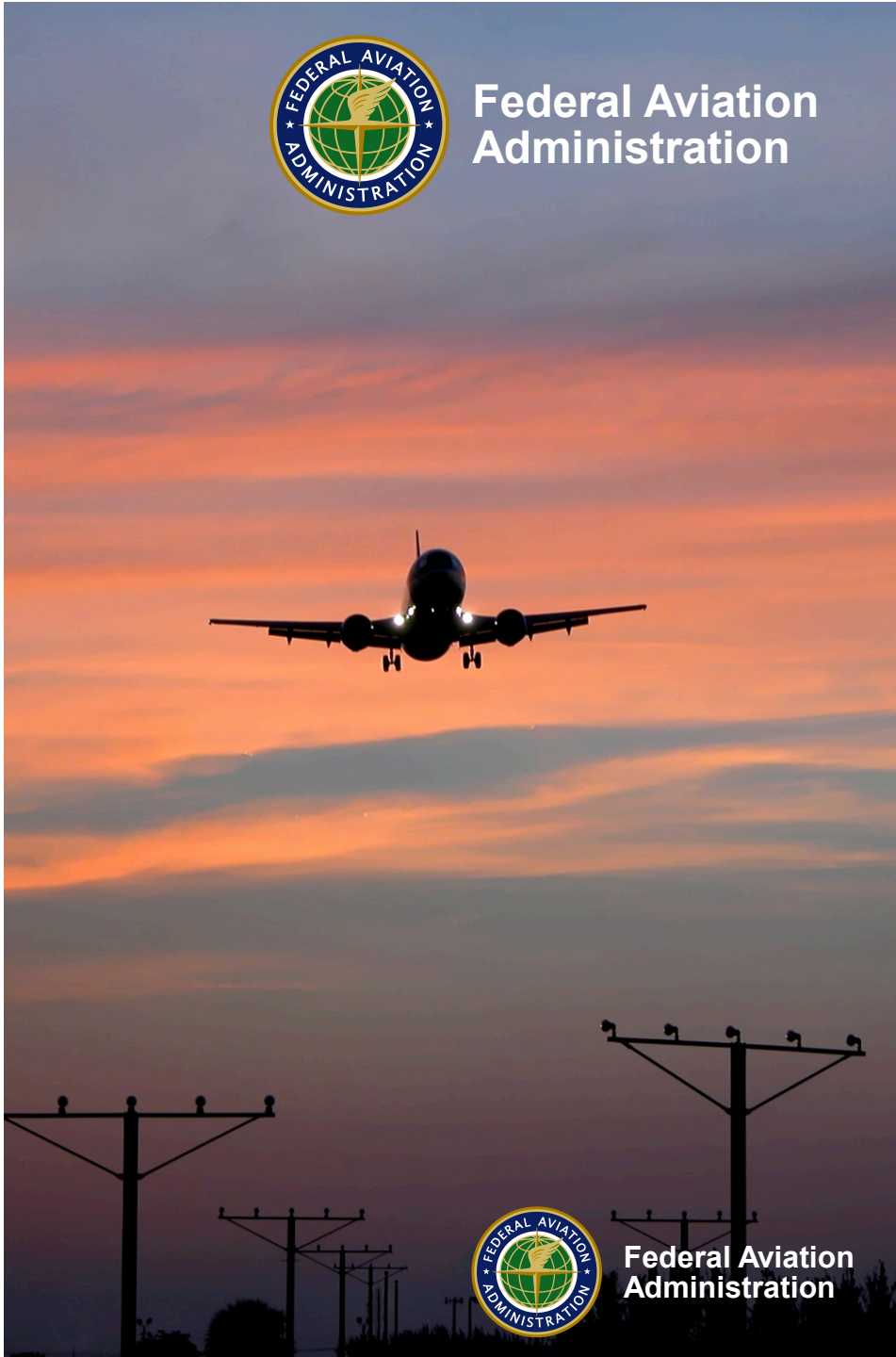
Software Assurance Challenges

George Romanski,

CSTA Aircraft Computer Software

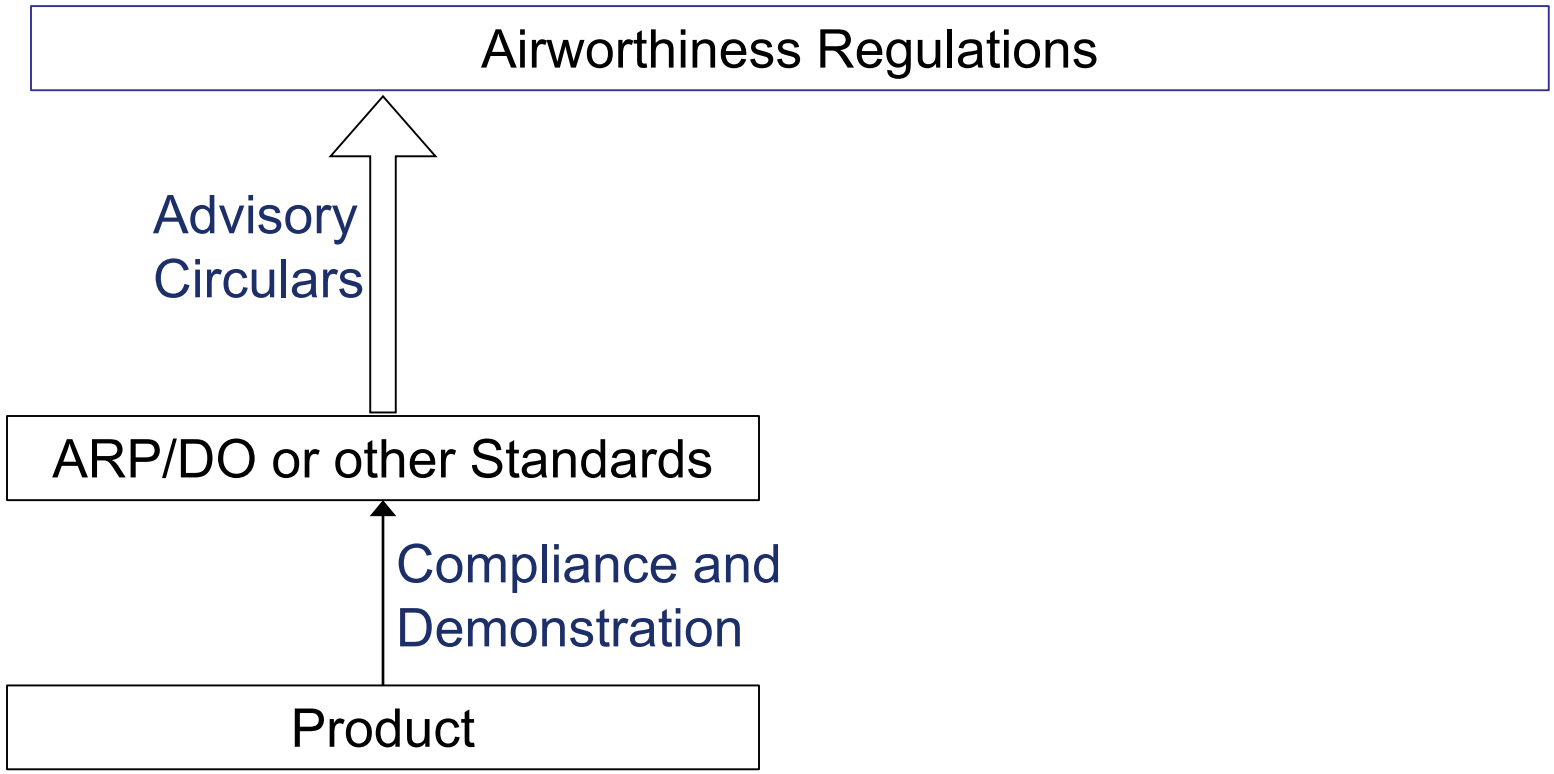
Date: August, 2019



Building trust in Software

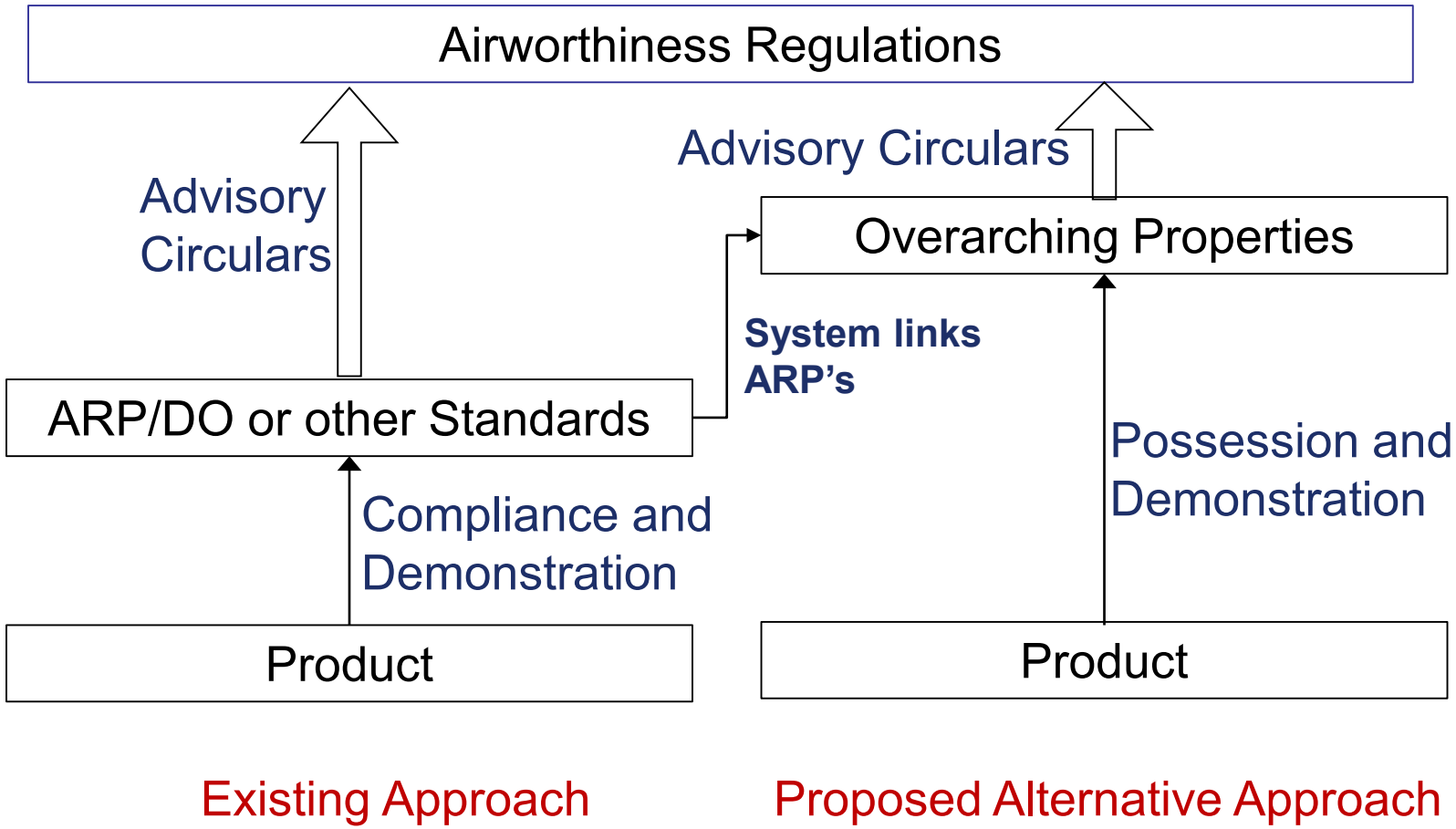
- Current approach to Software:
  - Lots of experience over many years
  - Very conservative design and implementation
  - Established guidelines understood well (mostly)
  - Prescriptive approach (everyone knows what to do)
  - Verification - Completion criteria understood
- What makes it hard?
  - Hard to scale up
    - But it's growing in size
    - Increasing complexity
  - Technology base is growing

Obtaining Approval - Current



Existing Approach

Obtaining Approval – Overarching Properties



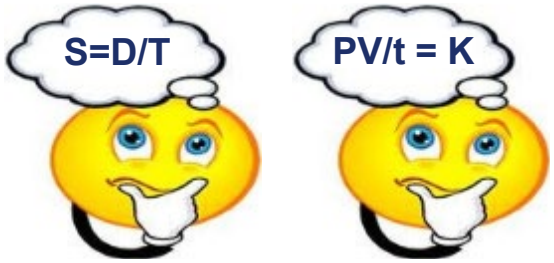
US Federal Aviation Regulations

- Parts 23 (General Aviation), Part 25 (Transport), Part 27 (Rotorcraft), Part 29 (Transport Category Rotorcraft)…
- “The equipment, systems, and installations must be designed and installed to ensure they perform their intended functions under all foreseeable operating conditions”

