Raytheon Technologies

Assured Autonomy: Need for engineering methods

Alessandro Pinto, Technical Fellow
Raytheon Technologies Research Center

NSF-PIRE Workshop – June 9, 2021

This document does not contain any export controlled technical data.

Raytheon Technologies: focused A&D company

Industry leading segments positioned for long-term value

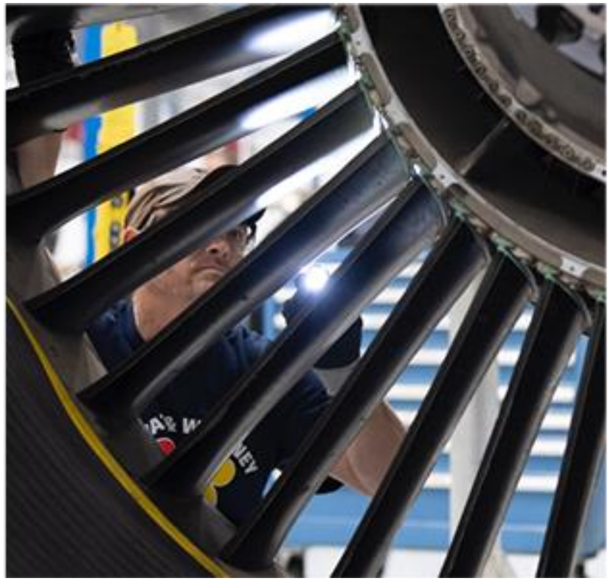
Collins Aerospace

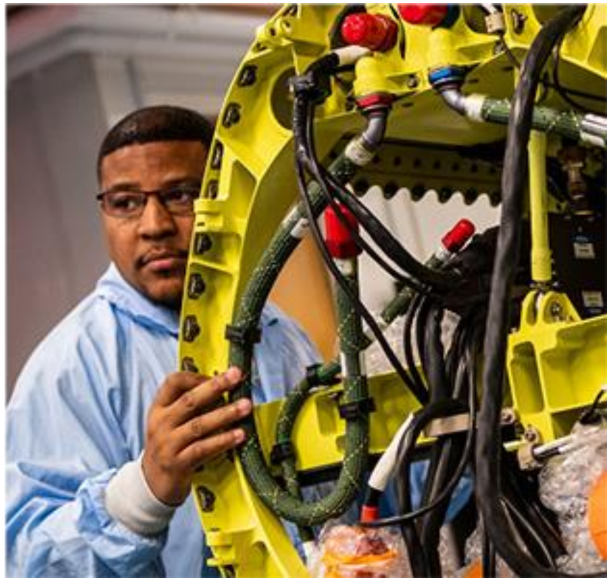
Raytheon Intelligence & Space

Pratt & Whitney

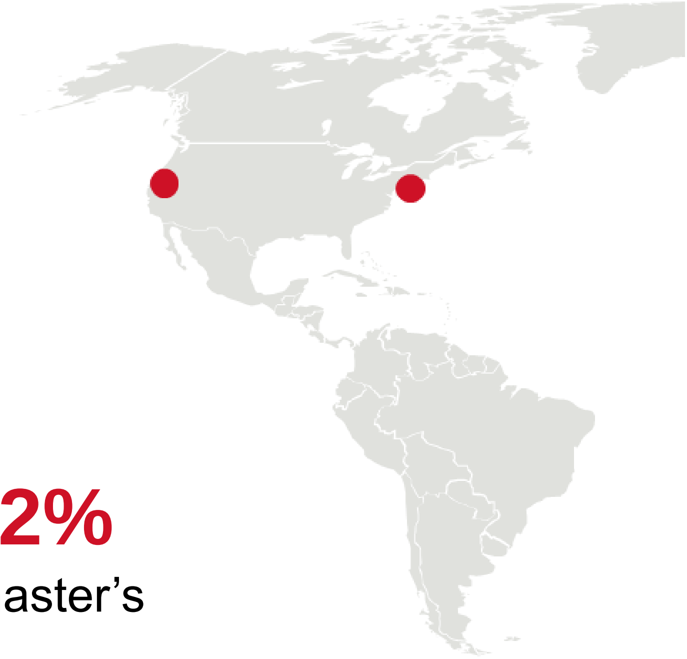
Raytheon Missiles & Defense

- Creates the world's most advanced aerospace and defense systems provider.
- Serves customers worldwide through a platform-agnostic, balanced and diversified portfolio.
- Delivers breakthrough technologies at an accelerated pace across high-value areas of A&D.
- Attractive financial profile with strong balance sheet and long-term cash flow generation.





Raytheon Technologies Research Center
Talent and locations



~300

Employees

85%

advanced degrees

69%

Doctorate

12%

master’s

East Hartford, Connecticut

Founded in 1929

Focuses on a broad range of system engineering, thermal, fluid, material and informational sciences

