Towards a Tool for Managing Validation Arguments in Systems Engineering

Dan Shapiro, Bryan Mesmer, Nicholaos Jones,
Paul Collopy, Jennifer Stevens

The University of Alabama in Huntsville

daniel.g.shapiro@gmail.com

Outline

- Validation vs Verification in Systems Engineering
    - Validation contexts
- Argument model structure
- Ideas enabling an argumentation tool
    - A vocabulary of primitive argument types
    - Constructing validation arguments by template instantiation
    - Evaluating argument models into probabilities over beliefs
    - Adding uncertainties and decisions to argument models
- Related work
- Next steps

Validation vs Verification in Systems Engineering

Colloquially:

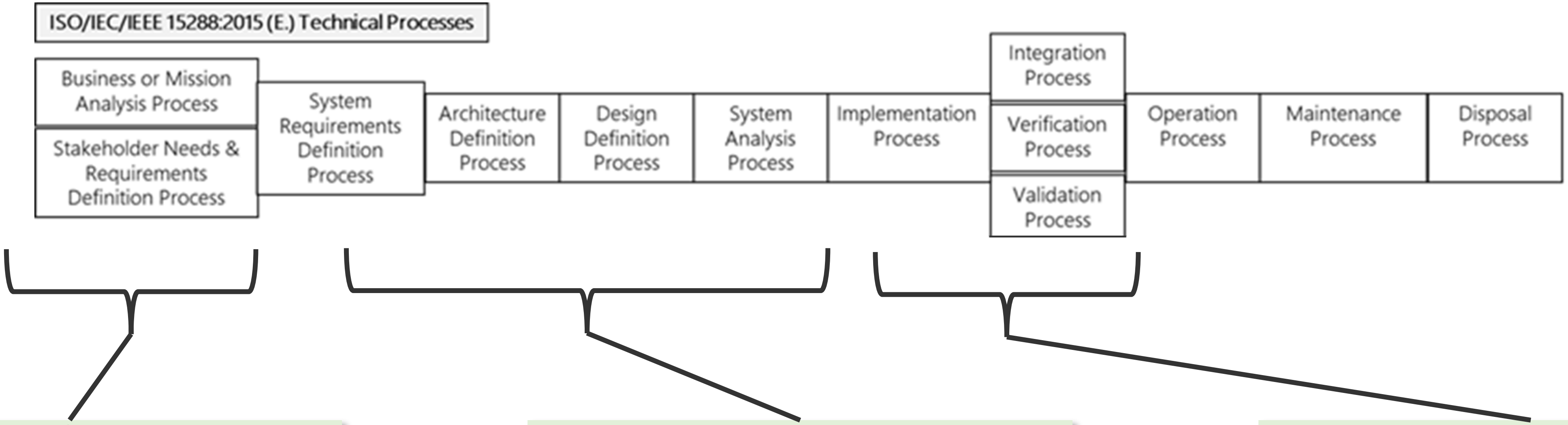
Verification: the process of determining that an artifact meets its stated requirements

Validation: the process of determining that an artifact will perform its intended tasks in the world

Properties of Validation

- Involves stakeholder preferences
- Requires judgment calls
- Concerns abstract and prospective claims about artifacts
- Concerns performance in environments that are often partially modeled and understood
- A system can meet requirements and still not be valid

Validation Arguments by Context


ISO/IEC/IEEE 15288:2015 (E.) Technical Processes
Business or Mission Analysis Process
Stakeholder Needs & Requirements Definition Process
System Requirements Definition Process
Architecture Definition Process
Design Definition Process
System Analysis Process
Implementation Process
Integration Process
Verification Process
Validation Process
Operation Process
Maintenance Process
Disposal Process

Program definition

- Back-of-the-envelope architecture
- Forming Coalitions
- Getting Stakeholder Buy-in, support
- Preliminary studies, concept studies

