Incremental Lifecycle Assurance of Critical Systems

Peter Feiler

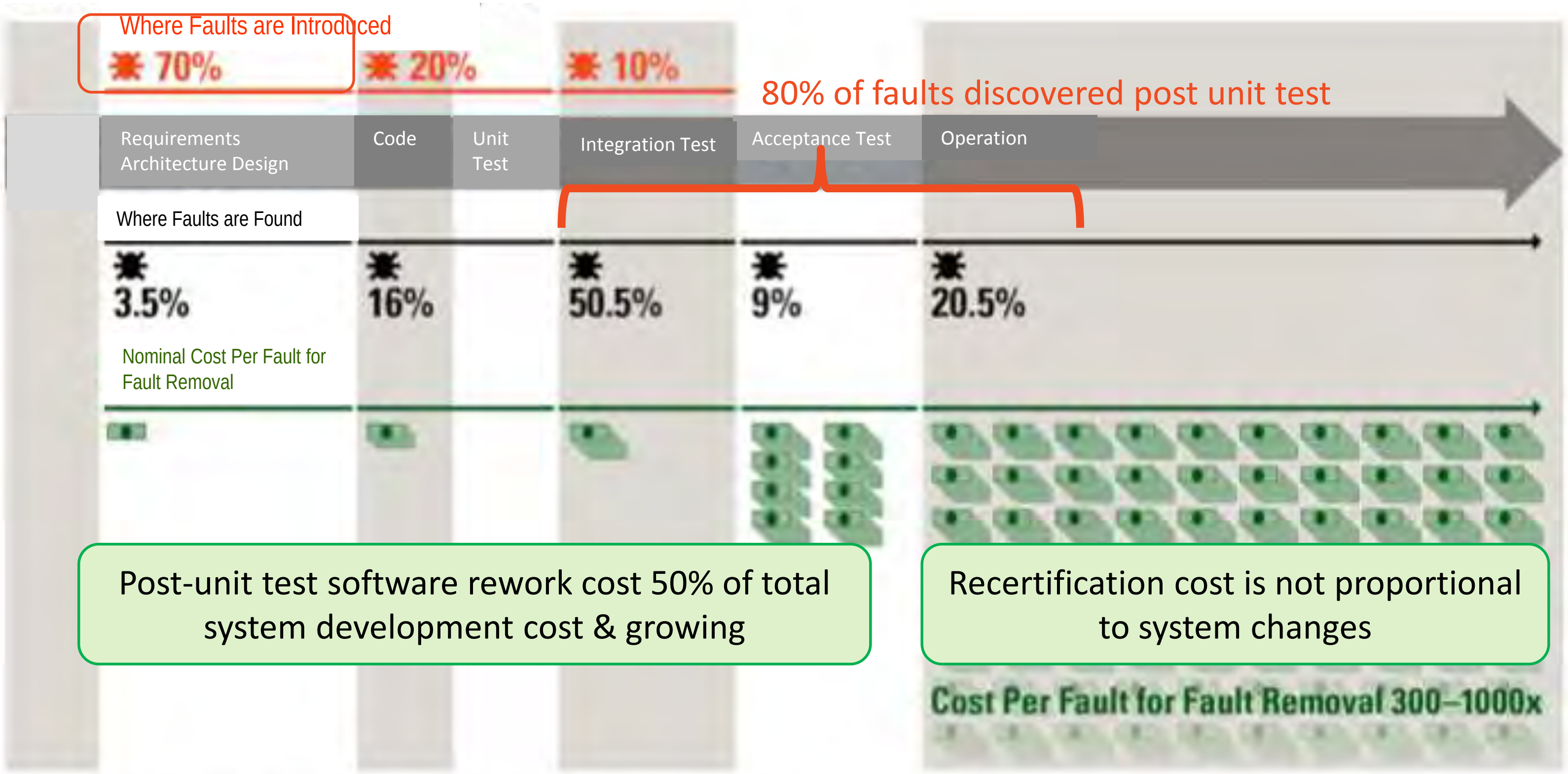
Outline

Critical System Assurance Challenges

Incremental Lifecycle Assurance Approach

ALISA Workbench

Critical System Assurance Challenges



Sources: *Critical Code*; NIST, NASA, INCOSE, and Aircraft Industry Studies

Years between labor-intensive system safety assessments
Software as major hazard source often ignored

Requirements and Architecture Design Constraints

Textual Requirements for a Patient Therapy System

The patient shall never be infused with a single air bubble more than 5ml volume.

When a single air bubble more than 5ml volume is detected, the **system** shall stop infusion within 0.2 seconds.