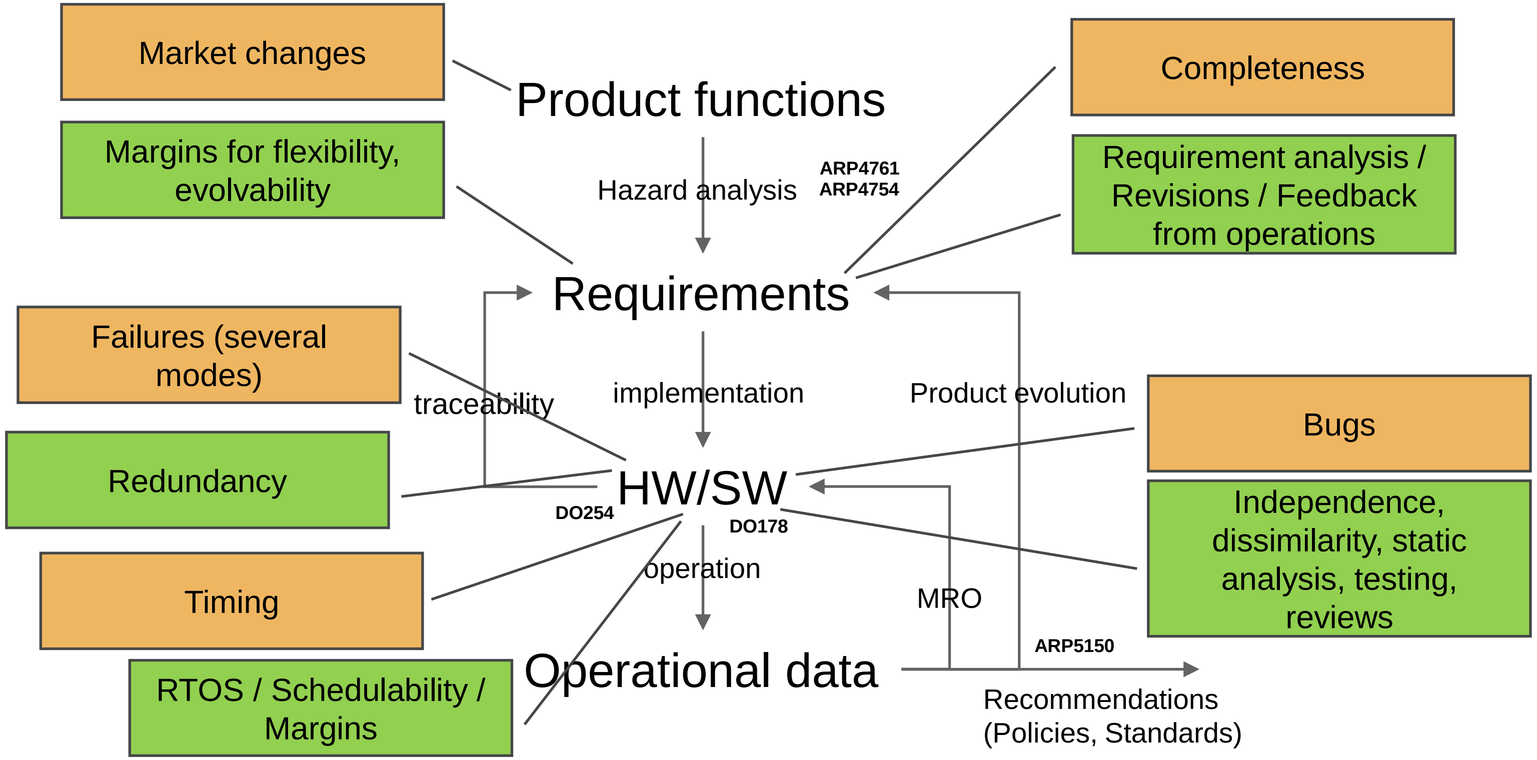
Berkeley, California

Established in 2009

Focuses on cyber- physical systems and embedded intelligence

This page does not contain any export controlled technical data.

Dealing with uncertainty – A traditional view



Market changes

Margins for flexibility, evolvability

Product functions

Hazard analysis

ARP4761
ARP4754

Completeness

Requirement analysis / Revisions / Feedback from operations

Requirements

