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 work arounds 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

Requirements error	%
Incomplete	21%
Missing	33%
Incorrect	24%
Ambiguous	6%
Inconsistent	5%

Rolls Royce Study

Managed awareness of requirement uncertainty can lead to 50% reduction in requirement changes

Selection	Weight	Precedence
Low Precedence	9	No experience of concept, or environment. Historically volatile.
Medium Precedence	3	Some experience in related environments. Some historic volatility.
High Precedence	1	Concept already in service. Low historic volatility.

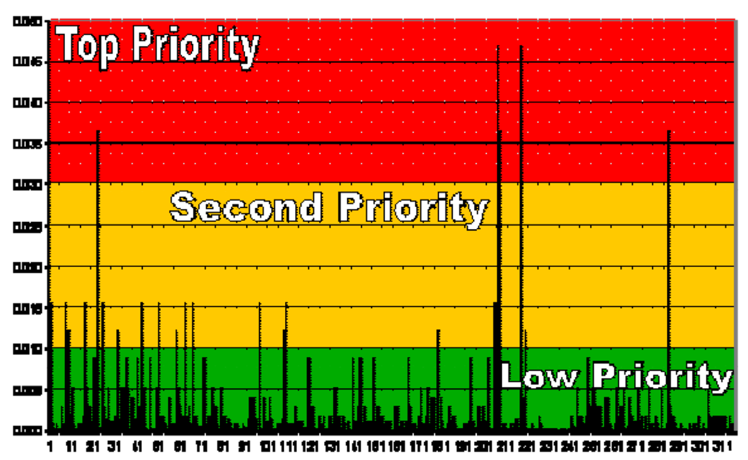


Figure 10. Requirements uncertainty analysis

U Minnesota Study

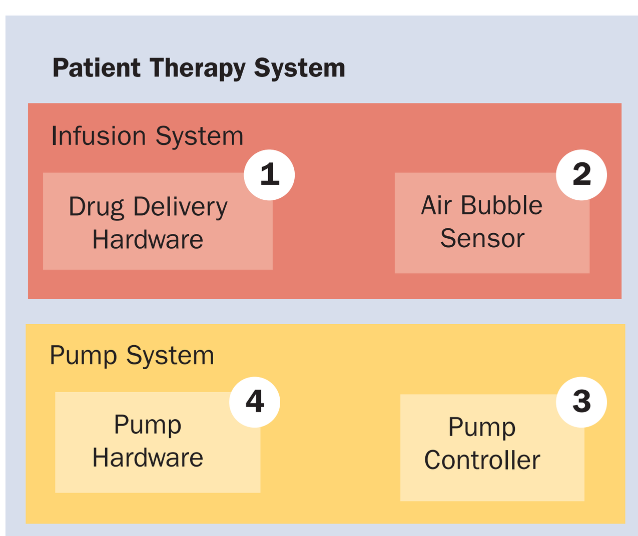
Requirements often span multiple architecture layers

Textual Requirements for a Patient Therapy System

1. The patient shall never be infused with a single air bubble more than 5ml volume.
2. When a single air bubble more than 5ml volume is detected, the system shall stop infusion within 0.2 seconds.
3. When piston stop is received, the system shall stop piston movement within 0.01 seconds.
4. The system shall always stop the piston at the bottom or top of the chamber.

