Aerospace Vehicle Systems Institute

Virtual Integration Process
Version 1.0

System Architecture Virtual Integration Program

John Chilenski, SAVI Principal Investigator
Don Ward, TEES SAVI Program Manager
NDIA M&S Subcommittee – Arlington, Virginia
8 April 2014
Outline

- SAVI Overview
- SAVI Version 1.0A Accomplishments
- PSSA with SAVI Consistency Checking Demonstration
- SAVI Version 1.0B Prospects
SAVI Objective and Themes

- Reduce costs/development time through early and continuous model-based virtual integration
  - Shift to new paradigm – integrated models rather than documents
    • Systems engineering in cross-domain context
    • Models provide basis for improvements
    • Models promote consistency – “absence of contradictions”
  - Architecture-centric approach – start with models, but more
    • Meld with requirements for traceability
    • Facilitate trade studies
  - Virtual Integration – early and continuous integrated analysis
    • Proof-based (consistency checked – but not all with formal models)
    • Component-based (hierarchical models)
    • Model-based (annotated models)

Integrate, analyze ... then build’
SAVI Drivers

• Correct Late Discovery of Software Faults

Where faults are introduced
Where faults are found

The estimated normalized cost for fault removal

System-level fault propagation due to incomplete/inconsistent requirements and mismatched assumptions.

0%, 9% 40x
20-100x
500-1000x

70%, 3.5% 1x
10%, 50.5% 16x
20%, 16% 5x
3-6x

20%
50.5%
10%
3.5%
70%

Requirements Engineering
System Design
Software Architectural Design
Component Software Design
Code Development
Unit Test
Integration Test
System Test
Acceptance Test

Sources:

8 Apr 2014
NDIA M&S Committee - Arlington, VA © AVSI
As-Is to To-Be → Single Truth Concept

- Models from multiple design teams contain multiple interdependent properties
  - Each design team identifies multiple ways of modeling (abstracting) these common properties - multiple models and tools
  - Each team abstracts properties in different ways
  - Each team’s approach to modeling common properties may not be equivalent

- Results: multiple truths
SAVI VIP

Higher Level Verification Checks

Develop Verification Checks

Define Dependencies

Register Dependencies

Perform Consistency Checks

Consistent?

NO

Resolve Inconsistencies by

Perform Verification Checks

Compliant?

YES

NO

Resolve Non-compliance by

Higher Level Models

Refine Model(s)

Lower Level Model(s)

Incorrect Higher Level Verification Check(s)

Incorrect Model(s) Refinement

Incorrect Verification Check

Incorrect Higher Level Model(s)

Incorrect Higher Level Verification Check(s)

Consistency Checks

Models and Verification Checks sent to Integrator

8 Apr 2014

NDIA SE M&S Committee - Arlington, VA © AVSI

© AVSI
SAVI Virtual Integration “Vee”

Predictive

Sensitivity analysis for uncertainty

Confidence in implementation

Validated

1. Requirements Engineering
2. System Design
3. Software Architectural Design
4. Component Structural Design
5. Component Hardware Design
6. High-level ADL Model
7. Detailed ADL Model
8. Specify Model-Code Interfaces
9. Hardware Development
10. Software Development
11. Integration Test
12. SW Int. Test
13. HW Int. Test
14. System Test
15. Acceptance Test

→ generation of test cases
← updating models with actual data

Keeping the system continuously integrated!

Model-driven artifact generation
Conformance of models and systems

→ flowchart is inside each of these triangles

8 Apr 2014
NDIA M&S Committee - Arlington, VA © AVSI
“Twin Peaks” Model by Bashar Nuseibeh*

MBD requires continuous iteration of the requirements models and properties and the development/implementation models and properties.

Sources:
*http://www.oro.open.ac.uk/2212/1/00910904.pdf
adapted from:
SAVI Capability Tree

**Main Focus**
**For SAVI V. 1.0A**

**Main Focus**
**For SAVI V. 1.0B**

**Main Focus**
**For SAVI V. 1.0C**

**Main Focus**
**For SAVI V. 1.0D**

**Legend**
- Identified, not exercised
- Exercised in prototype only
- Exercised in PoC demo
- Exercised in V. 1.0A
- Exercised adequately
WBS Safety Analysis

