An Incremental Life-cycle Assurance Strategy for Critical System Certification

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Peter H. Feiler
Nov 4, 2014
1. REPORT DATE  
**04 NOV 2014**

2. REPORT TYPE

3. DATES COVERED  
**00-00-2014 to 00-00-2014**

4. TITLE AND SUBTITLE  
**An Incremental Life-cycle Assurance Strategy for Critical System Certification**

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

6. AUTHOR(S)

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)  
**Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA, 15213**

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR’S ACRONYM(S)

11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT  
**Approved for public release; distribution unlimited**

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:

<table>
<thead>
<tr>
<th>a. REPORT</th>
<th>b. ABSTRACT</th>
<th>c. THIS PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>unclassified</td>
<td>unclassified</td>
<td>unclassified</td>
</tr>
</tbody>
</table>

17. LIMITATION OF ABSTRACT  
**Same as Report (SAR)**

18. NUMBER OF PAGES  
**46**

19a. NAME OF RESPONSIBLE PERSON

---

*Standard Form 298 (Rev. 8-98)*  
Prescribed by ANSI Std Z39-18
Outline

Challenges in Safety-critical Software-intensive systems
An Architecture-centric Virtual Integration Strategy with SAE AADL
Improving the Quality of Requirements
Architecture Fault Modeling and Safety
Incremental Life-cycle Assurance of Systems
Summary and Conclusion
Embedded software systems introduce a new class of problems not addressed by traditional system modeling & analysis.

Even with the autopilot off, flight control computers still "command control surfaces to protect the aircraft from unsafe conditions such as a stall," the investigators said.

The unit continued to send false stall and speed warnings to the aircraft's primary computer and about 2 minutes after the initial fault "generated very high, random and incorrect values for the aircraft's angle of attack."

This appears to be a unique event," the bureau said, adding that fitted with the same air-data computer. The advisory is "aimed at minimizing the risk in the unlikely event of a similar occurrence."

Autopilot Off

A "preliminary analysis" of the Qantas plunge showed the error occurred in one of the jet's three air data inertial reference units, which caused the autopilot to disconnect, the ATSB said in a statement on its Web site.

The crew flew the aircraft manually to the end of the flight, except for a period of a few seconds, the bureau said.

Even with the autopilot off, flight control computers still "command control surfaces to protect the aircraft from unsafe conditions such as a stall," the investigators said.

The unit continued to send false stall and speed warnings to the aircraft's primary computer and about 2 minutes after the initial fault "generated very high, random and incorrect values for the aircraft's angle of attack."

No Similar Event

"Airbus has advised that it is not aware of any similar event over the many years of operation of the Airbus," the bureau added, saying it will continue investigating.
Software Problems not just in Aircraft

May 7, 2010

Lexus GX 460 passes retest; Consumer Reports lifts "Don’t Buy" label

Consumer Reports is lifting the Don’t Buy: Safety Risk designation from the 2010 Lexus GX 460 SUV after recall work corrected the problem it displayed in one of our emergency handling tests. (See the original report and video, “Don’t Buy: Safety Risk—2010 Lexus GX 460.”)

We originally experienced the problem in a test that we use to evaluate what’s called lift-off steer. In this test, as the vehicle is driven through a turn, the driver quickly lifts his foot off the accelerator pedal to see how the vehicle reacts. When we did this with our GX 460, its rear end slid out until the vehicle was almost sideways. Although the GX 460 has electronic stability control, which is designed to prevent a vehicle from sliding, the system wasn’t intervening quickly enough to stop the slide. We consider this a safety risk because in a real-world situation this could cause a rear tire to strike a curb or slide off the pavement, possibly causing the vehicle to roll over. Tall vehicles with a high center of gravity, such as the GX 460, heighten our concern. We are not aware, however, of any reports of injury related to this problem.

Lexus recently duplicated the problem on its own test track and developed a software upgrade for the vehicle’s ESC system that would prevent the problem from happening. Dealers received the software fix last week and began notifying GX 460 owners to bring their vehicles in for repair.