Overarching Properties

Stakeholder Needs

- What we think we want !
- Intended Behavior,
- Requirements

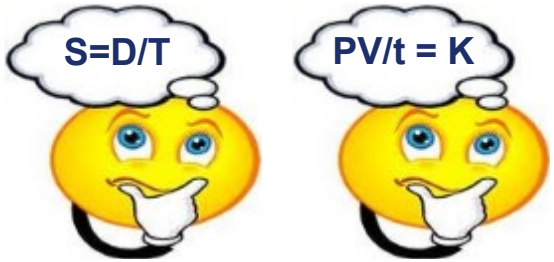


- Customers
- Subject Matter Experts
- Users

Overarching Properties

Stakeholder Needs

- What we think we want !
- Intended Behavior,
- Requirements



- Customers
- Subject Matter Experts
- Users

Recorded

Reviewed
Validated

1

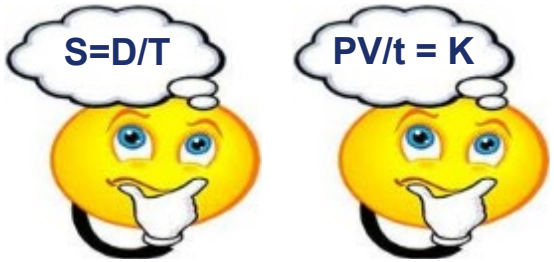
Defined Intended Behavior

Intent Property

Overarching Properties

Stakeholder Needs

- What we think we want !
- Intended Behavior,
- Requirements



- Customers
- Subject Matter Experts
- Users

Recorded

Reviewed Validated

1 Defined Intended Behavior

Intent Property

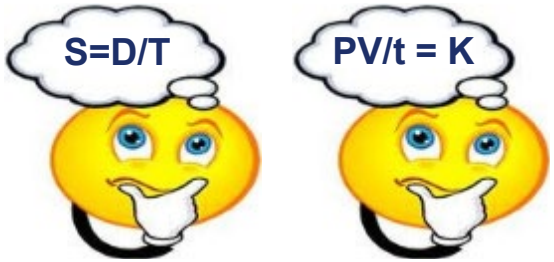
2 Correct Implementation

Correctness Property

Overarching Properties

Stakeholder Needs

- What we think we want !
- Intended Behavior,
- Requirements



- Customers
- Subject Matter Experts
- Users

Recorded

Reviewed Validated

1 Defined Intended Behavior

Intent Property

- **No Extraneous Behavior**
- **Or if present, then it does not compromise safety**

3

2 Correct Implementation

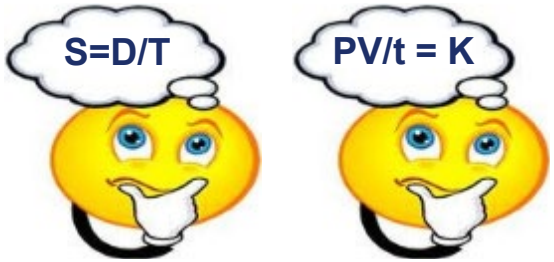
Correctness Property

Innocuity Property

Overarching Properties

Stakeholder Needs

- What we think we want !
- Intended Behavior,
- Requirements



- Customers
- Subject Matter Experts
- Users

Recorded

Reviewed
Validated

1

Defined Intended Behavior

Intent Property

No Implied Order

- **No Extraneous Behavior**
- **Or if present, then it does not compromise safety**

