Human Orientedness of System Safety

1

Goals and their agents

Problem Statement

- There is an emerging argument for use of actions, modality and agency as the means to reason about safety assurance (Cassano et al.).
- Case Notations (such as GSN) are devoid of semantics to support action, modality and agency, whereas GORE notations include varying degrees of action, modality and agency.
- Case and GORE notations still struggle with semiotics, with insufficient rationale for the symbology used.

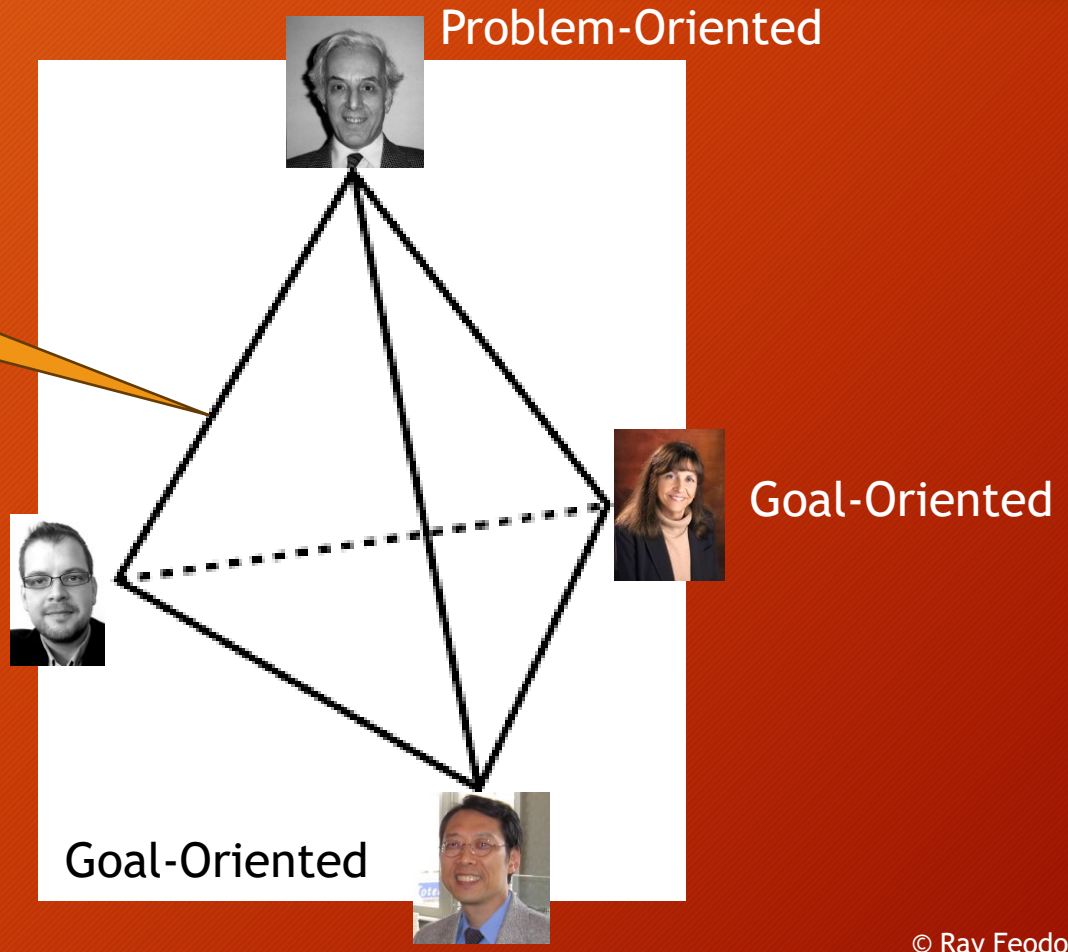
Modality (not meaning states and modes): Modal logic is a kind of logic used to represent statements about necessity and possibility. It plays a major role in philosophy and related fields as a tool for understanding concepts such as knowledge, obligation, and causation.

Problem Solution

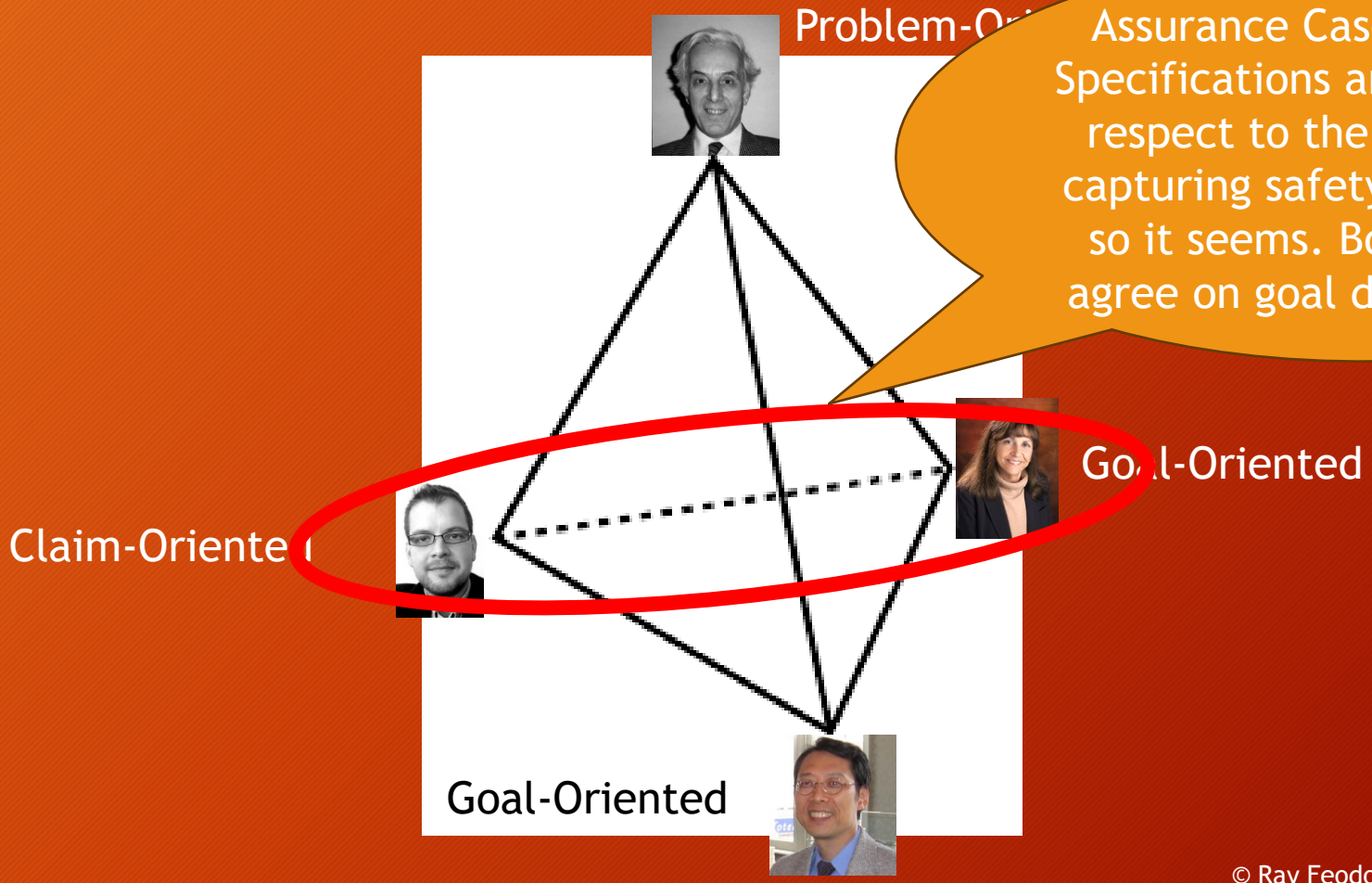
- Take observations from the last 20 years of the glancing of the case notation (and therefore safety “reasoning”) literature with that of the GORE literature and resolve that down to a GORE notation suitable for capturing design assurance reasoning.

Glancing academic areas

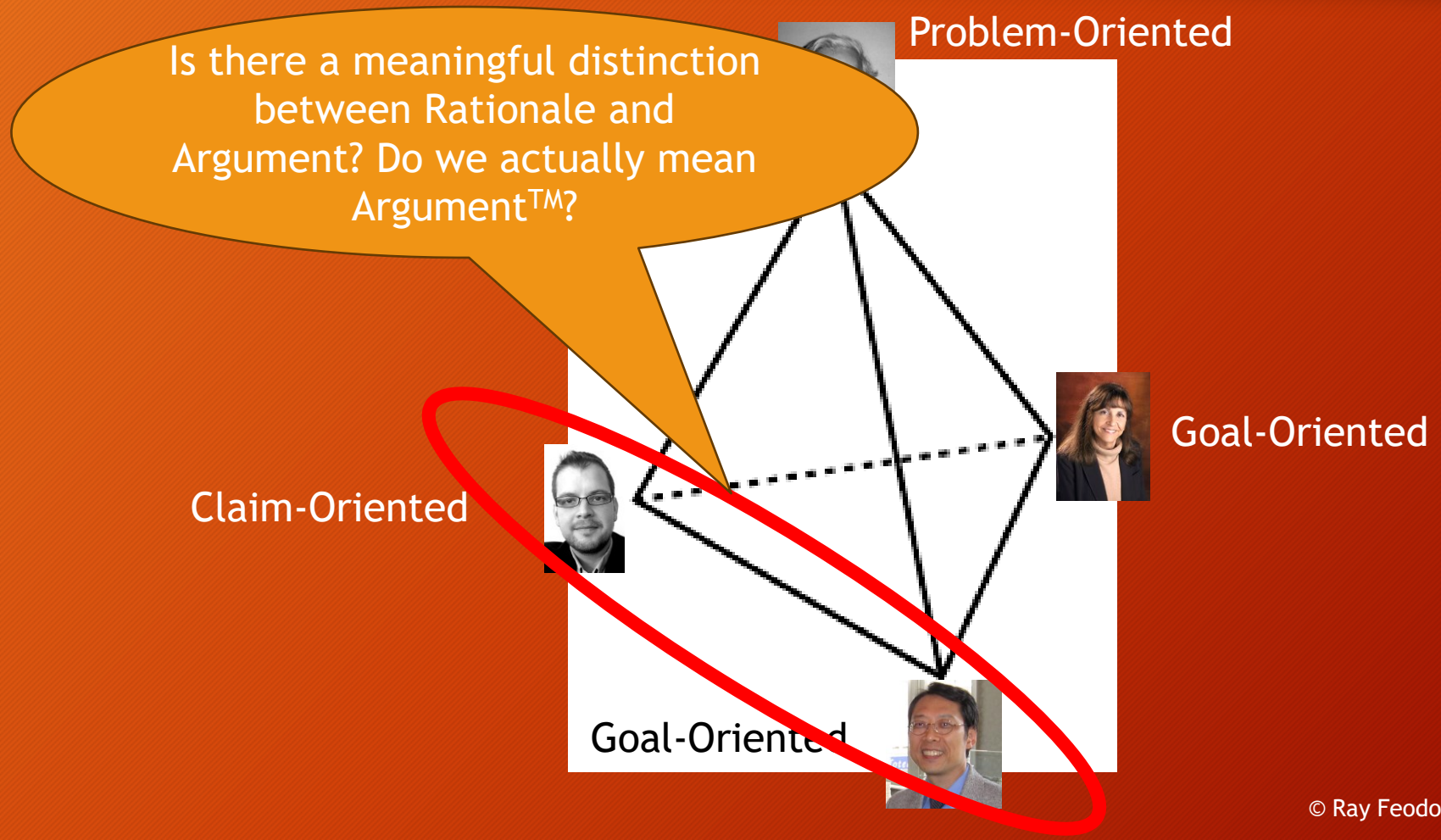
UML had the "3 Amigos", we'll do one better