We contacted the Lexus dealership from which we had anonymously bought the vehicle and made an appointment to have the recall work performed. The work took about an hour and a half.

Following that, we again put the SUV through our full series of emergency handling tests. This time, the ESC system intervened earlier and its rear did not slide out in the lift-off steer test. Instead, the vehicle understeered—or plowed—when it exceeded its limits of traction, which is a more common result and makes the vehicle more predictable and less likely to roll over. Overall, we did not experience any safety concerns with the corrected GX 460 in our handling tests.

Many appliances now rely on electronic controls and operating software. May 2010 Consumer Reports Magazine. But it turned out to be a problem for the Kenmore 4027 front-loader, which scored near the bottom in our February 2010 report. Our tests found that the rinse cycles on some models worked improperly, resulting in an unimpressive cleaning.

When Sears, which sells the washer, saw our February 2010 Ratings (available to subscribers), it worked with LG, which makes the washer, to figure out what was wrong. They quickly determined that a software problem was causing short or missing rinse and wash cycles, affecting wash performance. Sears and LG say they have reprogrammed the software on the models in warehouses and on about 65 percent of the washers already sold, including the ones we had purchased.

Our retests of the reprogrammed Kenmore 4027 found that the cycles now worked properly, and the machine excelled. It now tops our Ratings (available to subscribers) of more than 50 front-loaders and we’ve made it a CR Best Buy.

If you own the washer, or a related model such as the Kenmore 4044 or Kenmore Elite 4051 or 4219, you should get a letter from Sears for a free service call. Or you can call 800-733-2299.

How do you upgrade washing machine software?
High Fault Leakage Drives Major Increase in Rework Cost

Aircraft industry has reached limits of affordability due to exponential growth in SW size and complexity.

70% Requirements & system interaction errors
80% late error discovery at high rework cost

Where faults are introduced
Where faults are found

The estimated nominal cost for fault removal

Sources:

Major cost savings through rework avoidance by early discovery and correction
A $10k architecture phase correction saves $3M

Where faults are introduced
Where faults are found

The estimated nominal cost for fault removal

Sources:
Mismatched Assumptions in System Interactions

Why do system level failures still occur despite fault tolerance techniques being deployed in systems?

Embedded software system as major source of hazards
Model-based Engineering Pitfalls

Inconsistency between independently developed analytical models

Confidence that model reflects implementation

This aircraft industry experience has led to the System Architecture Virtual Integration (SAVI) initiative

The system

System models

System implementation
Why UML, SysML Are Not Sufficient

• System engineering
  – Focus on system architecture and operational environment
  – SysML developed to capture interactions with outside world, as a standardized UML profile
  – 4 pillars/diagrams: requirements, parameterics (added in SysML), structure, behavior
• Conceptual architecture
  – UML-based component model
  – Architecture views (DoDAF, IEEE 1471)
  – Platform Independent model (PIM)
• Embedded software system engineering
  – OMG Modeling and Analysis of Real Time Embedded systems (MARTE) as UML profile
    • Borrowed Meta model concepts from AADL
    • Focus on modeling implementations
  – xUML insufficient for PSM (Kennedy-Carter, NATO ALWI study)
Impact of Three Step Data Request Protocol

Data Provider

Data Consumer

Request Sensor Data

Request Current State

Request Target State

Receive Sensor Data

Receive Current State

Receive Target State

Apply algorithm

Loop Publish Updated State
Operating as ARINC653 Partitioned System

Data Consumer Requirement

• Process data in 1 second

Partitions

• Provide space and time boundary enforcement
• Execute periodically on a static timeline at 1 second rate

Data request protocols across partitions

How much time does consumer actually have to process the data?
Who pays for the communication overhead?
Model-based Engineering in Practice

Modeling is used in practice

- Modeling, analysis, and simulation in mechanical, control, computer hardware engineering

Current practice: software modeling close to source code

- Remember software through pictures
- MDE and MDA with UML
- Automatically generated documents

We need language for architecture modeling and analysis

- Strongly typed
- Well-defined execution and communication timing semantics
- Systematic approach to dealing with exceptional conditions
- Support for large-scale development
Outline

