Trusted Autonomy
Methods for Test and Evaluation

Gary Witus
Wayne State University

November 8, 2017
When Albert Einstein was at Princeton, he was known for walking around the campus grounds muttering to himself.

One day an enterprising reporter for the student newspaper decided to follow the Great Man around to write down what he was saying.

So he followed Einstein, only to hear him keep repeating the same phrase …
What are the Important Challenges for Systems Engineering in Acquisition of Autonomy-Enabled Systems (AES) ? ? ?
SE Challenges for AES

• **Reduced acquisition time**
  • TEVV of the autonomy capability requirements
  • Early start and over the lifecycle – capability and credibility

• **Requirements for behaviors and capabilities**
  • What to do and what to be able to do, under what conditions
  • V&V value and robustness to enhance *mission capability*
  • Manned-Unmanned-AES for an autonomy-enabled unit
    • *Mesh with unit Tactics, Techniques, and Procedures (TTP)*
    • *Expand TTP options so smaller units can do more*

• **Inform technology selection and source selection decisions**
  • Justification of claims – underlying evidence and assumptions
  • Technology development and competitive prototyping evidence
  • RFP package - what supporting evidence to submit
  • What to ask for, explain how it will be tested and evaluated
AES = Real Time CPS + Autonomous Behaviors and Interactions

Introduction, Discovery, and Cost of Software Faults

- Identified Need
- Requirement Development
- Architecture Development
- Detailed Design
- Implementation
- Integration
- Verification
- Validation
- Transition

70% of faults are introduced
3.5% faults are found
1x estimated nominal cost for fault removal

Opportunity to find faults as they are introduced when costs are low

20% of faults are introduced
16% faults are found
5x estimated nominal cost for fault removal

10% of faults are introduced
59.5% faults are found
20-80x estimated nominal cost for fault removal

20.5% faults are found
300-1000x estimated nominal cost for fault removal

Rework and certification is 70% of SW cost.

References:


Material supported by a SERC research activity
What Are AES Supposed to Do?

- **Select, adapt and blend behaviors to fit the situation**
  - Activate prescribed behaviors for the perceived situation
  - Resolve conflicting goals and activities
  - Avoid actions producing prohibited outcomes

- **Operate as part of a military operation**
  - Behaviors – percepts and activities matched to unit TTP
  - Instructions are OpOrds, FragOrds, within unit TTP
  - Recognize and report exception conditions
  - Interact with other agents – coordinate & support
Why is SE for Autonomy-Enabled Systems Hard?

- **Human functions moved to materiel requirements**
  - Training, selection and experience vs specifications
  - What is presumed and unstated for people must be expressed and required for machines
  - TTP, Field Manuals, OPORD, etc. designed for people
  - AES must work with commanders and human agents

- **OPORD expresses commander’s intent**
  - Intended outcomes, who accomplishes what, and how to coordinate – presumes subordinates figure out how
  - Autonomous capability has fit in at whatever level

- **No WBS or P-Spec for autonomy**

- **Limited experience** in developing and verifying autonomy requirements
Autonomy Architecture
Functional Decomposition

Start towards a “WBS” and “P-Spec” for autonomy
It’s complicated!
Claims for Trustworthy AES

- **Effective in team/unit operations**
  - Capable and robust, filling roles that enhance unit capability
  - Adapts to degraded conditions – external and internal
  - Meshes with TTP in coordinated activities
  - Reports status, accomplishments, opportunities and situations conflicting with task accomplishment

- **System properties enable calibrated trust** - commanders, operators, and adjacent agents understand
  - What it can and cannot do
  - When and what to use it for, and not
  - How to work with and instruct it
Puzzle Pieces – SE Framework for Model-Based Assurance Arguments

Assurance Argument Paradigm

Military Operation & Agent Behavior Dynamics Models

Conflict Detection & Arbitration

Behavior Requirements
• Prescribed Behaviors
• Prohibited Outcomes

Domain Specific Language

Situation Awareness
Execution Capability

Simulations, Virtual Exercises, DT/OT and Experimental Designs
Extended Assurance Argument Framework

- Explicit *scope* and *credibility* of claims, evidence and assumptions
  - Explicit scope and credibility composition calculus

**Scope and Credibility Composition Calculus**

- Claim
- Sub-claims
- Evidence
- Assumptions
- Sub-claim Assurance Arguments

**Heterogeneous Decomposition**

- Functional
- Operational
- External condition
- Etc.

