butter on it, and surrounded by a jar of jam, a pack of sugar, and an empty carton of milk. You conclude that conformity of your processes to DO178C has been attained. This is not the best explanation.

I have to do sit-ups?

Oh, abduction.

Choose wisely.

Choose as many that fit the story to be told.

What about defeasible reasoning?

OF NON-MONOTONIC REASONING

Counter argument reasoning suggested as a means to tear down a "case".

- Non-monotonic reasoning is a class of logics created to capture defeasible inferences.
  - Defeasible means the **relationship of support between premises and conclusion is tentative.**
  - Potentially **defeated by additional information**.
- Of note, **inductive and abductive reasoning are both non-monotonic**. Makes sense. Weakly or strongly, for or against.
- One can otherwise apply alternating supporting and weakening premises to **demonstrate the progression of the dialogue**.
  - Ad nauseam … or preferably until some stopping condition is reached. Probably when weakening premises are becoming abductive.

Is that like a gin sling, hold the sling?

> Defeasible reasoning finds its fullest expression in jurisprudence!

> Practically, defeasible inductive and abductive claims for and against are all part of the wash.

> Argue towards a balance of probabilities (for and against).

MONOTONIC TOWARDS FULMINATORY UTTERANCES

- Monotonic reasoning means that **in the face of more weakening premises the claim holds**.
  - Is this really a stasis point for a non-monotonic dialogue?
- Confidence in a safety claim might be that stasis point justified both:
  - **By presenting all the significant supporting vs. weakening premises.**
  - **By using non-monotonic reasoning over the design dialogue to claim the achievement of a state of monotonic stasis**.
- Unfortunately, argument notations without semantics to support non-monotonic reasoning appear to declare monotonic stasis is attained by ignoring scepticism.
  - **But it is BECAUSE they simply do not include semantics for attacking or weakening**.
  - That is, there is no means to interpret with any confidence a belief in the attainment of monotonic stasis.
    - Hence, the inclination to build a second confidence argument next to the assurance argument.

So it's the "case" that I can't be arguing if I am not in a dialogue or haven't shown the evolution of the dialogue?

Various safety case authors are warning against over-argumentation.

The problem might be in the notation.

Proof on the balance of probabilities (for and against).

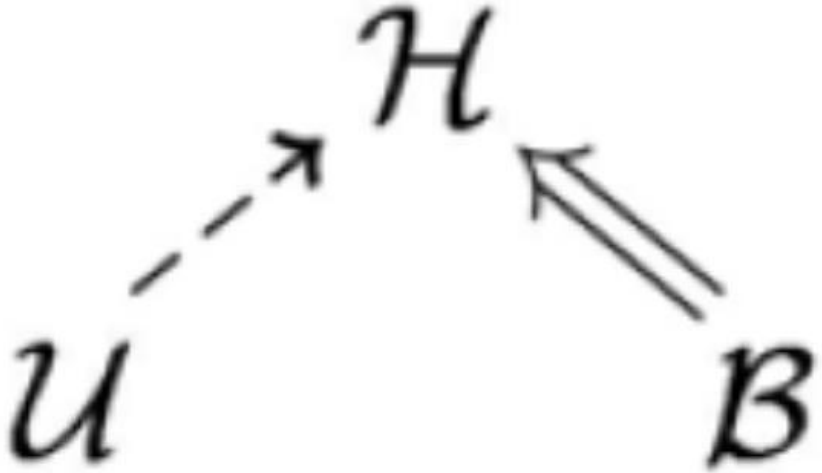
UML, SysML have the same fulminatory nature which is the likely appeal for GSN and CAE.

NON-MONOTONIC LOGICS FROM AI

Backing Undercutting Argument Framework (BUAF)

- Melds principles from Pollock and Toulmin.
- The basic notion is that there are **three forms of attack: rebuttal, undermining and undercutting**.
- However the notation is only to explain the intent of the calculus which is the algorithmic process applied by two computational **agents in a dialogue**.

Basic BUAF notation

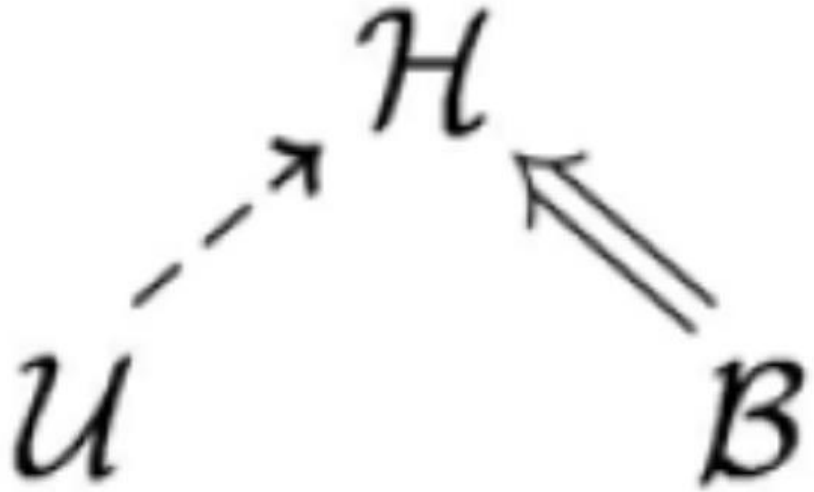


A ROSE BY ANY OTHER LEXICON

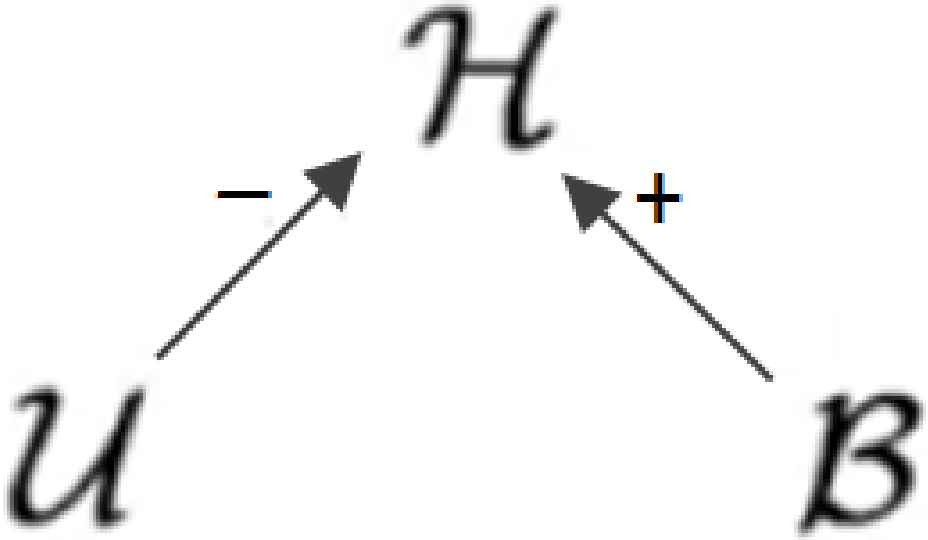
For, Against? +ve, -ve? Can also mean pros and cons yes?

Isn't that the direction of edges in CAE? Is it also an analogue of the causal links in BBN?

Backing and Undercutting via BUAF



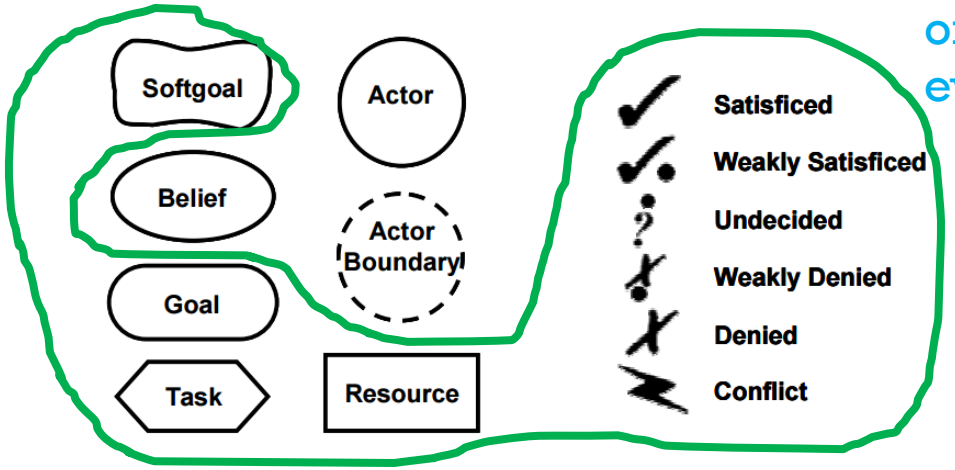
Backing and Undercutting via Contribution

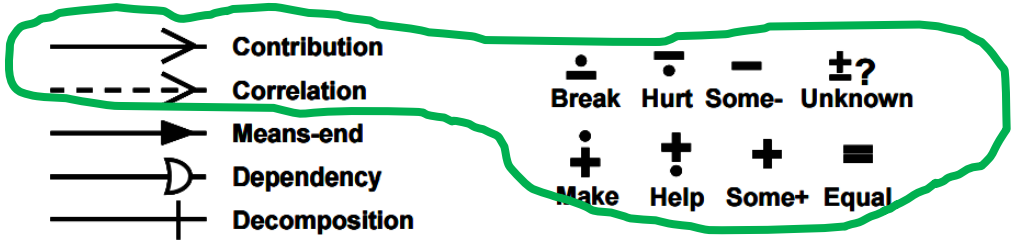


NON-MONOTONIC SEMANTICS

Weights the nodes of the graph

That is, weight the belief in the sufficiency of the claim or evidence





That is, weight the belief in the contribution of the contributor to the contributee

Weights the edges of the graph

But won't that give me more dimensions to my argument?

All just syntactic sugar for +ve and –ve degrees of support or attack.

Correlation is used to reflect on unwanted side effects … eerily akin to the Hollnagel's notion of emergence.

Might also have the pedagogical influence on Argumentors that is missing from GSN and CAE (and from UML/SysML).

ASSC 2018

Australian System Safety Conference 2018

May 23 to 25, 2018
in Melbourne
Australia

Conference Theme

Strengthening and Integrating System Safety Engineering for Australia's future

41

STIRRING THE POT

A demonstration of non-monotonic reasoning, framed by normative heuristics, to attain a methodological approach to achieving epistemic high standards.

MIXING MEMES IS GOOD!

- Habli, Wu, Attwood, and Kelly:
  - Claim to "extend" Goal Oriented Requirements Engineering with "Argument", and
  - Argue:
    - QAS:
      - is goal-oriented;
      - displays qualities of Zave and Jackson's $S, K \vdash R$ (a.k.a. Knowledge Frames)

Despite previously arguing rationale is not argument we now argue that argument is rationale(?)

Cf. Rushby, can a "case" notation be used for rationale?

We otherwise find closure mechanisms for reasoning over open sentences come in multiple formats.

Will I need my own PPE?

THE EXPERIMENT

- Starting with the example in Habli, Wu, Attwood, and Kelly:
  1. Model the Quality Attribute Scenarios (QAS) graphically (instead of by tablature)
  2. Add (so-called) ANTI-GOALS
  3. Include ANTI-ANTI-GOALS (to capture the mitigations for the ANTI-GOALS)
  4. Goal satisficing argument over a tree (a familiar structure to proponents of GSN), using QAS reasoning fragments

- Artefacts considered by Habli et al.:
  - Wheel Breaking System (WBS),
  - Spoiler, and
  - Reverse Thrust

Moving towards graphical Intent Specifications in URN

No deeper than the original example to be a fair comparison.