Challenges in Safety-critical Software-intensive systems
An Architecture-centric Virtual Integration Strategy with SAE AADL
Improving the Quality of Requirements
Architecture Fault Modeling and Safety
Incremental Life-cycle Assurance of Systems
Summary and Conclusion
AADL focuses on interaction between the three elements of a software-reliant mission and safety-critical systems.
The SAE AADL Standard Suite (AS-5506 series)

Core AADL language standard (V2.1-Sep 2012, V1-Nov 2004)

- Strongly typed language with well-defined execution and communication semantics
- Textual and graphical notation
- Standardized XMI interchange format

### Standardized AADL Extensions

- Error Model language for safety, reliability, security analysis
- ARINC653 extension for partitioned architectures
- Behavior Specification Language for modes and interaction behavior
- Data Modeling extension for interfacing with data models (UML, ASN.1, …)

### AADL Annex Extensions in Progress

- Requirements Definition and Assurance Annex
- Synchronous System Specification Annex
- Hybrid System Specification Annex
- System Constraint Specification Annex
- Network Specification Annex
AADL: The Language

Precise execution semantics for components
- Thread, process, data, subprogram, system, processor, memory, bus, device, virtual processor, virtual bus

Continuous control & event response processing
- Data and event flow, call/return, shared access
- End-to-End flow specifications

Operational modes & fault tolerant configurations
- Modes & mode transition

Modeling of large-scale systems
- Component variants, layered system modeling, packages, abstract, prototype, parameterized templates, arrays of components, connection patterns

Accommodation of diverse analysis needs
- Extension mechanism, standardized extensions
Architecture-Centric Quality Attribute Analysis

Single Annotated Architecture Model Addresses Impact Across Operational Quality Attributes

**Safety & Reliability**
- MTBF
- FMEA
- Hazard analysis

**Data Quality**
- Data precision/accuracy
- Temporal correctness
- Confidence

**Security**
- Intrusion
- Integrity
- Confidentiality

**Real-time Performance**
- Execution time/Deadline
- Deadlock/starvation
- Latency

**Resource Consumption**
- Bandwidth
- CPU time
- Power consumption

**Architecture Model**

Auto-generated analytical models
Multi-Fidelity End-to-end Latency in Control Systems

Common latency data from system engineering:
- Processing latency
- Sampling latency
- Physical signal latency

Impact of Scheduler Choice on Controller Stability
A. Cervin, Lund U., CCACSD 2006
Software-Based Latency Contributors

- Execution time variation: algorithm, use of cache
- Processor speed
- Resource contention
- Preemption
- Legacy & shared variable communication
- Rate group optimization
- Protocol specific communication delay
- Partitioned architecture
- Migration of functionality
- Fault tolerance strategy
Early Discovery and Incremental V&V through System Architecture Virtual Integration (SAVI)

- Aircraft: (Tier 0)
  - Aircraft system: (Tier 1)
    - Engine, Landing Gear, Cockpit, ...
    - Weight, Electrical, Fuel, Hydraulics, ...
  - LRU/IMA System: (Tier 2)
    - Hardware platform, software partitions
    - Power, MIPS, RAM capacity & budgets
    - End-to-end flow latency
  - System & SW Engineering:
    - Mechatronics: Actuator & Wings
    - Safety Analysis (FHA, FMEA)
    - Reliability Analysis (MTTF)
  - OEM & Subcontractor:
    - Subsystem proposal validation
    - Functional integration consistency
    - Data bus protocol mappings
  - Subcontracted software subsystem: (Tier 3)
    - Tasks, periods, execution time
    - Software allocation, schedulability
    - Generated executables
  - Repeated Virtual Integration Analyses:
    - Power/weight
    - MIPS/RAM, Scheduling
    - End-to-end latency
    - Network bandwidth

Proof of Concept Demonstration and Transition by Aerospace industry initiative
- Architecture-centric model-based software and system engineering
- Architecture-centric model-based acquisition and development process
- Multi notation, multi team model repository & standardized model interchange