Glancing academic areas

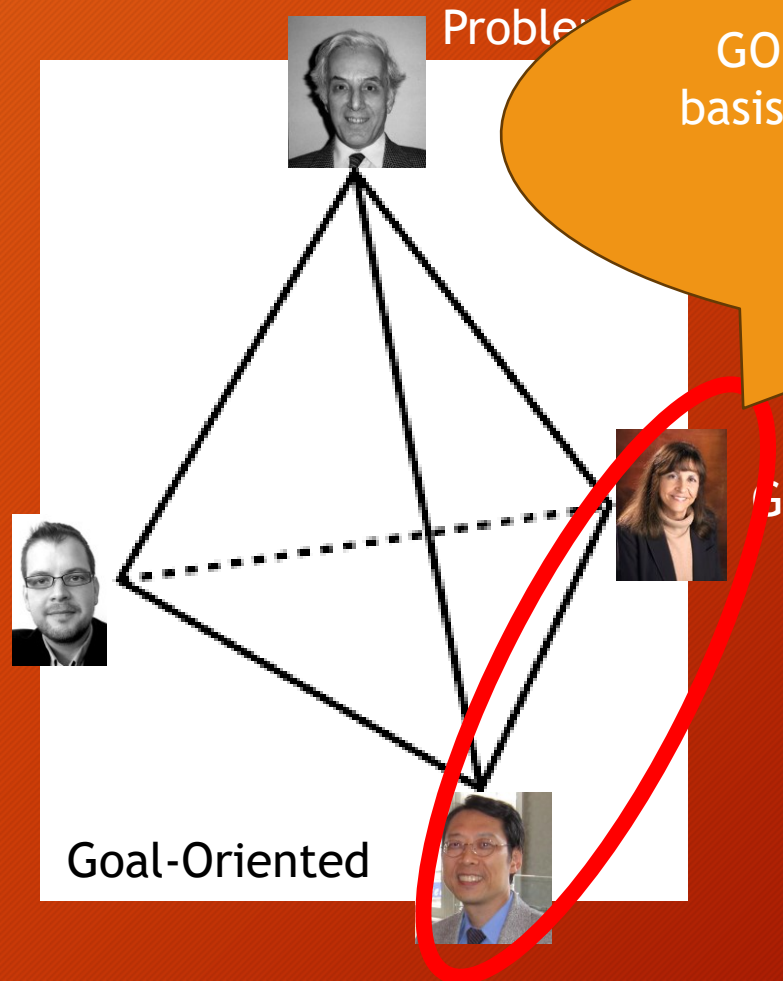


Glancing academic areas



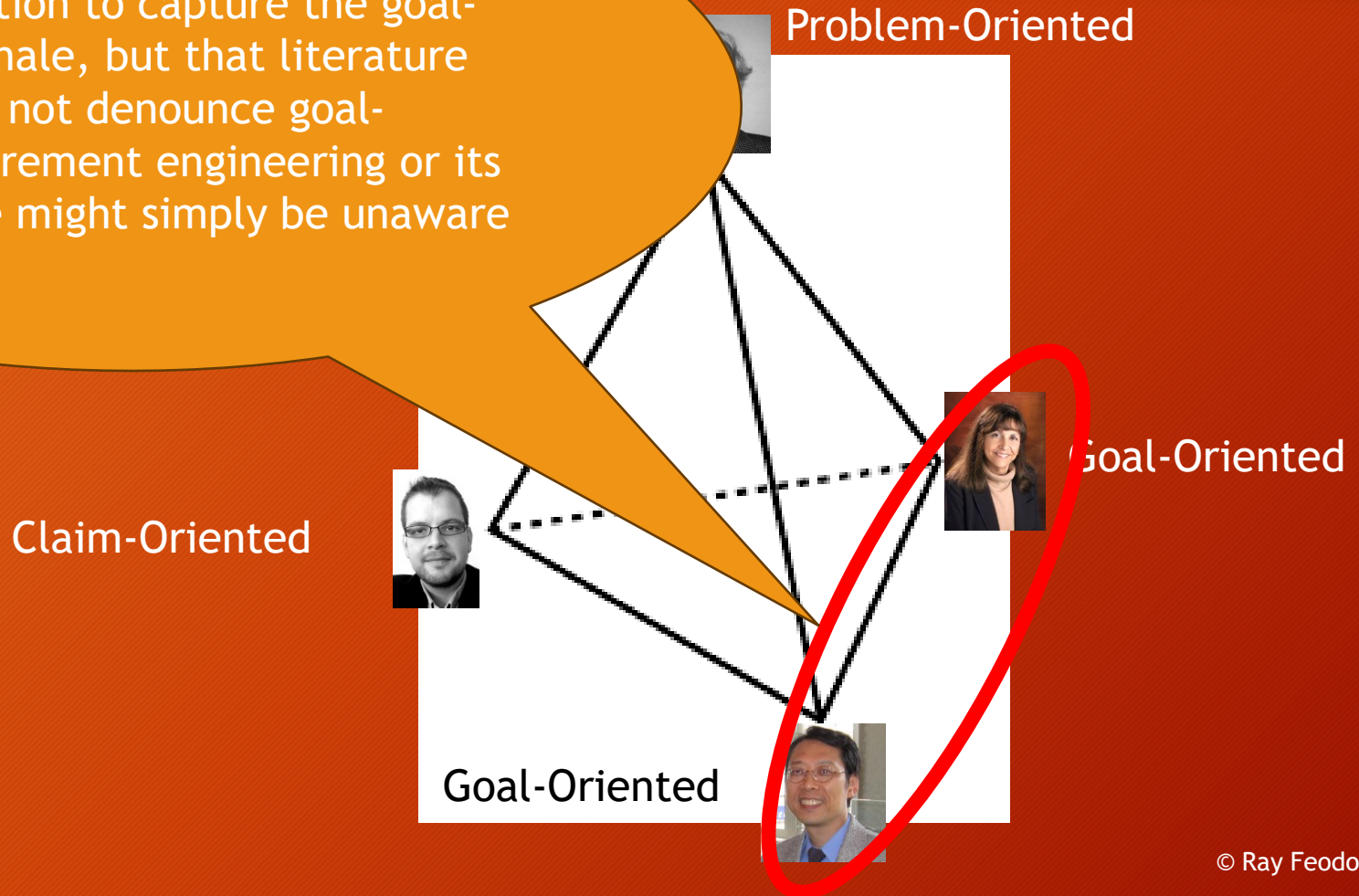
Glancing academic areas

GORE notations have, as their basis, the same cognitive science roots behind Intent Specifications.

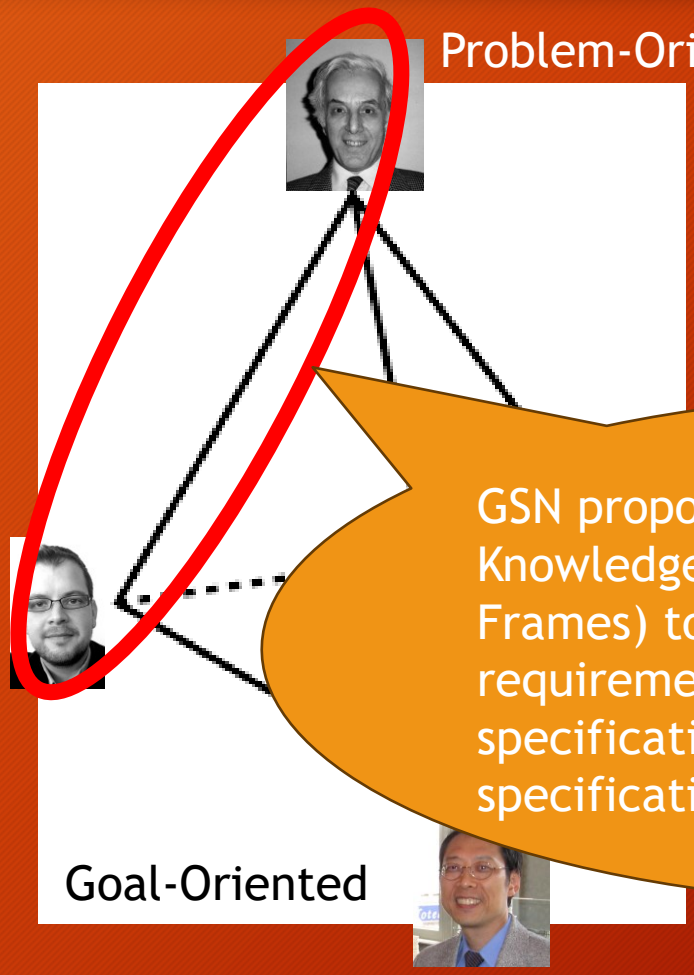


Glancing academic areas

Intent Specification literature does not specify a notation to capture the goal-oriented rationale, but that literature certainly does not denounce goal-oriented requirement engineering or its notations. We might simply be unaware of GORE?

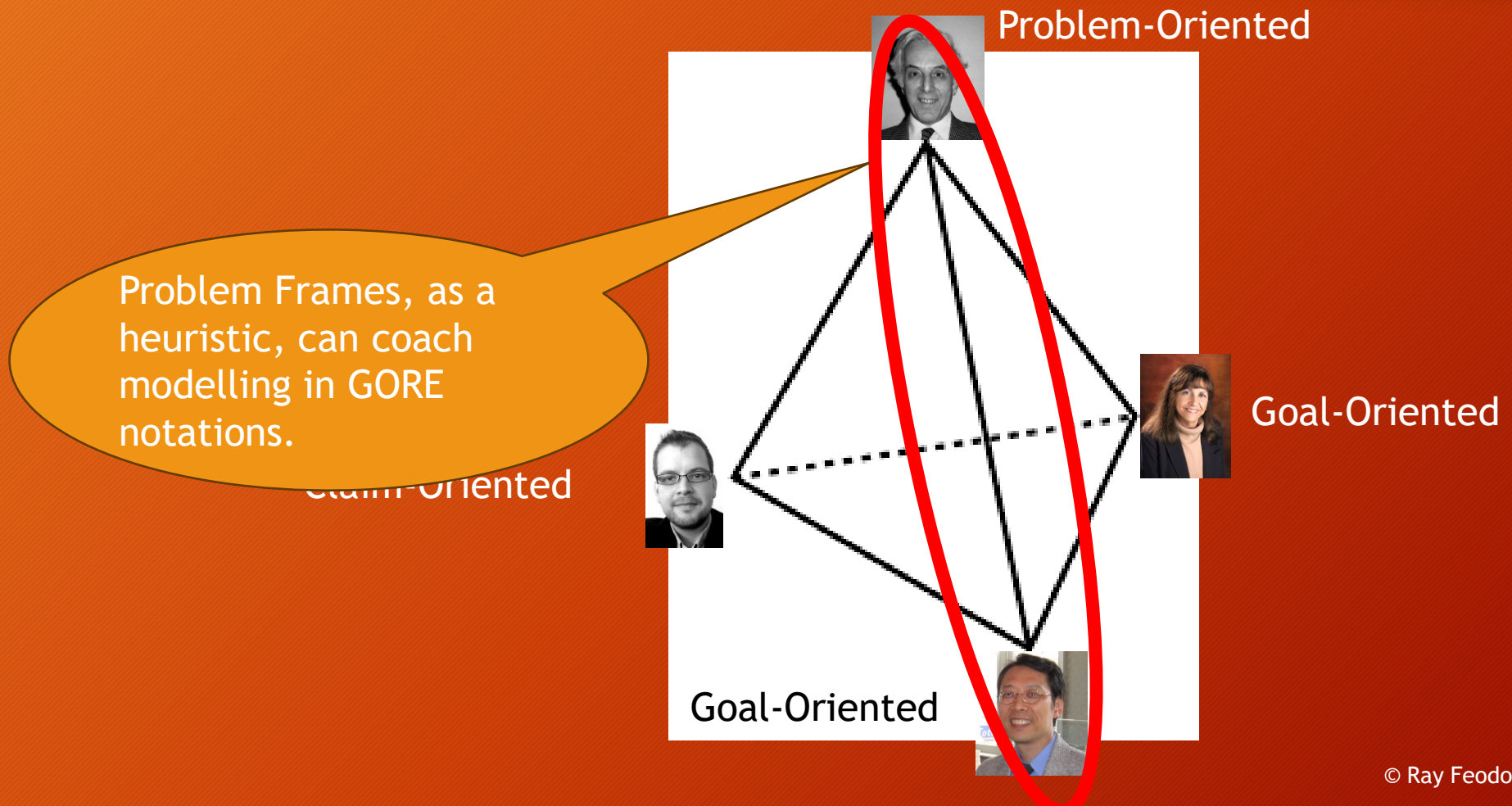


Glancing academic areas

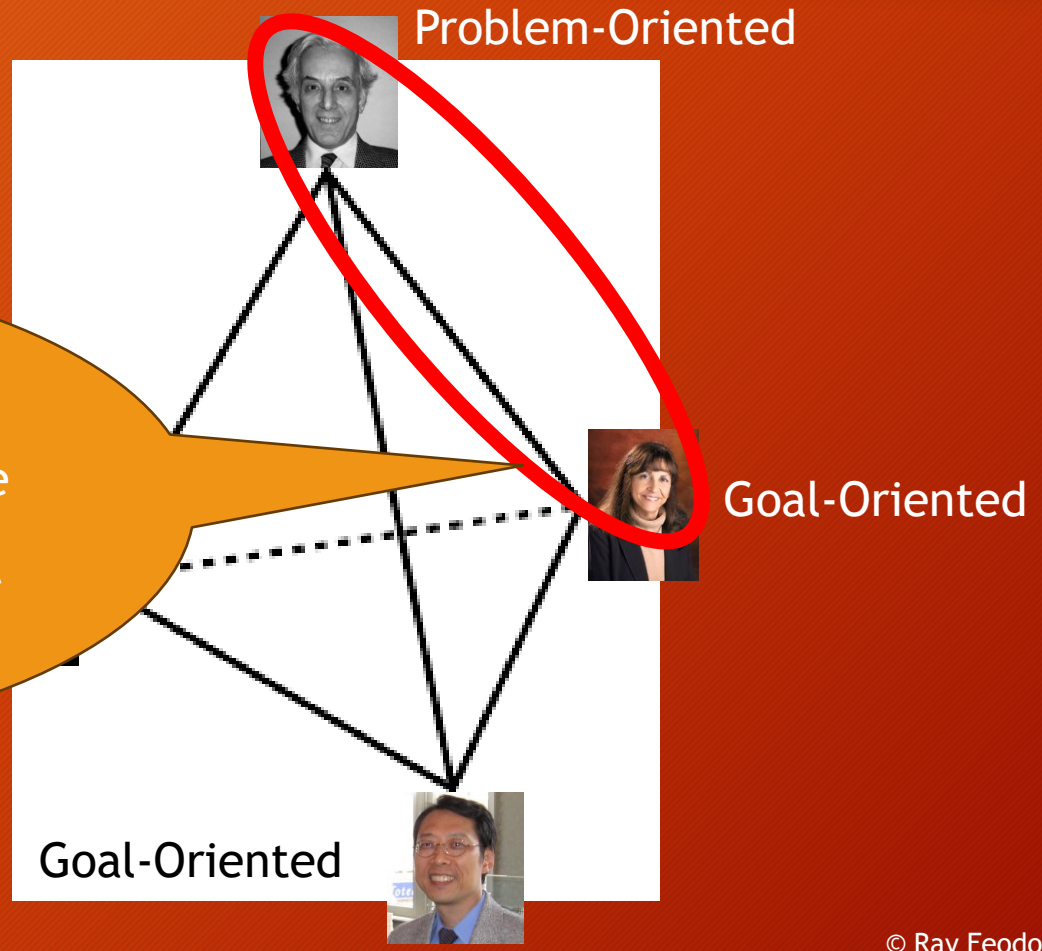


GSN proponents recognise the notion of Knowledge Frames (and thereby Problem Frames) to capture rationale for user requirements and supporting system specification correctness. So, specification correctness is a goal.

Glancing academic areas



Glancing academic areas

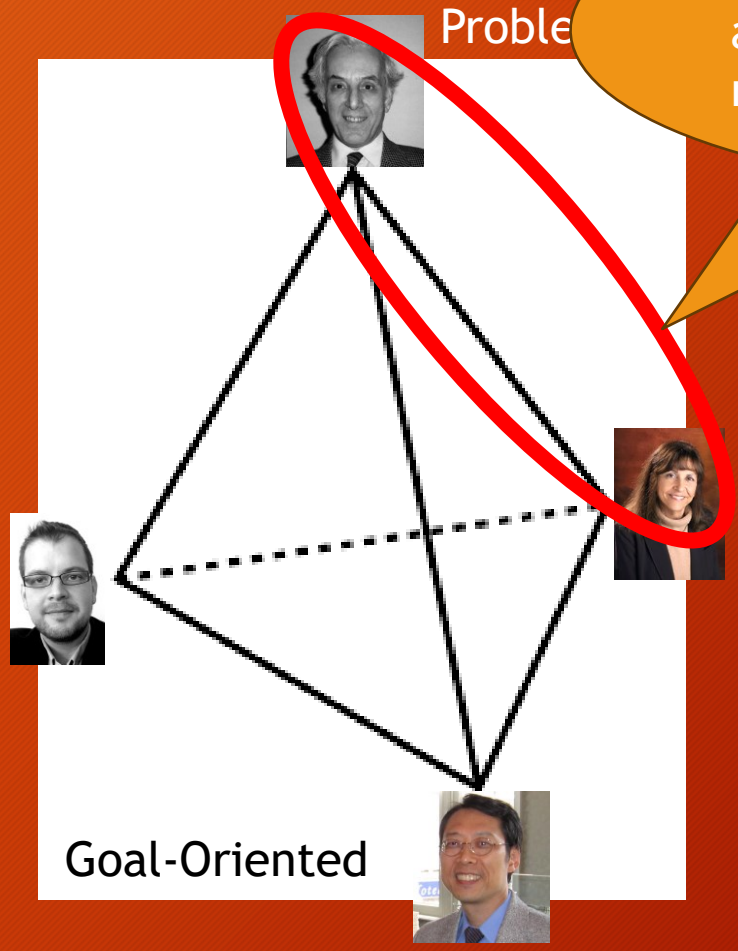


In fact, Thomas (a protégé of Leveson) feels requirements are "function" with a schema, that we note, maps directly to Jackson's Specification and its phenomenon* decorations.