Failures (several modes)

traceability

implementation

Product evolution

Bugs

Redundancy

HW/SW

DO254

DO178

Independence, dissimilarity, static analysis, testing, reviews

Timing

operation

MRO

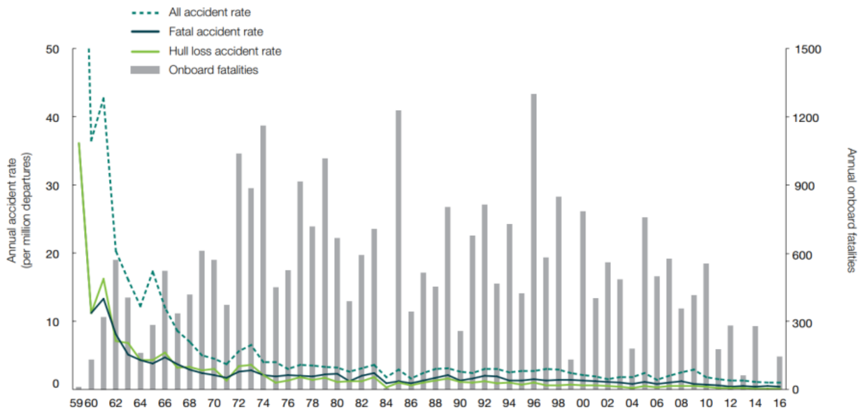
ARP5150

RTOS / Schedulability / Margins

Operational data

Recommendations
(Policies, Standards)

(not meant to be exhaustive)



Statistical Summary of Commercial Jet Airplane Accidents. Worldwide Operations | 1959 – 2016
[Boeing]