- Multi-tier system & software architecture (in AADL)
- Incremental end-to-end validation of system properties
Multi-Notation Approach to Architecture-centric Virtual System and Software Integration

AADL

Application Software Runtime Architecture
(task & communication)

Application Software Components
(source code)
Java, UML, Simulink

Computer Platform Architecture
(processors & networks)

Hardware Components
(circuits & logic)
VHDL

SysML

Physical System Architecture
(interface with embedded SW/HW)

Physical Components
(mechanical, electrical, heat)
Simulink, Modelica

Operational Environment
(People, Use scenarios)
UML

Control Engineering

Application Software Engineering

Electrical Engineering

SAVI Approach
Model delivery with interchange standards
Model repository content with intra and inter-model consistency
Tool chain flexibility for contractor

Embedded Software Engineering

System Engineering

Mechanical Engineering

Software Engineering Institute
Architecture-centric Virtual Integration Practice (ACVIP)

- Iterative architecture design, safety analysis, and requirement decomposition
- Stakeholder and Quality Attribute (QA) driven architecture-centric requirement specification
- Architecture-centric virtual integration and compositional verification of requirements
- Model-based architecture specifications & multi-dimensional QA analysis
- Testing against verified specifications and models
- Assurance plan and execution

BUSINESS AND MISSION GOALS
ARCHITECTURE
SYSTEM

IMPLEMENT AND EVOLVE
DESIGN
IMPLEMENT
SATISFY
CONFORM
Outline

Challenges in Safety-critical Software-intensive systems
An Architecture-centric Virtual Integration Strategy with SAE AADL
Improving the Quality of Requirements
Architecture Fault Modeling and Safety
Incremental Life-cycle Assurance of Systems
Summary and Conclusion
Certification & Recertification Challenges

Certification: assure the quality of the delivered system
- Sufficient evidence that a system implementation meets system requirements
- Quality of requirements and quality of evidence determines quality of system

Certification related rework cost
- Currently 50% of total system cost and growing

Recertification Challenge
- Desired cost of recertification in proportion to change

Improve quality of requirements and evidence

Perform verification compositionally throughout the life cycle
## Industry Practice in DO-178B Compliant Requirements Capture

### Industry Survey in 2009 FAA Requirements Engineering Study

<table>
<thead>
<tr>
<th>Notation</th>
<th>System Requirements</th>
<th>Data Interconnect (ICD)</th>
<th>High-Level Software Requirements</th>
<th>Low-Level Software Requirements</th>
<th>Hardware Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>English Text or SHALL Statements</td>
<td>39</td>
<td>27</td>
<td>36</td>
<td>32</td>
<td>29</td>
</tr>
<tr>
<td>Tables and Diagrams</td>
<td>31</td>
<td>30</td>
<td>30</td>
<td>19</td>
<td>18</td>
</tr>
<tr>
<td>UML Use Cases</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>UML Sequence Diagrams</td>
<td>1</td>
<td>3</td>
<td>6</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>UML State Diagrams</td>
<td>1</td>
<td>1</td>
<td>7</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Executable Models (e.g. Simulink, SCADE Suite, etc.)</td>
<td>7</td>
<td>1</td>
<td>8</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>Data Flow Diagrams (e.g. Yourdon)</td>
<td>4</td>
<td>6</td>
<td>9</td>
<td>9</td>
<td>9</td>
</tr>
</tbody>
</table>

**Tool**

<table>
<thead>
<tr>
<th>Database (e.g., Microsoft Access)</th>
<th>System Requirements</th>
<th>Data Interconnect (ICD)</th>
<th>High-Level Software Requirements</th>
<th>Low-Level Software Requirements</th>
<th>Hardware Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOORS</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Rational ROSE®</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>RDD-100®</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Requisite Pro®</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>SCADE Suite</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Simulink</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Salt</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Spreadsheets (e.g., Microsoft Excel)</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>State</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Word Processor (e.g., Microsoft Word)</td>
<td>19</td>
<td>20</td>
<td>18</td>
<td>17</td>
<td>16</td>
</tr>
<tr>
<td>VAPS™</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Designer’s Workbench™</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Proprietary Database. SCADE like engineering tool</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Interleaf</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>BEACON</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>CaliberRM</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>XM</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Wiring diagram</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