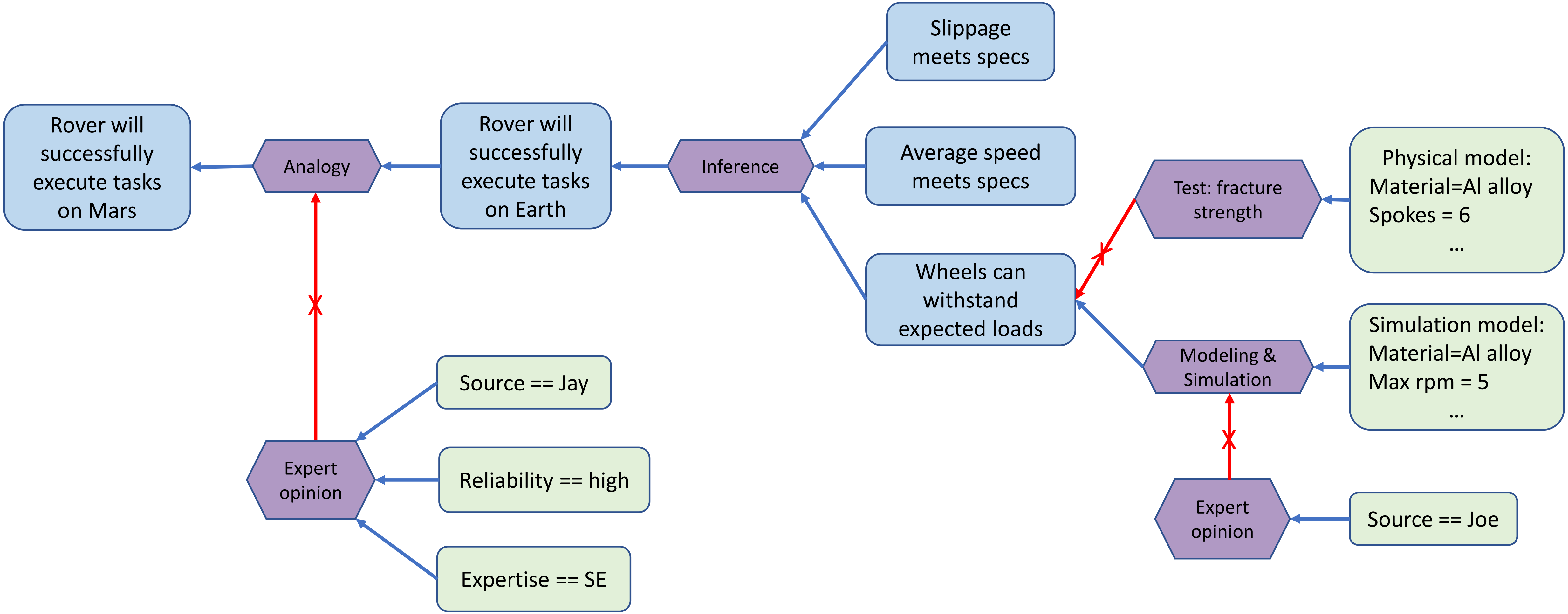
Artifact design

- Conceptual designing
- Program Planning
- Preliminary Design Review (PDR)
- Critical Design Review (CDR)

End-artifact evaluation

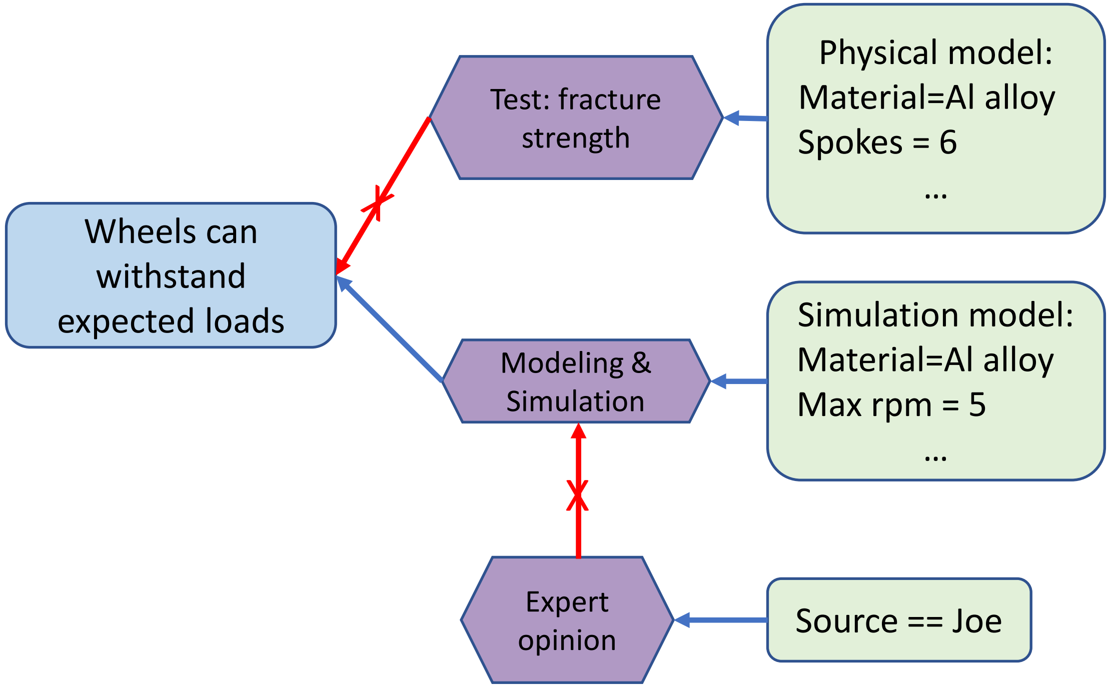
- Design certification (DCR, Acceptance)
- Test
- Demonstration

A Validation Argument Example



Argument Model Structure

- Toulmin[1] argument models contain claims, premises, evidence and warrants
  - Claims, premises & evidence encode beliefs
  - Warrants are justifications – reasons why we should believe the claims given the premises
- Warrants can support or attack premises, claims, or other warrants



1. *Toulmin, S. E. (1958). The use of arguments. Cambridge: University Press.*

Everyday Warrants (Proof Standards)

- Trial by combat (I’m right because my champion is stronger)
- Proof by sigil (a recognized authority says it is good)
- Proof by social norm (we have always done it this way)
- Proof by demonstration ($3B sold; 30-year track record; flashy example)