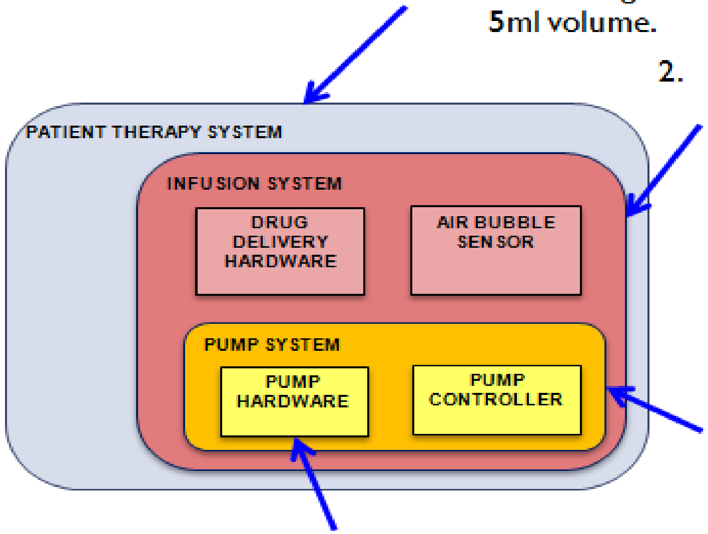
When piston stop is received, the **system** shall stop piston movement within 0.01 seconds.

The **system** shall always stop the piston at the bottom or top of the chamber.

U Minnesota Study

Same Requirements Mapped to an Architecture Model

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.



4. The **system** shall always stop the piston at the bottom or top of the chamber.
3. When piston stop is received, the **system** shall stop piston movement within 0.01 seconds.