**Argument Calculus**

- Intersections
- Unions
- Statistical Aggregation
- Etc.

Over the development lifecycle

- Assumptions replaced with evidence or converted into sub-claims
- Evidence accumulated from models and tests
Who Is Working With the Assurance Argument Approach

• **NASA**
  - Satellites and other “one shot” systems
  - Inductive machine learning subsystems

• **FAA**
  - Safety critical systems
  - Establish domain of assured safety

• **FDA**
  - New medical devices
  - Approved scope for early use

• **NHTSA regulators, automotive and insurance industries**
  - Traditional “experience accumulation” found unsuitable
  - Safety and scope of safety

• **DARPA research**
  - Real-time learning AES
Why Use Assurance Arguments

- New and evolving technologies. Limited experience. Failure is costly. *Acquisition decisions cannot wait.*
- Inform acquisition decisions with model-based evidence, assumptions and arguments
- Evolve evidence, arguments and assumptions over the lifecycle
- Explicit vendor information requirements & evaluation

**Scope:** The range of conditions

**Credibility:** Confidence in the claim

*Different Scope => Different Credibility*
State-Transition Modeling to Assess Military Utility

• Improve execution of unit Tactics, Techniques and Procedures (TTP)
  • Potential to enable new TTP
    • (Early Synthetic Prototyping discovery)

• Enhanced warfighter and unit capability
  • Earlier detection, faster reaction
  • Extended vision and reach
  • Force protection – troops out of harms way
  • Increased trucks-to-troops and tooth-to-tail ratios
  • Increased loitering endurance and attentiveness

• Reduced training time

• Autonomy requirements for military utility?
Operational Effectiveness
State-Transition Modeling

From Preceding Stage

Enter in LOS

Red Searching, Blue Driving on Planned Route, LOS

Red Firing, Blue Driving on Planned Route, LOS

Red Searching, Blue Driving on Planned Route, NLOS

Red Searching, Blue Waiting in Protected Position, NLOS

End of Stage Reached

To Next Stage, Not Having Come Under Fire

Pause for Red to Resume FOR Search over

To Next Stage, Having Come Under Fire

Enter in NLOS

Red Acquires Blue & Begins Firing

Blue Locates Red & Begins Escape to Protected Position

Red Firing, Blue Waiting in Protected Position, NLOS

Blue Reaches Protected Position

Blue Killed

Red Firing, Blue Waiting in Protected Position, NLOS

Red Searching, Blue Driving on Planned Route, NLOS

Red Searching, Blue Driving on Planned Route, LOS

Red Firing, Blue Driving on Planned Route, LOS

Red Searching, Blue Driving on Planned Route, LOS
Test, Demonstration & Transition Plan

- Co-develop with TARDEC
- Leverage related Automotive Research Center (ARC) project
  - Develop rigorous assurance argument model
- Demonstrate and test working with autonomy-enabled convoy S&T project
  - Autonomy in Operational Energy (AiOE)
    - TARDEC core funding
    - Army S&T funding supplementing core funding
  - Model-based development
  - Explicit goal to develop SE procedures for autonomy-enabled systems
AES SE Challenges

- Behavior & capability requirements will be imperfect and evolve
  - Incorrect, incomplete, inconsistent, untestable requirements
  - Building blocks to refine over the lifecycle
- Combinatoric explosion of TEV&V conditions
- Emergent effects from interactions with external agents and other autonomous subsystems
  - MOSA – emergent interaction effects among independently developed sub-systems
- Adjudication and blending of competing/conflicting behaviors
  - A system function above individual behaviors
  - Detect conflicts, gaps and inconsistencies in requirements
• Questions?
• Advice?
• Perspectives?
• Opinions?
• Discussion?