Requirement driven design process

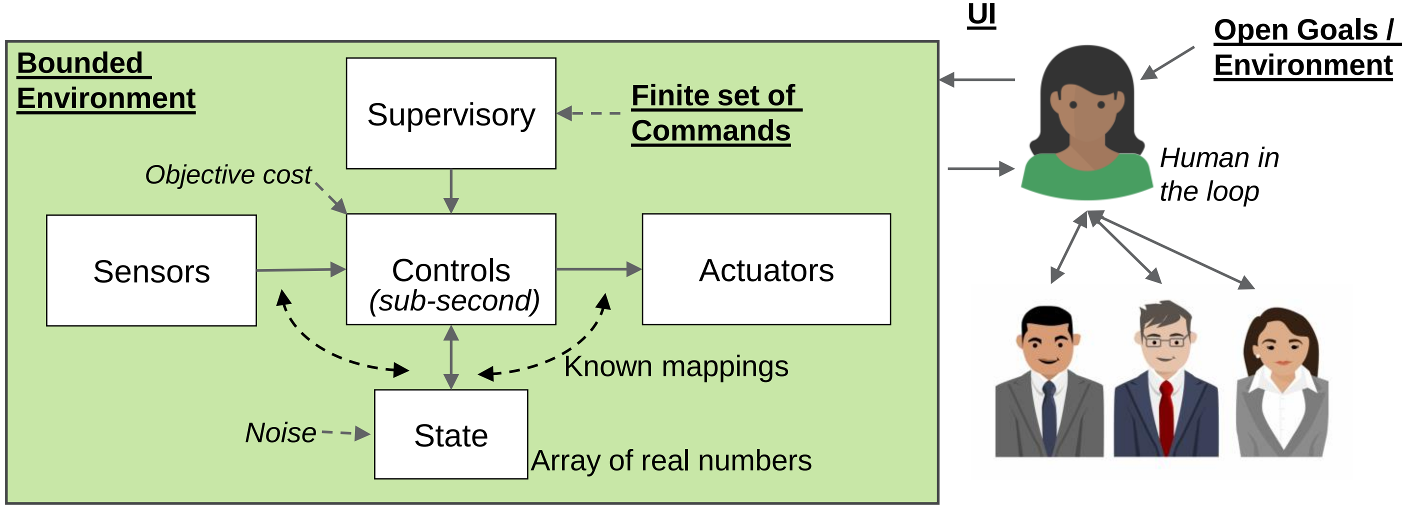
"The unique nature of software essentially reduces the software safety problem to the safety of the software requirements provided to the programmers". [National Academies of Sciences, Engineering, and Medicine. "Advancing aerial mobility: A national blueprint (2020)"]

Controlled vs. more autonomous systems

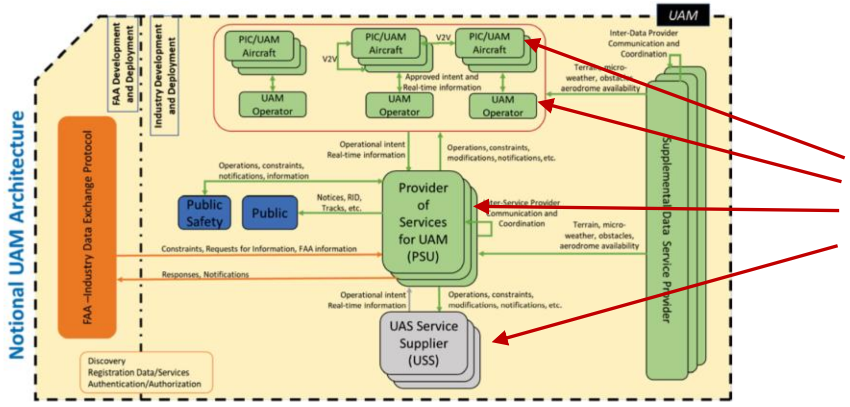
Taxonomy

- Controlled Systems
- Planning Systems
- Learning System

[Jose Brustoloni. "Autonomous Agents: Characterization and Requirements". *CMU-CS-91-204*]