Importance of understanding system boundary

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

NIST Study

We have effectively specified a system partial architecture

Outline

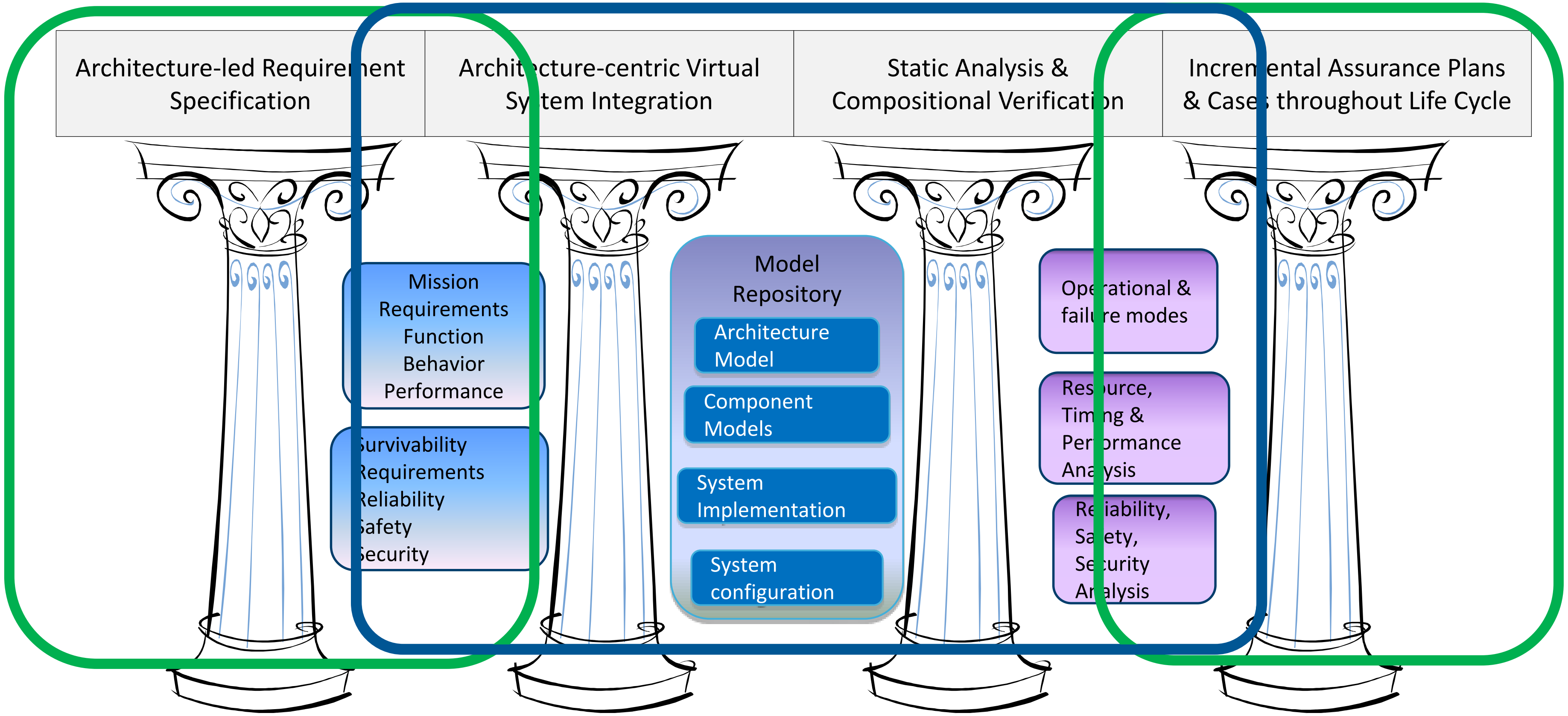
Critical System Assurance Challenges

Incremental Lifecycle Assurance Approach

ALISA Workbench

Assurance and Qualification Improvement Strategy

Assurance: Sufficient evidence that a system implementation meets system requirements



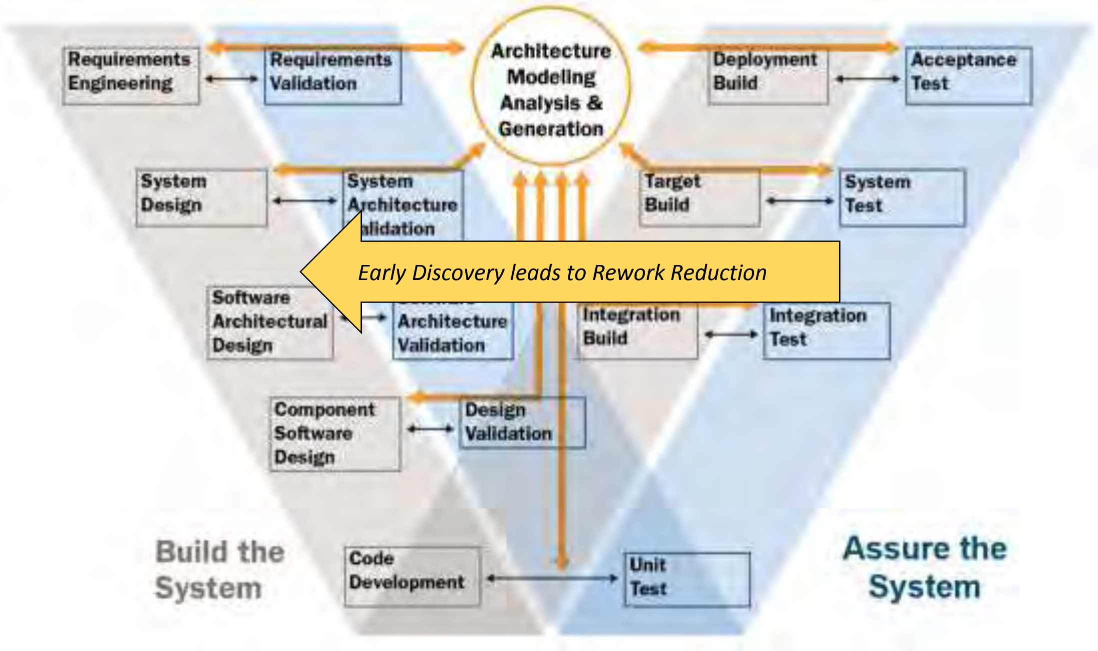
Early Problem Discovery through Virtual System Integration and Analysis

Improved Assurance through Better Requirements and Automated Verification

2010 SEI Study for AMRDEC Aviation Engineering Directorate

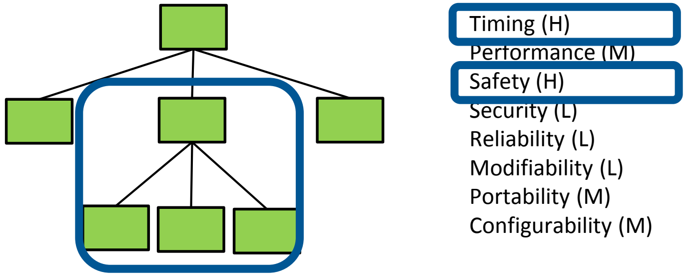
Three Dimensions of Incremental Assurance

Incremental assurance throughout lifecycle
Early discovery through virtual system integration
Return on Investment study by SAVI*