Importance of understanding system boundary

Same Requirements Mapped to an Architecture Model



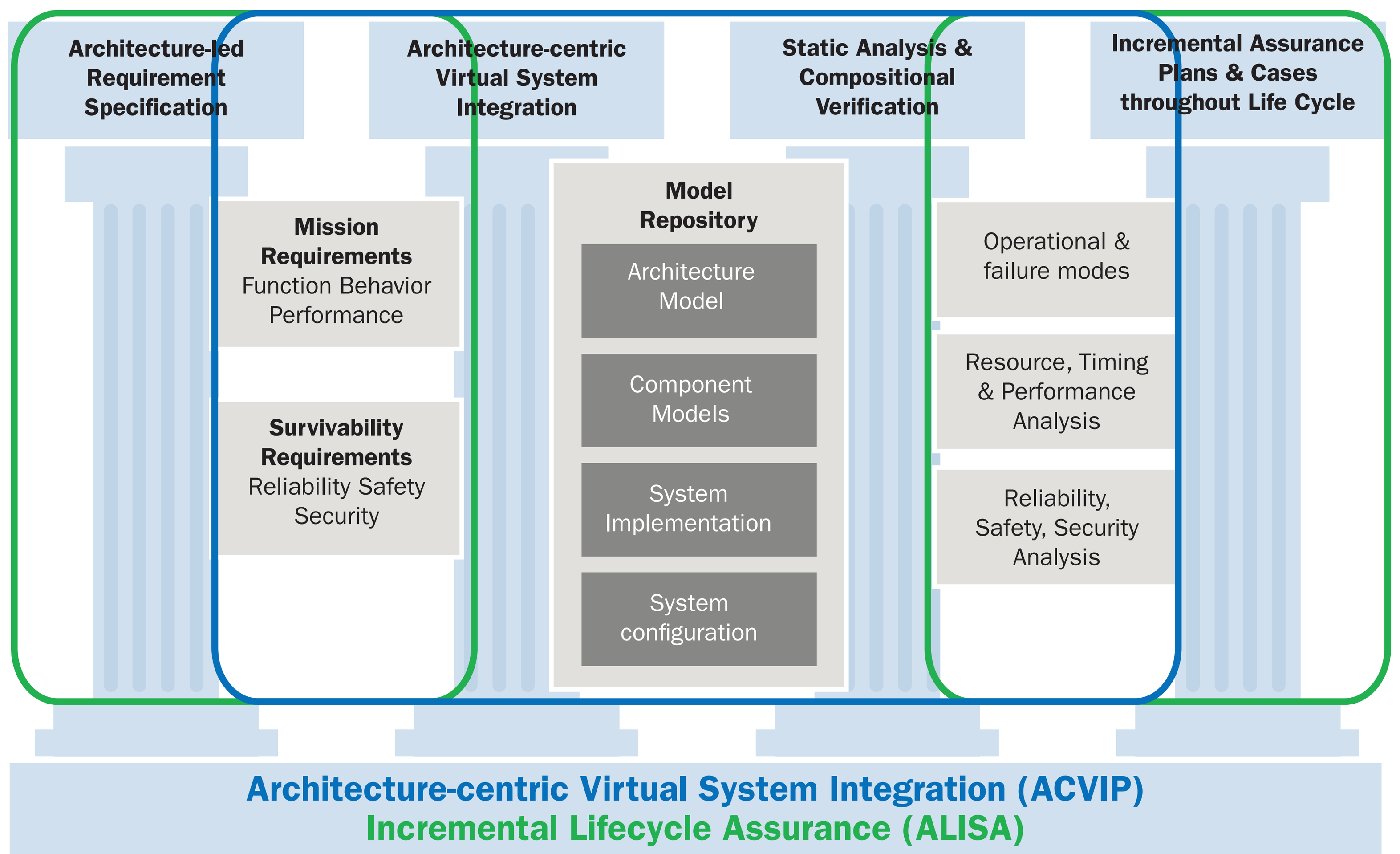
We have effectively specified a system partial architecture

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



Project Approach

Architecture-Led Incremental System Assurance (ALISA) Approach

Semantically Consistent Unification of Modeling Concepts from Different Perspectives And their Use in Existing Practice Standards

- **Goal, Intent, Requirement, Assumption, Claim**
- **Obstacle, Fault, Defect, Hazard, Vulnerability, Challenge**
- **Verification Method, Activity, Result, Evidence, Counter evidence**

ALISA Workflow & Eclipse-based Workbench

FY15 Focus

- **Architecture-focused Requirements & Hazard Analysis**
- **Architecture-led Contract- based Compositional Analysis & Verification**
- **Assurance Plan with Multi-valued Argumentation Logic**

AMRDEC JMR Situational Awareness Requirements Case Study (Early Life Cycle)
SAVI Multi-layered multi-dimensional aircraft verification (Multi-phase)
Rolls Royce Engine Control Certification Study (Late Life Cycle)