QUALITY ATTRIBUTE SCENARIOS (QAS) IN A NUTSHELL

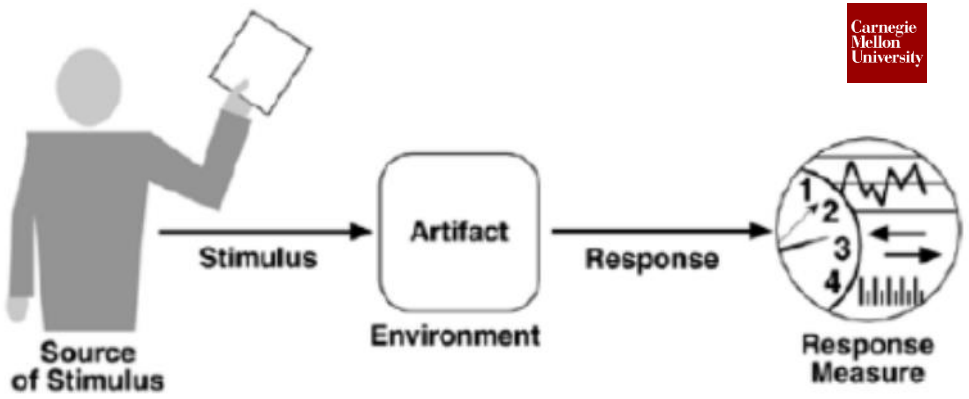
By tablature

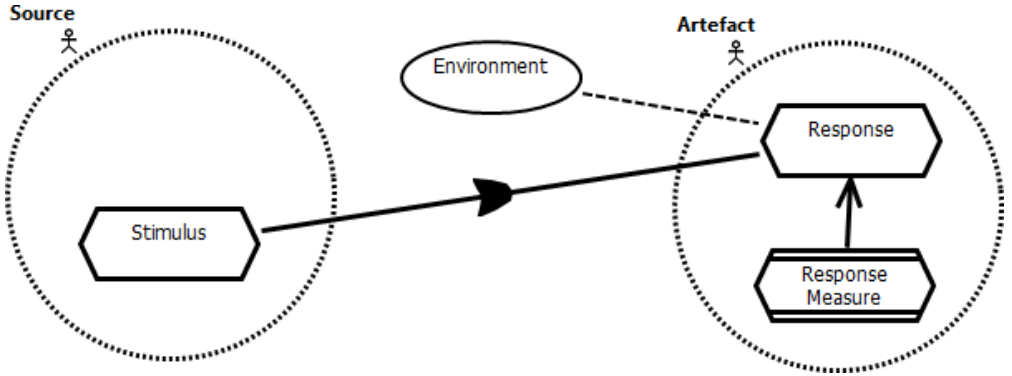
UNIVERSITY of York

Portion of Goal	Possible Value
Artefact	WBS
Context	NOT (Airframe is on ground AND aircraft is in landing/taxiing/RTO flight phase)
Stimulus	N/A
Response	All wheel brakes are applied

By graph

Carnegie Mellon University



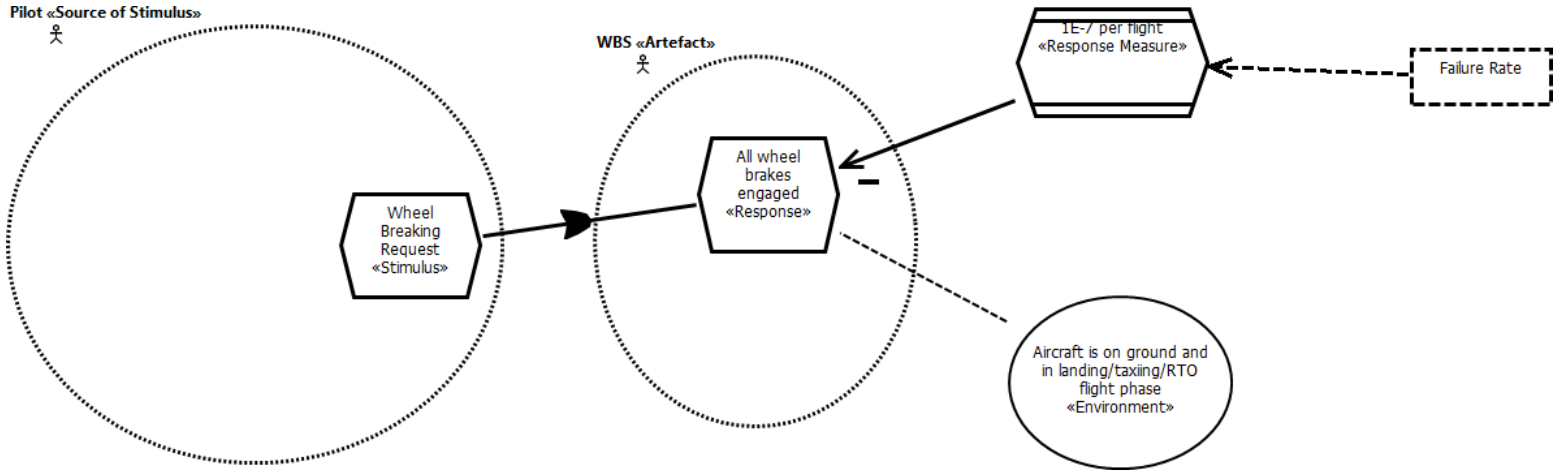


Anticipatory Failure Determination Approach (AFDA)

The QAS model appears to be an analogue of the notions within AFDA of SEOR: Source, Effect, Object and Result. AFDA has roots in research and application back to 1960s.

INTERPRETATION OF QAS ... IN GRL

aetiology
noun
(philosophy) (of an explanation) in terms of causal precedents, as opposed, for instance, to the intentions of an agent



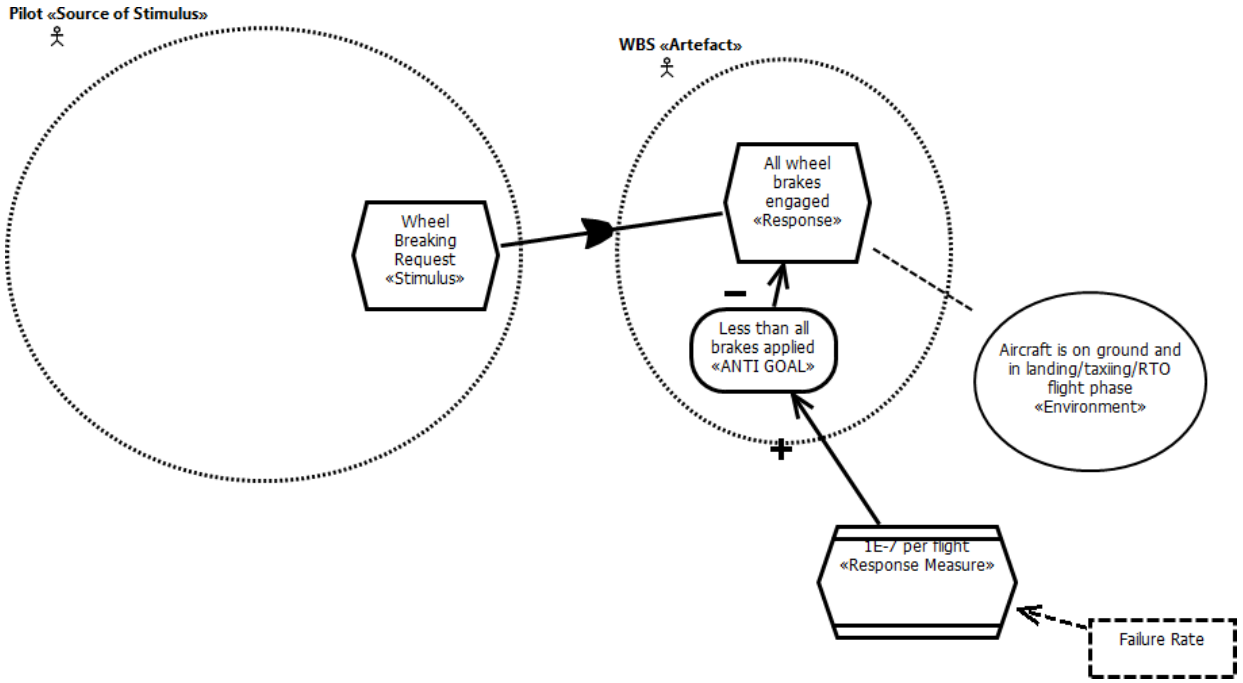
"The <artefact> shall <respond> upon <stimulus> when <context>"

How do I do THAT in GSN?

- Native use of GRL's KPI notation
- Fault is negative contribution to the intended function
- We apply a validated closure mechanism for reasoning over open sentences using a graphical calculus.

APPLYING HABLI ET AL NOTION OF ANTI-GOAL

UNIVERSITY of York



"The <artefact> shall <respond> upon <stimulus> when <context>"

Did we not reject rebuttal semantics in GSN when ignoring Toulmin?

Is the world of goals really black and white?

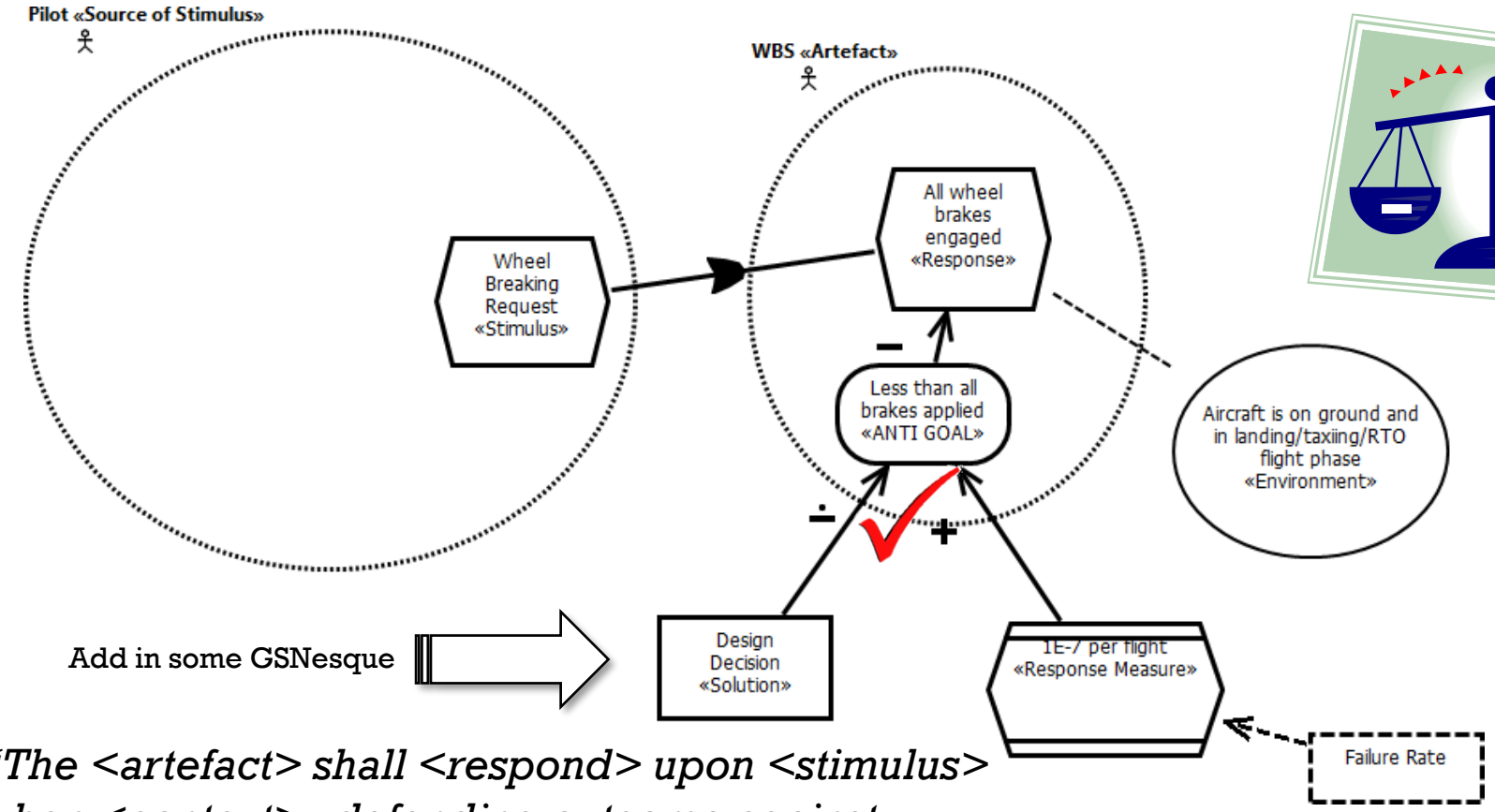
Are ANTI-GOALS a stab at defeasibility or at rebuttal?

ANTI-GOALS are simply an opposing GOAL

A failure rate is a positive contribution to the ANTI-GOAL

GO FURTHER, PROVIDE ANTI-ANTI-GOAL

Yes, your rebuttal does look big in that argument!