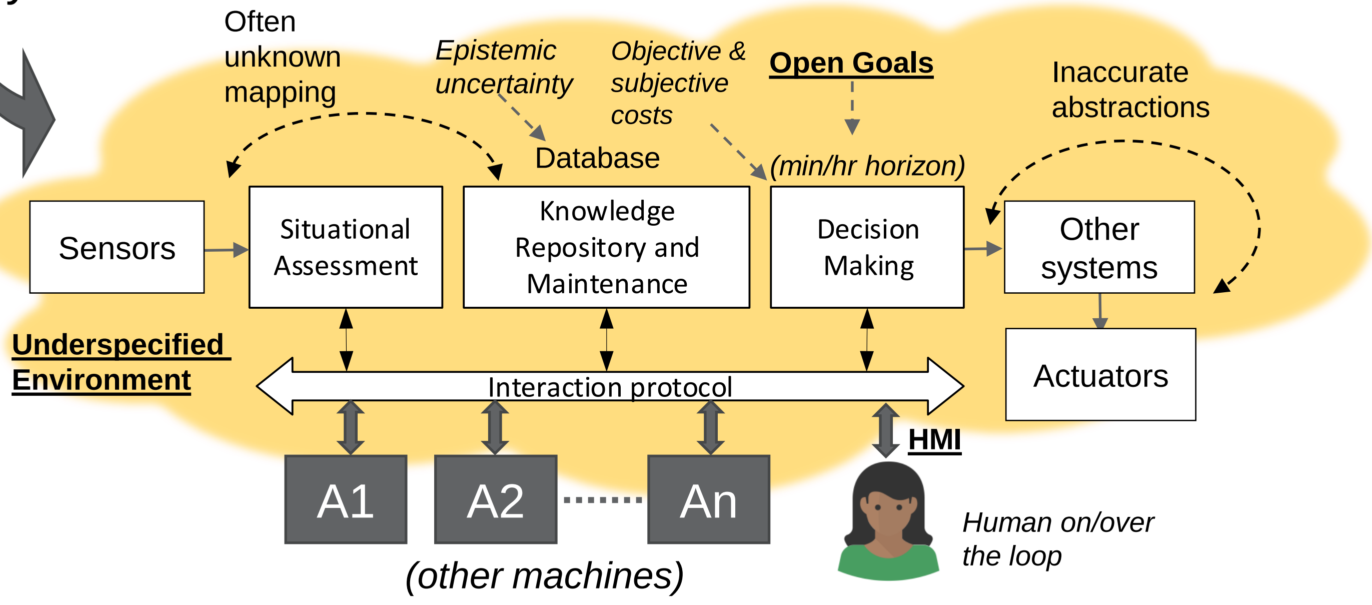


Increasing operations tempo and #vehicles, and cost constraints demand for autonomy at all levels of the UAM hierarchy



UAM
Notional UAM Architecture
FAA Development and Deployment
Industry Development and Deployment
FAA –Industry Data Exchange Protocol
PIC/UAM Aircraft
PIC/UAM Aircraft
PIC/UAM Aircraft
V2V
V2V
UAM Operator
UAM Operator
UAM Operator
Approved intent and Real-time information
Inter-Data Provider Communication and Coordination
Terrain, micro-weather, obstacles, aerodrome availability
Operational intent Real-time information
Operations, constraints, modifications, notifications, etc.
Operations, constraints, notifications, information
Public Safety
Public
Notices, RID, Tracks, etc.
Provider of Services for UAM (PSU)
Inter-Service Provider Communication and Coordination
Terrain, micro-weather, obstacles, aerodrome availability
Constraints, Requests for Information, FAA information
Responses, Notifications
Operational intent Real-time information
Operations, constraints, modifications, notifications, etc.
UAS Service Supplier (USS)
Supplemental Data Service Provider
Discovery
Registration Data/Services
Authentication/Authorization

FAA. "Urban Air Mobility (UAM) – Concept of Operations v1.0"



Things to work on

(Infrastructure and techniques; not in any particular order)