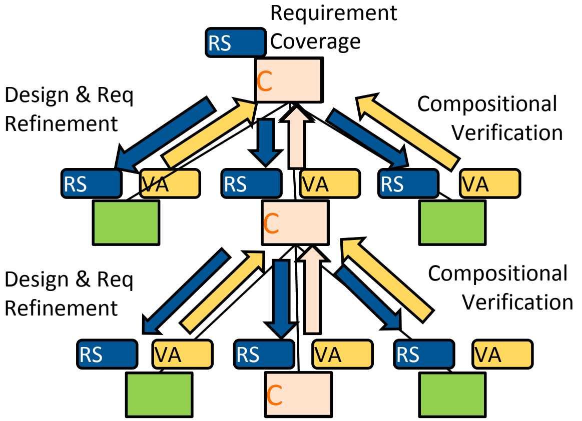


*System Architecture Virtual Integration (SAVI) Aerospace industry initiative

Priority focused architecture design exploration for high payoff
Measurable improvement (Rolls Royce)

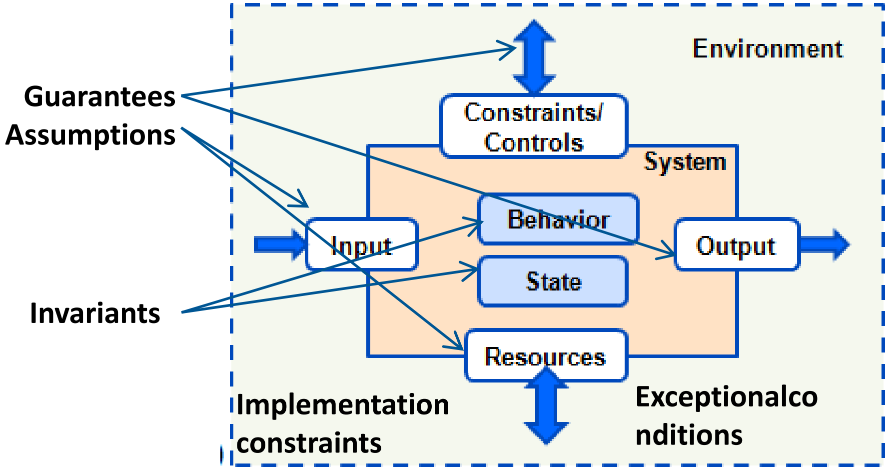


Compositional verification and partitions to limit assurance impact

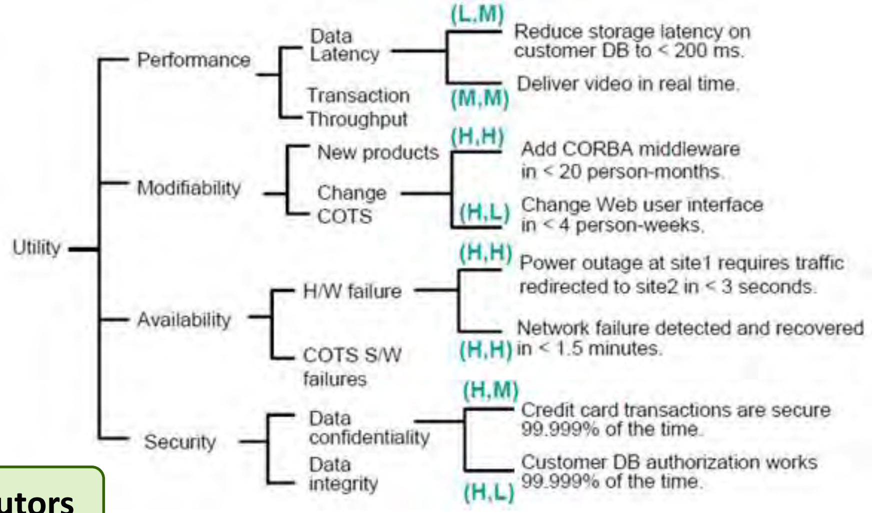


Three Dimensions of Requirement Coverage

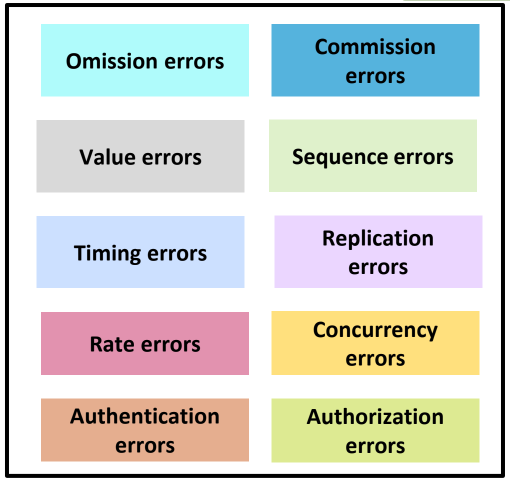
System interactions, state, behavior



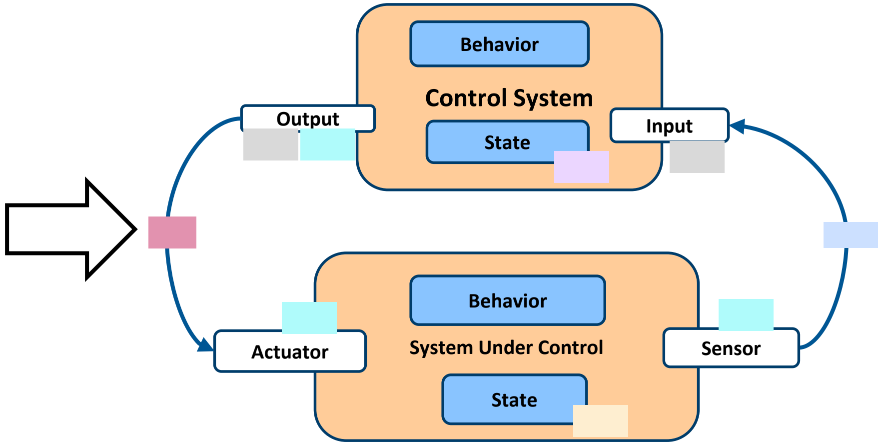
Design & operational quality attributes



Fault impact & contributors



Fault Propagation Taxonomy



Impact and Alignment

DoD Acquisition and Industry Organizations

- OASD R&E: Champion maturation and insertion of virtual system integration into DoD programs
- DARPA research successes in HACMS program
- AMRDEC Joint Multi-Role (JMR) Tech Demo: maturation of Virtual System Integration for Future Vertical Lift (FVL) program
- Aerospace industry System Architecture Virtual Integration (SAVI) initiative Multi-year investment: Boeing, Airbus, Embraer, suppliers, FAA, NASA, DoD
- Rolls Royce engine control system case study

Standard Development

- Draft SAE AADL Requirement Specification standard
- Revision of SAE S18 ARP4761 System Safety Analysis standard

Regulatory Certification Agencies

- FDA: Guidance on medical device (re-)certification
- Underwriters Lab: medical device integration guidance (AAMI/UL2800)
- NRC: Educational workshop series on software system assurance

Outline

Critical System Assurance Challenges

Incremental Lifecycle Assurance Approach

ALISA Workbench

Modeling Notations in ALISA Prototype

ReqSpec Represent stakeholder and system requirements

- Document-based and architecture-led
- Verifiable system requirements
- Coverage and uncertainty

Verify Specify intended verification activities

- Across lifecycle on different artifacts and layers of system architecture
- Via verification methods (manual, automated)
- Supported: OSATE Analyses, Java, Resolute, Agree, JUnit