*coming a few slides

Glancing academic areas

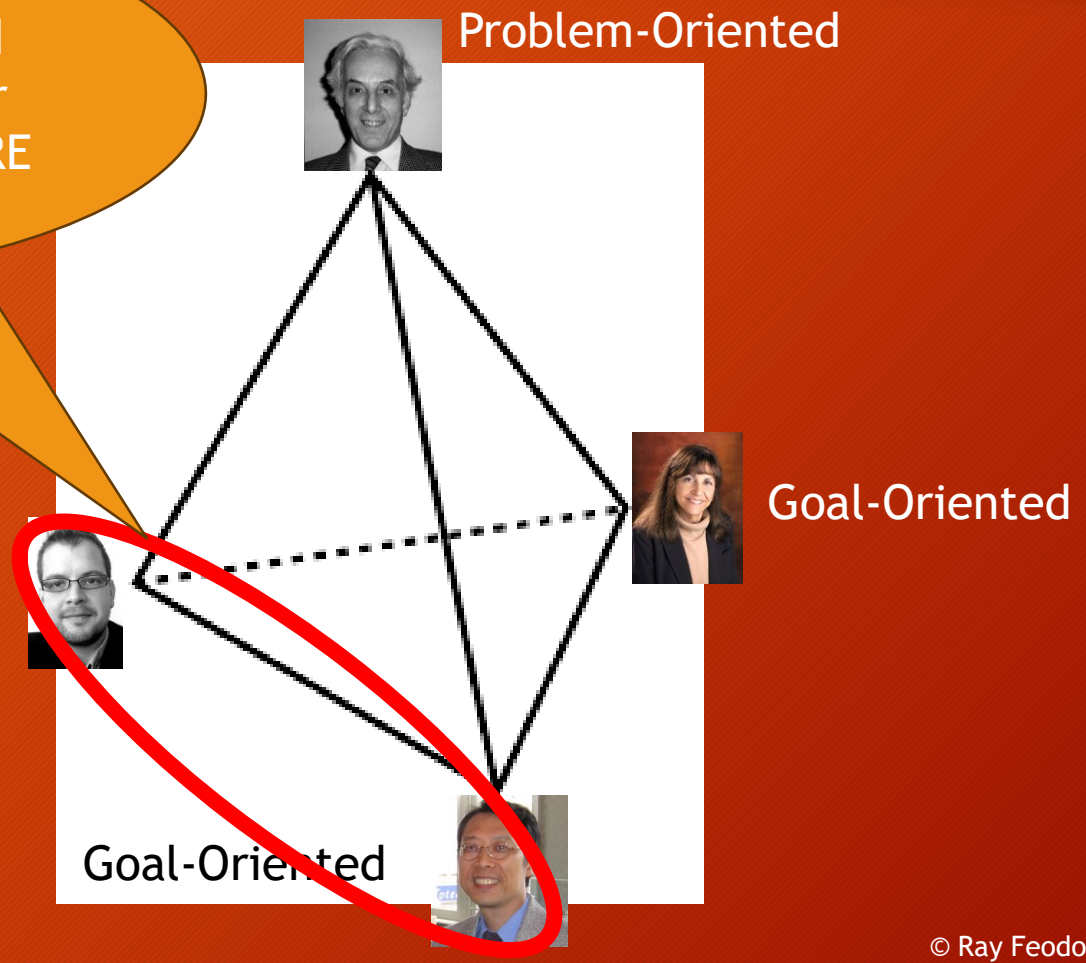
Thomas also codifies hazards as, essentially, anti-requirements*.



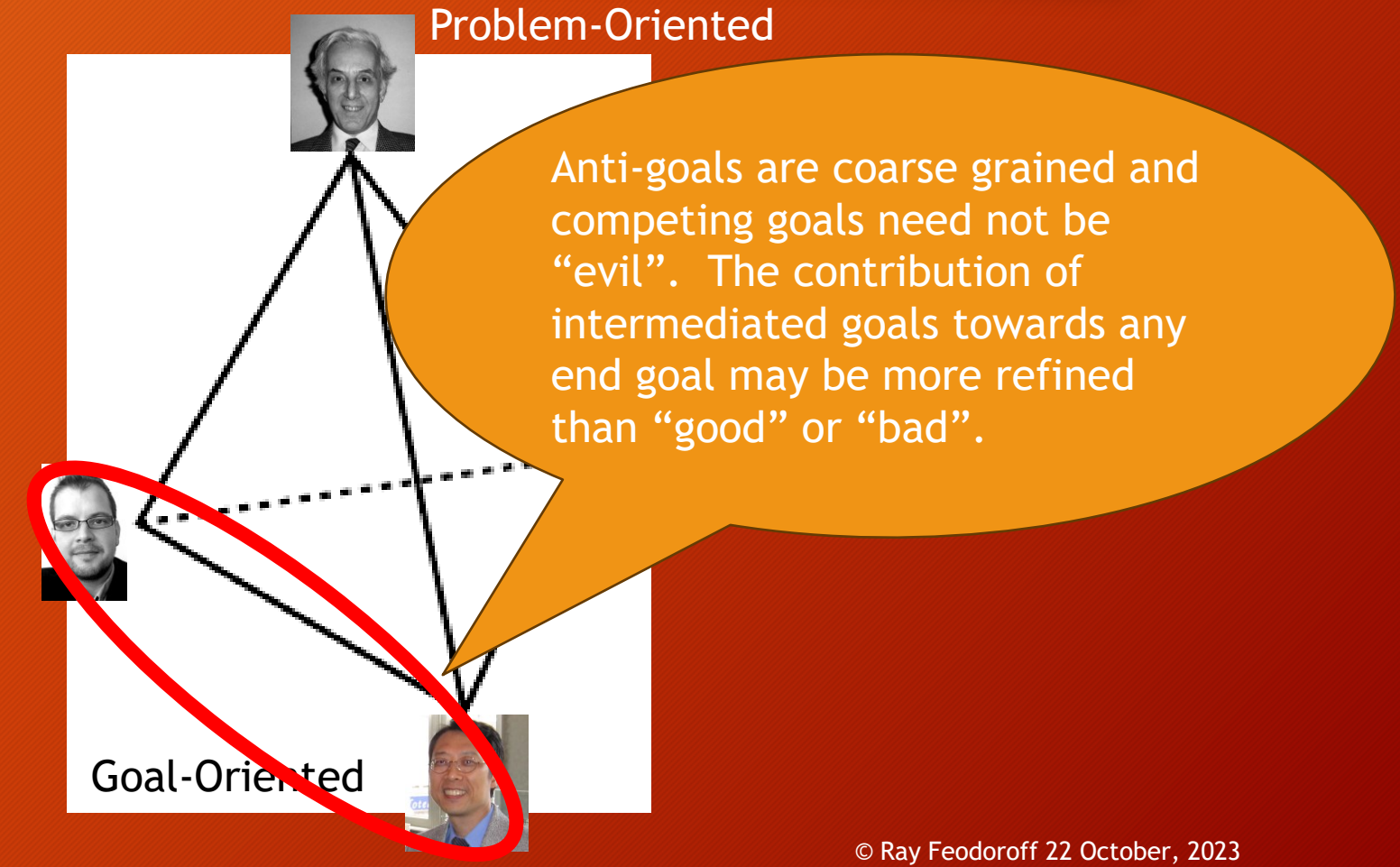
*coming a few slides

Glancing academic areas

It turns out “Argumentors" eventually became interested in (so-called) anti-goals – over a decade or more behind GORE proponents.

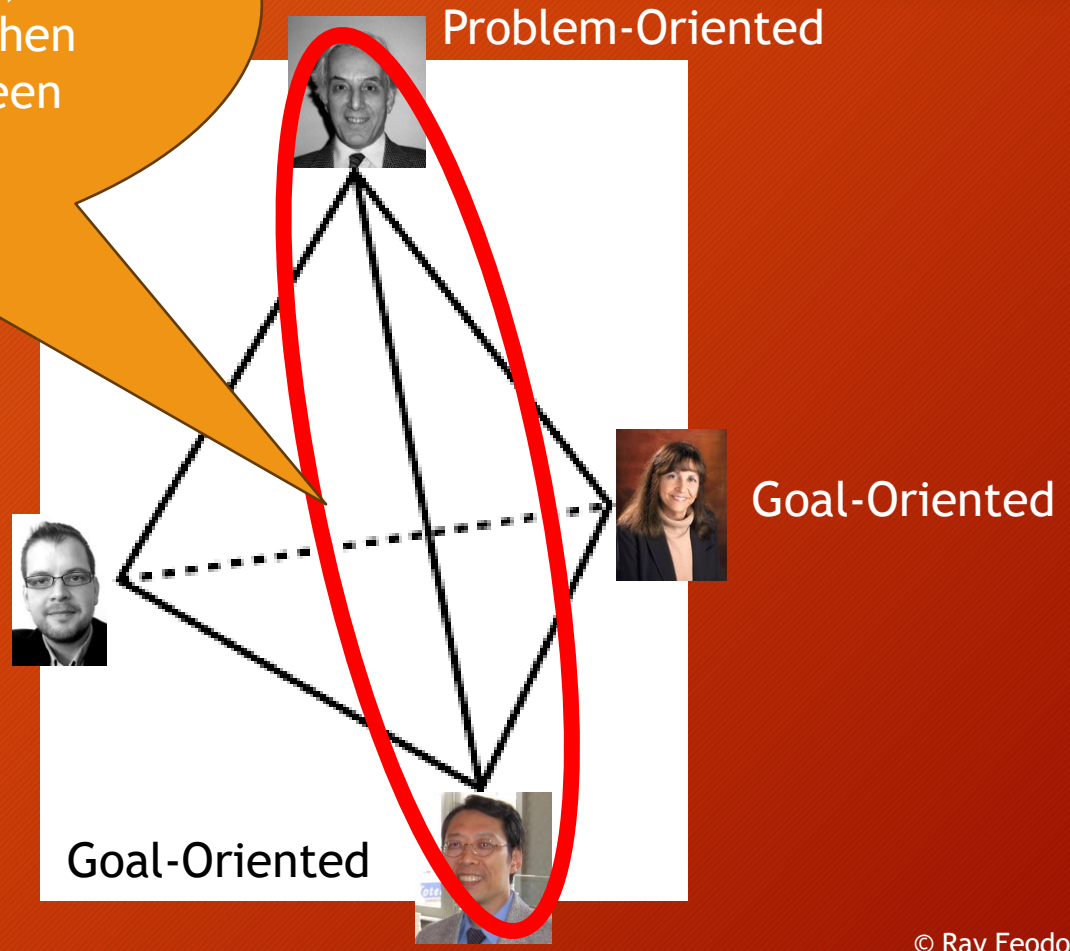


Glancing academic areas



Gl areas

If the debate between goals versus requirements is solved, when operationalisable (doable) goals are allocated to agents, then is there still a difference between problem and goal orientation?



Perceived benefits

- Using GORE notations for design assurance reasoning:
  - May provide economy of design assurance reasoning, because we break away from the third party non-associative assurance author syndrome.
  - Would bring the necessity and sufficiency arguments into the design process in a way that phased safety cases have otherwise failed.
    - Just depends on the modality selected, and the semiotics.
  - Would aim to include semantics that lines up the argumentative and the proof-based approaches.

Argumentation and Proof alignment

Goal Oriented	Specification Oriented	Intended Properties
Attainment	$C \Rightarrow \Diamond T$	Liveness
Maintenance	$\Box\ (C \Rightarrow T)$	
Cessation	$C \Rightarrow \Diamond \neg T$	
Avoidance	$\Box\ (C \Rightarrow \neg T)$	Safety

Argumentation and Proof alignment

Goal Oriented	Specification	
Attainment	$C \Rightarrow \Diamond T$	
Maintenance	$\Box\,(C \Rightarrow T)$	
Cessation	$C \Rightarrow \Diamond \neg T$	
Avoidance	$\Box\,(C \Rightarrow \neg T)$	Safety

This list of verbs comes from motivational psych and appear to be the canonical tool set we mere mortals use for expression of intention.

Argumentation and Proof alignment

Goal Oriented	Specification Oriented	Intended Properties
Attainment	$C \Rightarrow \Diamond T$	
Maintenance	$\Box\,(C \Rightarrow T)$	
Cessation	$C \Rightarrow \Diamond \neg T$	
Avoidance	$\Box\,(C \Rightarrow \neg T)$	

While goals can be "fluffy" we need eventually decompose them into operationalisable (doable) actions. Did you know then that even goals can (eventually) be expressed as temporal logic?

Argumentation and Proof alignment

Goal Oriented	Specification Oriented	Intended Properties
inment	$C \Rightarrow \Diamond T$	Liveness
	$\Box (C \Rightarrow T)$	
n	$C \Rightarrow \Diamond \neg T$	
ce	$\Box (C \Rightarrow \neg T)$	Safety

In formal modelling: A liveness property asserts that something good eventually happens.
A safety property asserts that nothing bad happens during execution.

Argumentation and Proof alignment

Goal Oriented	Specification Oriented	Intended Properties
Attainment	$C \Rightarrow \Diamond T$	Livene
Maintenance	$\Box\,(C \Rightarrow T)$	
Cessation	$C \Rightarrow \Diamond \neg T$	
Avoidance	$\Box\,(C \Rightarrow \neg T)$	Safety

The problem for design assurance, and therefore for requirements specification, is asserting that something good will always be happening.

Argumentation and Proof alignment

Goal Oriented	Specification	Intended Properties
Attainm		
Maintena		
Cessation	$C \Rightarrow \Diamond \neg T$	
Avoidance	$\Box\,(C \Rightarrow \neg T)$	Safety

Ask ChatGPT what the difference is between the manner of use of these verbs when used in problem or goal statements.

Solution Approach

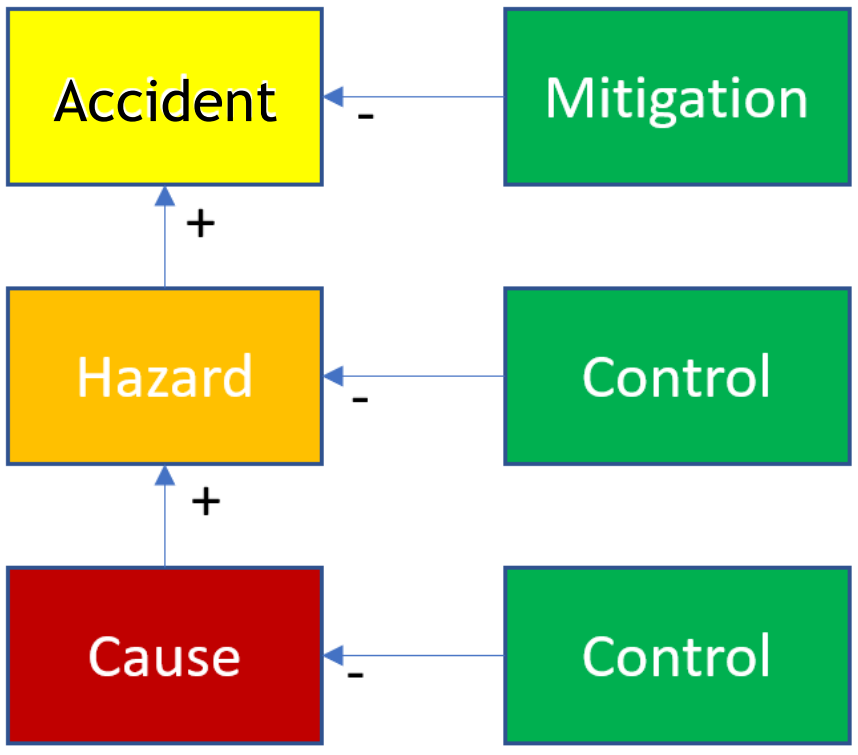
- Three phases:
  - Phase 1: Begin development of the theoretic basis for a requirement notation with embedded design assurance reasoning (you are here).
  - Phase 2: Develop a meta-model, or as the Problem Frame community would have it, a Domain and Requirement Description Language (are we there yet?).
  - Phase 3: Develop a graphical goal-oriented notation that embodies the theoretics, taking care with both the semantics and the semiotics (will we ever get there?).