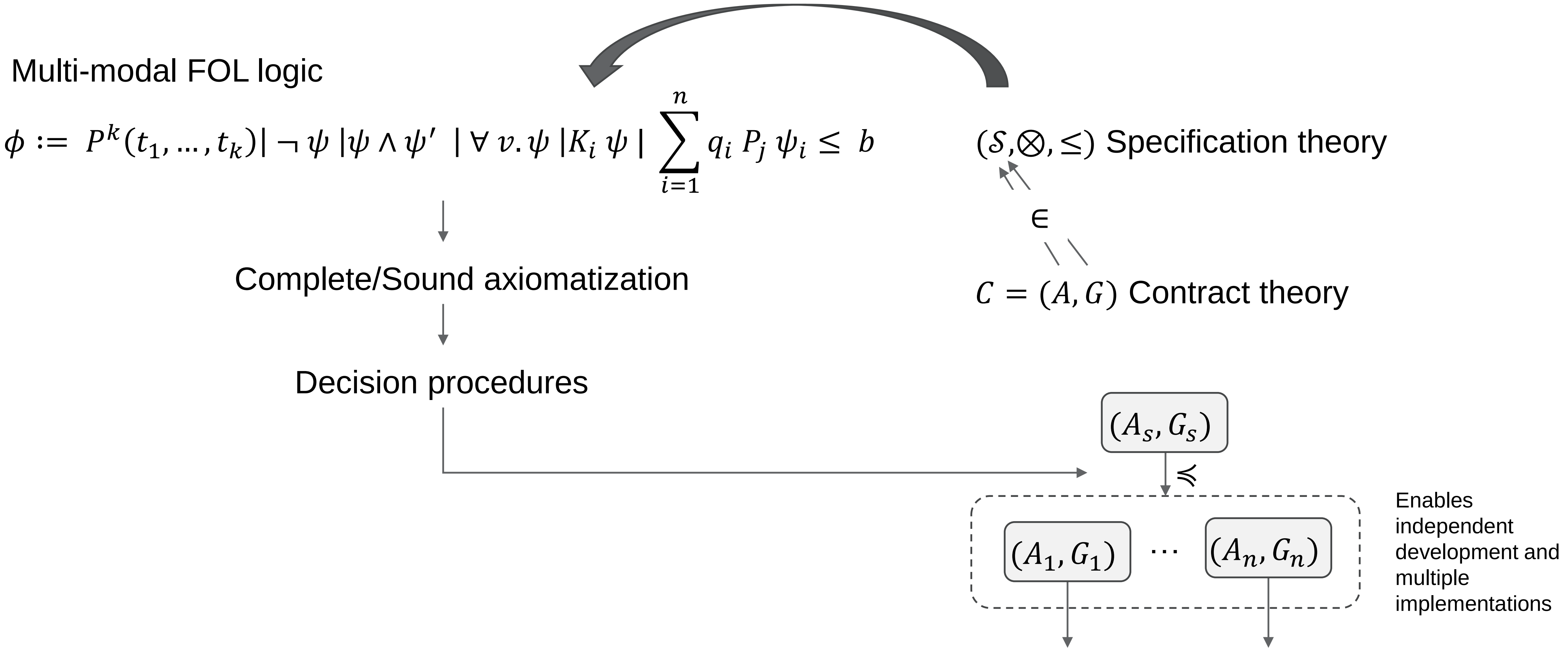
- Shared understanding (common representations) and protocols
- Modeling / tracking human “state” (inform, don’t annoy ; assurance of the HMS)
- Explainability (to engineers, regulators, operators, other machines)
- Environment architecture / design, ground infrastructure
- Cybersecurity
- Reliable comms
- Low-SWAPC, safe, secure, autonomous platforms
- Scalable decision making
- Contingency identification, isolation, recovery
- [and many others…]

Things to work on : need for engineering methods

Incremental, compositional design and analysis methods for autonomy

- Making requirements important
- Compositional framework (for scalability, evolvability, multiple implementations with guarantees)
- Methods that accommodate reasoning about all forms of uncertainty
- Development of models (removing the formal methods roadblocks)
- Methods to verify component compliance (formal verification, falsification, xUQ)
- Incremental deployment of autonomy features / environment complexity

Reasoning compositionally about uncertainty: Formal underpinning



Multi-modal FOL logic

$$\phi := P^k(t_1,\ldots,t_k) \mid \neg\,\psi \mid \psi \wedge \psi' \mid \forall\, v.\psi \mid K_i\,\psi \mid \sum_{i=1}^{n} q_i\, P_j\, \psi_i \leq b$$

Complete/Sound axiomatization

Decision procedures

$(\mathcal{S},\otimes,\leq)$ Specification theory

$\in$

$C = (A,G)$ Contract theory

(A_s,G_s)

$\preccurlyeq$

(A_1,G_1) $\cdots$ (A_n,G_n)

Enables independent development and multiple implementations

[A.Pinto, “Analysis and Design of Uncertain Cyber-Physical Systems” (in preparation)]