Add in some GSNesque

"The <artefact> shall <respond> upon <stimulus> when <context>, defending outcome against <ANTI GOAL> by using < Design Decision>"

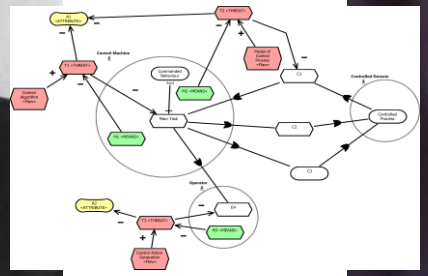
Design Decision counteracts Failure and Avoids ANTI GOAL

Think of this as a petite Argumentlette

IF ANT-GOALS, WHY NOT AGENTS VS ANTI-AGENTS?

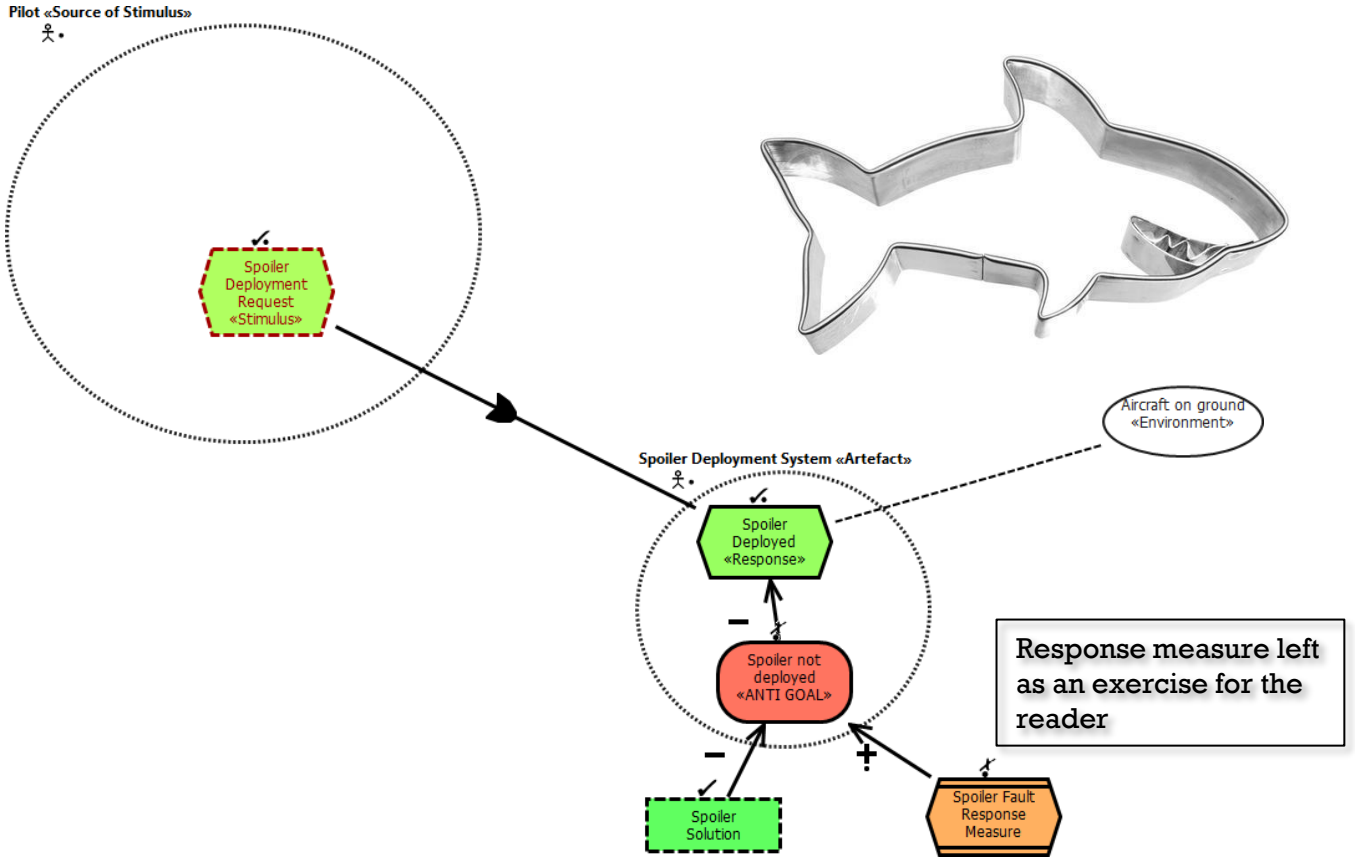
So it was an obtuse reference to a slang term that is used in the American popular culture as a transitive verb to mean throw out or get rid of?

So like QAS, STPA is just a heuristic?



Would you believe, i style notations are also used in security modelling*

VISITING THE ANTI-GOAL OF SPOILER DEPLOYMENT



"The <artefact> shall <respond> upon <stimulus> when <context>"

So the cookie cutting metaphor implicates that strategy is a concept and not just a lexical bubble in a notation?

Ditto, just cookie cut it!

Claim belief in the levels of satisfaction.

The tool allows multiple sceptical scenarios to be captured.

INCORPORATING ALL THE OAS REASONING

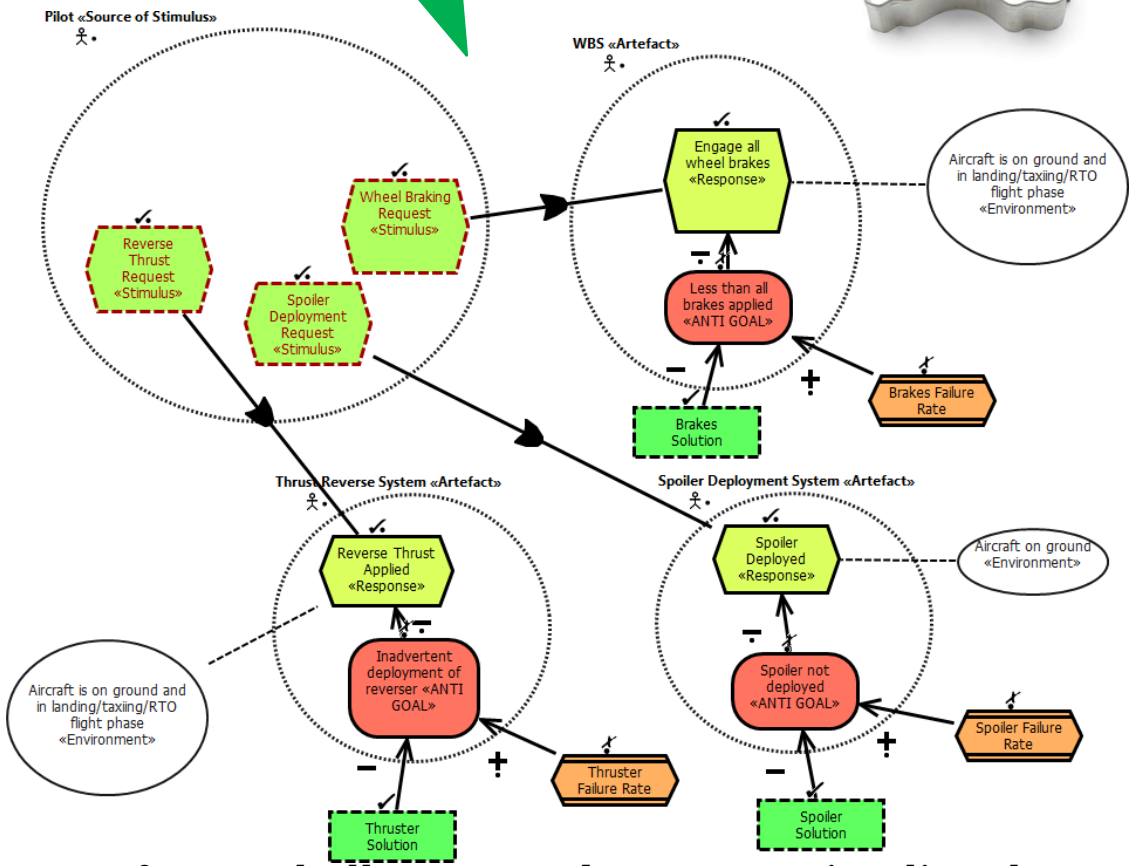
Concept

Lexical Element

Context

You think that is a context?

This is a context!



"The <artefacts> shall <respond> upon <stimuli> when <contexts>"

But weren't we told quite emphatically that "concepts" meant lexical bubbles in a notation?

Does that mean context, as a concept, is like a jar of cookies?

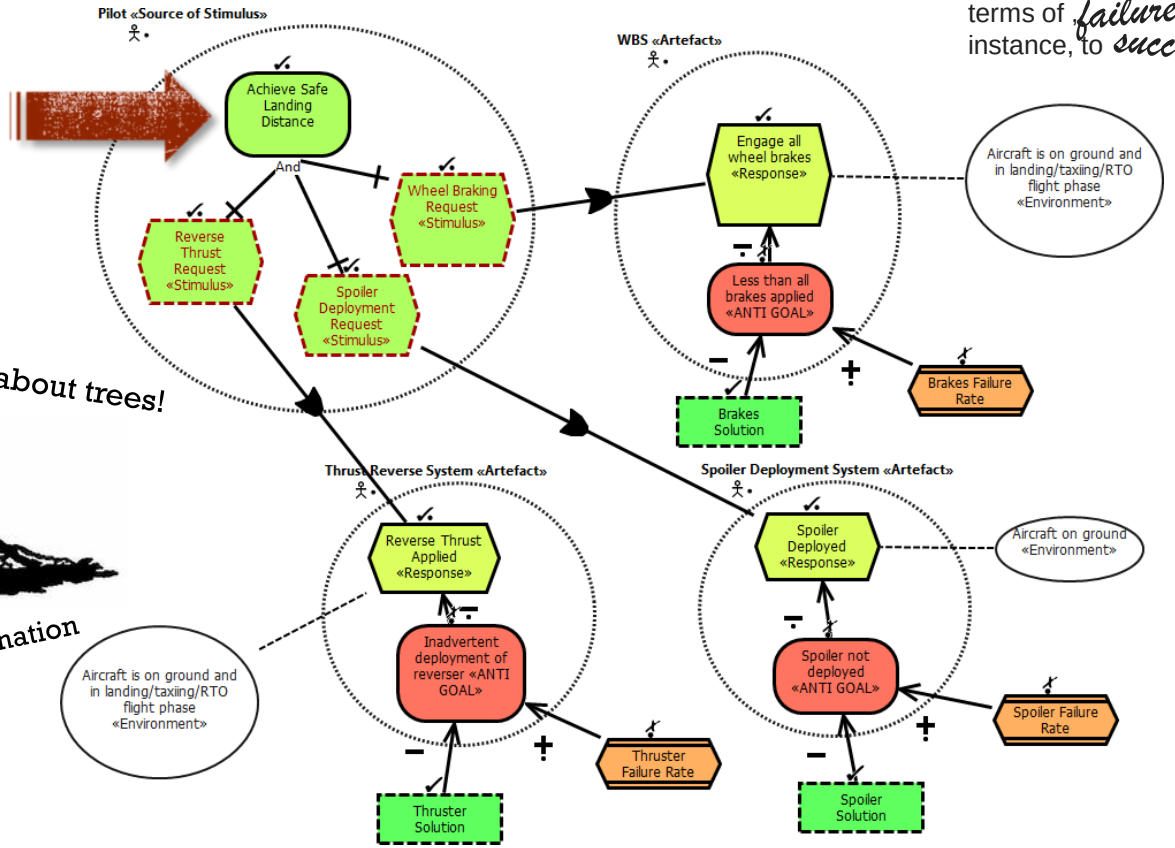
Voila!

Kelly argues for graphical argument …

… why stop at contextual narrative?

FACILITATING THE AGENT ORIENTED ARGUMENT

aetiology
noun
(philosophy) (of an explanation) in terms of *failures* as opposed, for instance, to *successes*



There's something about trees!

Justification or Explanation over a tree

"The <artefacts> shall <respond> upon <stimuli> when <contexts> to attain safe landing distance"

Hollnagel says: "... failures and successes are equivalent in the sense that they have the same origin".

Is that the somewhat like mixing Intention and Causation?