Proof by Pumpkin

- A specialization of proof by demonstration

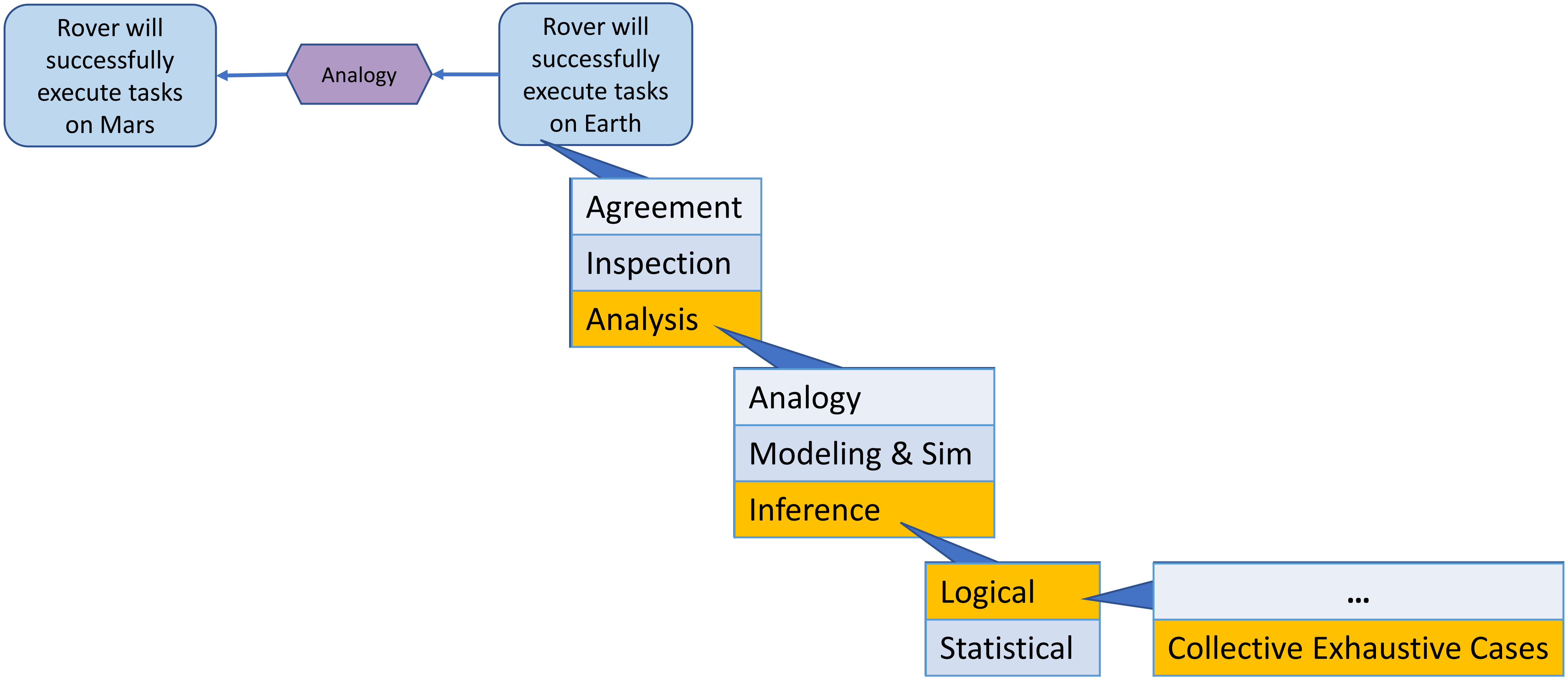
Warrant Types in Systems Engineering

Conjecture: systems validation employs a small vocabulary of warrant types that capture engineering standards of proof. They can be represented by a hierarchy with inheritance of critical questions (CQs) that determine if the warrant is apt.

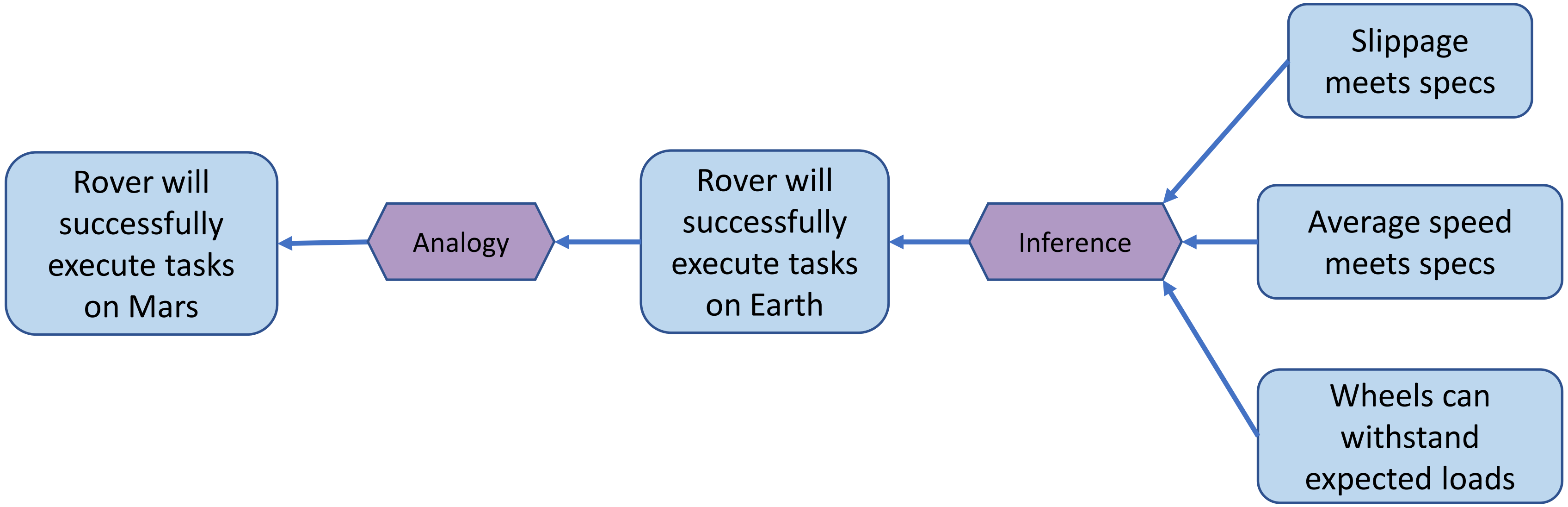
Warrant Type			Critical Questions
AGREEMENT			Is claim subject to agreement?
	Attestation		Is the claim knowable?
		Expert Opinion	Is the expert relevant to the claim?
		Common Knowledge	Are there exceptions to the rule in this context?
	Assumption		Is the claim reasonable, material & convenient?
	Declaration		Does the agent have the authority to assert the claim?
INSPECTION			Is the claim knowable via inspection?
	Demonstration		Is the demonstration representative of the use case?
	Test		Does the test address the claim? Are there defeating cases?
ANALYSIS			Is the claim subject to analysis?
	Analogy		Are the source and target environments, tasks, and systems sufficiently close?
	Modeling & Sim		Does the simulation address the claim? Are there defeating conditions?
	Inference		Is the inference cogent? Are there defeating facts?