**Need analyzable & executable specifications**

- Other (Specify)XML: 1
- Operational models or prototypes: 1 1 1
- UML: 1 1

**© 2014 Carnegie Mellon University**
There is more to requirements quality than “shall”’s and stakeholder traceability

**IEEE 830-1998 Recommended Practice for SW Requirements Specification**

<table>
<thead>
<tr>
<th>Requirements error</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incomplete</td>
<td>21%</td>
</tr>
<tr>
<td>Missing</td>
<td>33%</td>
</tr>
<tr>
<td>Incorrect</td>
<td>24%</td>
</tr>
<tr>
<td>Ambiguous</td>
<td>6%</td>
</tr>
<tr>
<td>Inconsistent</td>
<td>5%</td>
</tr>
</tbody>
</table>

IEEE Std 830-1998 characteristics of a good requirements specification:
- Correct
- Unambiguous
- Complete
- Consistent
- Ranked for importance and/or stability
- Verifiable
- Modifiable
- Traceable

**System to SW requirements gap [Boehm 2006]**

*How do we verify low level SW requirements against system requirements?*

When StartUpComplete is TRUE in both FADECs and SlowStartupComplete is FALSE, the FADECStartupSW shall set SlowStartupInComplete to TRUE.
Stakeholder Needs and Requirement Categories

<table>
<thead>
<tr>
<th>Type of Stakeholder Requirement</th>
<th>Types of System Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service or Functional</td>
<td>Functional Requirements</td>
<td>Describe qualitatively the system functions or tasks to be performed in operation.</td>
</tr>
<tr>
<td>Operational</td>
<td>Performance Requirements</td>
<td>Define quantitatively the extent to which the system performance and are or task.</td>
</tr>
<tr>
<td>Interface</td>
<td>Operational Requirements</td>
<td>Define the operational needs of the system, including human element, system.</td>
</tr>
<tr>
<td>Environmental</td>
<td>Interface Requirements</td>
<td>Define how the system is related to its environment, including human element.</td>
</tr>
<tr>
<td>Utilization Characteristics</td>
<td>Operational Requirements</td>
<td>Define operational characteristics and interfaces for the environment, including human element.</td>
</tr>
<tr>
<td>Human Factors</td>
<td>Operational Requirements</td>
<td>Define the operational characteristics and interfaces for the environment, including human element.</td>
</tr>
<tr>
<td>Logistical</td>
<td>Adaptable</td>
<td>Define potential extension, growth, and adaptability.</td>
</tr>
<tr>
<td>Design and Realization Constraints</td>
<td>Physical Constraints</td>
<td>Define constraints on weight, volume, cost, and other performance characteristics.</td>
</tr>
<tr>
<td>Process Constraints</td>
<td>Design Constraints</td>
<td>Define the limits on the optional parameters and their impacts.</td>
</tr>
<tr>
<td>Project Constraints</td>
<td>Environmental Conditions</td>
<td>Define the environmental conditions, including temperature, humidity, air quality, and so on.</td>
</tr>
<tr>
<td>Project Constraints</td>
<td>Logical Requirements</td>
<td>Define the logical requirements for the system, including the need for personnel, spare parts, and so on.</td>
</tr>
<tr>
<td>Business Model Constraints</td>
<td>Policies and Regulations</td>
<td>Define relevant and applicable laws, regulations, and standards.</td>
</tr>
<tr>
<td></td>
<td>Cost and Schedule Constraints</td>
<td>Define, for example, the cost and schedule constraints.</td>
</tr>
</tbody>
</table>

**Table 2. Example of Stakeholder Requirements Classification. (SEBoK Original)**

**Leveson System Theoretic Framework**

**System Development**
- Congress and Legislatures
  - Legislation
  - Government Reports
  - Lobbying
  - Hearings and open meetings
- Government Regulatory Agencies
  - User Associations, Unions, Insurance Companies, Courts

**System Operations**
- Congress and Legislatures
  - Legislation
  - Government Reports
  - Lobbying
  - Hearings and open meetings
  - Accidents
- Government Regulatory Agencies
  - User Associations, Unions, Insurance Companies, Courts

**System, operational environment, development and V&V process**

[Diagram showing system development and operations process]
Mixture of Requirements & Architecture Design Constraints

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.