3

2

Correct Implementation

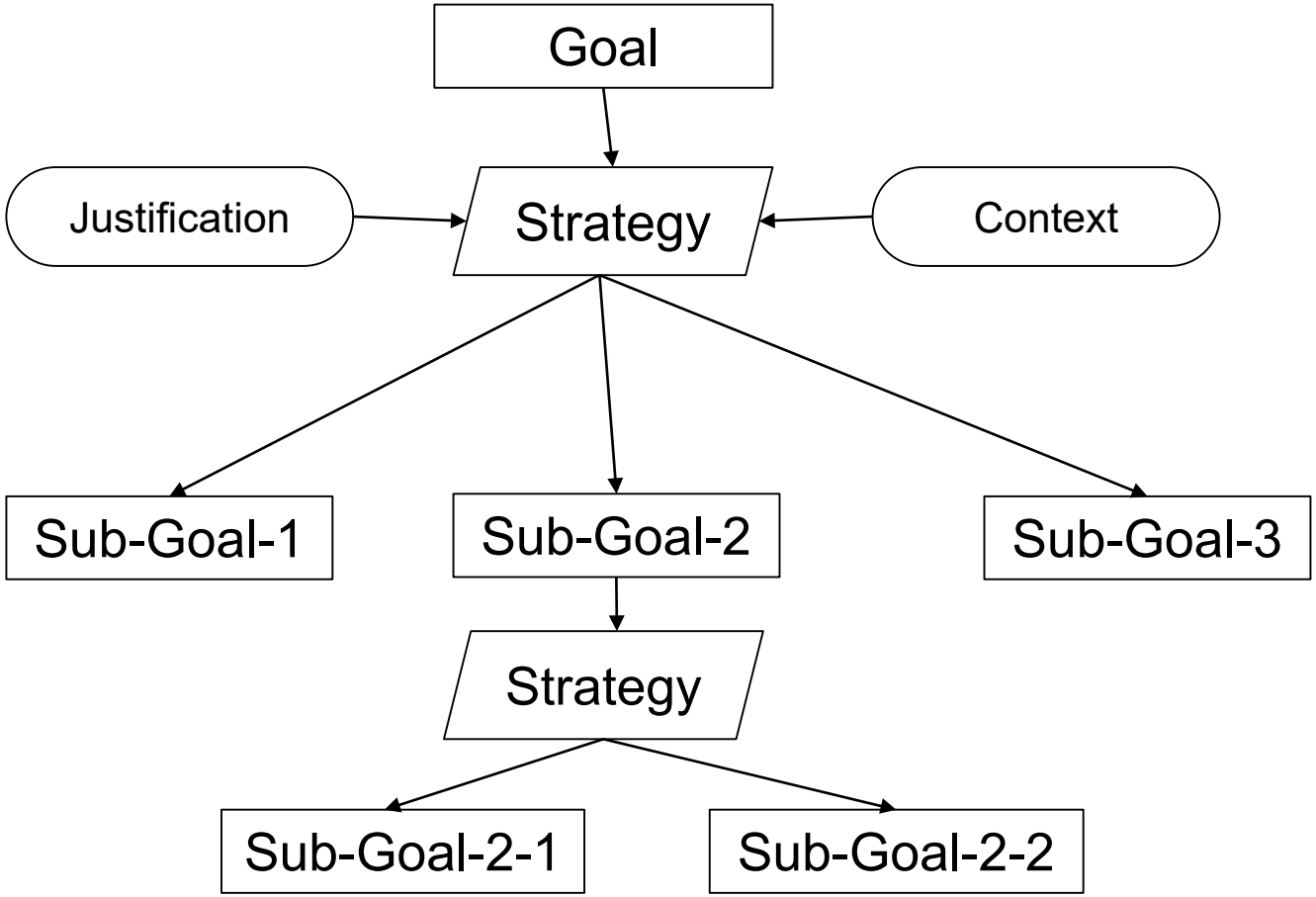
Correctness Property

Innocuity Property

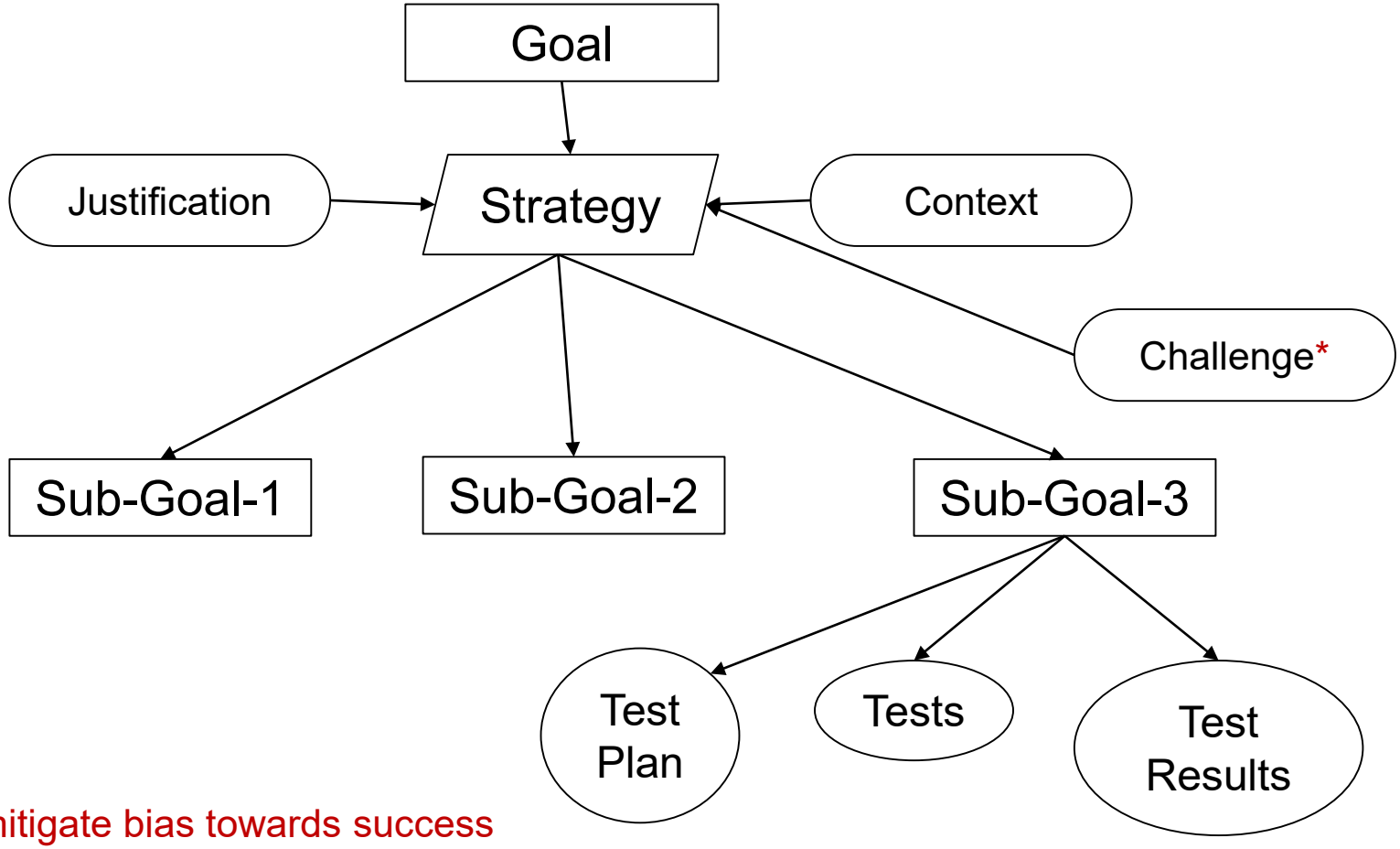
How to show Product “Posesses” the properties

- Build Assurance Case
  - Communicates a line of reasoning which ties the ownership of the OPs to evidence
  - Should be a structured, **compelling** argument
- Many notations exist
  - Goal Structuring Notation (GSN)
  - Toulmin
  - Etc.
- Structured Text proposed
  - Can be manipulated by tools
  - Can be translated to graphical forms

Goal Structuring Notation



Goal Structuring Notation



* To mitigate bias towards success

Templates and Evidence Schemes

- Developing an approach to produce Assurance Case Templates
- Template Catalog
  - Will help Assurance case adoption
  - Lower cost of certification through reuse

Note!

Assurance Case Templates will help with Understanding the Argument

Verification evidence still required (e.g. Testing)

Bounding Behavior at higher level

- Use “Safety Nets” around non-deterministic part of system
- Multiple monitors possible (with voting?)
- System boundary used in Safety Case
  - Safety properties more exposed
  - Software elements can cross check
  - Helps lower Assurance levels (without compromising safety)

Positions are not fixed – yet!