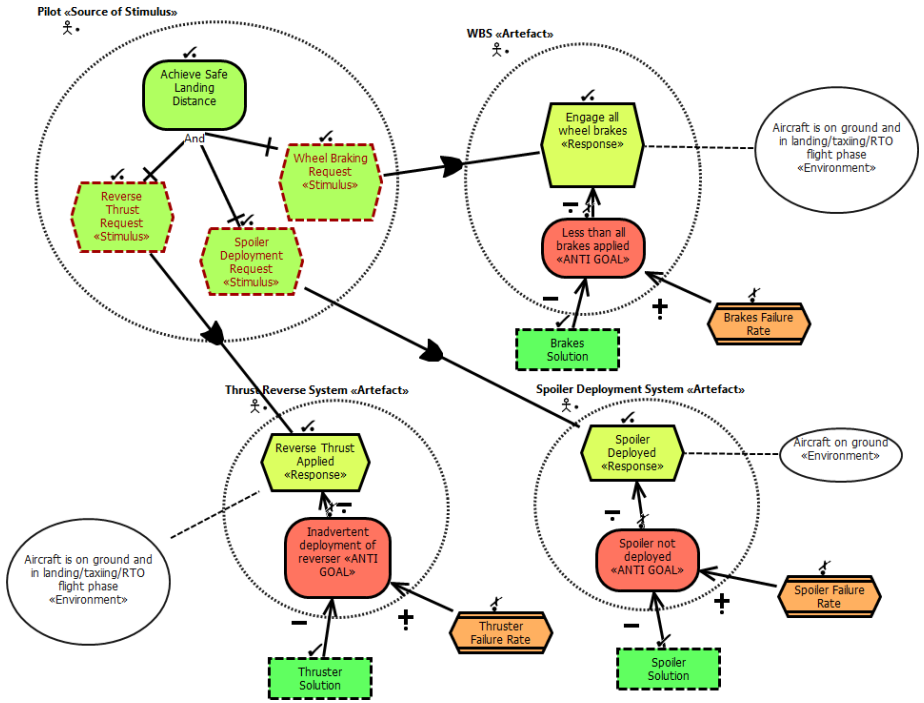
Argument of a Aetiological nature.

GSN approach is not economical in comparison

COMPREHENSIBILITY

Don't I also need 14 more GSN trees, one behind each of my assurance claim points, on each of the solved-by edges, to show defeasible satisfaction? Or was that confidence? How else do we emulate a bag of assertions?

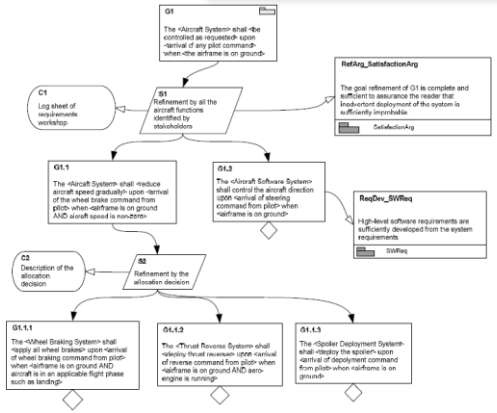
By Agent Formalism

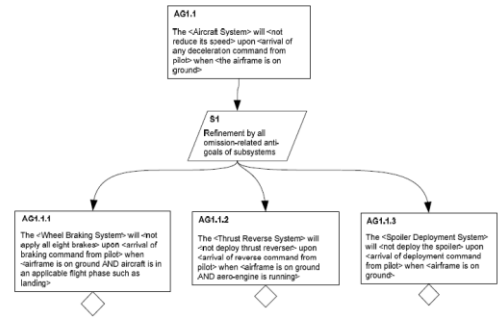


Argue with both Intention and Causation combined

By Goal Formalism

Reason by QAS twice per goal,
then argue in GSN once by goal,
then argue a second time in GSN by anti-goal





Source	some entity that generates a stimulus
Stimulus	a condition or event that needs to be considered
Artifact	the thing that is stimulated
Environment	conditions under which the stimulus occurs
Response	what the artifact should do on arrival of the stimulus
Measure	how to measure the response to determine it is satisfactory

Goal QAS

Source	some entity that generates a stimulus
Stimulus	a condition or event that needs to be considered
Artifact	the thing that is stimulated
Environment	conditions under which the stimulus occurs
Response	what the artifact should do on arrival of the stimulus
Measure	how to measure the response to determine it is satisfactory

Anti-goal QAS

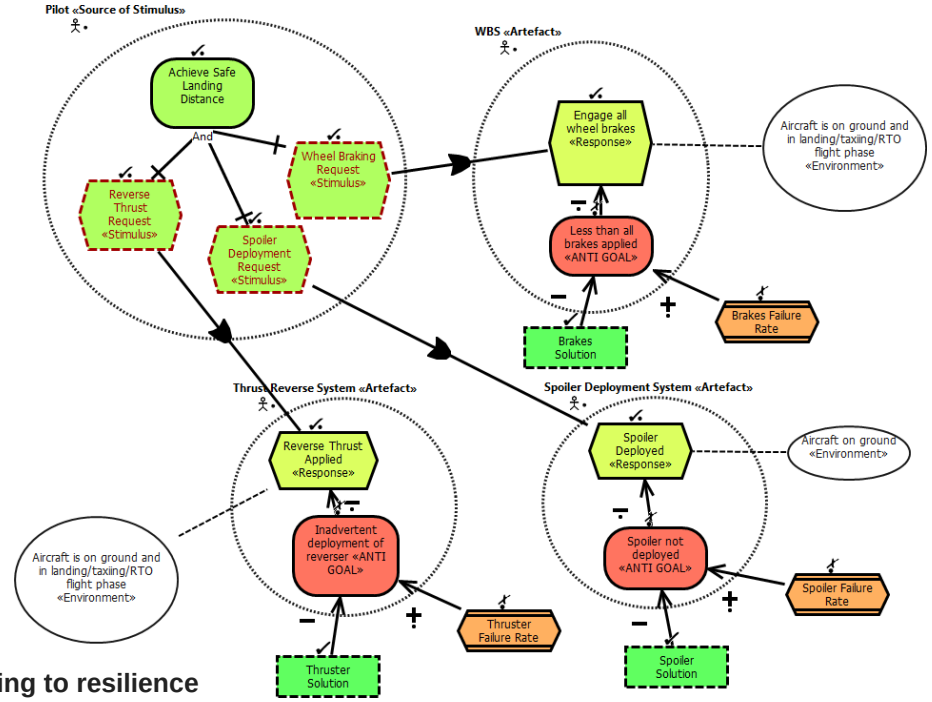
SAFETY DOMAIN CAPTURE (SUCH AS SYSTEM MODELS)

Neither GSN nor

20th ANNIVERSARY

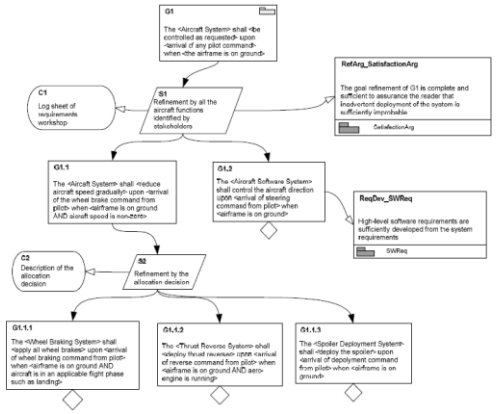
Toulmin "notation", having been designed to be completely general, does not explicitly capture concepts that relate to the safety domain (such as system models).

By Agent Formalism

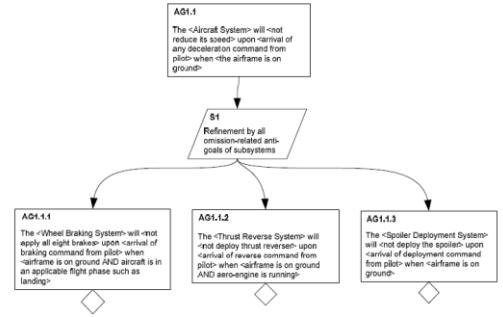


aetiologics leading to resilience
noun
(philosophy) (of an explanation) in terms of causal precedents, ***leading to variation from*** the intentions of an agent

By Goal Formalism



Source	some entity that generates a stimulus
Stimulus	a condition or event that needs to be considered
Artifact	the thing that is stimulated
Environment	conditions under which the stimulus occurs
Response	what the artifact should do on arrival of the stimulus
Measure	how to measure the response to determine it is satisfactory

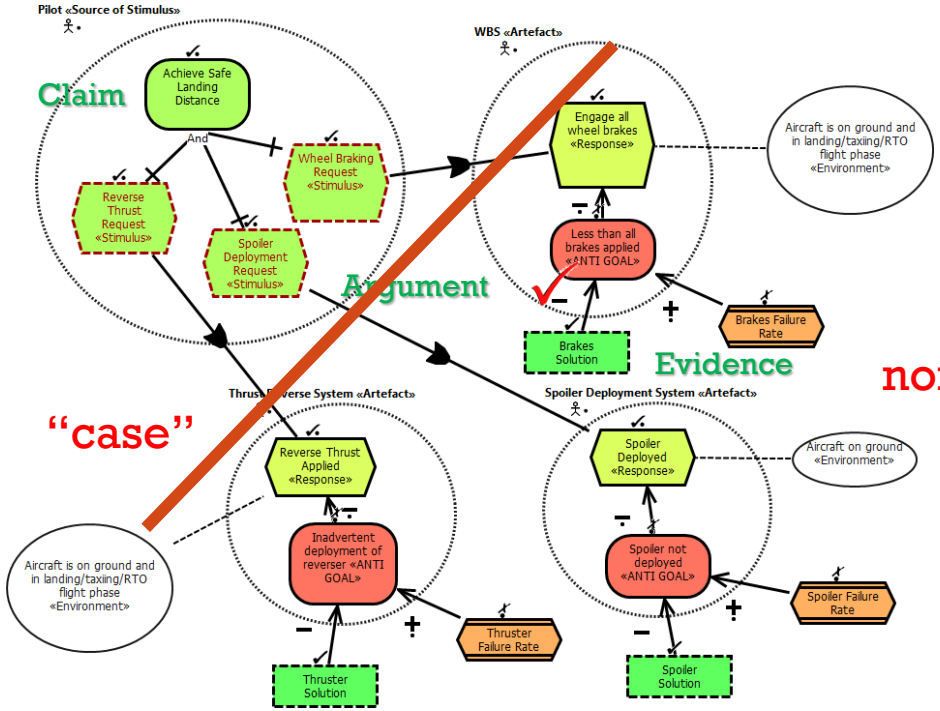


Source	some entity that generates a stimulus
Stimulus	a condition or event that needs to be considered
Artifact	the thing that is stimulated
Environment	conditions under which the stimulus occurs
Response	what the artifact should do on arrival of the stimulus
Measure	how to measure the response to determine it is satisfactory

$AgentFormalisms \supseteq GoalFormalisms$

Oh, you have hitched onto Fitch?

Paraphrasing Zave and Jackson: *Agent formalisms have all the recommended expressive capabilities for modelling of control information to attain soundness in Requirements Engineering.*



$$\frac{QAS \vdash (S, K \vdash R)\quad S_{WBS}, K_{WBS} \vdash R_{WBS}\quad S_S, K_S \vdash R_S\quad S_T, K_T \vdash R_T}{R_{WBS}, R_S, R_T \vdash Safe_{Landing}}$$

non-monotonic "rationale"

Therefore, Goal formalisms alone DO NOT have all the recommended expressive capabilities for modelling of control information to attain soundness in Requirements Engineering

Which one of the argument patterns does this resemble?