Constructing Validation Arguments by Template Instantiation

- Select Warrants appropriate to a claim

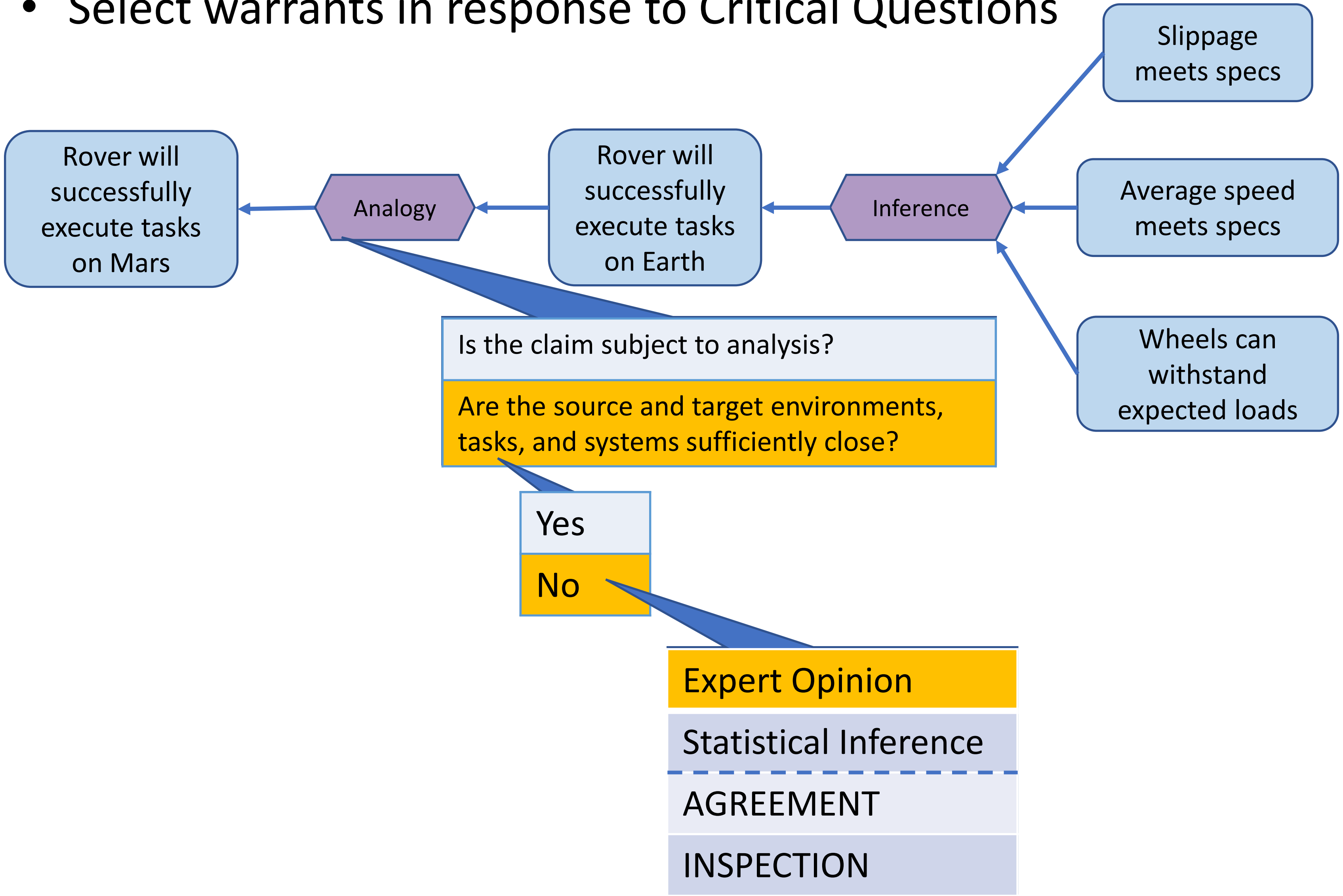

Rover will successfully execute tasks on Mars
Analogy
Rover will successfully execute tasks on Earth
Agreement
Inspection
Analysis
Analogy
Modeling & Sim
Inference
Logical
Statistical
…
Collective Exhaustive Cases