Requirements and Design Information

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.

Typical requirement documents span multiple levels of a system architecture

We have made architecture design decisions.

We have effectively specified a partial architecture

Adapted from M. Whalen presentation
System Specification and Requirements Coverage

Environmental Assumptions

Requirements Guarantees Assumptions

Precondition Postcondition Invariant

Interaction contract: match input assumption with guarantee

Implementation constraints

Developmental Requirements

Modifiability

Assurability

Quality attribute utility tree

Mission Requirements

Function

Behavior

Performance

Dependability Requirements

Reliability

Safety

Security

Exceptional condition

Interaction contract: match input assumption with guarantee

Implementation constraints

Exceptional condition

Interaction contract: match input assumption with guarantee

Implementation constraints

Exceptional condition
Architecture-led Requirement & Hazard Specification

Error Propagation Ontology

Leveson pattern
Outline

Challenges in Safety-critical Software-intensive systems
An Architecture-centric Virtual Integration Strategy with SAE AADL
Improving the Quality of Requirements
Architecture Fault Modeling and Safety
Incremental Life-cycle Assurance of Systems
Summary and Conclusion
AADL Error Model Scope and Purpose

System safety process uses many individual methods and analyses, e.g.

- hazard analysis
- failure modes and effects analysis
- fault trees
- Markov processes

Goal: a general facility for modeling fault/error/failure behaviors that can be used for several modeling and analysis activities.

Annotated architecture model permits checking for consistency and completeness between these various declarations.

Related analyses are also useful for other purposes, e.g.

- maintainability
- availability
- Integrity
- Security

SAE ARP 4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment
Demonstrated in SAVI Wheel Braking System Example

Error Model Annex can be adapted to other ADLs
Error Propagation Contracts

Incoming/Assumed
- Error Propagation: Propagated errors
- Error Containment: Errors not propagated

Outgoing/Contract
- Error Propagation
- Error Containment

Bound resources
- Error Propagation
- Error Containment
- Propagation to resource

Legend
- Propagation of Error Types
- Not propagated
- Error Flow through component:
  Path P1.NoData->P2.NoData
  Source P2.BadData
  Path processor.NoResource -> P2.NoData

"Not" on propagated indicates that this error type is intended to be contained. This allows us to determine whether propagation specification is complete.
System engineering activity with focus on failing components.
Discovery of Unexpected PSSA Hazard through Repeated Virtual Integration

**Event Log:**
```
EGI Logic
- Oper'l
  - Failed
  - Corrupted

EGI HW
- Oper'l
  - Failed

EGI

Flights Mgmt System
- Auto Pilot
  - Operational
  - Failed
- FMS Processor
  - Operational
  - Failed
- FMS Power
  - Anticipated: NoService

EGI maintainer adds corrupted data hazard to model. Error Model analysis of integrated model detects unhandled propagation.

- Vibration causes boards to touch which causes EGI data corruption
- Unexpected propagation of corrupted Airspeed data results in Stall due to miss-correction
- CorruptedData
- NoData
- Stall
- NoService
```

**Diagram:**
- Auto Pilot
- FMS Processor
- FMS Power
- EGI Logic
- EGI HW
- Flights Mgmt System

**Error Message:**
```
Outgoing propagation (Failure, CorruptedData) is not handled. Expected incoming (Failure)
```
Recent Automated FMEA Experience

Failure Modes and Effects Analyses are rigorous and comprehensive reliability and safety design evaluations

- Required by industry standards and Government policies
- When performed manually are usually done once due to cost and schedule
- If automated allows for
  - multiple iterations from conceptual to detailed design
  - Tradeoff studies and evaluation of alternatives
  - Early identification of potential problems