GSN proponents call on Zave and Jackson

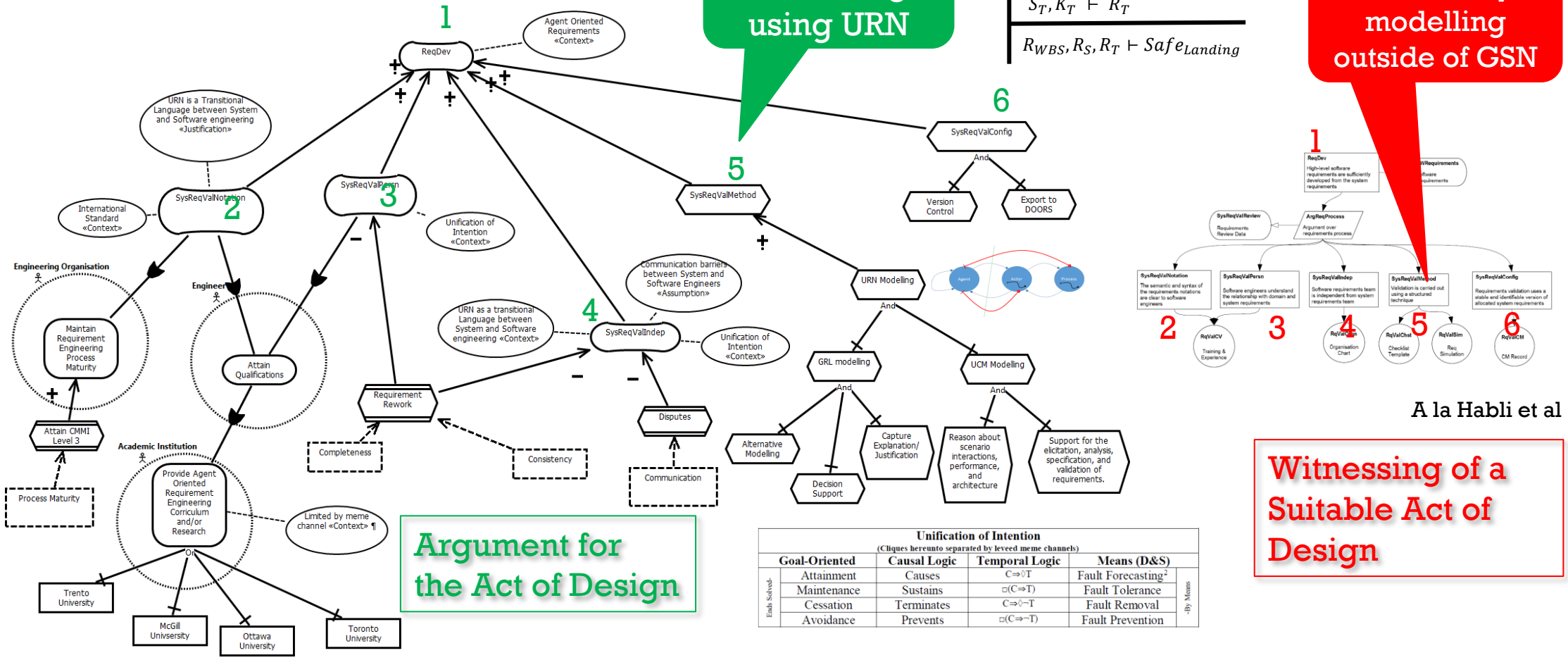
Splits "case" and rationale in same vein Rushby intimates.

SOFTWARE REQUIREMENTS VALIDATION ARGUMENT

Validate by modelling using URN

$$QAS \vdash (S, K \vdash R)$$
$$S_{WBS}, K_{WBS} \vdash R_{WBS}$$
$$S_S, K_S \vdash R_S$$
$$S_T, K_T \vdash R_T$$
$$\overline{R_{WBS}, R_S, R_T \vdash Safe_{Landing}}$$

Validate by modelling outside of GSN



A la Habli et al

Argument for the Act of Design

Unification of Intention
(Cliques hereunto separated by leveed meme channels)

Ends Solved-	Goal-Oriented	Causal Logic	Temporal Logic	Means (D&S)	-By Means
	Attainment	Causes	$C \Rightarrow \Diamond T$	Fault Forecasting[2]	
	Maintenance	Sustains	$\Box(C \Rightarrow T)$	Fault Tolerance	
	Cessation	Terminates	$C \Rightarrow \Diamond \neg T$	Fault Removal	
	Avoidance	Prevents	$\Box(C \Rightarrow \neg T)$	Fault Prevention	

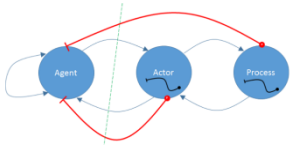
Witnessing of a Suitable Act of Design

CONCLUSION: SAFETY CASES CAN EQUAL INTENT SPECIFICATIONS (V.V.)

- In ITU-T Z.151 actors, goals, requirements, features, aspects and tactics provide a normative taxonomological basis to act as an Architecture Description Terrain. Justification for actors, goals, requirements, features, aspects and tactics can thus provide a normative Assurance Argument Terrain.
  - The range of epistemic standards addressed by semantics in ITU-T Z.151 can supply that embedded justification.
- IEEE 42010 Systems and Software Engineering Architecture Description includes goals describing the nature required of rationale supporting architectural descriptions.
  - ITU-T Z.150 can act as the requirements for a notation that satisfies those IEEE 42010 goals.
  - ITU-T Z.151 acts then as a reference design for the language specification.
- That the semantics of argument as described by IEEE 15026 System and Software Assurance is a subset of ITU-T Z.151 means ITU-T Z.151 also acts as a bridging standard between IEEE 42010 and IEEE 15026.
  - This acts to amplify embedded architectural rationale into assurance claims where the rationale addresses system quality attributes and their trade-offs.
- The goal-oriented nature of ITU-T Z.150/151 also threads goal-oriented rationale into the architectural description to meet the intent of Intent Specifications, since both come from the same cognitive science basis.
  - This might therefore meld York and MIT thinking into a unified model of Agent Oriented Assurance Cases with nothing more than a meme shift.

How do I do THAT in GSN?

REFINING EPISTEMICS INTO LOGICS



May be sufficient in medium levels of assurance (Do178C Level C Mission Critical) where semi-formal notations such as UML/SysML already sit as acceptable.

$$\int_{Explain}^{Justify} Argue\,\langle Problems \mapsto Solutions(URN(s)), s \in [S, K \vdash \mathrm{R}; means(m), m \in \{tasks, aspects, features \subset tactics\}]\rangle$$

Unification of Intention

(Cliques hereunto separated by leveed meme channels)

Ends Solved-	Goal-Oriented	Causal Logic	Temporal Logic	Means (D&S)	-By Means
	Attainment	Causes	C⇒◊T	Fault Forecasting	
	Maintenance	Sustains	□(C⇒T)	Fault Tolerance	
	Cessation	Terminates	C⇒◊¬T	Fault Removal	
	Avoidance	Prevents	□(C⇒¬T)	Fault Prevention	
	Needs	Requirements	Specifications	Design Decisions	

To make Rushby proud as you can run SMT over GRL!

GRL — URN — UCM — Translate — Pick a formal notation — Tasks, Aspects, Features — URN

LOTUS!
Petri-Nets!
Z-Notation!
Event-B?
When something more than semi-formal is required

ASSC 2018

Australian System Safety Conference 2018

May 23 to 25, 2018
in Melbourne
Australia

Conference Theme

Strengthening and Integrating System Safety Engineering for Australia's future

ENQUIRIES?

https://www.researchgate.net/profile/Ray_Feodoroff

ASSC 2018

Australian System Safety Conference 2018

May 23 to 25, 2018
in Melbourne
Australia

Conference Theme

Strengthening and Integrating System Safety Engineering for Australia's future

BACKUP!

Be afraid, be very afraid …

ASSC 2018

Australian System Safety Conference 2018

May 23 to 25, 2018
in Melbourne
Australia

Conference Theme

Strengthening and Integrating System Safety Engineering for Australia's future

INTENTIONAL ENTERPRISE ARCHITECTURE

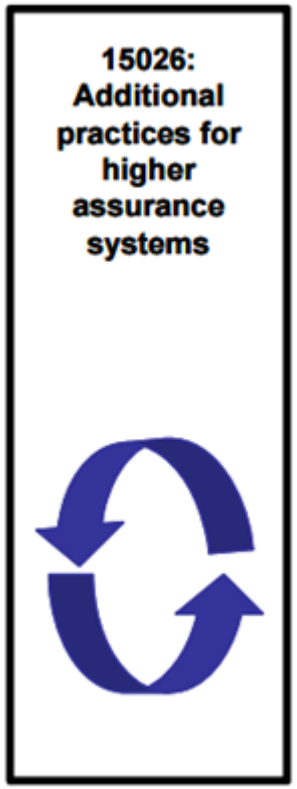
The model for attainment of CMMI Level 3 Agent Oriented Assurance

PERCEIVED PROBLEM CONTEXT

- Around 2009 CMU SEI proposed a structured means for review of architecture descriptions which asked the loaded question:
  - Is the rationale for key decisions captured?
- Around the same time Emery & Hilliard lament the lack of *'normative guidance for architecture rationale or decision capture'* within ISO/IEC/IEEE 42010
- The real question for Assurance is, of course:
  - Does the rationale explain why the decision is apt in terms of meeting assurance goals set for the design?
- The "other" question for Assurance is, of course:
  - Does the argument need to sit outside of the normal design artefacts?

CLAIM

- URN (ITU-T Z.150-Z.151) is a means **to fill recognise gaps in ISO/IEC/IEEE 42010** as the means for rationale and design decision capture over the Architectural Terrain.
- Due to the synergy between the semantics of URN and that of IEEE 15026, use of URN might be interpreted as either (or both):
  - Acting simply as '**additional practices for higher assurance**', or
  - Reduction of the span of 'additional practices (required) for higher assurance', **having already captured arguments** for the attainment of assurance goals by the design, within the design



ARGUMENT

Try substituting GSN into the argument

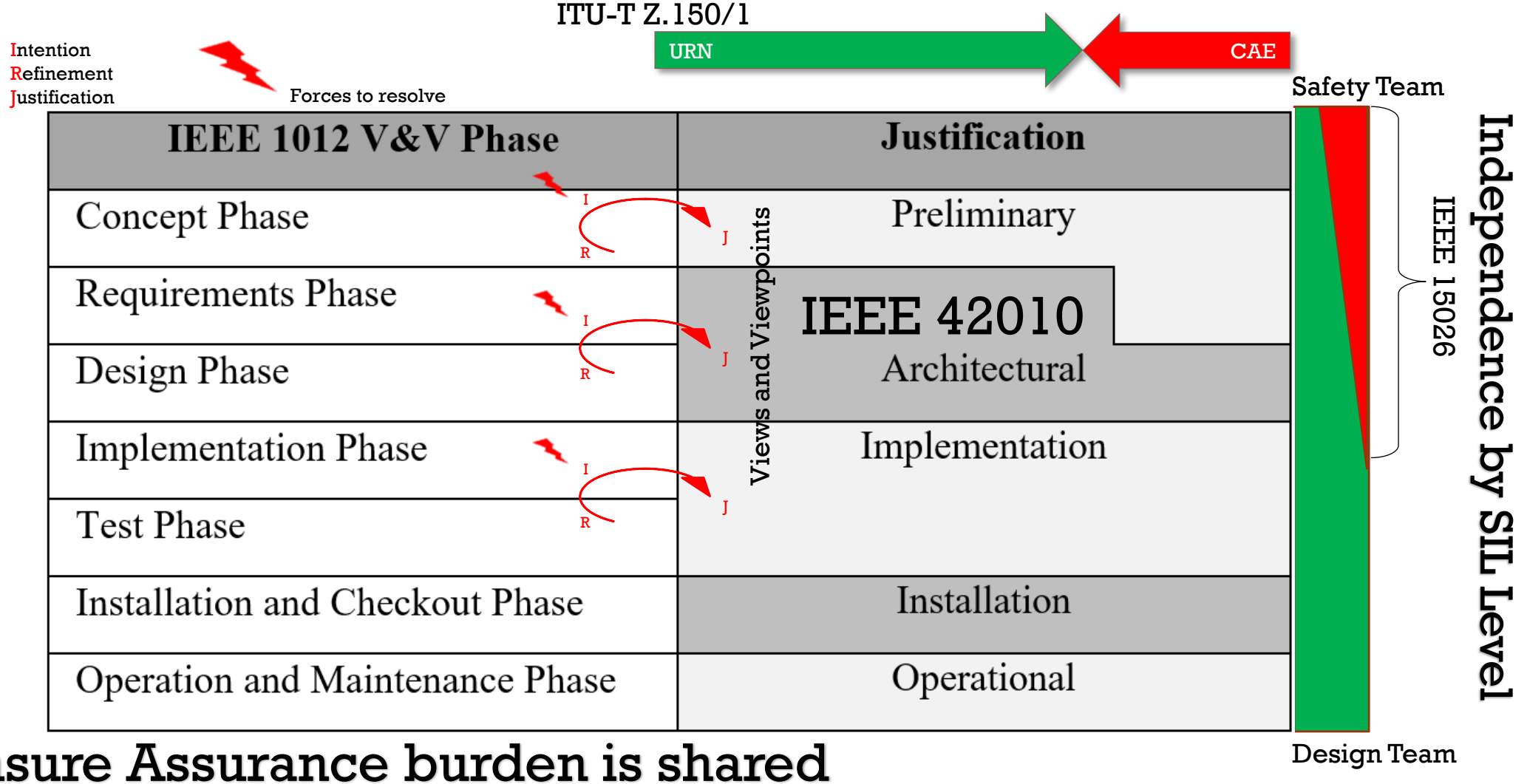
- Goals, requirements, features, aspects and tactics provide a normative taxonomological basis to act as an Architecture/Implementation Description Terrain.
- Justification for goals, requirements, features, aspects and tactics can thus provide a normative Argumentation Terrain.
- URN can capture rationale over first class modelling of goals, requirements, features, aspects and tactics to cover at least Preliminary and Architecture Justifications.
- As URN is a light weight notation, the rest is simply off the shelve process models and architecture representation schemes.