- **Technical and Operational Validation in Actual Projects** Access to Actual Project Information
- **Measurably Increased Assurance Confidence** Credit for Analytical Evidence
- **Measurably Reduced Defect Leakage & Assurance Cost** Apply COQualMO and SAVI ROI

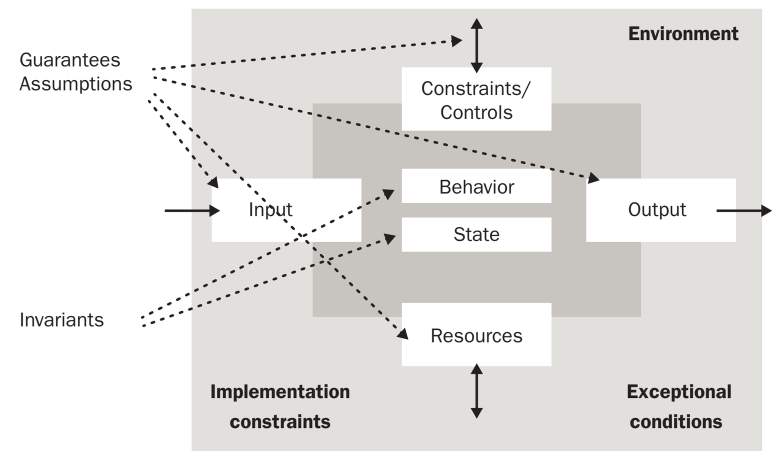
Measurement-driven Assurance Cost and Confidence Improvement through Incremental Lifecycle Assurance

FY16 Focus

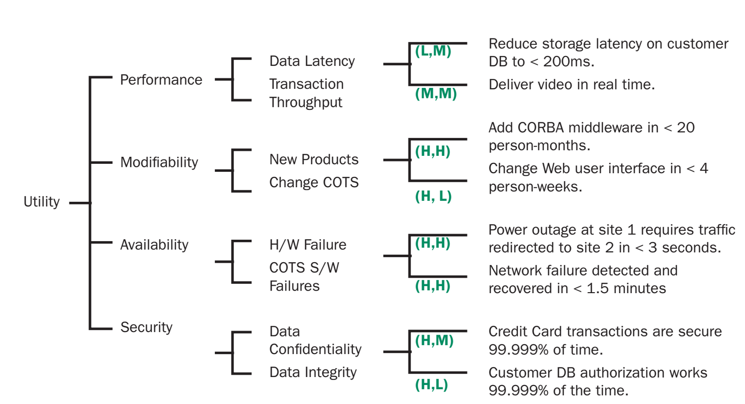
- **Anticipated Improvement Thresholds** 25% Higher Requirement/Hazard Coverage 35% Higher Evidence Confidence 25% Reduced Uncertainty Impact
- **Assessment of Potential for Proportional Recertification Cost** Benefit and Risk of Partial Verification

Three Dimensions of Requirement Coverage

System interactions, state, behavior

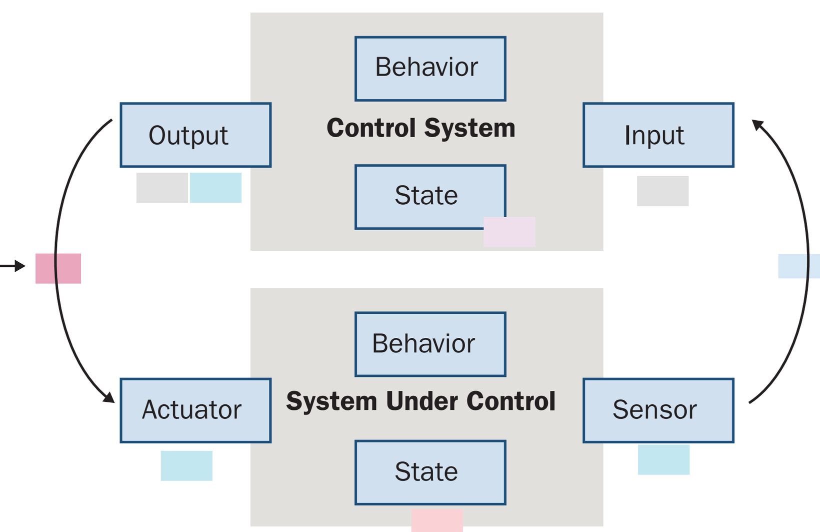


Design & operational quality attributes



Fault impact & contributors

Omission errors	Commission errors
Value errors	Sequence errors
Timing errors	Replication errors
Rate errors	Concurrency errors
Authentication errors	Authorization errors