Constructing Validation Arguments by Template Instantiation


Rover will successfully execute tasks on Mars
Analogy
Rover will successfully execute tasks on Earth
Inference
Slippage meets specs
Average speed meets specs
Wheels can withstand expected loads

Constructing Validation Arguments by Template Instantiation

- Select warrants in response to Critical Questions



Slippage meets specs

Rover will successfully execute tasks on Mars

Analogy

Rover will successfully execute tasks on Earth

Inference

Average speed meets specs

Wheels can withstand expected loads

Is the claim subject to analysis?

Are the source and target environments, tasks, and systems sufficiently close?

Yes

No

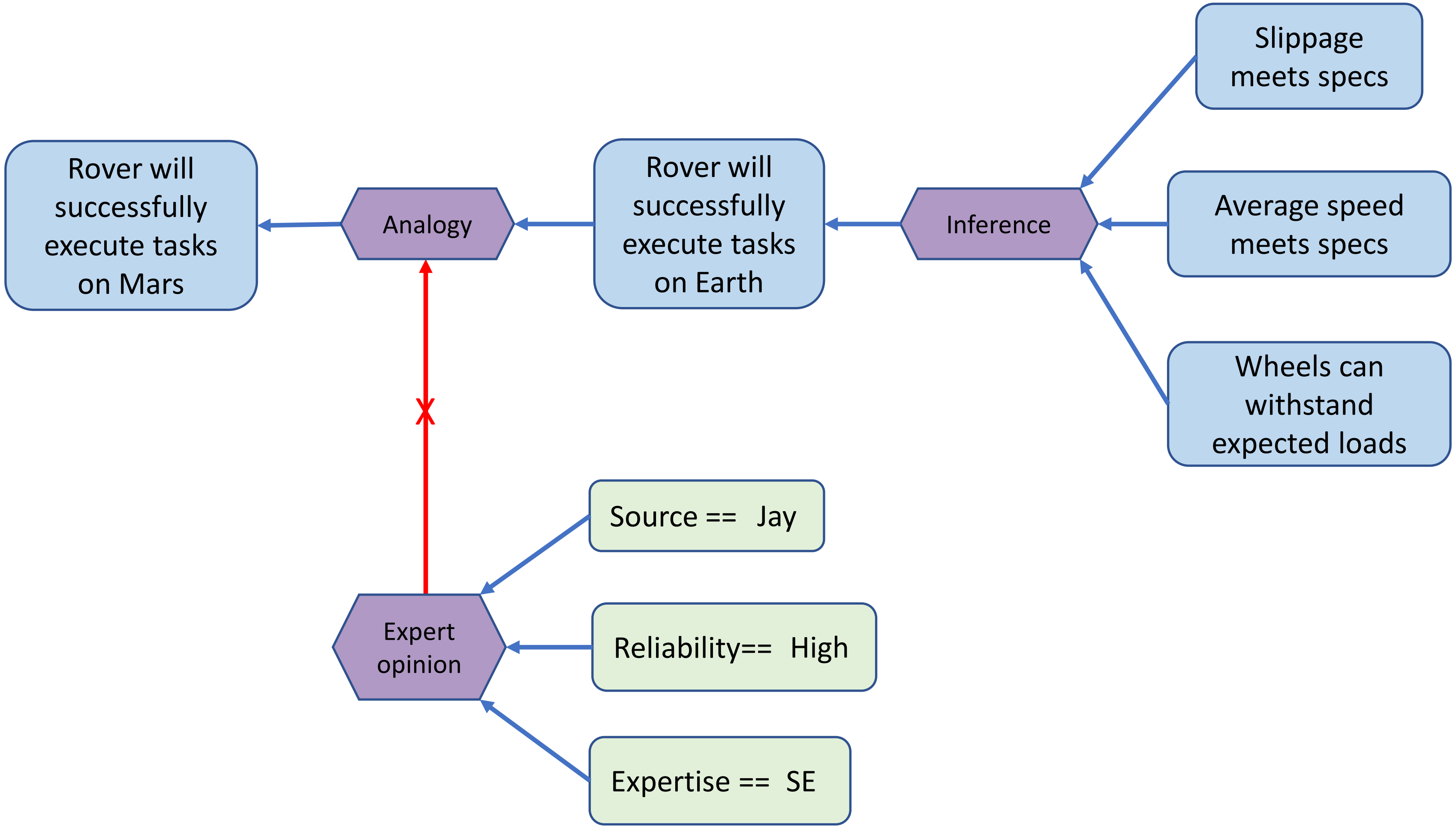
Expert Opinion

Statistical Inference

AGREEMENT

INSPECTION

A Validation Argument Example

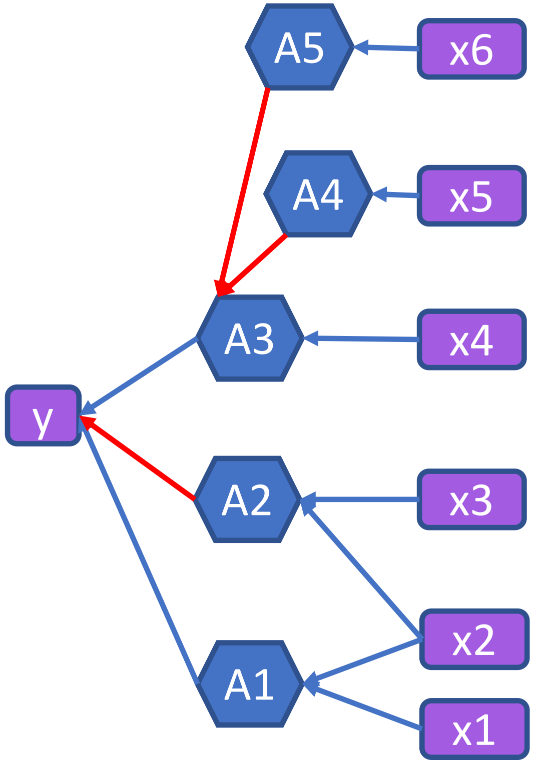

Rover will successfully execute tasks on Mars
Analogy
Rover will successfully execute tasks on Earth
Inference
Slippage meets specs
Average speed meets specs
Wheels can withstand expected loads
X
Expert opinion
Source == Jay
Reliability== High
Expertise == SE

Evaluating Argument Models

- Determine what to believe given conflicting rationale
- Identify a probability distribution over beliefs (novel in argument models)