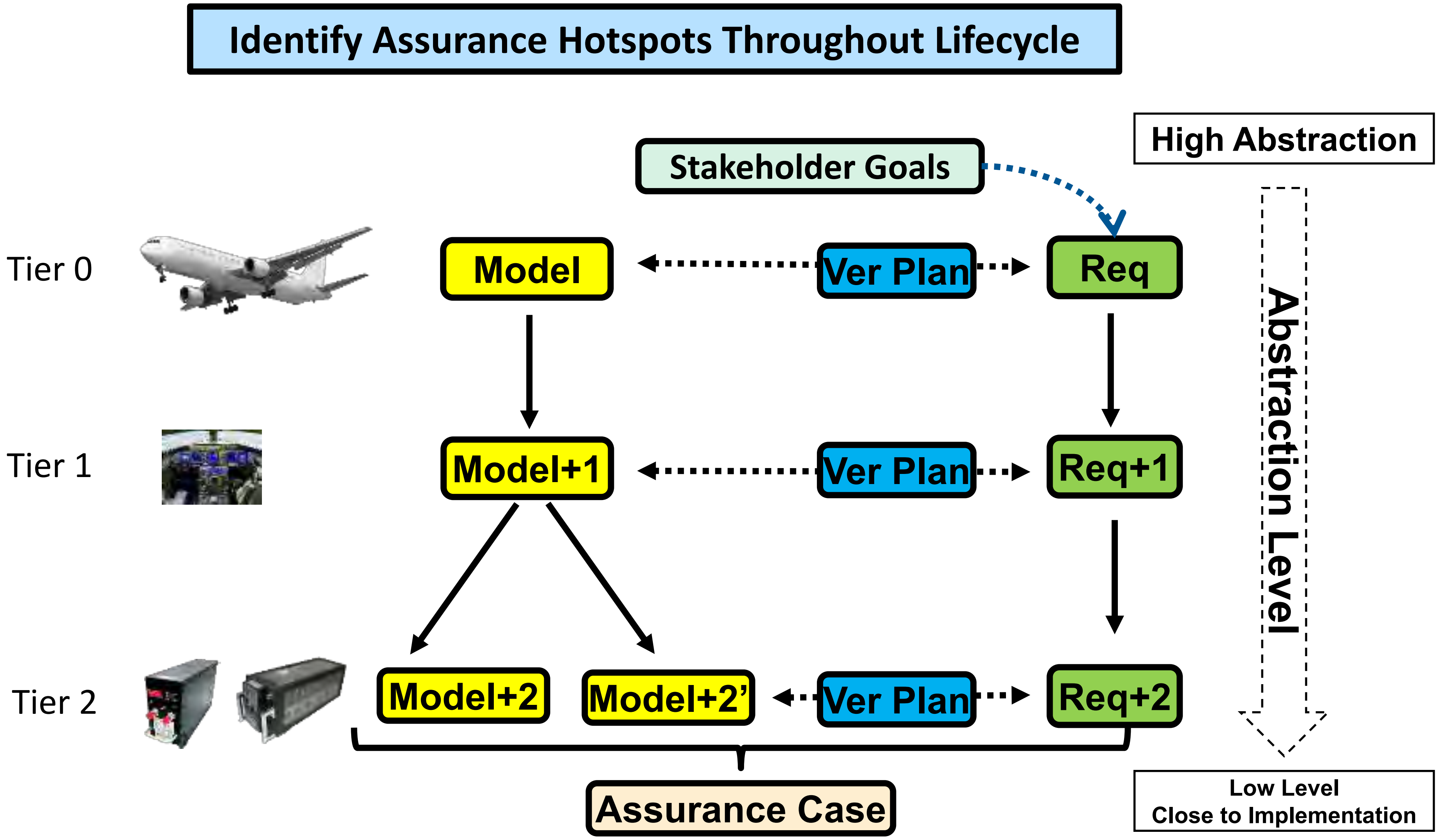
Alisa Compositionally configure assurance cases

- Reasoning logic of how verification activities satisfy requirement