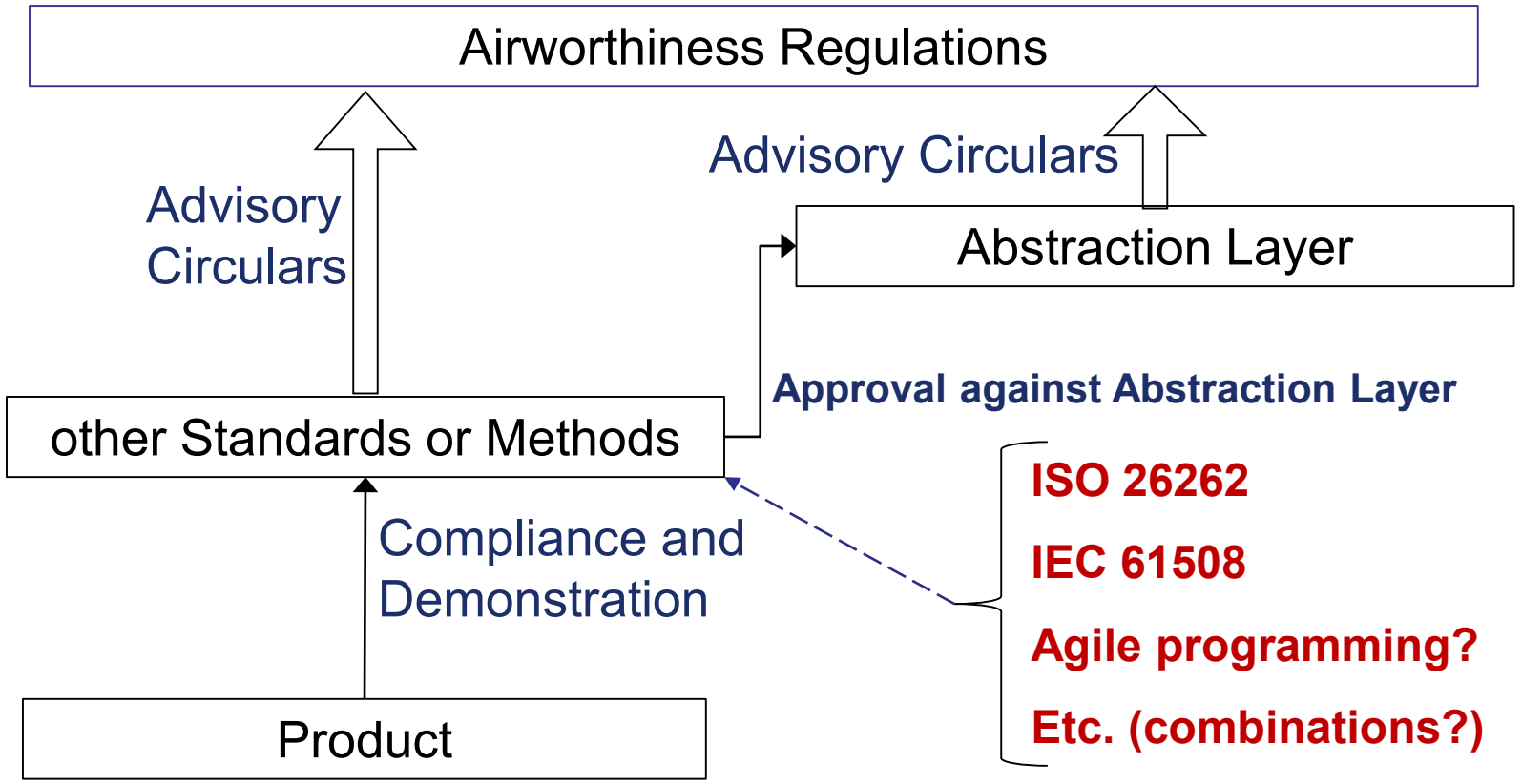
- Some
  - Looking to offer more flexibility for applicants
  - Use of Risk based process adjustments
  - Use of Risk based architecture adjustments
- Other
  - Concerns with applicants having more flexibility:
    - Lack of approval uniformity
    - Hard to educate auditors to reach consistent approval
    - Cannot reach legal approval obligations

Still a work in Progress

Use Case trials continue

- RESSAC project
  - Components of small UAS
  - Assurance case constructed (partial)
  - Concluded that Assurance case was better than mapping to “Criteria”
- Geofencing application
  - Work done at NASA
  - Assurance case built
  - Evidence cases were proposed but not completed for the entire project.
- Other projects underway and expected to start soon

Obtaining Approval – Alternative Approach



Abstraction Layer Task Force

- Just started
- FAA, EASA Industry
- Small “focused” group
- Using “Essence” of DO documents (rationale)
  - Recorded and
  - Implied
- Willing to learn from other industries/domains
- Offers more flexibility to Applicants
- Expands stable bases for Authorities