- One equation, applied recursively to assess the probability of claims, premises, and that warrants are *apt*

$$\boldsymbol{p(y)} = \sum_{\vec{E}} \boldsymbol{p}\left(y \middle| \vec{E}\right) \boldsymbol{p}\left(\vec{E}\right)$$

for $\vec{E}$ in truth values of antecedents(y)



Determine the Probability of a (Leaf) Premise

- Directly assess leaf nodes (subjectively or statistically)

Reliability (Joe) == high

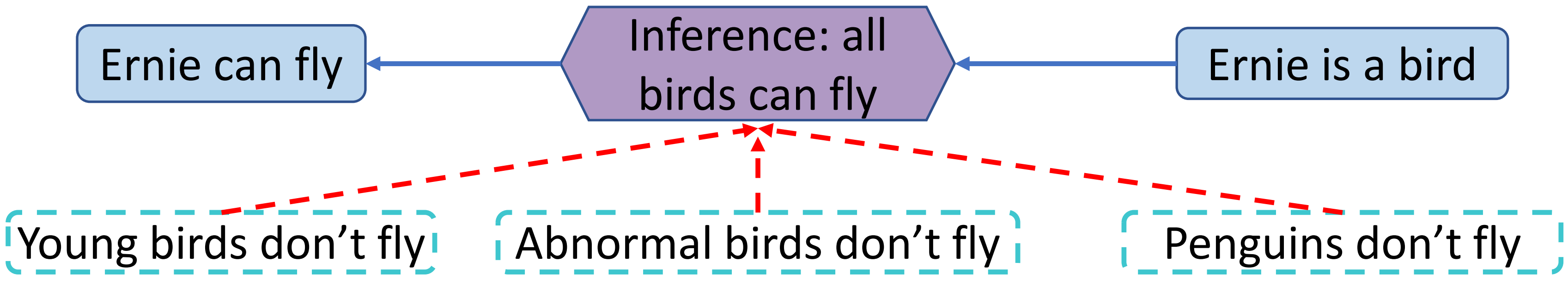
0.8

Simulation model:
Material=Al alloy
Max rpm = 5
…

1.0 (given)

Assessing the Probability of a Warrant

- A warrant is *apt* if it is a relevant model for drawing conclusions in the context



- If all you know is “Ernie is a bird”, what is the probability “all birds can fly” is a good model for drawing conclusions about Ernie?
  - Formally, the probability that no observation will invalidate the defeasible inference represented by the warrant

This assessment is independent of the warrant’s conclusion.
It concerns the applicability of the model.

Determine the Probability that a Warrant is Apt

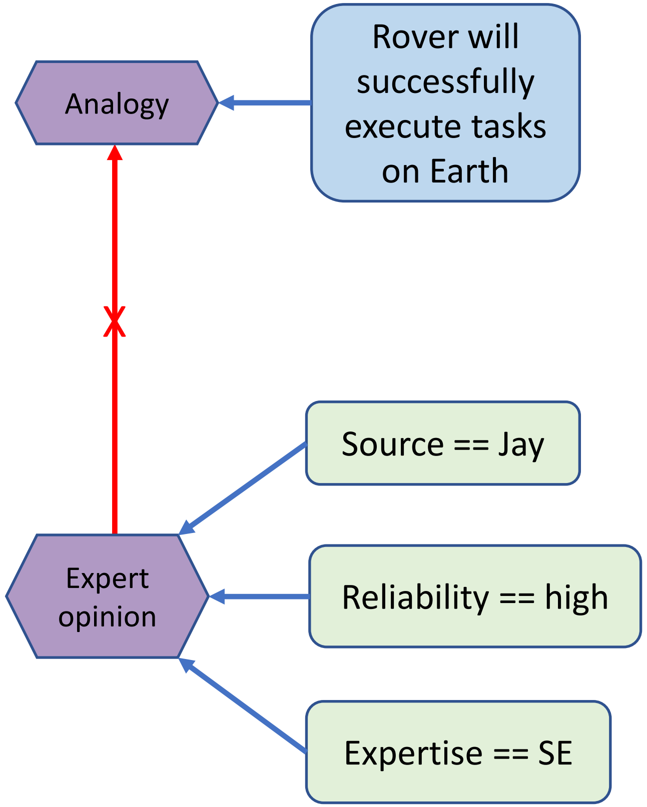
- Given the premises of a warrant, and all combinations of arguments against it, how likely is the warrant apt?