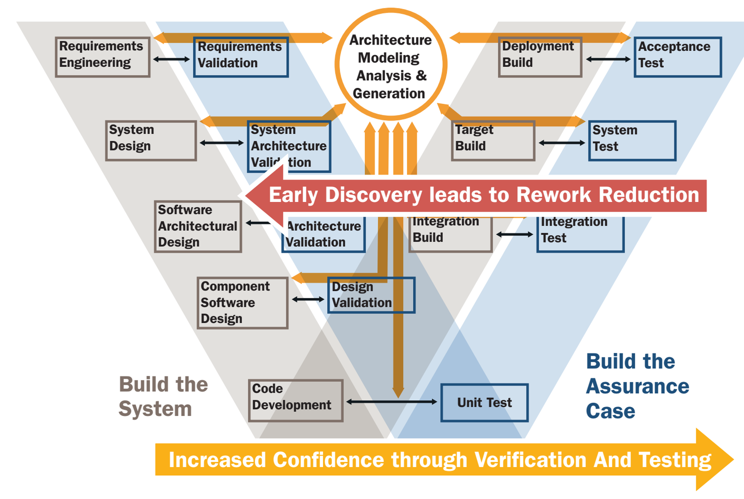


Fault Propagation Ontology

Three Dimensions of Incremental Assurance

Incremental assurance through virtual system integration for early discovery

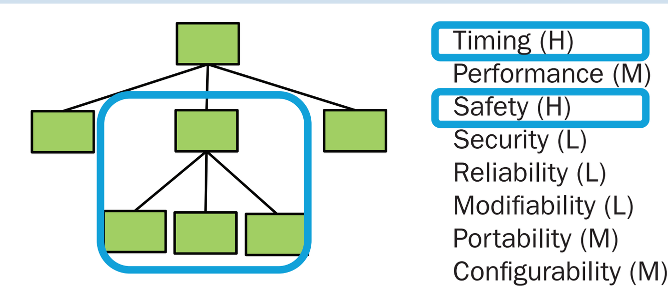
Return on Investment study by SAVI*



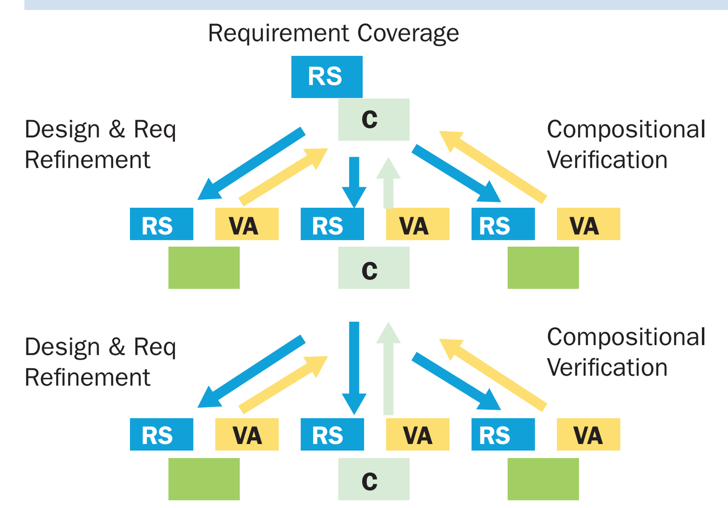
*System Architecture Virtual Integration (SAVI) Aerospace industry initiative

Priority focused architecture design exploration for high payoff

Measurable improvement (Rolls Royce)



Compositional verification and partitions to limit assurance impact



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

Distribution Statement A: Approved for Public Release;
Distribution is Unlimited

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