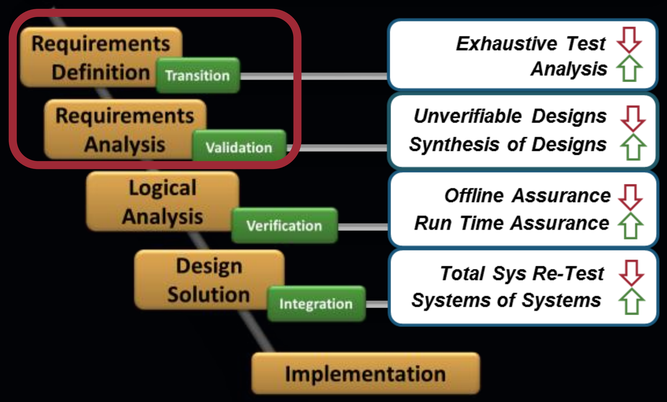
Verification and Validation of Autonomous Systems
Verifiable Requirements for Complex Systems
Air Force Research Laboratory

Strategy

Providing formal assurance arguments; Increasing trust in the next gen highly complex and autonomous systems



Technical Areas

- Formal Design and Analysis
- Run Time Assurance
- Compositional Systems of Systems Cert
- Synthesis of UAV Mission Plans

Leadership

- Co-Lead OSD Autonomy COI TEVV WG
- Support AFRL Autonomy S&T lead in TEV&V

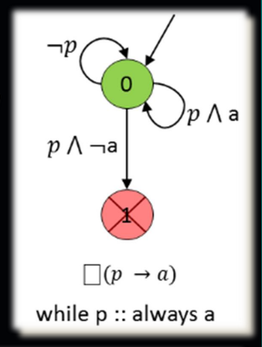
Formalized Requirements

Enables early **Validation** and provides a foundation for architecture and model **Verification**

SpeAR (Specification and Analysis of Requirements)
https://github.com/lgwagner/spear/

- **Formal patterns to capture requirements**
- **Supports 30 KSU Requirements patterns**
- **AFRL / Rockwell Collins developed additional patterns: *while*, *initial*, *delta*, *range*, & *transition***

while p :: always a	$\Box(p \rightarrow a)$
while p :: exists a	$\Box(p \rightarrow \Diamond a)$
while p :: a proceeds b	$\Box(p \rightarrow (\neg b\, U ((a \vee \neg p) \vee \Box \neg b)))$
while p :: a responds to b	$\Box(p \rightarrow ((b \rightarrow (p\, U (a \wedge p))) U (\neg p \vee \Box((b \rightarrow (p\, U (a \wedge p)))))))$



While the Tank Low Level Sensor is off, the pump shall be on and the valve shall be closed
while (low_sensor == #OFF) :: always (pump_state == #ON and valve_state == #CLOSED)

Accomplishments

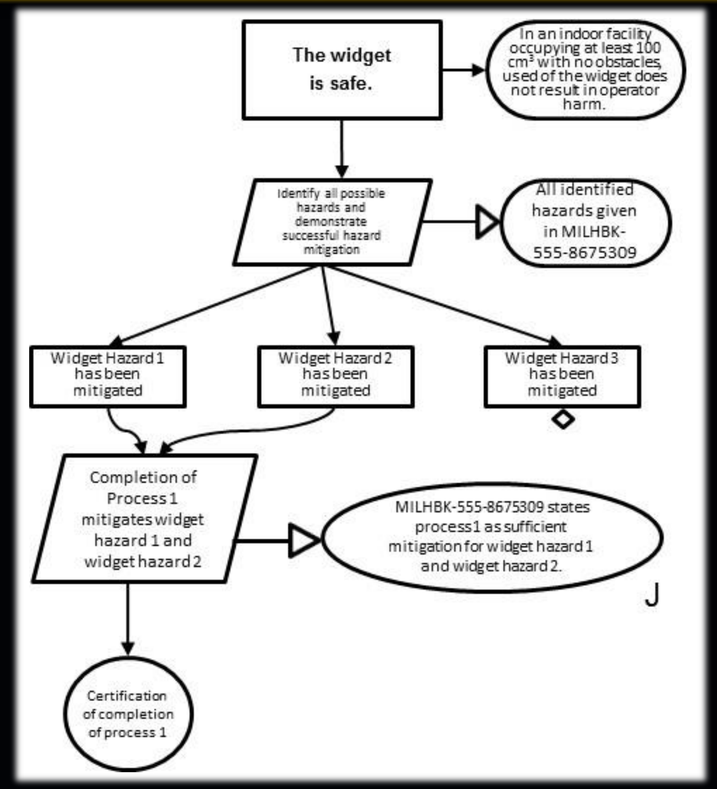
- Refined Patterns: Applied to 90% of AutoGCAS Requirements
- Completed Two Tanks Control Challenge Problem
- SpeAR v2.0 released to public in April 2016

Future Work

- Applying to control oriented UxV autonomy Challenge Problem
- Transition to Lockheed Martin's Quantum Annealing compositional V&V of Control Systems models

Assurance Cases for Certification of Autonomy

Providing evidence of system safety through multiple V&V techniques like M&S, testing, formal verification, and run time assurance



Assurance (Safety) Case is a "…comprehensive and defensible argument that a system is acceptably safe (or secure) to operate in a particular context."
– Professor Tim Kelly, University of York