EVIDENCE

Intentional and Independent V&V

Intentional

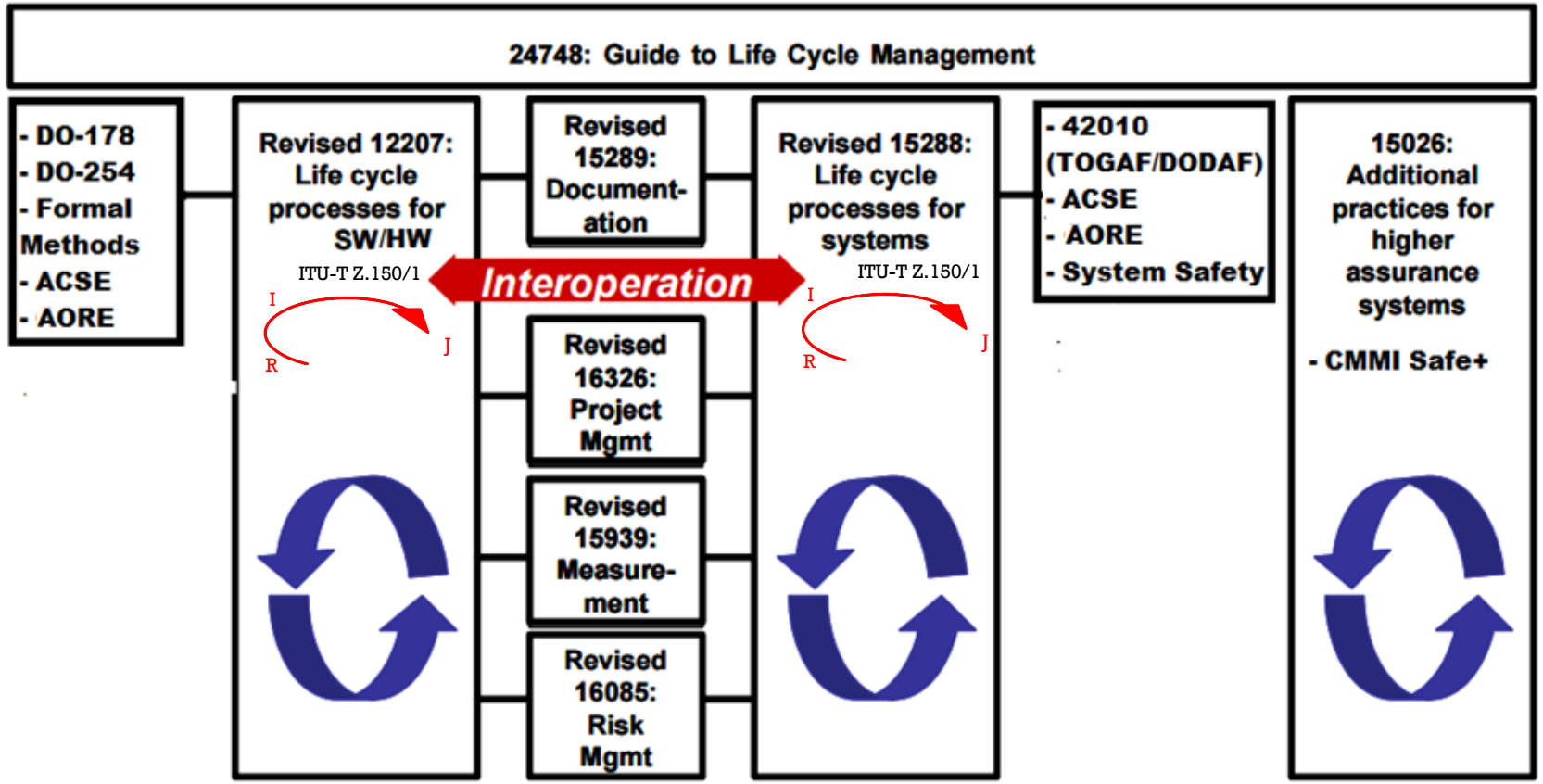
ITU-T Z.150/1



Ensure Assurance burden is shared

EVIDENCE

JUST A WAFER THIN LIGHT WEIGHT NOTATION TO CAPTURE THE RATIONALE FROM A ORCHESTRATED PROCESS

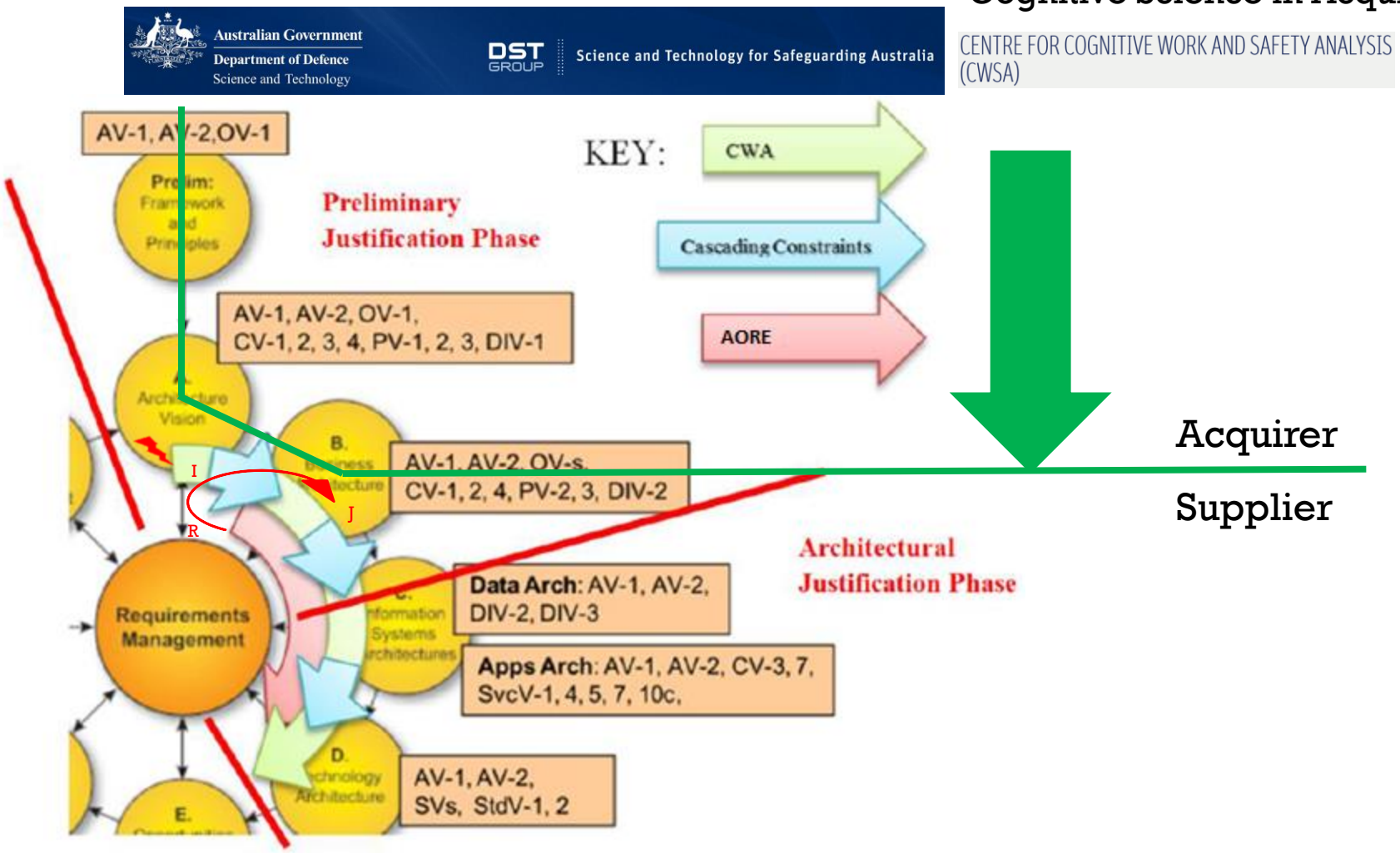


ACSE=Applied Cognitive System Engineering

AORE=Agent Oriented Requirements Engineering

CAPTURE THE RATIONALE IN VIEWPOINTS

Cognitive Science in Acquirer to Supplier transition



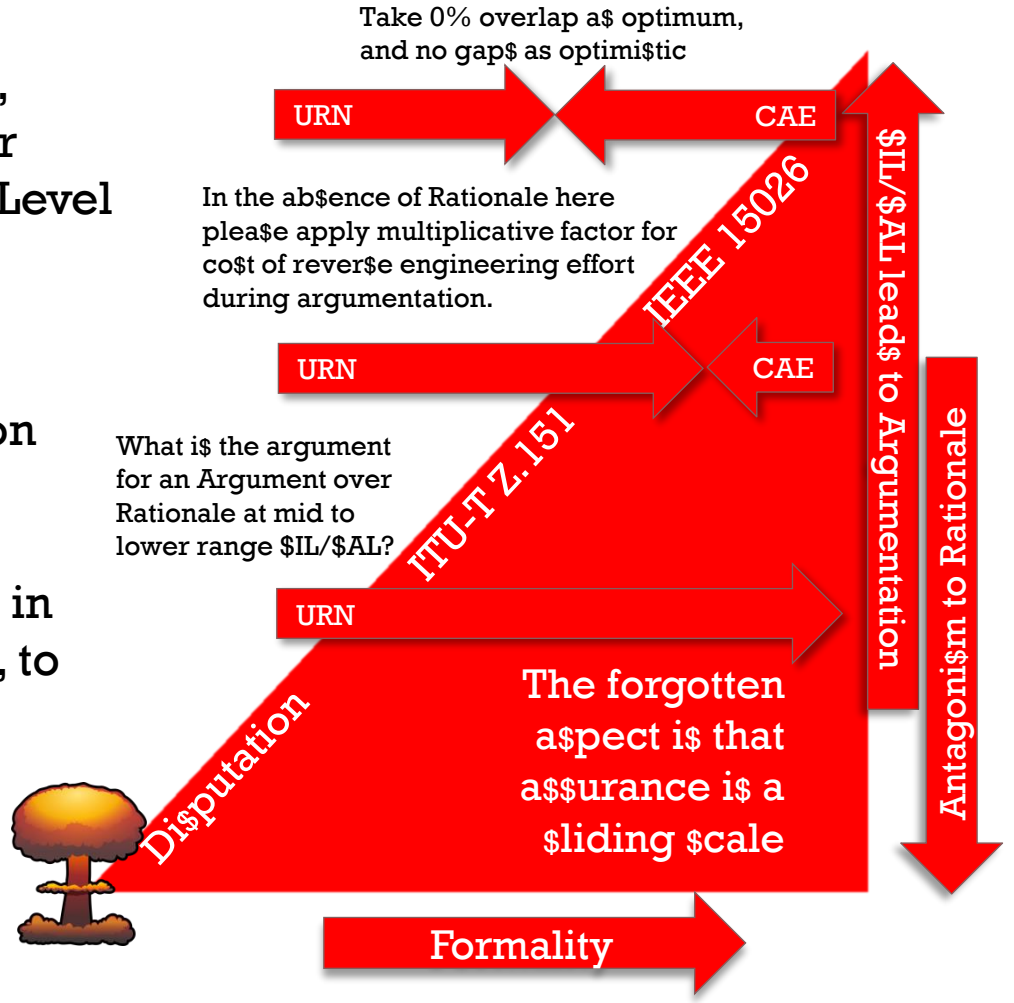
Assurance argument captured in Architectural Viewpoints.

EVIDENCE

Intention ver$u$ $IL/$AL

If one require$ two notation$, one for Rationale and one for Argument, then the $IL/$AL Level might be a mean$ for demarcation.

But what if Argument relie$ on the antagoni$m to Rationale, incurred during time poor project $chedule$, generally in low a$$urance environment$, to ju$tify the ($o-called) "difference"?



Take 100% re-arguing overlap a$ wor$t case

$tuttering of Argumentation

Take URN a$ repre$entative of rea$oning technique$

Argue twice-twice?