- Assumptions, preconditions on verification activities
- Scoped assurance plans and focused assurance tasks

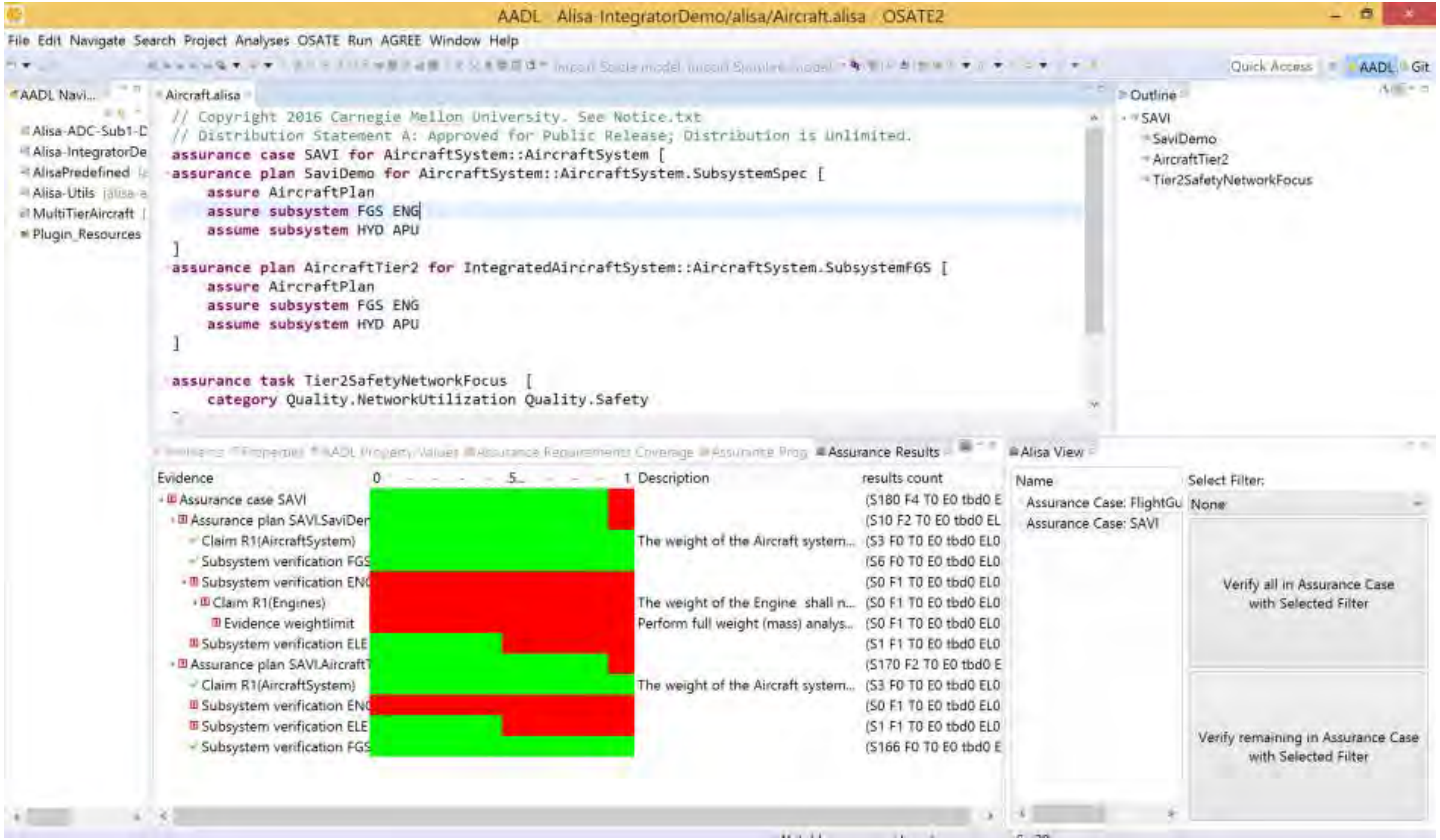
Assure Manage assurance state and results