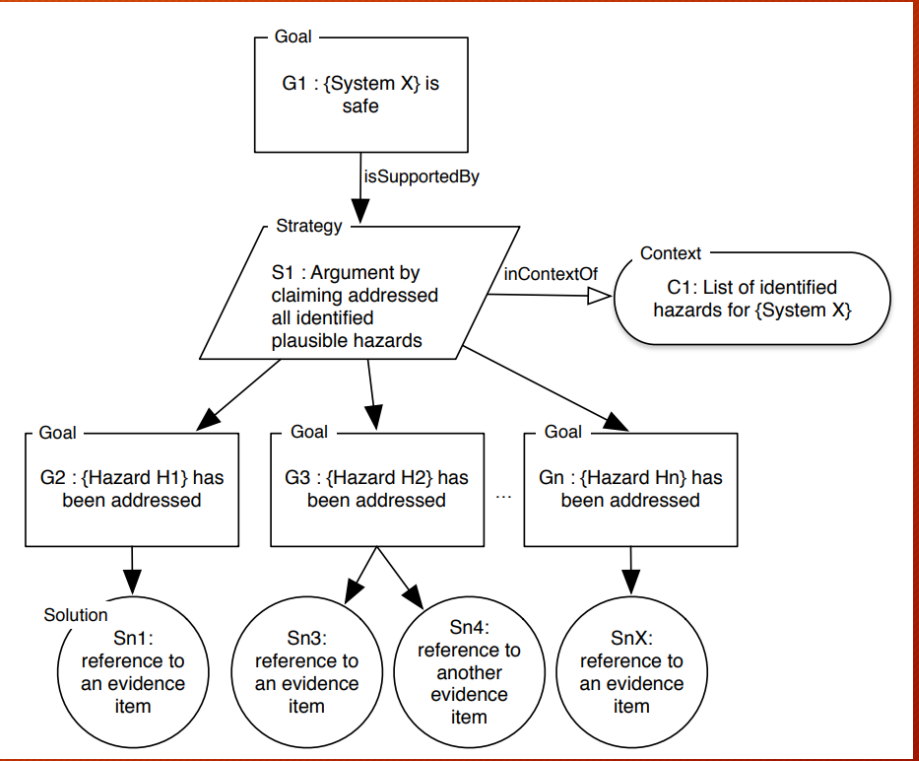
Phase 1

9

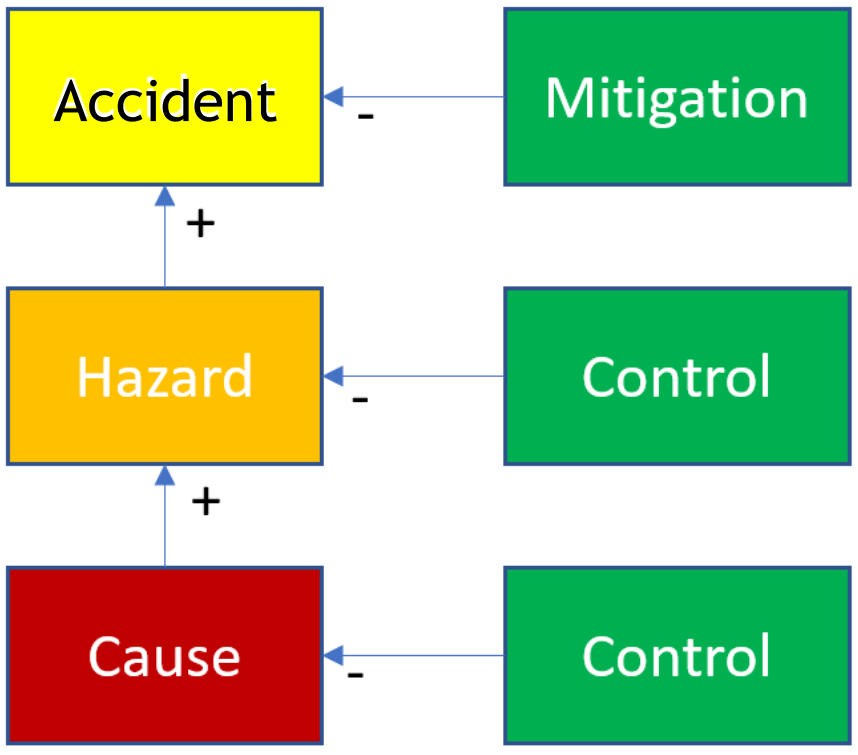
What is the theoretical basis for our notation?

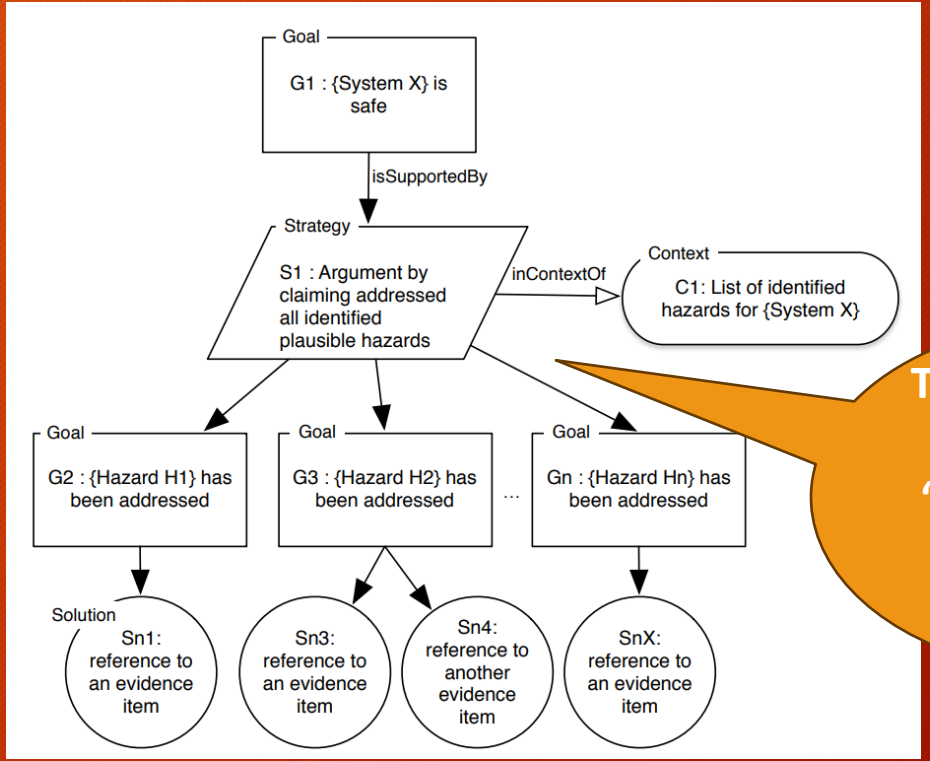
Challenges in Safety Reasoning with GSN





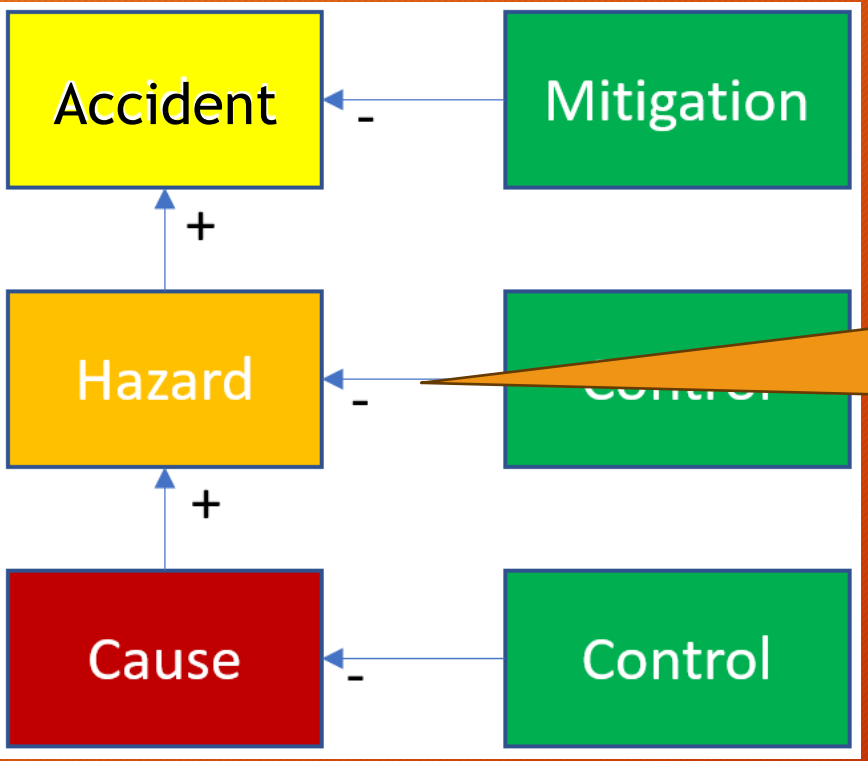
Challenges in Safety Reasoning with GSN

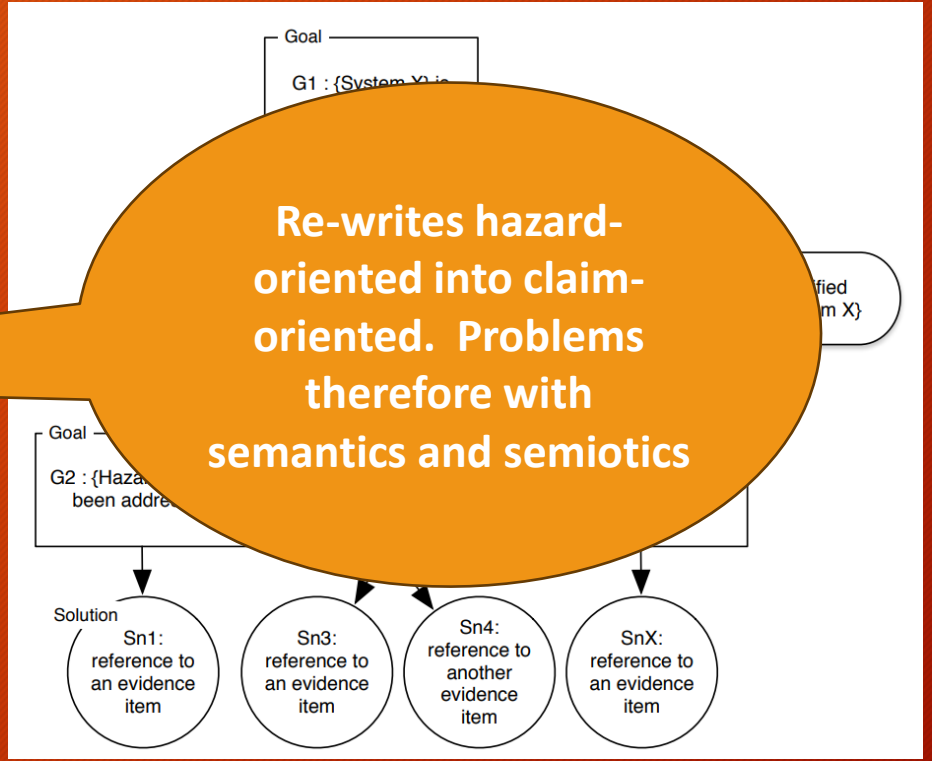




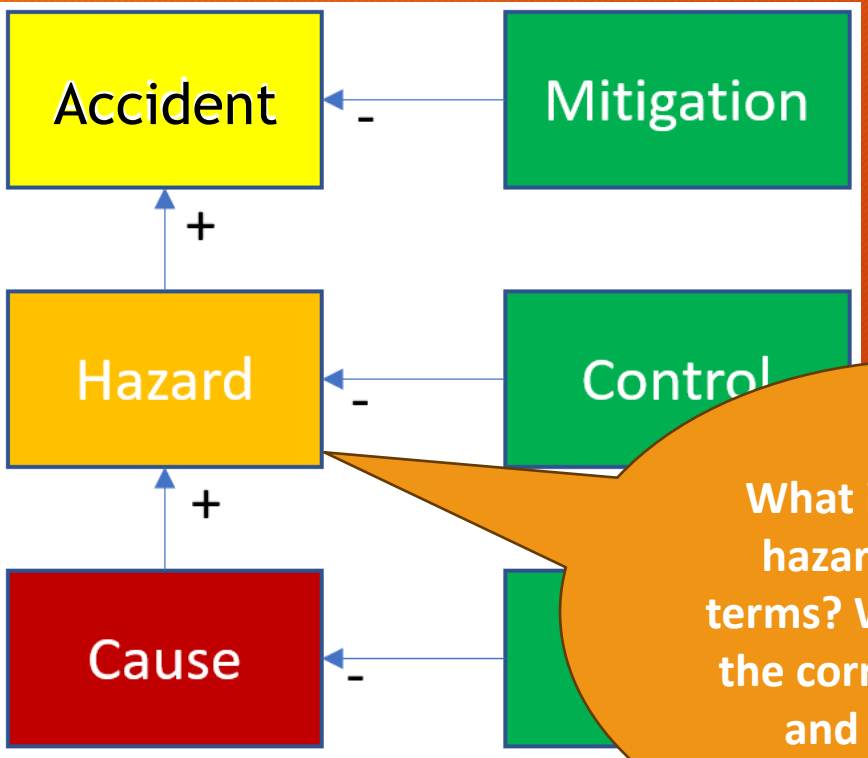
The predominant argument "pattern" that is used to reason about safety

