Incremental Lifecycle Assurance of Critical Systems

Critical System Assurance Challenge
The traditional development lifecycle using existing methods of system engineering result in:

- Assurance-related post-unit test software rework at 50% of total system cost and growing
- Labor-intensive system safety analysis without addressing software as major hazard source
- High percentage of operator workarounds for software fixes due to high recertification cost

NIST Study
Current requirement engineering practice relies on stakeholders traceability and document reviews resulting in high rate of requirement change.

Rolls Royce Study
Managed awareness of requirement uncertainty can lead to 50% reduction in requirement changes.

U Minnesota Study
Requirements often span multiple architecture layers.

Incremental Lifecycle Assurance Goals
- Improve requirement quality through coverage and managed uncertainty
- Improve evidence quality through compositional analytical verification
- Measurably reduce certification related rework cost through virtual integration and verification automation

Assurance & Qualification Improvement Strategy
Assurance: Sufficient evidence that a system implementation meets system requirements

Incremental Assurance
Focus: Incremental Assurance

Three Dimensions of Incremental Assurance
- Priority focused architecture design exploration for high pay-off
- Measurable improvement (Rolls Royce)

UML State Machine Statechart: Business layer System Under Control

Impact and Alignment
- AMRDEC Joint Multi-Role (JMR) Tech Demo: maturation of ACVIP for Future Vertical Lift (FVL)
- Aerospace industry System Architecture Virtual Integration (SAVI) multi-year initiative
- Standards: SAE AS-2C (AADL Requirements, Constraints), SAE S18 (ARP4761 System Safety)
- Regulatory agencies: NRC, FDA, AAMI/UL

Contact: Peter Feiler | phf@sei.cmu.edu