Argue once

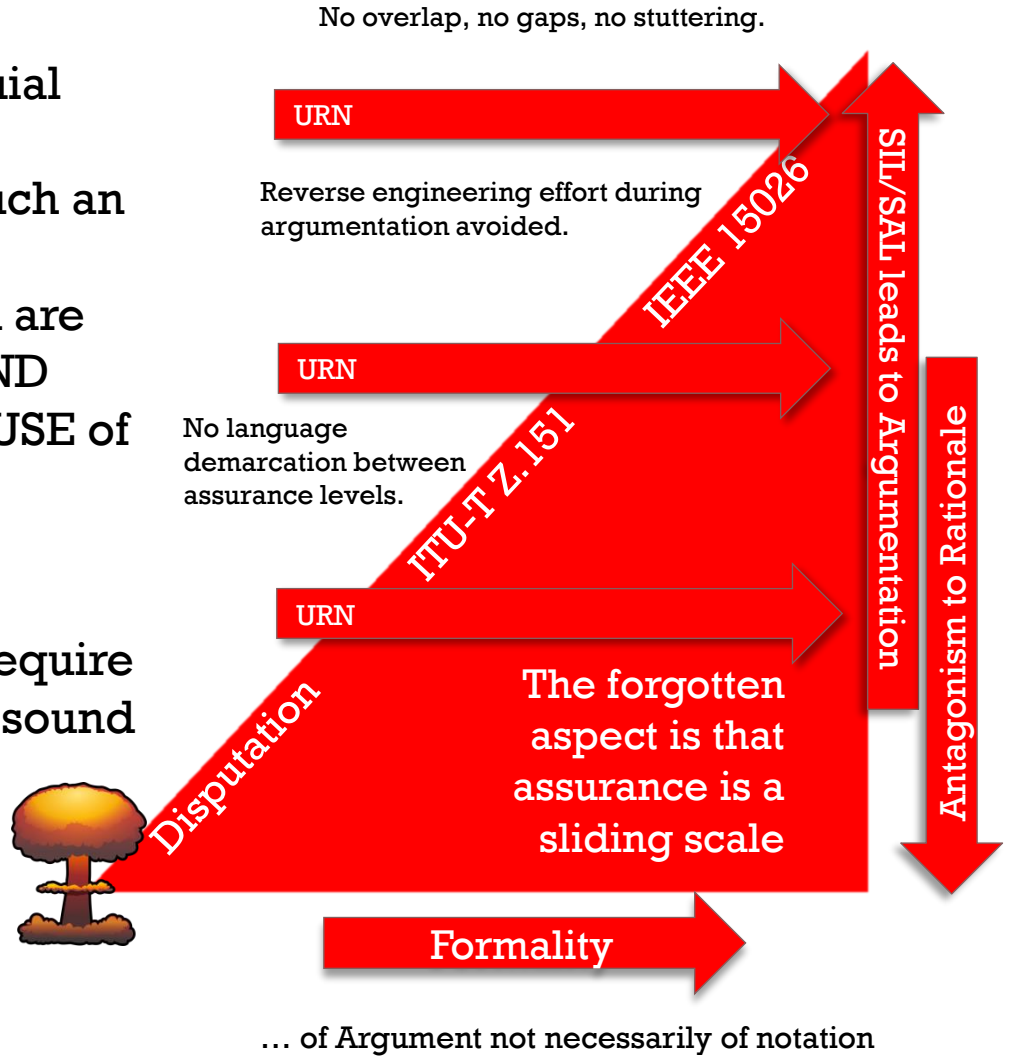
Argue nonce

EVIDENCE

Intention versus SIL/SAL

If solved-by is only a colloquial ends-means, AND Claims Argument Evidence is as much an Abstraction Hierarchy AND Justification and Explanation are the two uses of Argument AND Argument is required BECAUSE of the SIL/SAL level THEN two notations are not needed.

The notation will, however, require Agent Formalisms to ensure sound Requirement Engineering with supporting semantics for Justification/Explanation of the aptness of a design to meet assurance goals.

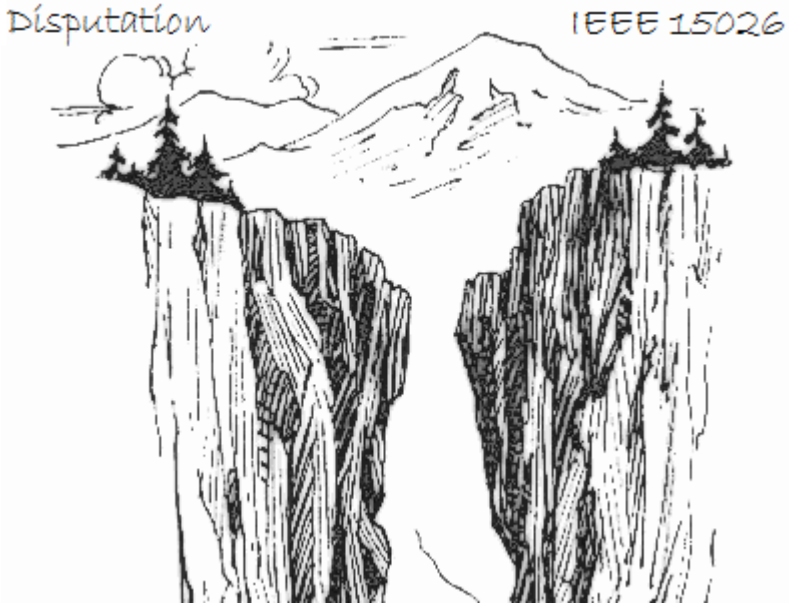


Argue once

Argue nonce

CONCERN ADDRESSED

- In the absence of any other reasoning layer, turning "on" Independent Assurance Argument, at the extreme right of the scale, may be counter-productive as it **creates a "language" chasm between Design and Safety teams.**



ASSC 2018

Australian System Safety Conference 2018

May 23 to 25, 2018
in Melbourne
Australia

Conference Theme

Strengthening and Integrating System Safety Engineering for Australia's future

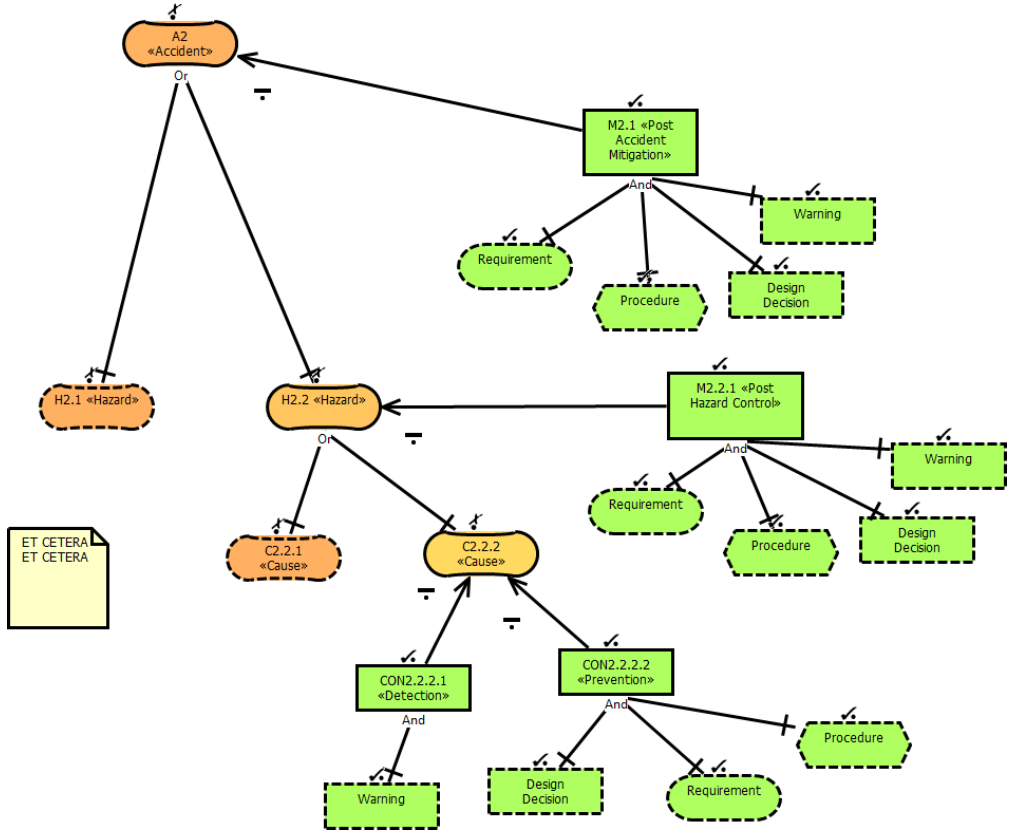
70

TREES VS TABLATURE

You can’t see the argument for the obfuscation by tablature.

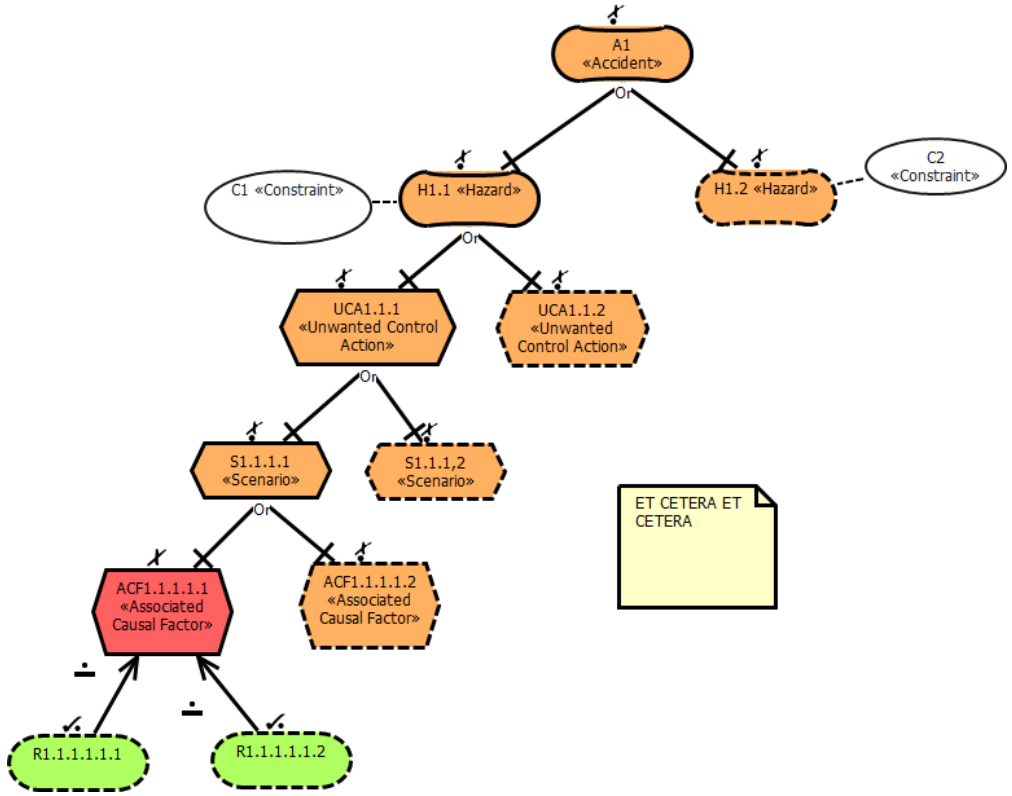
CASSANDRA TABLES AS AN ARGUMENT TREE

- The hidden in the database there is a model that can act as an structured argument.
- The model in tools like Cassandra also lends itself to representations in an argument tree.
- This is akin to the safety case pattern of all hazards are mitigated.



STPA TABLATURE AS AN ARGUMENT TREE

- The STPA Primer obfuscates an argument tree by use of multiple tables.
- Many STPA toolsets maintain this rage.
- This is akin to the safety case pattern of all hazards are mitigated.
- Safety Constraints from STPA are an equivocation of Safety Case Contracts.