Largest analysis of satellite to date consists of 26,000 failure modes

- Includes detailed model of satellite bus
- 20 states perform failure mode
- Longest failure mode sequences have 25 transitions (i.e., 25 effects)
Outline

Challenges in Safety-critical Software-intensive systems
An Architecture-centric Virtual Integration Strategy with SAE AADL
Improving the Quality of Requirements
Architecture Fault Modeling and Safety
Incremental Life-cycle Assurance of Systems
Summary and Conclusion
Reliability & Qualification Improvement Strategy

2010 SEI Study for AMRDEC
Aviation Engineering Directorate

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mission Requirements</td>
<td>Model Repository</td>
<td>Operational &amp; failure modes</td>
<td>Resource, Timing &amp; Performance Analysis</td>
</tr>
<tr>
<td>Function</td>
<td>Architecture Model</td>
<td></td>
<td>Reliability, Safety, Security Analysis</td>
</tr>
<tr>
<td>Behavior</td>
<td>Component Models</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Performance</td>
<td>System Implementation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Survivability Requirements</td>
<td>System configuration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reliability</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safety</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Four pillars for Improving Quality of Critical Software-reliant Systems
### Verification Actions

#### Table 2. Main Ontology Elements as Handled within Verification. (SEBoK Original)

<table>
<thead>
<tr>
<th>Element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Attributes (examples)</td>
</tr>
<tr>
<td>Verification Action</td>
<td>A verification action describes what must be verified (the element as reference), on which element, the expected result, the verification technique to apply, on which level of decomposition.</td>
</tr>
<tr>
<td>Verification Procedure</td>
<td></td>
</tr>
<tr>
<td>Verification Tool</td>
<td></td>
</tr>
<tr>
<td>Verification Configuration</td>
<td></td>
</tr>
<tr>
<td>Risk</td>
<td></td>
</tr>
<tr>
<td>Rationale</td>
<td></td>
</tr>
</tbody>
</table>

#### Table 3. Verification Techniques. (SEBoK Original)

<table>
<thead>
<tr>
<th>Verification Technique</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inspection</td>
<td>Technique based on visual or dimensional examination of an element; the verification relies on the human senses or uses simple methods of measurement and handling. Inspection is generally non-destructive, and typically includes the use of sight, hearing, smell, touch, and taste, simple physical manipulation, mechanical and electrical gauging, and measurement. No stimuli (tests) are necessary. The technique is used to check properties or characteristics best determined by observation (e.g., paint color, weight, documentation, listing of code, etc.).</td>
</tr>
<tr>
<td>Analysis</td>
<td>Technique based on analytical evidence obtained without any intervention on the submitted element using mathematical or probabilistic calculation, logical reasoning (including the theory of predicates), modeling and/or simulation under defined conditions to show theoretical compliance. Mainly used where testing to realistic conditions cannot be achieved or is not cost-effective.</td>
</tr>
<tr>
<td>Analogy or Similarity</td>
<td>Technique based on evidence of similar elements to the submitted element or on experience feedback. It is absolutely necessary to show by prediction that the context is invariant that the outcomes are transposable (models, investigations, experience feedback, etc.). Similarity can only be used if the submitted element is similar in design, manufacture, and use; equivalent or more stringent verification actions were used for the similar element, and the intended operational environment is identical to or less rigorous than the similar element.</td>
</tr>
<tr>
<td>Demonstration</td>
<td>Technique used to demonstrate correct operation of the submitted element against operational and observable characteristics without using physical measurements (no or minimal instrumentation or test equipment). Demonstration is sometimes called ‘field testing’. It generally consists of a set of tests selected by the supplier to show that the element response to stimuli is suitable or to show that operators can perform their assigned tasks when using the element. Observations are made and compared with predetermined/expected responses. Demonstration may be appropriate when requirements or specification are given in statistical terms (e.g., meant time to repair, average power consumption, etc.).</td>
</tr>
<tr>
<td>Test</td>
<td>Technique performed onto the submitted element by which functional, measurable characteristics, operability, supportability, or performance capability is quantitatively verified when subjected to controlled conditions that are real or simulated. Testing often uses special test equipment or instrumentation to obtain accurate quantitative data to be analyzed.</td>
</tr>
<tr>
<td>Sampling</td>
<td>Technique based on verification of characteristics using samples. The number, tolerance, and other characteristics must be specified to be in agreement with the experience feedback.</td>
</tr>
</tbody>
</table>
Integrated Approach to Requirement V&V through Assurance Automation