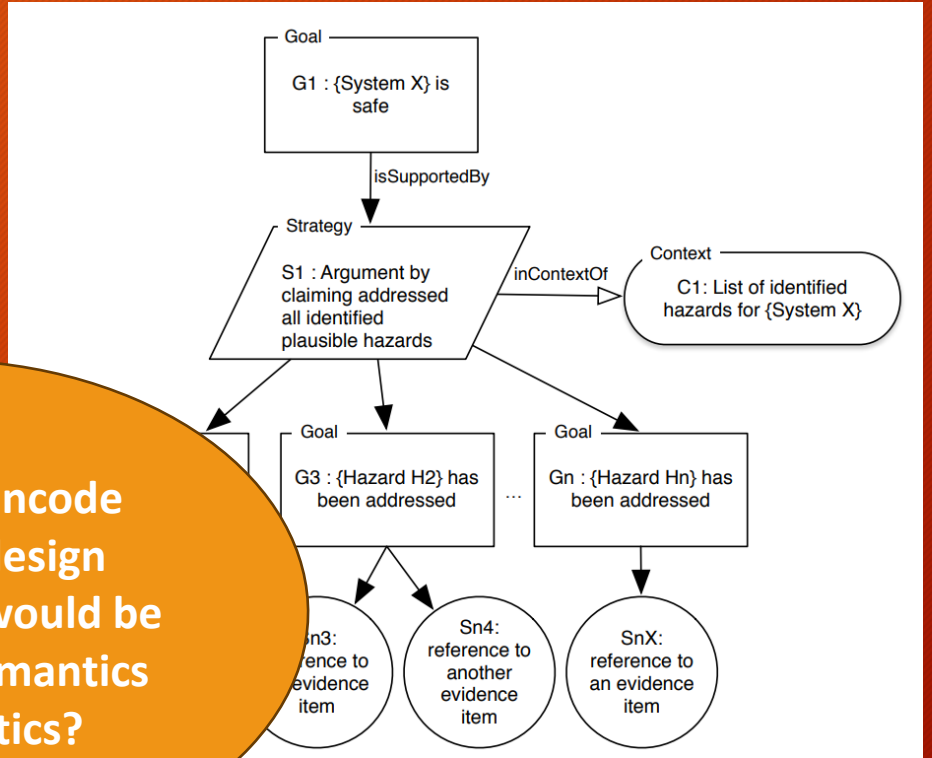
Challenges in Safety Reasoning with GSN





Challenges in Safety Reasoning with GSN

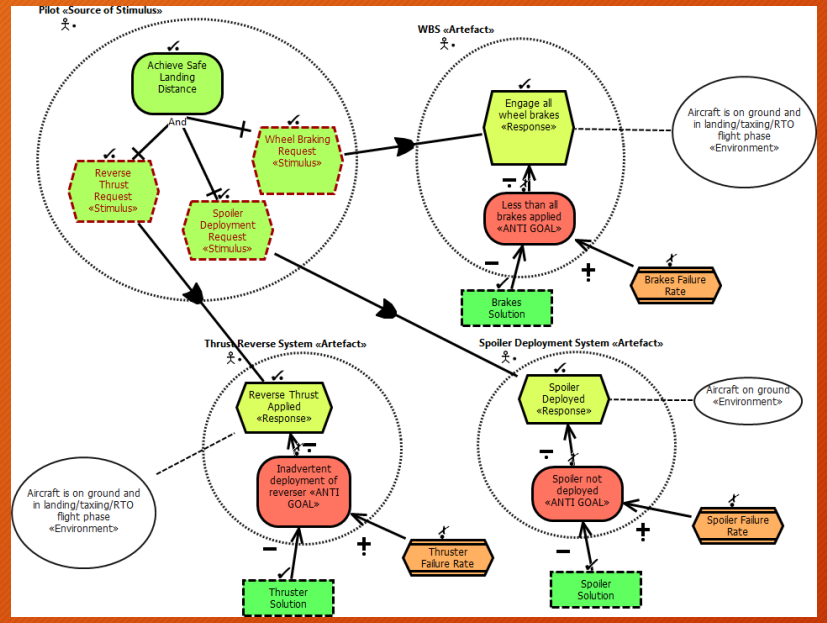




What if we encode hazards in design terms? What would be the correct semantics and semiotics?

Recapping previous work

Using GORE instead of GSN



No Information Loss

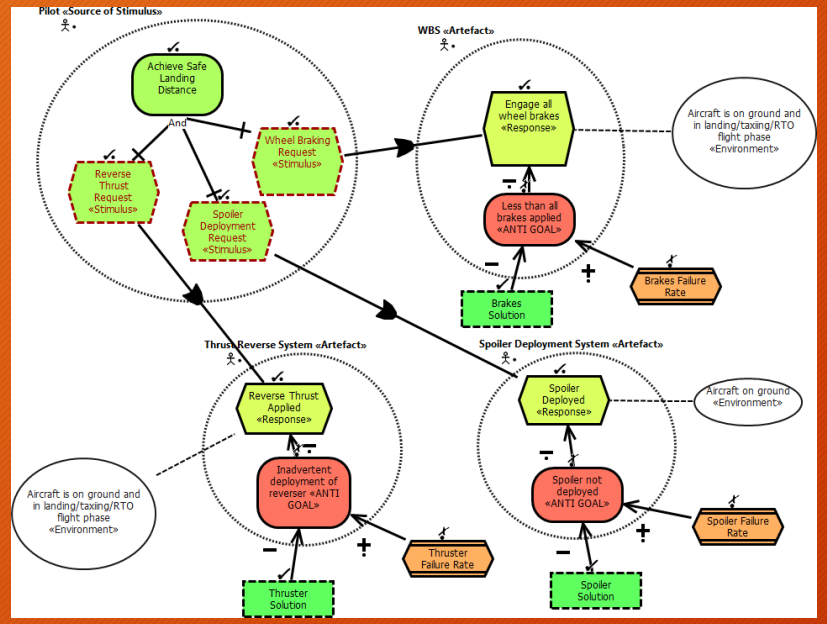
$$QAS \vdash (K, S \vdash R)$$
$$K_{WBS}, S_{WBS} \vdash R_{WBS}$$
$$K_S, S_S \vdash R_S$$
$$K_T, S_T \vdash R_T$$

$$R_{WBS}, R_S, R_T \vdash Safe_{Landing}$$

Recapping previous work

Quality Attribute Scenarios (from CMU), described as goal-oriented by GSN practitioners. GSN practitioners also conveniently claim QAS are analogous to Knowledge Frames.

Using GORE instead of GSN



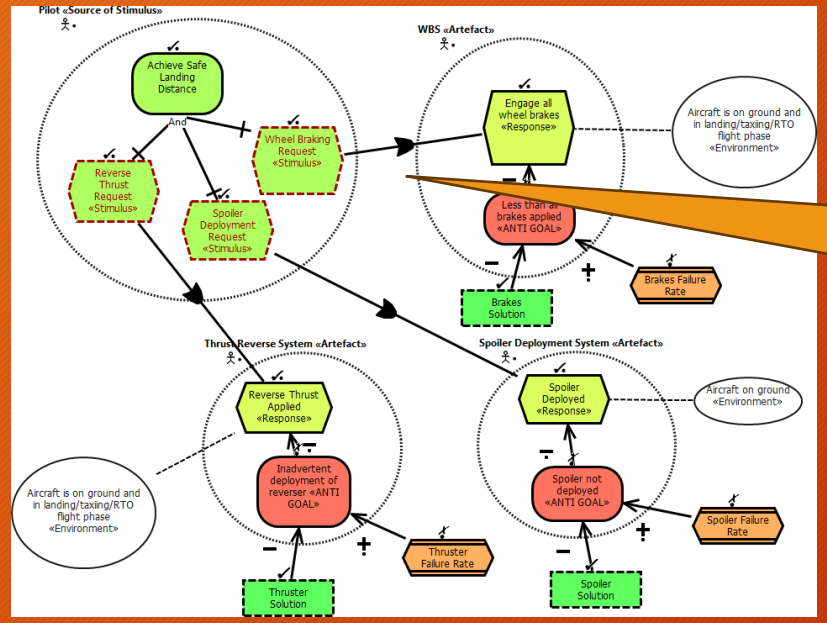
No Information Loss

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

$$R_{WBS}, R_S, R_T \vdash Safe_{Landing}$$

Recapping previous work

Using GORE instead of GSN



No Information Loss

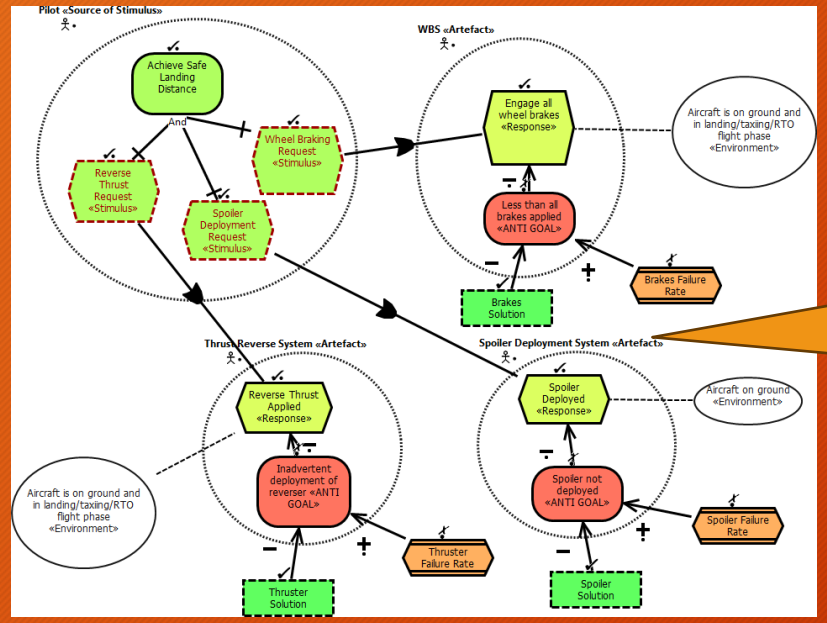
$$QAS \vdash (K, S \vdash R)$$

QAS expressed graphically, look something (or somewhat) like this!

$$R_{WBS}, R_S, R_T \vdash Safe_{Landing}$$

Recapping previous work

Using GORE instead of GSN



No Information Loss

$QAS \vdash$

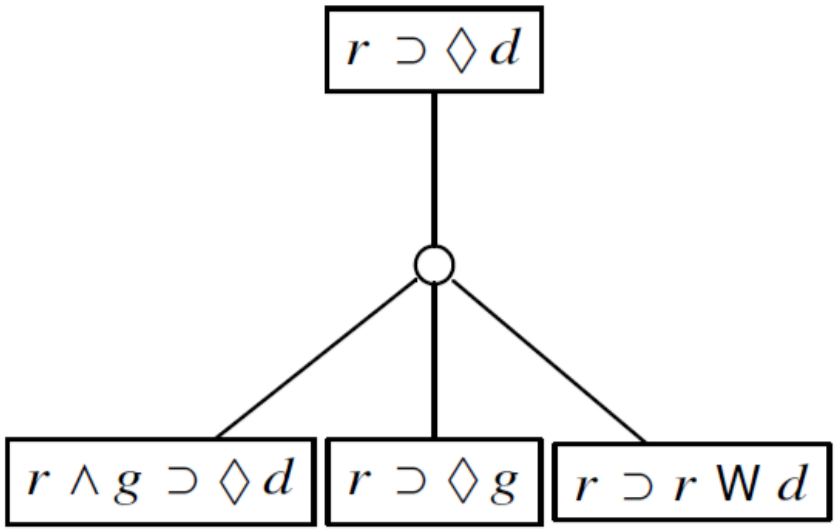
K_{WI}

K_T,

R_{WBS}, R_S

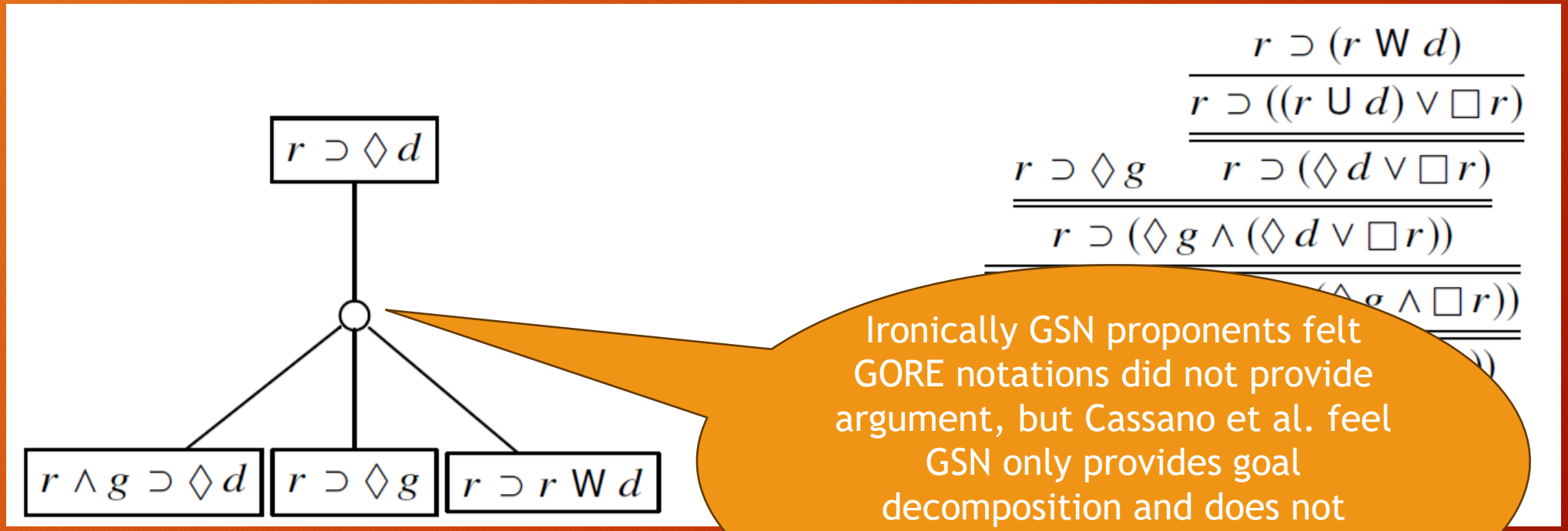
One diagram replaces several disjoint representations. The right semantics? The right semiotics? Certainly, superior in terms of economy and of comprehension?

Pattern Based v Proof (Cassano et al.)



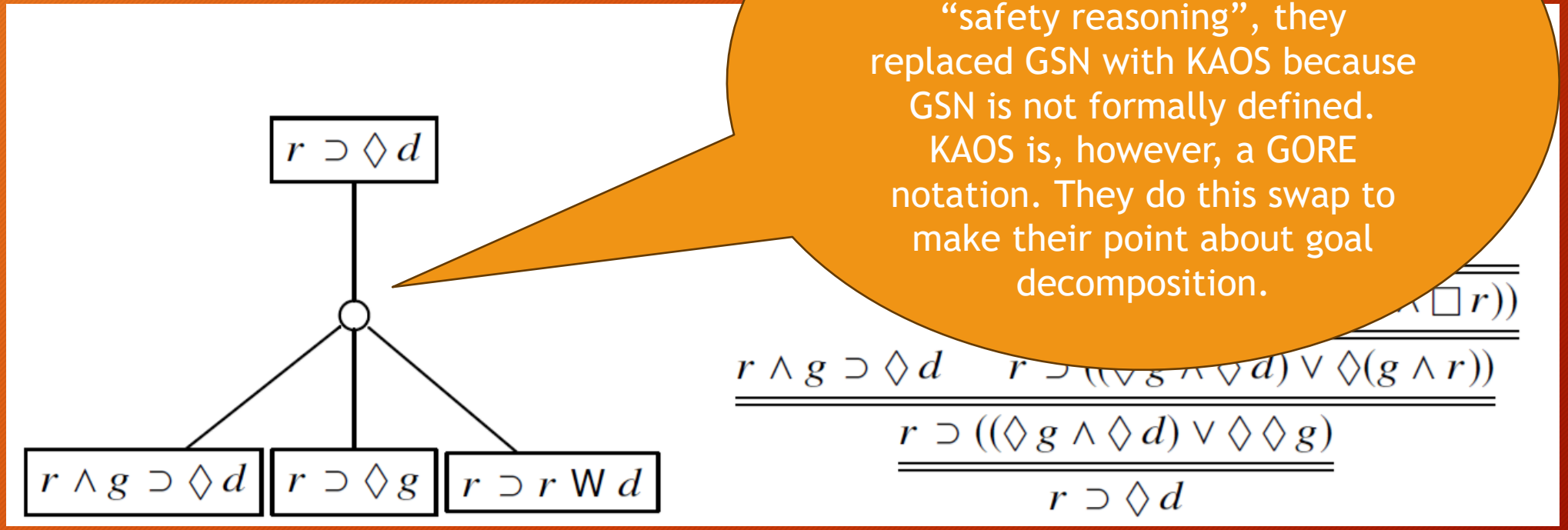
$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{r \supset (r \,\mathsf{W}\, d)}{r \supset ((r \,\mathsf{U}\, d) \vee \Box r)} \quad r \supset \Diamond g}{r \supset (\Diamond g \wedge ((\Diamond d \vee \Box r))} \quad r \supset (\Diamond d \vee \Box r)}{r \supset ((\Diamond g \wedge \Diamond d) \vee (\Diamond g \wedge \Box r))}}{r \supset ((\Diamond g \wedge \Diamond d) \vee \Diamond(g \wedge r))} \quad r \wedge g \supset \Diamond d}{r \supset ((\Diamond g \wedge \Diamond d) \vee \Diamond \Diamond g)}}{r \supset \Diamond d}$$

Pattern Based v Proof (Cassano et al.)