ASSC 2018

Australian System Safety Conference 2018

May 23 to 25, 2018
in Melbourne
Australia

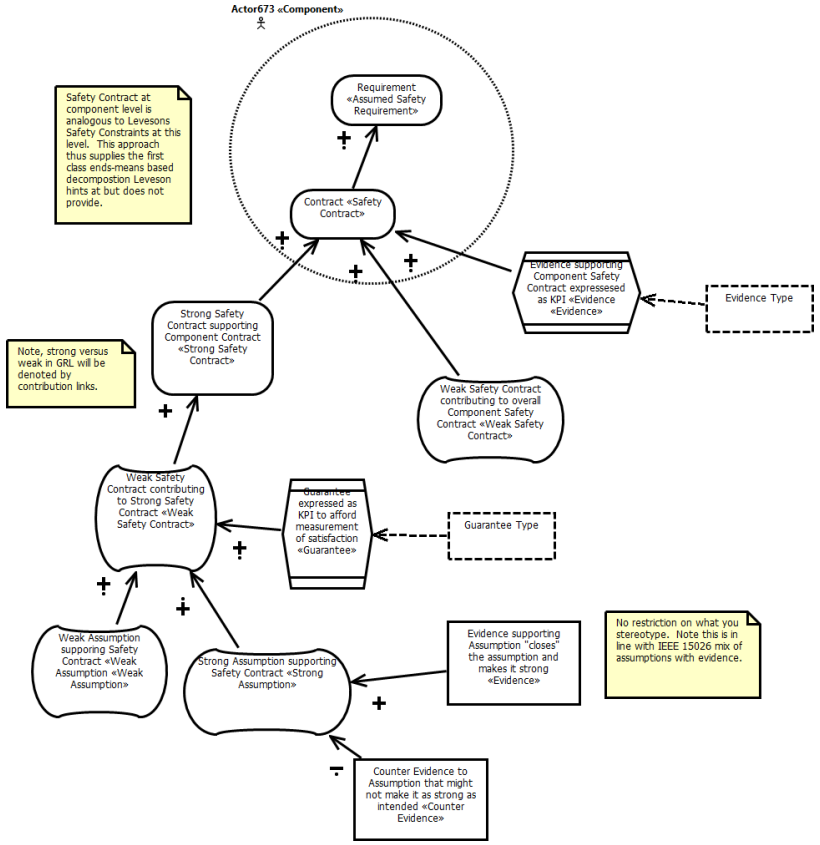
Conference Theme

Strengthening and Integrating System Safety Engineering for Australia's future

SAFETY CONTRACTS

Need they be so expensive?

USING AGENT FORMALISMS SAVES ON TRANSFORMATION COST



- According to Sljivo, Gallina, Carlson, and Hansson:
  - The cost for achieving certification is estimated at 25-75% of the development costs
  - Recommend semi-auto generation of safety case (a.k.a. GSN) fragments from Safety Contracts.
- Or you can do Safety Contract modelling in GRL as part of the requirements modelling.
- Feel free to add an aetiological aspect to act as counter-argument (or non-monotonic style thinking).
- Safety Case contracts are an equivocation of Safety Constraints from STPA.

ASSC 2018

Australian System Safety Conference 2018

May 23 to 25, 2018
in Melbourne
Australia

Conference Theme

Strengthening and Integrating System Safety Engineering for Australia's future

75

ANNOTATION OF DESIGN TO SUPPORT AUTO-GSN

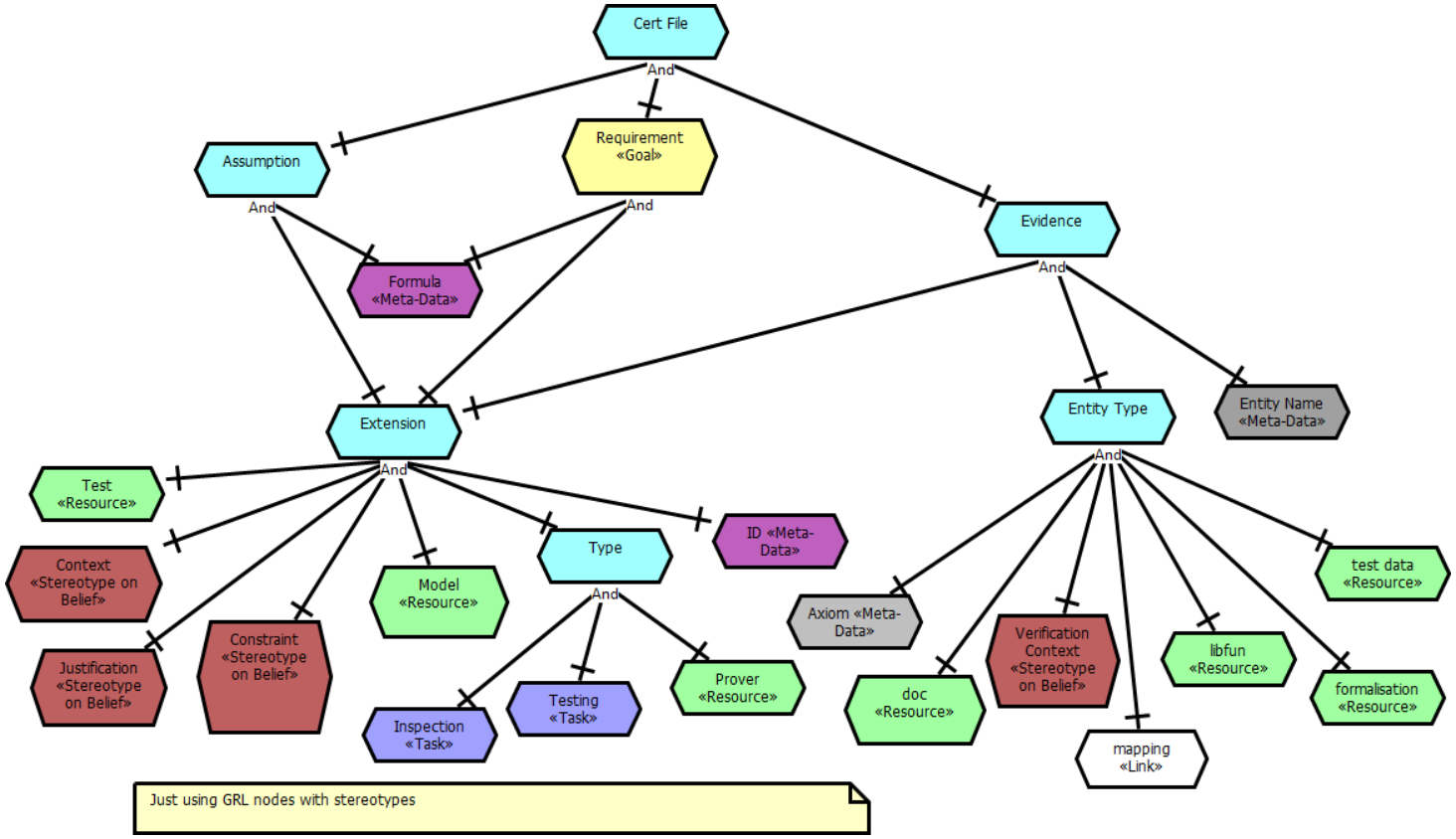
But what if we annotate GRL?

BACKGROUND KNOWLEDGE = $S, K \vdash R$?

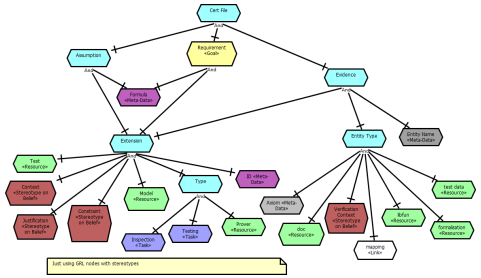
- Basir, Denney and Fischer keep aside meta-data for the purpose of forward engineering a GSN argument … later.
- They argue for additional information to represent background knowledge that cannot be produced directly by the formal verification phase.
- It thus needs to be specified in the form of contexts, assumptions, justifications, and constraints.

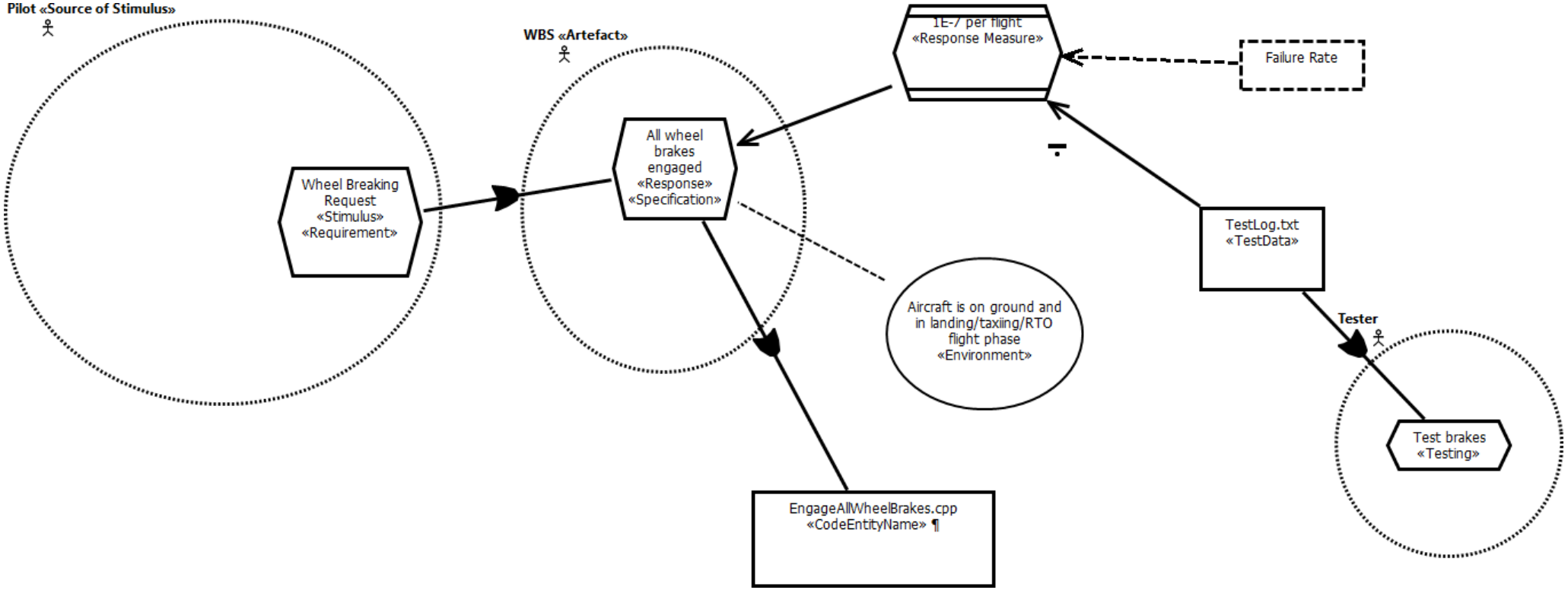
- CertFile ::= Assumption* Requirement* Evidence*
- Formula ::= Signal::Type | Signal :: bus(Type*) | Signal1=Signal2 | Formula => Formula | Formula /\ Formula
- Requirement ::= requirement(Formula, Extension*)
- Assumption ::= assumption(Formula, Extension*)
- Evidence ::= evidence(EntityType, EntityName, Extension*)
- Extension ::= text(Text) | context(Text) | justification(Text) | constraint(Text) | model(Text) | type(VerifType) | id(Id)
- EntityType ::= axiom | vc | libfun | testdata | doc | mapping | formalization | …
- VerifType ::= inspection | testing | prover(P) | …
- Mapping ::= mapping(ModelEntityName, CodeEntityName)

$S, K \vdash R =$ RATIONALE?



AGAIN WITH THE MEME MIXING!





ASSC 2018

Australian System Safety Conference 2018

May 23 to 25, 2018
in Melbourne
Australia

Conference Theme

Strengthening and Integrating System Safety Engineering for Australia's future

SLANDER OR IS IT LIBEL?

Hopefully its humour

86

- Otherwise a reference to a slang term that is used in the American popular culture as a transitive verb to mean throw out or get rid of.
- Or Maxwell Smart, Agent 86.

WHY IS A DUCK?

BECAUSE IT MAY BE EPISTEMICALLY LUCKY.

- This is a surrealist joke fashioned after a thought experiment that acts as a test for modal aspects of epistemic belief.

- The Argumentor is walking by a pond and sees a duck near the reeds on the other side. The duck swims into the reeds, so that the Argumentor no longer sees it. The Argumentor forms the justified true belief that there is a duck in the reeds. Unknown to the Argumentor however the duck that he saw was not in fact a duck. It was a decoy used by hunters to entice other birds to the area.
- Luckily for the Argumentor however there was a real duck in the reeds, so his belief is true. But his belief was only epistemically lucky.

WHAT'S THE DIFFERENCE BETWEEN A COGNITIVE ENGINEER AND A SAFETY PRACTITIONER?

System Engineers throw rocks at Safety Practitioners.

Everyone throws rocks at Cognitive Engineers.

HOW MANY SAFETY PRACTITIONERS DOES IT TAKE TO CHANGE A LIGHT BULB?

It depends upon the reasonableness of the exported constraints …

… and if and only if they can first agree on a definition of high voltage.