Systemic Assurance

Dr. Bill Scherlis, Carnegie Mellon University

5th Annual SERC Sponsor Research Review
February 25, 2014
Georgetown University
Hotel and Conference Center
Washington, DC

www.sercuarc.org
SERC – Systemic Assurance – outline

1. Software Assurance as an emerging major SE focus
2. Perspective on systems development and sustainment
3. Challenges for baseline software assurance practice
4. Evidence of the opportunity – practices and technology
5. ROI and the economic case
6. Conops for the systemic assurance project
1. Software assurance as an emerging major focus

- Attention and evidence
  - DSB foreign software: T&E
  - PCAST cybersecurity: Arch
  - Section 933 NDAA
  - The SysE role: Higher stakes
    - Toyota $1.1B, ECSS, Healthcare.gov, F-35, ...

- Driver – roles for software
  - Increasingly critical, broadly pervasive, expectedly nimble
2. Perspective on systems devt and sustainment

Payloads over Platforms: Charting a New Course

Proceedings Magazine - July 2012 Vol. 138/7/1,313

By Admiral Jonathan W. Greenert, U.S. Navy

We need to move from ‘luxury-car’ platforms—with their built-in capabilities—toward dependable ‘trucks’ that can handle a changing payload selection.

Navy platforms, particularly ships and aircraft, are large capital investments frequently designed to last for 20 to 50 years. To ensure our Navy stays relevant, these platforms have to adapt to the changing fiscal, security, and technological conditions they will encounter over their long service lives. It is unaffordable, however, to adapt a platform by replacing either it or its integral systems each time a new mission or need arises. We will instead need to change the modular weapon, sensor, and unmanned vehicle “payloads” a platform carries or employs. In addition to being more affordable, this decoupling of payload...
SOSCOE is a tailoriable software toolkit to support legacy and SOA applications for the Tactical Domain. Enables a loosely coupled system with “Plug and Play” of new hardware and software applications. Allows the user to establish an “Investment Strate evolutionary and incremental change.”
Platforms and payloads – structures and practices

- Structure of systems, supporting artifacts, and organizations
  - Framework+apps model
  - Rich supply chains and socio-technical ecosystems
  - Architectural commitment, ownership, evolution
  - Allied models, tests, analytics, and other data

- Processes, practices, and teams
  - Evolutionary methods – IID and “agile at scale”
  - Powerful tools – developers and teams
  - Data intensive – development and quality
  - Rapid deployment – “DevOps”
    - Shift of balance from development to sustainment/modernization
NB: Software and systems engineering – the evolving role

- **Building material of choice**
  - Largest single asset class (NRC STEP) – pervasive and critical in systems
  - No plateau of capability anywhere in sight

- **Cybersecurity**
  - The *materiel* of defense and offense
  - The manifestation of the assets being protected

- **Diverse roles**
  - Manifesting capability and autonomy
  - Enabling interlinking of systems of systems
  - Affording nimble response to changes in mission and infrastructure
    - The locus of the changeable

- **Consequence**
  - Routine activity gives way to automation
  - Hence more of the engineering activity is “innovative”
3. Challenges for baseline assurance practice

- Realities of modern (non-specialist) evaluation/certification
  - Growing need for higher levels of assurance – *safety and security*
  - Process compliance giving way to product evaluation – *freezing issue*
  - Snapshot – *no dynamism*
  - After the fact – *information loss and reverse engineering reqts*
  - Whole system – *vs incremental re-certification*
  - No verification (A1; EAL7) – *no positive assurance*
  - Technical difficulties – *concurrency, autonomy, ...*
  - IP difficulties – *what can the evaluator see?*
  - IP difficulties – *what can the prime see?*

- Judgments regarding T&E
  - Practices out of phase with modern devt reality
  - Not at pace with cybersecurity requirements
  - Not exploiting potential of current technology
Perspective – particular challenges of software

• The technology
  ▪ Rapid continuing progress in technology and practice – *no plateau*
  ▪ Quantitative ROI elusive – *measurement for critical attributes*

• The ecology
  ▪ STE focus on selection/configuration – *not empty-page coding*

• Influences on adoption of quality practices
  ▪ Measurement difficulty – *Debt? Cost to complete? Quality?*
  ▪ Relating quality and capability and timeliness – *push out the curve*
  ▪ Adoption criteria – *ROI vs. engineering judgment*
  ▪ Diffuseness of system design and technical heritage – TRL++, 6.x++, ?
    ▪ Non-appropriability and weak “attributability”
4. Evidence of opportunity – practices & technology

- **Process and team culture**
  - SDL (Howard, Lipner), BSIMM (McGraw et al.)
    - Common features: Engagement and feedback across entire lifecycle
  - Systems processes and software processes – a convergence

- **Technical advances in the software domain**
  - **Semantics** intensive and **data** intensive
    - Models, analyses, tools, languages
  - Ubiquity of advanced **tooling** and **modeling** and **analytics**
    - Individual engineers, small teams, larger orgns, supply chains
    - Internal business case and broad adoption at leading vendors

- **Interplay of SysE and SwE**
  - **Actions and enactment**: process models, teams, organizations
    - Conflicting decision drivers
      - Risk, quality attributes, functional attributes, cost, schedule
      - Interplay/trade-offs of *ilities
      - Architectural/interface/API choices
  - **Artifacts**: Data, models, tools, and process support
    - Interplay of diverse models and abstractions
5. ROI and the economic case

- **Challenges**
  - **Arm’s length** and alignment of incentives
    - Cf. Commercial best practice, particularly vendors
    - *Arm’s length enhances the measurement challenge!*
  - Acquisition culture and normative practices
  - **Sustainment → modernization**
    - Cf. Depot/organic capability and engagement models
    - Cf. DevOps process patterns
  - C&A and T&E standards and practices
  - Training and technical refresh

- **Opportunity**
  - There is a business case at successful adopters
    - Developer ROI; Team ROI; Organizational ROI
  - The cases combine measurement and judgment
    - Advancing the frontier of measurement
  - The accretion of assets supports incremental improvement
    - Assets include data, models, and evidence in support of claims
    - DIS premise: evidence
6. ConOps for systemic assurance

**Summary**: Provide practices for systemic assurance of safety, reliability, availability, maintainability, evolvability, and adaptability.

**Impact**: Advancement in modeling, analysis, tooling, and process in support of rapid and effective certification of systems in development and recertification of systems in sustainment/modernization.

**Validation**: Achieve this through a strategy that links technical advancement with validation effort including prototyping, case studies and field trials, development of measures, and engagement with assurance stakeholders.

**Status**: Project initiation in 2014. This effort builds on a long record of engagement on the challenges of assurance at scale for component-based complex systems, including architecture, resiliency, modeling, analysis, tooling, concurrency, and other areas.
Conops – the Seven Steps

1. Identify baseline and intervention models for a selection of current standards

2. Advance capability for traceability to support explicit modeling and chains of evidence.

3. Design and implement experiments to address the challenge of rapid recertification.

4. Develop a framework for assessment of architecture-derived quality attributes

5. Develop requirements elicitation and management approaches that better address quality and policy objectives.

6. Augment and collaborate with diverse existing efforts focused on technical means to address particular quality criteria.

7. Identify and advance areas to support increasing automation. The key hypothesis is that assurance-related interventions will increase productivity throughout the lifecycle, leading to a "positive benefit" model.