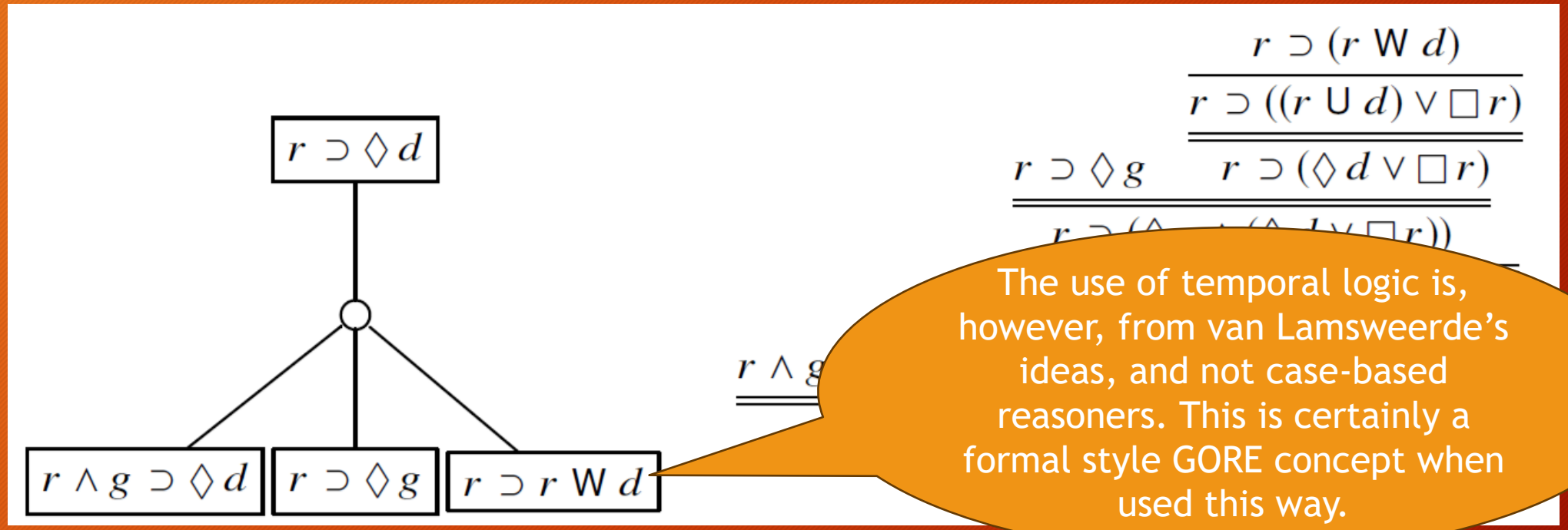


Pattern Based v Proof (Cassano et al.)

While GSN is used as a “witness” by Cassano et al., since they are objecting to case notations as “safety reasoning”, they replaced GSN with KAOS because GSN is not formally defined. KAOS is, however, a GORE notation. They do this swap to make their point about goal decomposition.

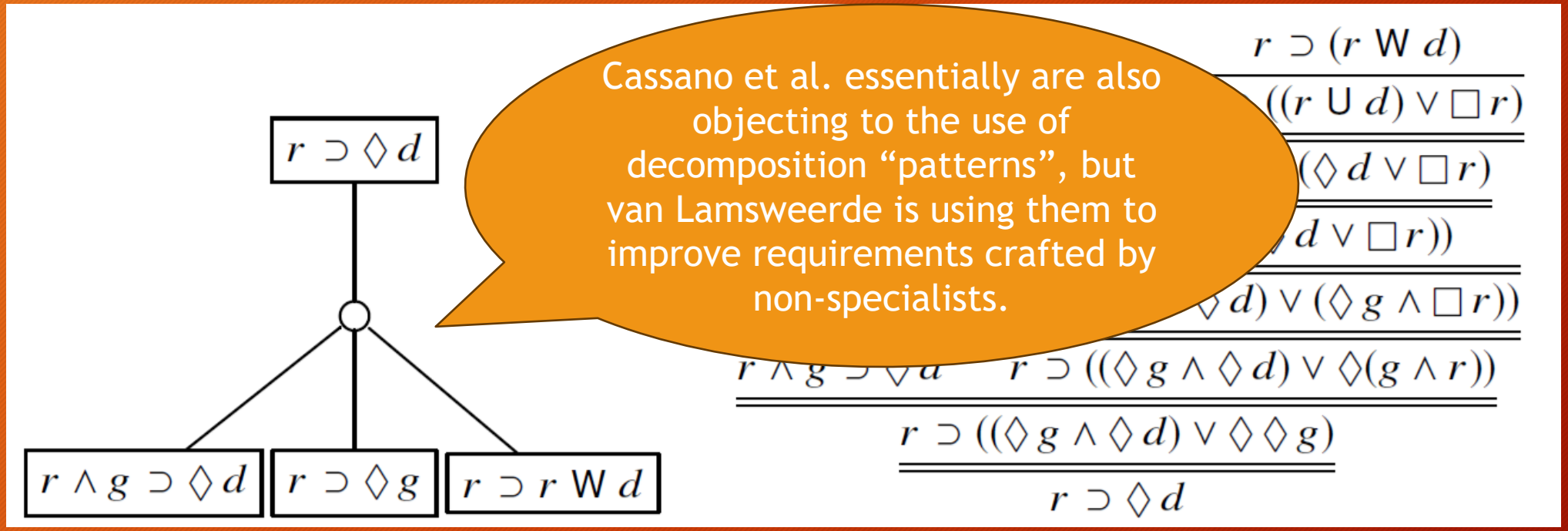


Pattern Based v Proof (Cassano et al.)



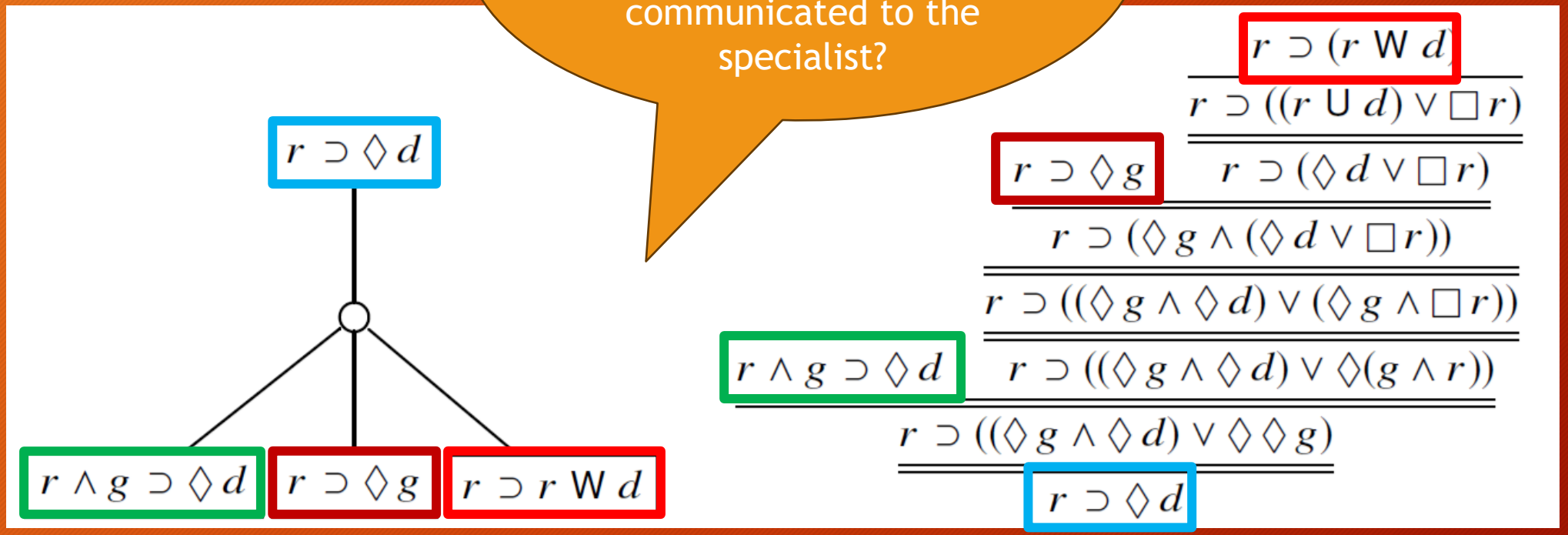
The use of temporal logic is, however, from van Lamsweerde's ideas, and not case-based reasoners. This is certainly a formal style GORE concept when used this way.

Pattern Based v Proof (Cassano et al.)

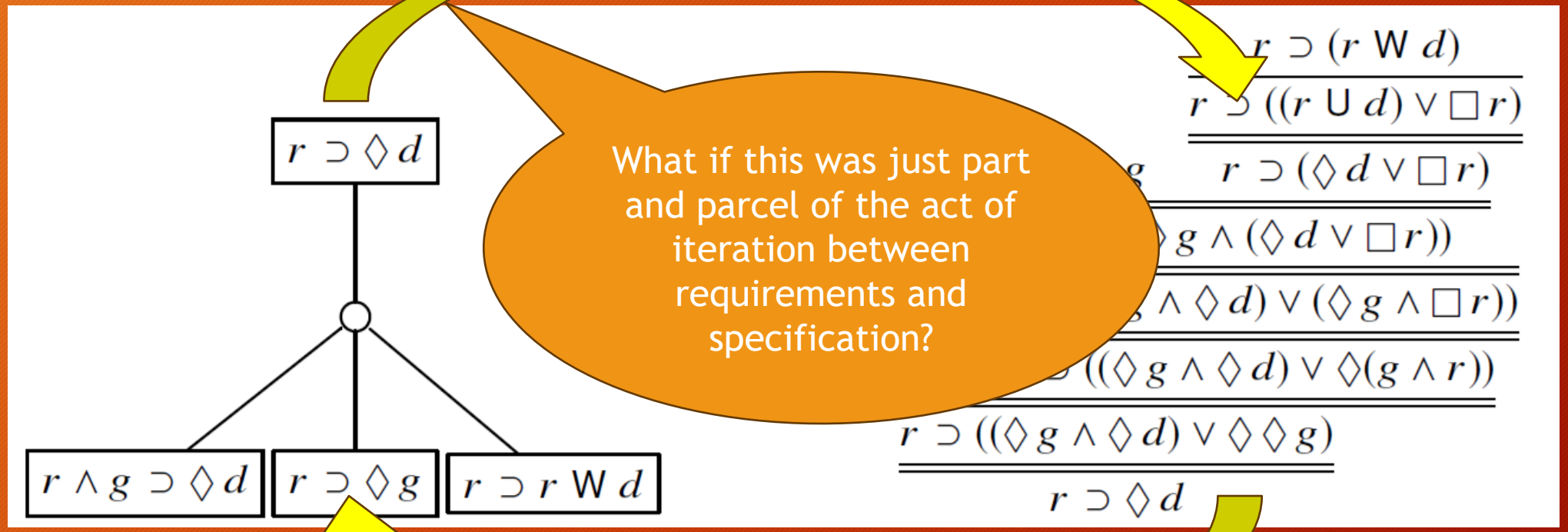


Pattern Based v Pr… …o et al.)

So, what if the patterns underwent proving? What if this allowed the non-specialist means to communicated to the specialist?



Pattern Based v Proof (Cassano et al.)



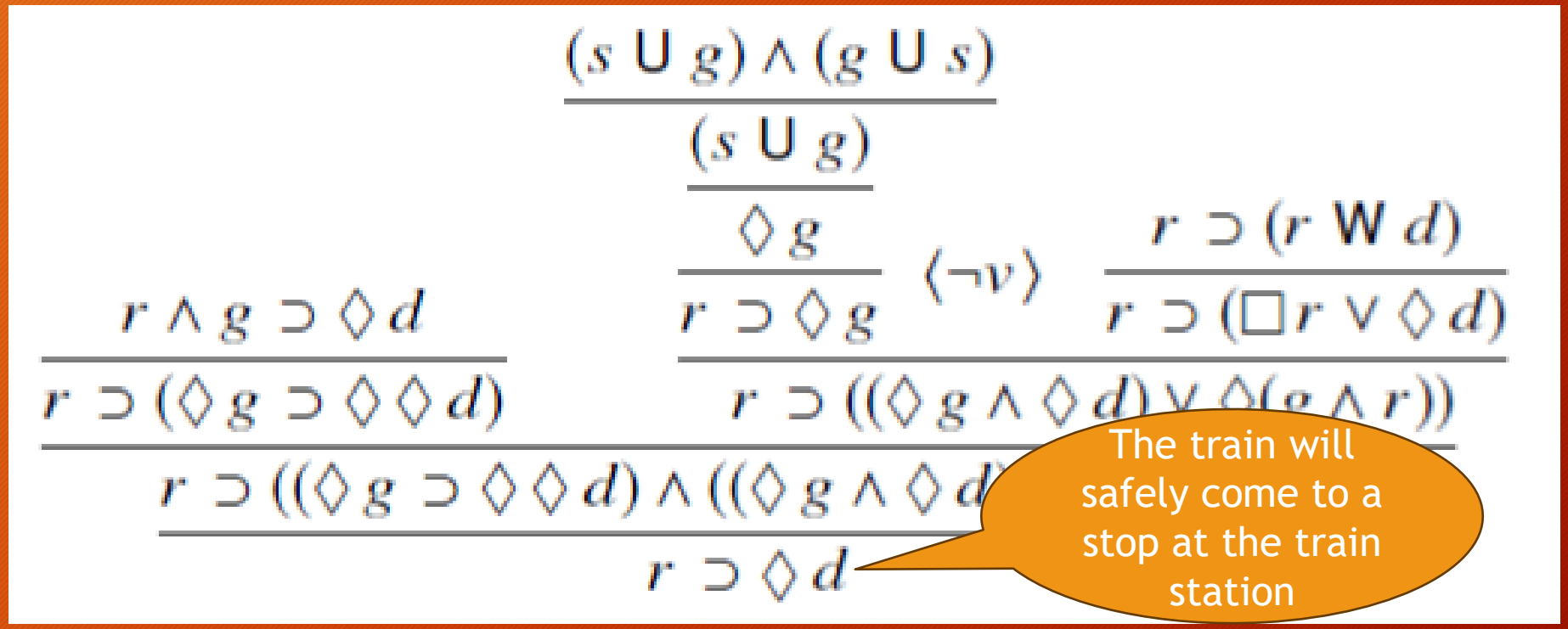
Introduction of skepticism into a proof (Cassano et al.)