Requirement coverage
Assumption evidence

Generated assurance cases

Safety hazards are part of the picture

Evidence records in terms of claims that requirements have been met

Linkage to automated test harnesses
Secure Mathematically-Assured Composition of Control Models

Key Problem
Many vulnerabilities occur at component interfaces. How can we use formal methods to detect these vulnerabilities and build provably secure systems?

Technical Approach
- Develop a complete, formal architecture model for UAVs that provides robustness against cyber attack
- Develop compositional verification tools driven from the architecture model for combining formal evidence from multiple sources, components, and subsystems
- Develop synthesis tools to generate flight software for UAVs directly from the architecture model, verified components, and verified operation system

Accomplishments
- Created AADL model of vehicle hardware & software architecture
- Identified system-level requirements to be verified based on input from Red Team evaluations
- Developed Resolute analysis tool for capturing and evaluating assurance case arguments linked to AADL model
- Developed example assurance cases for two security requirements
- Developed synthesis tool for auto-generation of configuration data and glue code for OS and platform hardware

16 months into the project
Draper Labs could not hack into the system in 6 weeks
Had access to source code
Building the Assurance Case throughout the Life Cycle

**Continuous Confidence Measure throughout Life Cycle that a System Meets its Requirements**

**Architecture-centric Virtual Integration**

- **Architecture Led Requirements Specification**
- **Virtual Architecture Integration & Analysis**
- **Design Validation by Virtual Integration**
- **Code Coverage Testing**
- **System Integration Lab Testing**
- **Flight Test**

**Incremental Evolution and Execution of Assurance Plans**

- **Incremental Architecture & Requirement Evolution**

**Auto-generated Assurance Cases**

- Need for Multi-valued Argumentation Logic
- Confidence = Requirement Quality + Evidence Quality

**Auto-generation from verified models**
- AADL&SCADE/Simulink
- Ada SPARK/Ravenscar
- MISRA C

**Incremental Contract-based Compositional Verification**

**Build the System**

**Build the Assurance Case**

**FY15/16 line funded project**

Confidence = Requirement Quality + Evidence Quality

Incremental Life-Cycle Assurance
Feller, Nov 4, 2014
© 2014 Carnegie Mellon University
Outline

Challenges in Safety-critical Software-intensive Systems
An Architecture-centric Virtual Integration Strategy with SAE AADL
Improving the Quality of Requirements
Architecture Fault Modeling and Safety
Incremental Life-cycle Assurance of Systems
Summary and Conclusion
Architecture-centric Virtual System Integration & Incremental Life-cycle Assurance

Reduce risks
- Analyze system early and throughout life cycle
- Understand system wide impact
- Validate assumptions across system

Increase confidence
- Validate models to complement integration testing
- Validate model assumptions in operational system
- Evolve system models in increasing fidelity

Reduce cost
- Fewer system integration problems
- Incremental evidence through compositional verification
- Fewer verification steps through generation from single source and verified models
References

AADL Website www.aadl.info and AADL Wiki www.aadl.info/wiki
Blog entries and podcasts on AADL at www.sei.cmu.edu
AADL Book in SEI Series of Addison-Wesley
On AADL and Model-based Engineering
http://www.sei.cmu.edu/library/assets/ResearchandTechnology_AADLandMBE.pdf
On an architecture-centric virtual integration practice and SAVI
http://www.sei.cmu.edu/architecture/research/model-based-engineering/virtual_system_integration.cfm
On an a four pillar improvement strategy for software system verification and qualification