Let A == Analogy is apt
R == Rover will successfully execute tasks on earth
E == Expert opinion is apt

$$p(A) = \sum_{R} p(A|R)p(R)$$

$$p(A) = \sum_{R,E} p(A|R,E)p(R)p(E)$$

Requires user assessment

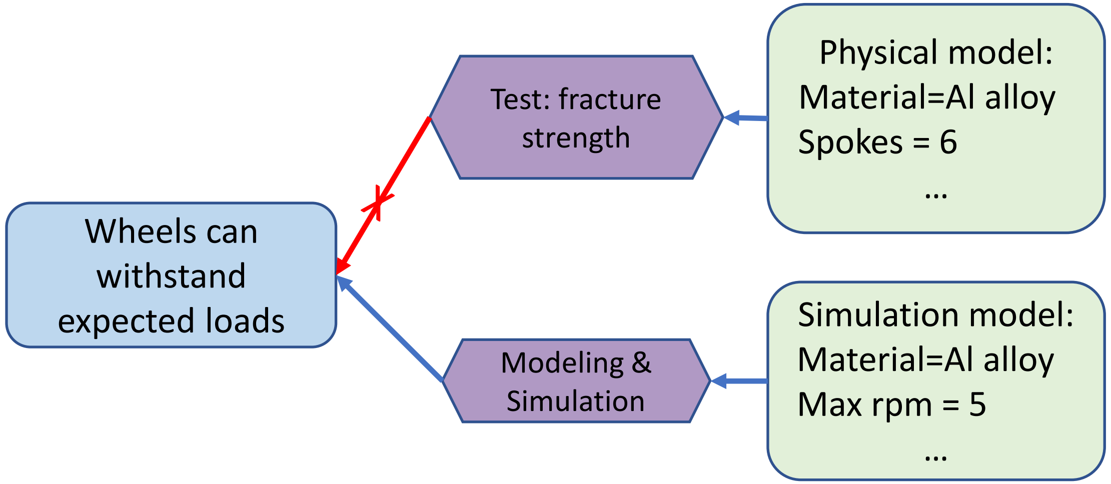


Determine the Probability of a Claim/Premise

- Find p(y)==“wheels can withstand expected loads” given all combinations of arguments pro and con

Let TFS == test warrant showing fracture strength < load is apt

MS == simulation warrant showing wheels withstand loads is apt



Wheels can withstand expected loads

Test: fracture strength

Modeling & Simulation

Physical model:
Material=Al alloy
Spokes = 6
…

Simulation model:
Material=Al alloy
Max rpm = 5
…

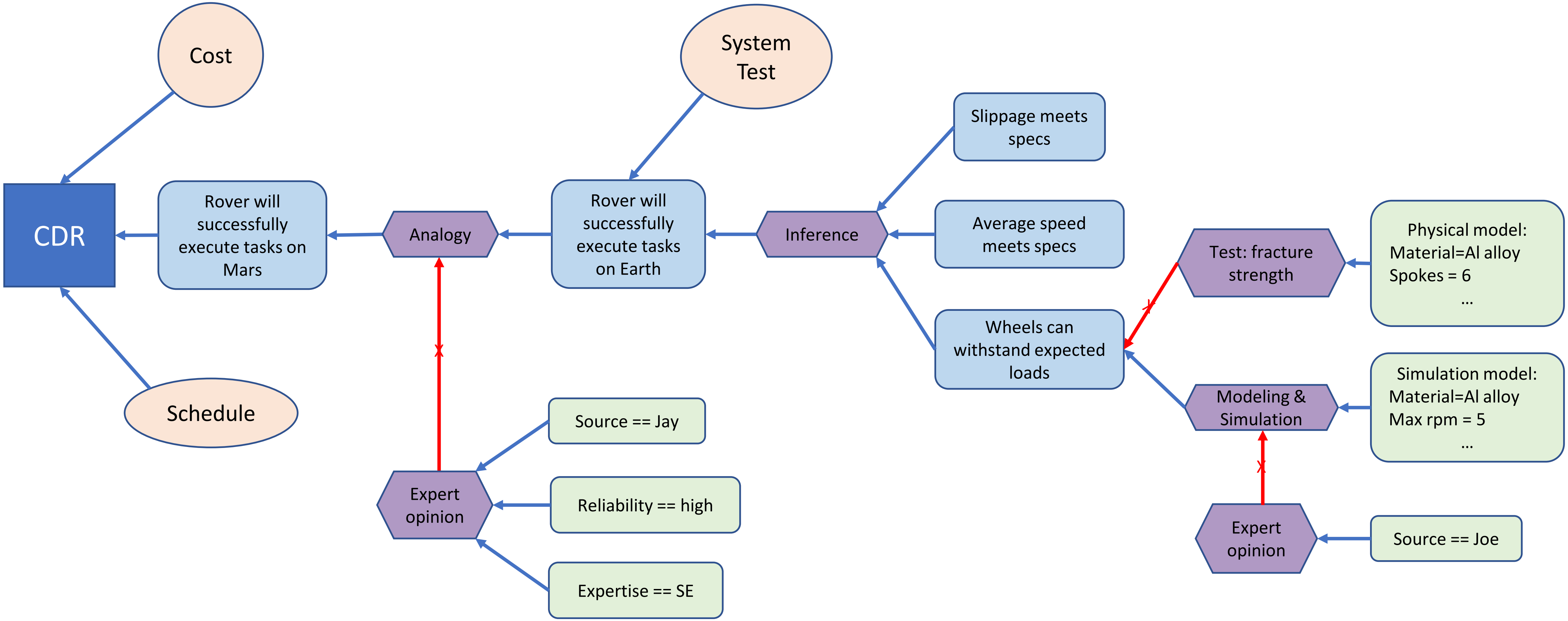
$$p(y) = \sum_{TFS,MS} p(y|TFS,MS)p(TFS)p(MS)$$