$$\dfrac{\dfrac{\dfrac{(s \mathbin{\mathsf{U}} g) \wedge (g \mathbin{\mathsf{U}} s)}{(s \mathbin{\mathsf{U}} g)}}{\Diamond g}}{r \supset \Diamond g} \langle \neg v \rangle \qquad \dfrac{r \supset (r \mathbin{\mathsf{W}} d)}{r \supset (\Box r \vee \Diamond d)}$$

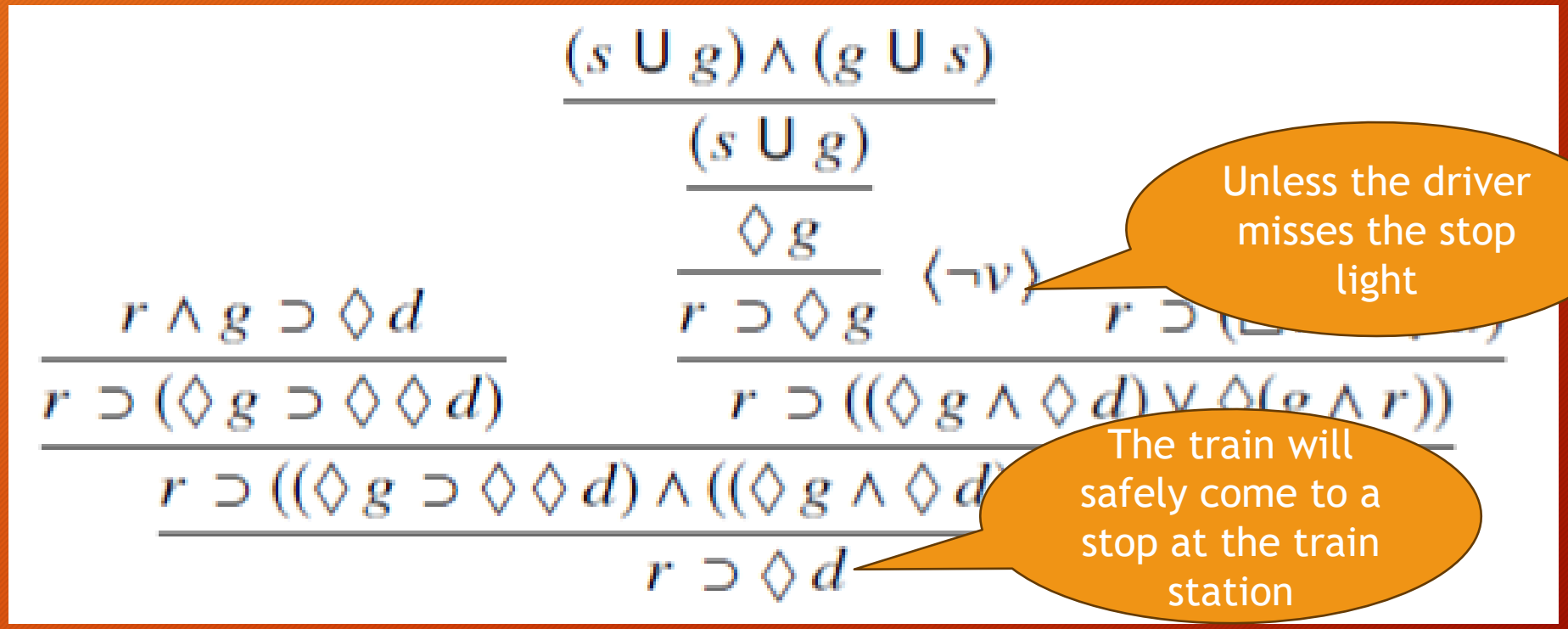
$$\dfrac{\dfrac{r \wedge g \supset \Diamond d}{r \supset (\Diamond g \supset \Diamond \Diamond d)} \qquad r \supset ((\Diamond g \wedge \Diamond d) \vee \Diamond (g \wedge r))}{r \supset ((\Diamond g \supset \Diamond \Diamond d) \wedge ((\Diamond g \wedge \Diamond d) \vee \Diamond (g \wedge r)))}$$

$$r \supset \Diamond d$$

Introduction of skepticism into a proof (Cassano et al.)

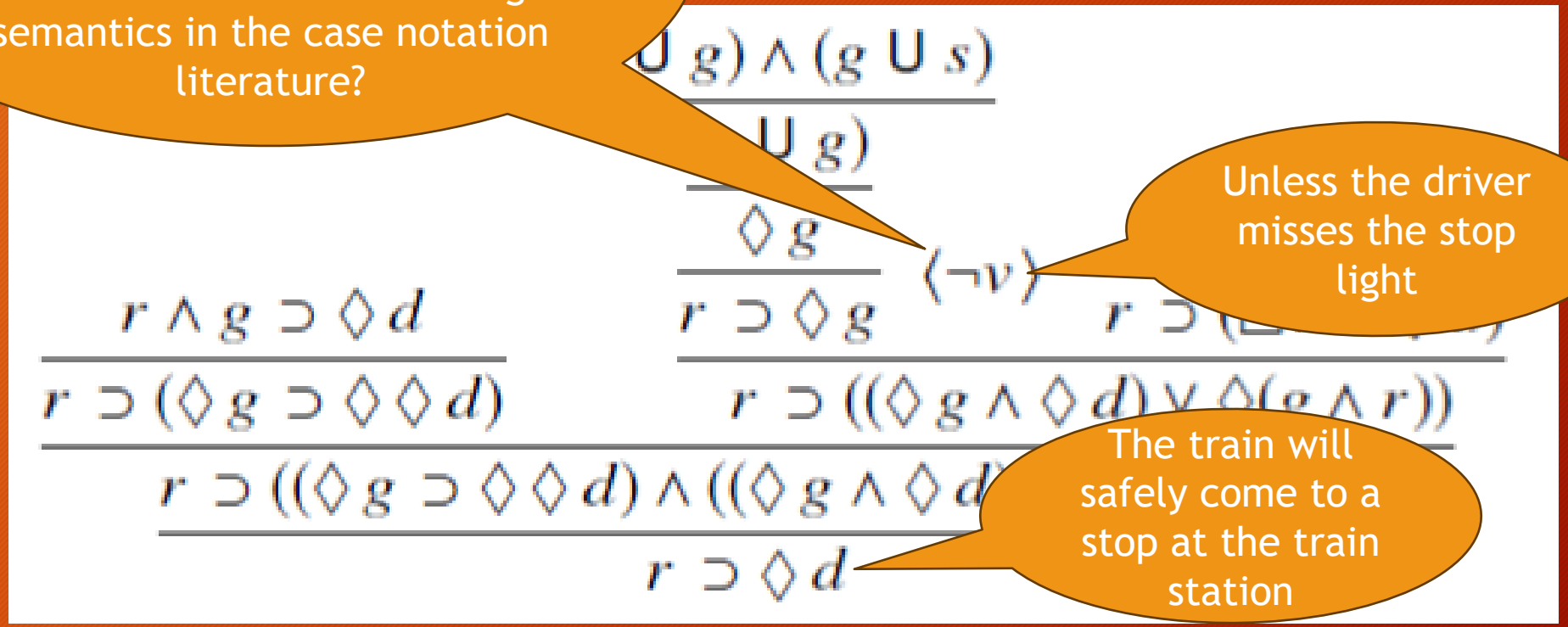


Introduction of skepticism into a proof (Cassano et al.)



Introduction of skepticism into a proof (C

So, is this the influence on proofs by the late breaking discussion on counterfactual or non-monotonic reasoning semantics in the case notation literature?



Unless the driver misses the stop light

The train will safely come to a stop at the train station

Problems as Requirement Decompositions (Jackson, Hall, Rapanotti)

$$W, S_O^C \vdash R$$

So, we've seen a similar style of notation.

Problems as Requirement Decompositions (Jackson, Hall, Rapanotti)

$$W, S_O^C \vdash R$$

So, we've seen a similar style of notation.

For when:
"sound and complete theories for realistic systems are elusive"!

Problems as Requirement Decompositions (Jackson, Hall, Rapanotti)

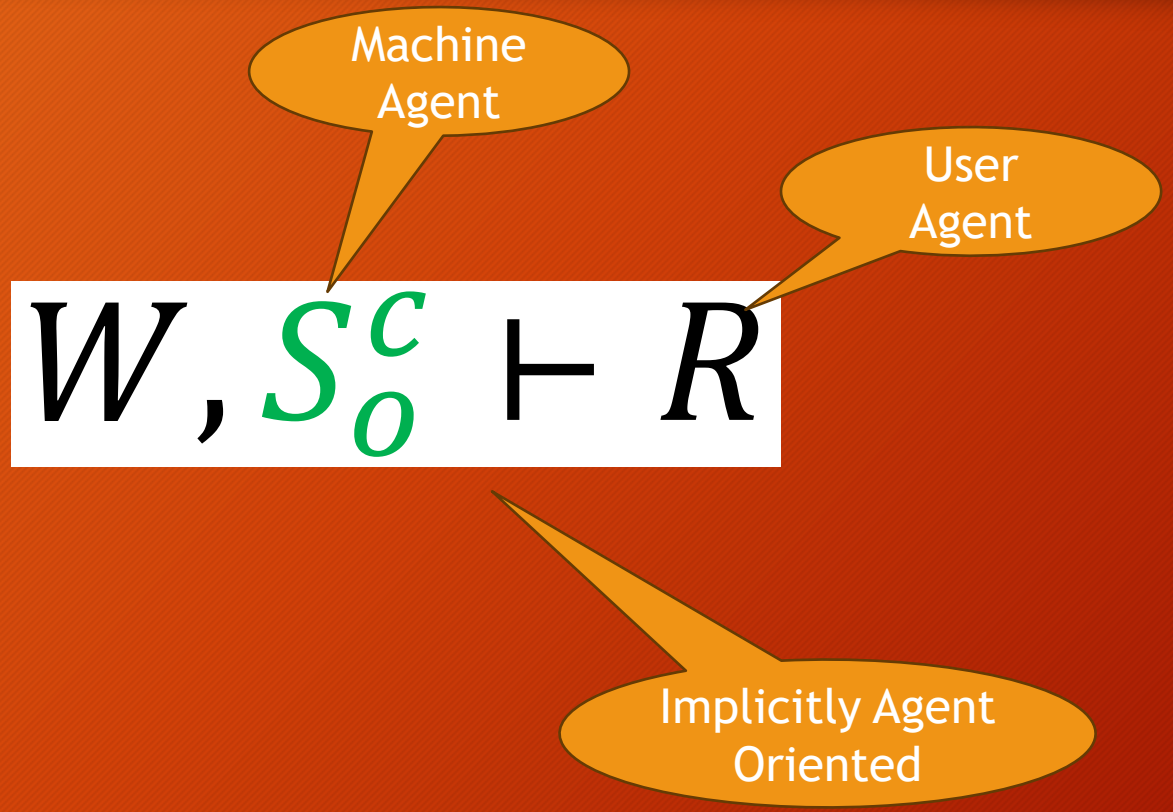
$$W, S_O^C \vdash R$$

So, we've seen a similar style of notation.

For when:
"sound and complete theories for realistic systems are elusive"!

That is, not precise nor mathematical (at least preliminarily, or when user requirements are involved).

Problems as Requirement Decompositions (Jackson, Hall, Rapanotti)



Problems as Requirement Decompositions (Jackson, Hall, Rapanotti)

Where else have we seen this?

$$W, S_O^C \vdash R$$

Problems as Requirement Decompositions (Jackson, Hall, Rapanotti)

Where else have we seen this?

$$W, S_o^c \vdash R$$

User or Machine Agent

$$\mathrm{R} \triangleq \langle sc(S), ca(c), co(o) \rangle$$

Requirement Function (Thomas)

phenomenon controlled

phenomenon observed

Hazards as Anti-Requirements (Thomas)

We wanted a means to encode hazards in design terms! Thomas suggests, what we might call, anti-requirements.

Described here in Problem Frame "speak".

$$H^{Omission}: W, S_o^{\neg c} \vdash \bar{R}$$

$$H^{Commission}: W, S_o^{c} \vdash \bar{R}$$

Hazards as Anti-Requirements (Thomas)

$$H^{Omission}: W, S_o^{\neg c} \vdash \bar{R}$$
$$H^{Commission}: W, S_o^{c} \vdash \bar{R}$$

The set of all $\bar{R}$

So, our specification goal is $R \notin \overline{\mathbb{R}}$

Mixed logics (if they were permissible)

$$(W, S_o^c \vdash R) \Rightarrow\!\circ\, W'$$

So, we want to set the next state of the world in relation to the current "tick", also such that $R \notin \overline{\mathbb{R}}$.

Mixed logics (if they v

So, we want decompose a requirement to a specification that sees action “*c*” when “*o*” *occurs in the domain “W”.*

$$(W, S_o^c \vdash R) \Rightarrow\!\circ\, W'$$

Mixed logics (if they v

So, we want decompose a requirement to a specification that sees action “*c*” when “*o*” *occurs in the domain “W”.*

$$(W, S_o^c \vdash R) \Rightarrow\!\circ\, W'$$

S	R	W’
$C \Rightarrow\!\Diamond\, T$	Achieve X	Achieved X
$\Box(C \Rightarrow T)$	Maintain X	Maintained X
$C \Rightarrow \neg T$	Cease X	Ceased X
$\Box(C \Rightarrow \neg T)$	Avoid X	Avoided X

The point being we’ve already talked about goal intentions capped to a set of verbs, expressible in temporal logic.