- Multi-valued logic evaluation of verification action and results
- Acceptable risk factors (e.g., design assurance levels)
- Time phased execution of assurance plans

Automated Incremental Assurance Workbench



ALISA Workbench Screenshot



Assurance Case Execution and Metrics

User guided filtered views

- Filtering on requirement type, quality attribute, development phase
- User definable categories for requirements, verification methods and activities

Assurance Metrics

- Requirement coverage measures
  - Model element, quality, and failure effect taxonomy coverage
- Multi-valued verification result measures and their aggregates
  - Pass, fail, incomplete, conditional, backups
- Weighted requirement claims, verification activity results
  - Reflect importance, uncertainty (volatility, precedence, impact)

Guidance throughout lifecycle (Spotlight)

- Based on requirement specifications and precedent and volatility ratings
- Utilize COCMO II to derive worst-case and best-case estimates of effort

Case Studies

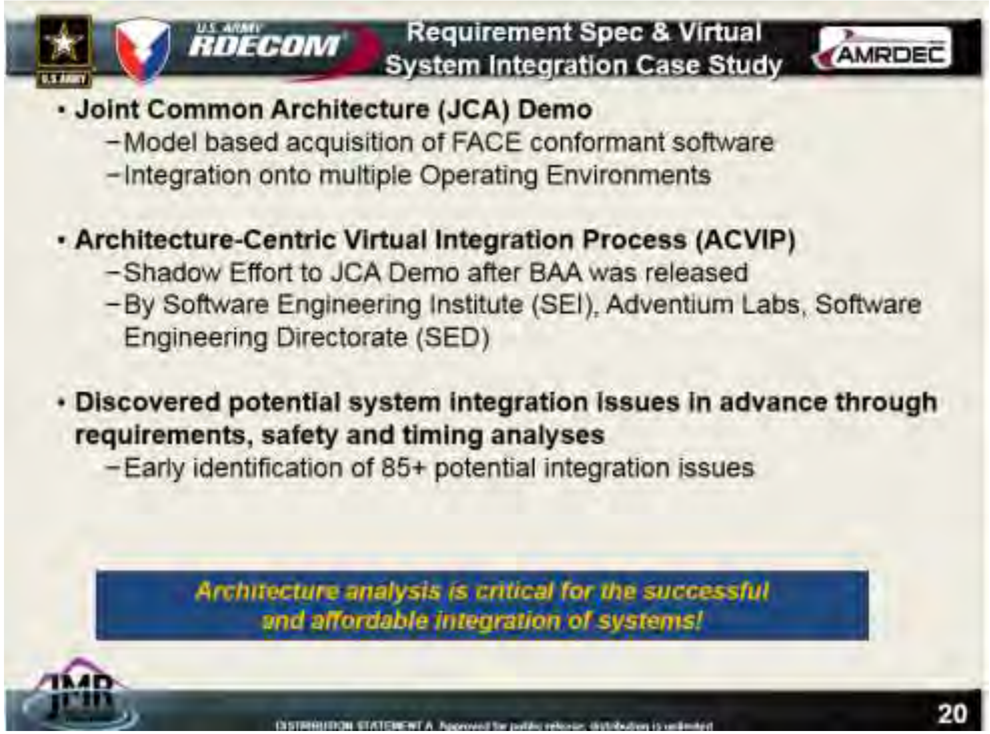
Multi-Tier Aircraft Model

- Demonstrate incremental and compositional approach to assurance cases

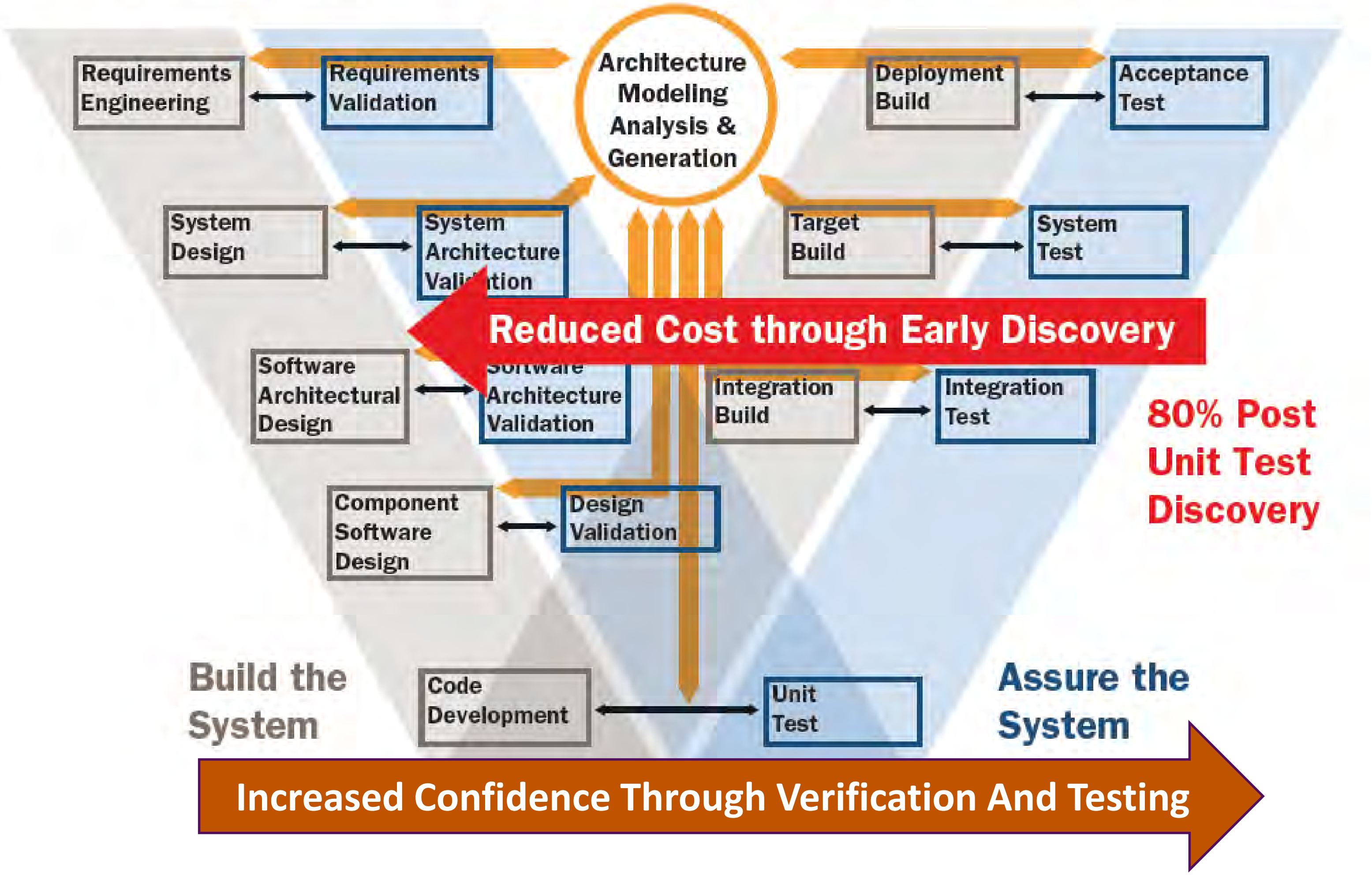
Stepper Motor diagnostics and design verification

- Demonstrate diagnostic of original customer design and verification of three design improvements

Situational awareness system



Benefits of Virtual System Integration and Incremental Lifecycle Assurance



Contact Information

Presenter / Point of Contact

Peter H. Feiler

SEI Fellow

Telephone: +1 412.268.7790

Email: phf@sei.cmu.edu