Requires user assessment

Adding Uncertainties and Decisions to Argument Models

- Assess the conditional probability of claims given additional uncertainties and the aptness of warrants pro and con
- Access standard methods for decision making under uncertainty given conflicting rationale

A Validation Argument with



Cost

System Test

Slippage meets specs

CDR

Rover will successfully execute tasks on Mars

Analogy

Rover will successfully execute tasks on Earth

Inference

Average speed meets specs

Test: fracture strength

Physical model:
Material=Al alloy
Spokes = 6
…

Wheels can withstand expected loads

Modeling & Simulation

Simulation model:
Material=Al alloy
Max rpm = 5
…

Schedule

Source == Jay

Expert opinion

Reliability == high

Expertise == SE

Expert opinion

Source == Joe

Related Work

- Structured argumentation tools for systems engineering
  - AdvoCate – Denney, E. and Pai, G. (2018) ‘Tool support for assurance case development’, Automated Software Engineering, vol. 25, no. 3, pp. 435–499.
  - ASCE – safety case construction https://www.adelard.com/partners_files/customer_collateral/MK95v10_ASCE_5.pdf
  - D-CASE Editor – a typed editor for assurance cases http://deos.or.jp/technology/D-CaseEditor/
- Argumentation in systems engineering
  - Ben Smith, Martin Feather and Terry Huntsberger. "A Hybrid Method of Assurance Cases and Testing for Improved Confidence in Autonomous Space Systems," AIAA 2018-1981. 2018 AIAA Information Systems-AIAA Infotech @ Aerospace. January 2018.
  - Feather, Martin S. et al. “Planning for V&V of the Mars Science Laboratory rover software.” 2004 IEEE Aerospace Conference Proceedings (IEEE Cat. No.04TH8720) 1 (2004): 682-697 Vol.1.
  - Graydon, P. J. and Holloway, C. M. (2016) An Investigation of Proposed Techniques for Quantifying Confidence in Assurance Arguments: NASA/TM–2016–219195.
  - Goodenough, J. B., Weinstock, C. B. and Klein, A. Z. (2013) ‘Eliminative Induction: A Basis for Arguing System Confidence’, 35th International Conference on Software Engineering (ICSE).
  - Bittmann, S., Barn, B. and Clark, T. (2014) ‘Domain–specific reasoning for method engineering based on Toulmin's argumentation theory’, International Journal of Knowledge and Learning, vol. 9, 1-2, pp. 104–123.
  - D. Shapiro, D., & Shachter, R. (2002). User-agent value alignment. Stanford Spring Symposium, Workshop on Safe Agent Learning.
- Argumentation more broadly
  - International Competition on Computational Models of Argumentation
  - Prakken, H., Wyner, A., Bench-Capon, T., & Atkinson, K. (2013). A formalisation of argumentation schemes for legal case-based reasoning in ASPIC+. *Journal of Logic and Computation*, first published online May 9, 2013 doi:10.1093/logcom/ext010

Summary

- Validation reasoning occurs in practice from systems conception through final artifact evaluation
- Toulmin style argumentation models capture validation reasoning for and against claims about system properties.
- Validation arguments involve a small number of fundamental warrant types
- They can be composed via a template-based editor that applies critiques (critical questions) to augment argument models
- We can evaluate validation arguments into a distribution over beliefs
- We can combine arguments for and against claims with decision models
- These building blocks enable creation of a tool for managing validation reasoning in systems engineering

Next Steps

- Build a prototype editing tool
  - Developers define primitive templates and associated constraints
  - Users (systems engineers) specialize and apply those templates to build validation arguments recorded in a library of reusable, domain-specific parts
- Illustrate potential benefit for managing validation process
  - Audit trail, validation status checks, clarity of reasoning
- Demonstrate benefit of merging argumentation with decision models
  - Show value of information for conducting a test to support a go/no-go decision in the presence of conflicting arguments
- Document work
  - A vocabulary of primitive systems validation arguments
  - A formal semantics for defeasible probabilistic reasoning in systems engineering
  - Systems validation as argumentation from program conception to deployment
  - The design of an argumentation tool for validation in systems engineering

Contact Information

Daniel Shapiro	daniel.g.shapiro@gmail.com
Bryan Mesmer	bryan.mesmer@uah.edu
Nicholaos Jones	nick.jones@uah.edu
Paul Collopy	paul.collopy@gmail.com
Jennifer Stevens	jennifer.s.stevens@nasa.gov