Mixed logics (if they were permissible)

$$(W, S_o^c \vdash R) \Rightarrow\!\circ\, W'$$

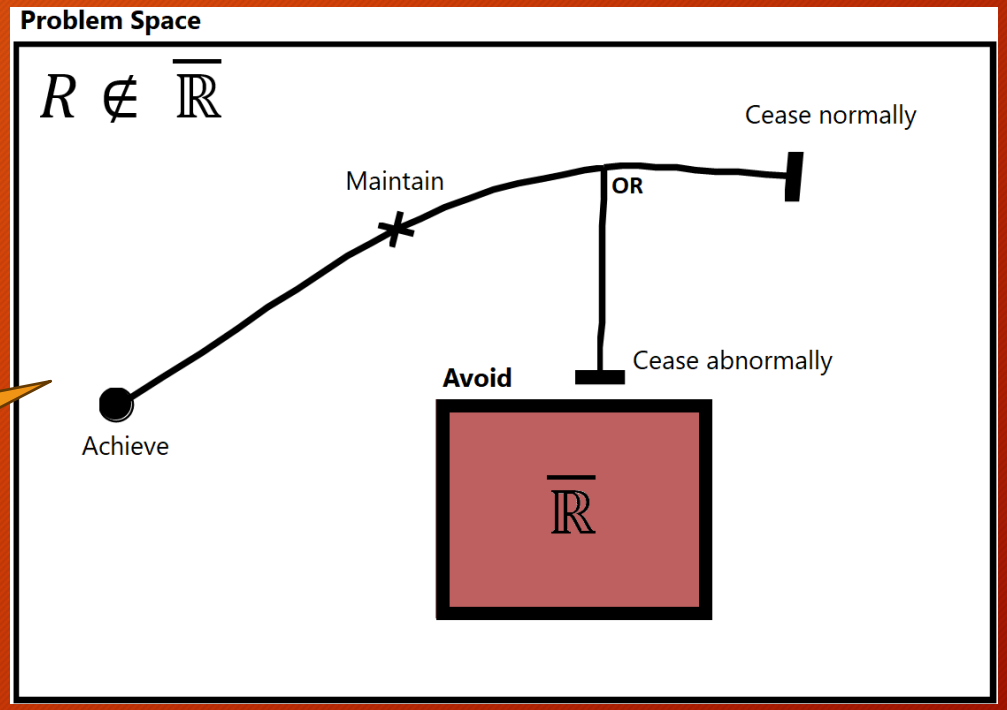
S	R	W'
$C \Rightarrow\!\Diamond\, T$	Achieve X	Achieved X
$\Box(C \Rightarrow T)$	Maintain X	Maintained X
$C \Rightarrow \neg T$	Cease X	Ceased X
$\Box(C \Rightarrow \neg T)$	Avoid X	Avoided X

The difference between a goal and a claim may only be that the claim is the past participle verb form of the goal. Or so I claim

Liveness as a 2D spatial “calculus”

Goal Oriented	Specification Oriented	Intended Properties
Attainment	$C \Rightarrow \Diamond T$	Liveness
Maintenance	$\Box\ (C \Rightarrow T)$	
Cessation	$C \Rightarrow \Diamond \neg T$	
Avoidance	$\Box\ (C \Rightarrow \neg T)$	Safety

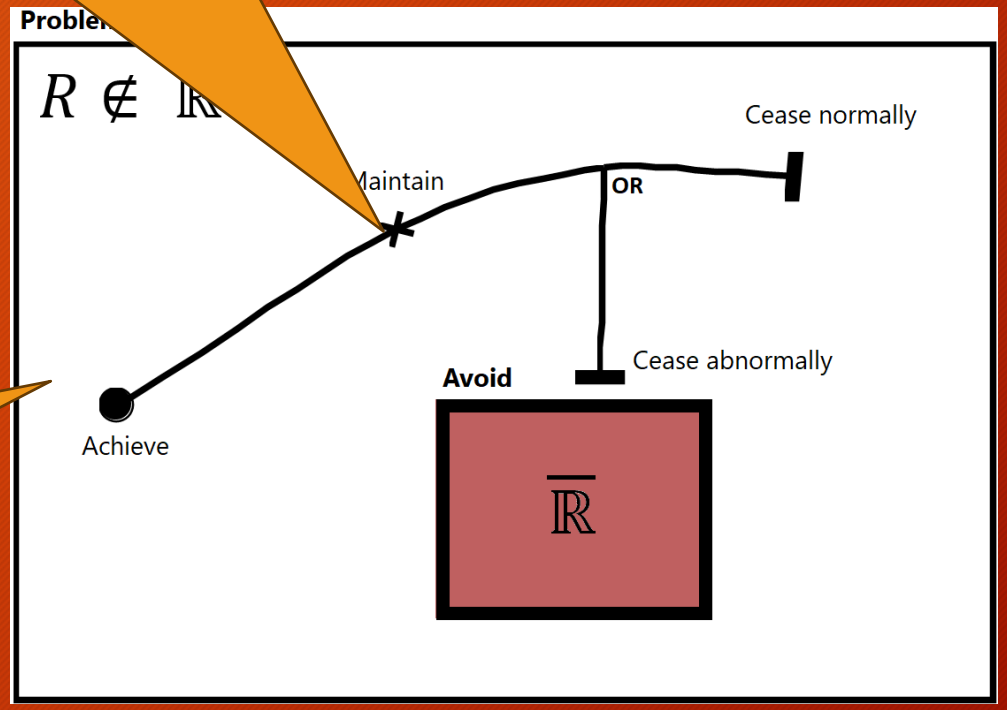
So, “spatially” the problem for liveness in specification is to AVOID states or conditions through definition of system behavior.



Liveness as

Essentially this is what Thomas suggests, when using the antithesis of the hazard to set "responsibilities" thence onto requirements.

Goal Oriented	Specification Oriented	Intended Properties
Attainment	$C \Rightarrow \Diamond T$	Liveness
Maintenance	$\Box\ (C \Rightarrow T)$	
Cessation	$C \Rightarrow \Diamond \neg T$	
Avoidance	$\Box\ (C \Rightarrow \neg T)$	Safety

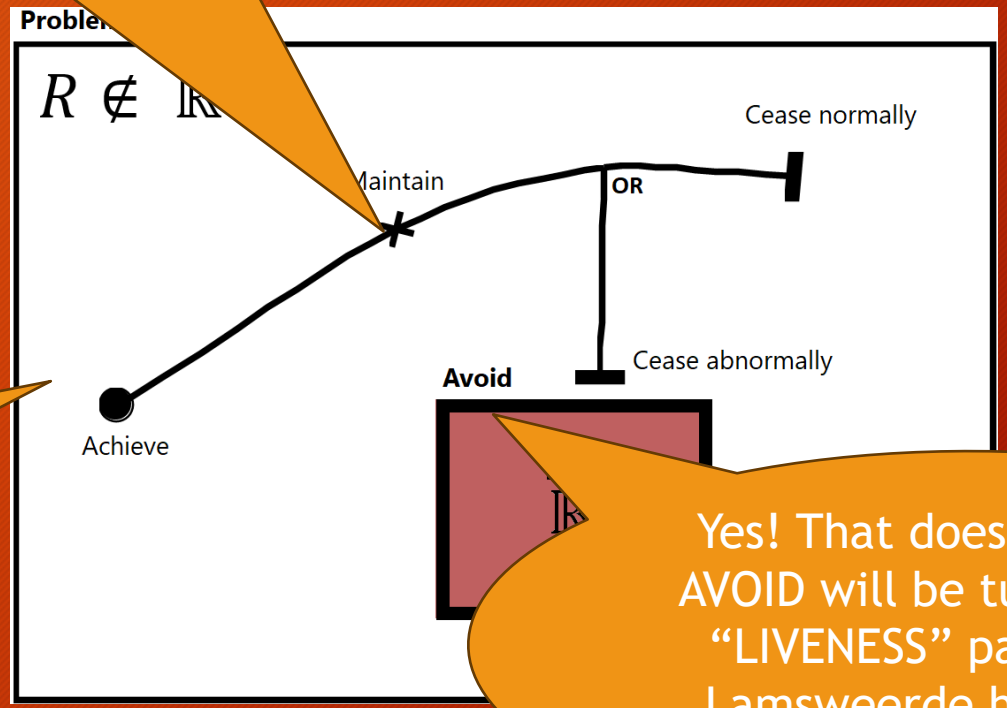


So, "spatially" the problem for liveness in specification is to AVOID states or conditions through definition of system behavior.

Liveness as

Essentially this is what Thomas suggests, when using the antithesis of the hazard to set "responsibilities" thence onto requirements.

Goal Oriented	Specification Oriented	Intended Properties
Attainment	$C \Rightarrow \Diamond T$	Liveness
Maintenance	$\Box\ (C \Rightarrow T)$	
Cessation	$C \Rightarrow \Diamond \neg T$	
Avoidance	$\Box\ (C \Rightarrow \neg T)$	Safety



So, "spatially" the problem for liveness in specification is to AVOID states or conditions through definition of system behavior.

Yes! That does mean that AVOID will be turned into a "LIVENESS" path, as van Lamsweerde has already described.

Decomposition with Argumentation (Jackson, Hall, Rapanotti)

$$\frac{W_1, CA_1, S_1 \vdash R_1;\ \ldots; W_n, CA_n, S_n \vdash R_n}{W, J, S \vdash R}$$

So, we use a means directed approach to decompose our requirements

Decomposition with Argumentation (Jackson, Hall, Rapanotti)

And thereby our specifications are decomposed.

$$\frac{W_1, CA_1, S_1 \vdash R_1;\ \ldots; W_n, CA_n, S_n \vdash R_n}{W, J, S \vdash R}$$

Decomposition with Argumentation (Jackson, Hall, Rapanotti)

$$\frac{W_1, CA_1, S_1 \vdash R_1;\ \ldots; W_n, CA_n, S_n \vdash R_n}{W, J, S \vdash R}$$

With an explanation that justifies the "fitness-for-purpose" of S_n towards entailment of J.

Decomposition with Argumentation (Jackson, Hall, Rapanotti)

$$\frac{W_1, CA_1, S_1 \vdash R_1;\ \ldots; W_n, CA_n, S_n \vdash R_n}{W, J, S \vdash R}$$

That is ..

$$CA_1, \ldots, CA_n \vdash J$$

Homage to "cases" if kept as separate argument from the design graph.

Decomposition with Argumentation (Jackson, Hall, Rapanotti)

$$\frac{W_1, CA_1, S_1 \vdash R_1;\ \ldots; W_n, CA_n, S_n \vdash R_n}{\qquad\qquad}$$

Appears have missed the memo on non-monotonic reasoning?

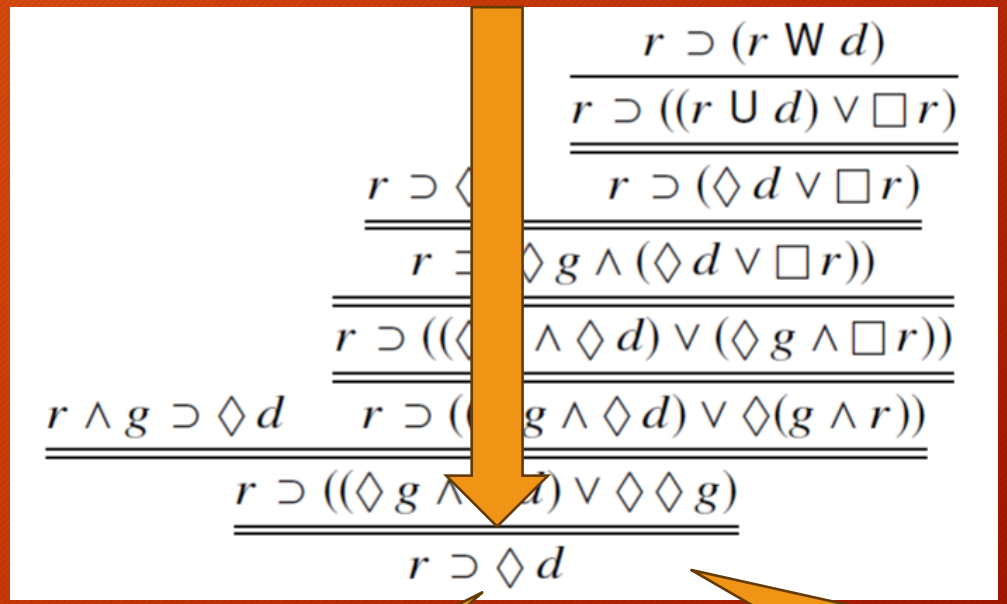
$$CA_1, \ldots, CA_n \vdash J$$

The illusion

$$\frac{W_1, CA_1, S_1 \vdash R_1 \quad \ldots \quad W_n, CA_n, S_n \vdash R_n}{W, J, \ldots \vdash R}$$

Means-Directed decomposition with "rationale" to find $S_{1..n}$

Top-Down Explanation?



Bottom-Up Justification?

Structured Argument or Proof of "root"

Skeptical Consequence

Provides the quality of Indefeasibility (Rushby)

Non-Monotonic Reasoning operator

Meaning by argumentation, not by mathematical proof per se.

$$W, S_o^c \vdash\!\sim R$$

With the quality of a monotonic non-decreasing function providing proof of satisfaction of top goal.

Problem Oriented is Goal Oriented

$$W_{[P]}, G \vdash\sim P$$
$$W_{[G]}, R \vdash\sim G$$
$$W_{[R]}, S \vdash\sim R$$

van Lamsweerde has already proposed this

Reflects the influence of the 6 Variable Model

Preserves the previously sacrosanct expression

We essentially expand the model to give us a means-directed abstraction hierarchy

Everything old is new again

Control Theoretic

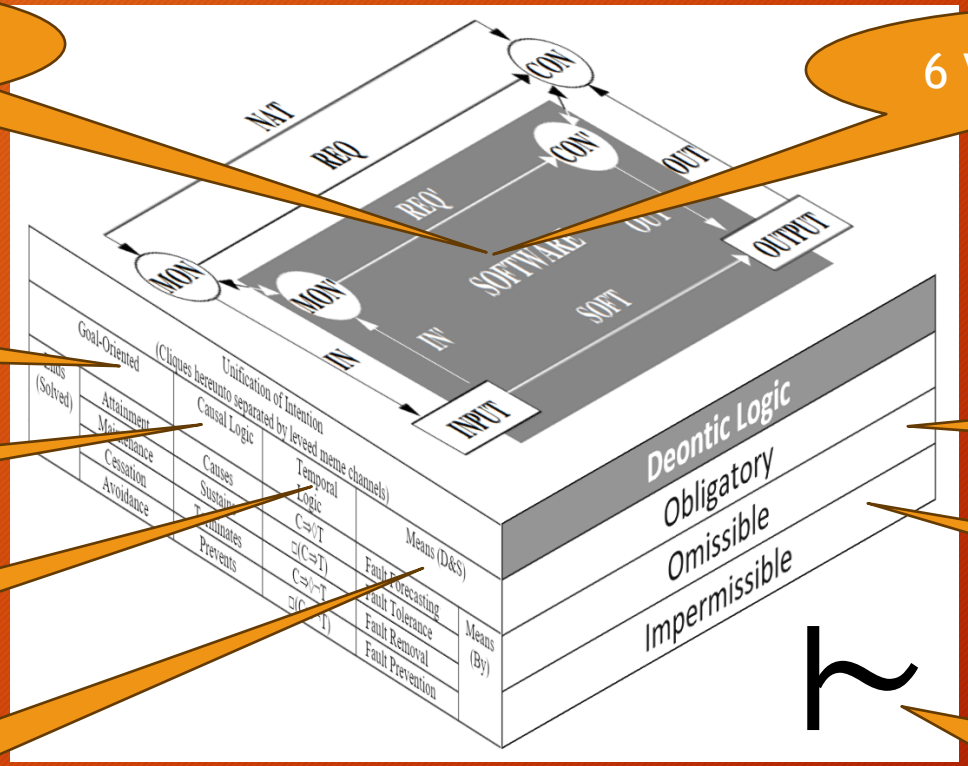
6 Variable Model

Goal Intention

Semi-Formal Causal Logic

Temporal Logic

Tactics



Optional, possibly risky

"Avoid"

Just needs non-monotonic reasoning weaved throughout

Next Steps

- As mentioned previously:
  - Phase 2: Develop a meta-model, or as the Problem Frame community would have it, a Domain and Requirement Description Language (are we there yet? Will need iterating between the theory and the DRDL).
  - Phase 3: Develop a graphical goal-oriented notation that embodies the theoretics, taking care with both the semantics and the semiotics (will we ever get there? Certainly, there is a candidate notation already available, but may need modification. It will need be vetted against the DRDL to scope the changes or decide upon a clean slate).

Enquiries?

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

References in report at: https://ascsa.org.au/conferences/2023/#technical-program