• Selected as a pathfinder/demonstration for SAVI analysis
  – Existing “S-18 Aircraft” WBS in Aerospace Information Report (AIR) 6110
  – Example of 4754A development process and supporting 4761 safety analysis
  – Specific focus on WBS PSSA within process flow
• Highlight the iterative design process
  – First safety evaluation
  – Refinement through system development
• Use of commercial and open-source tools
  – Industry standard or low/no cost tools and capabilities in SAVI infrastructure
  – Provide means for “mapping” data to/from state-of-art analysis tools
PSSA in Development Process Context

Adapted from ARP 4754A Fig. 5 – Interaction between Safety and Development Processes

ARP 4754A Processes DO178/DO254
AFE 61 Model Overview

• The model set for the AFE 61 WBS PSSA consists of five models for the simplified WBS
  – A set of requirements from AIR 6110
  – A Publisher/Subscriber model forming the basis for an ICD later in the project
  – A SysML model documenting the architecture at the beginning of the project
  – An AADL model documenting the refined (final) architecture model at the end of the project
    • Along with the associated Error Model supporting the automated safety analyses
  – A solid geometry model documenting the location of components in 3-space
# Requirements Model

## A/C Reqts (excerpt)

### Aircraft Requirements (excerpts)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
<th>Derived</th>
<th>Traced From</th>
</tr>
</thead>
<tbody>
<tr>
<td>S18-ACFT-R-009</td>
<td>Aircraft shall have a means to decelerate on the ground in accordance with 14CFR 25.735</td>
<td>Minimum standard required for aircraft certification</td>
<td>14 CFR Part 25.735</td>
</tr>
<tr>
<td>S18-ACFT-R-0110</td>
<td>Aircraft shall have autobrake function</td>
<td>Derived</td>
<td>Technology improvements in CAT IIIb auto-landing capability and market research, report MRS 18-XXX about the customer needs</td>
</tr>
<tr>
<td>S18-ACFT-R-0135</td>
<td>Aircraft shall provide an anti-skid function.</td>
<td>Derived</td>
<td>All weather operation and stability of the aircraft during runway</td>
</tr>
<tr>
<td>S18-ACFT-R-0184</td>
<td>Aircraft shall have hydraulically-driven brake function</td>
<td>Derived</td>
<td>The pilot shall be allowed to override the autobrake function.</td>
</tr>
<tr>
<td>S18-ACFT-R-0185</td>
<td>The pilot shall be allowed to override the autobrake function.</td>
<td>14 CFR 25.735(2)</td>
<td>Traced From 14 CFR Part 25.735(2)</td>
</tr>
</tbody>
</table>

### Aircraft FHA (excerpt)

#### Aircraft FHA (excerpts)

<table>
<thead>
<tr>
<th>Failure Condition (Hazard Description)</th>
<th>Phase</th>
<th>Condition on Aircraft/Crew</th>
<th>Effect of Failure on Aircraft/Crew</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of Deceleration Capability</td>
<td>Landing, RTO, Taxi</td>
<td>See Below</td>
<td>See Below</td>
<td></td>
</tr>
<tr>
<td>a. Unannunciated loss of Deceleration Capability</td>
<td>Landing, RTO</td>
<td>Catastrophic</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. Announced loss of Deceleration Capability</td>
<td>Landing, RTO</td>
<td>Hazardous</td>
<td></td>
<td></td>
</tr>
<tr>
<td>c. Unannounced loss of Deceleration Capability</td>
<td>Taxi</td>
<td>Major</td>
<td></td>
<td></td>
</tr>
<tr>
<td>d. Announced loss of Deceleration Capability</td>
<td>Taxi</td>
<td>No Safety Effect</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### WBS FHA (excerpt)

#### Work Breakdown Structure FHA (excerpts)

<table>
<thead>
<tr>
<th>Function</th>
<th>Failure Condition (Hazard Description)</th>
<th>Phase</th>
<th>Effect of Failure on Aircraft/Crew</th>
<th>Classification</th>
<th>Reference to Supporting Material</th>
<th>Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decelerate Aircraft using Wheel Braking</td>
<td>Total Loss of wheel braking</td>
<td>Landing or RTO</td>
<td>See Below</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. Unannounced loss of wheel braking</td>
<td>Landing or RTO</td>
<td>Crew detects the failure when the brakes are opened. The crew uses spoilers and thrust reversers to maximum extent possible. This may result in a runway overrun.</td>
<td>Hazardous</td>
<td>S18 Aircraft FTA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. Announced loss of wheel braking</td>
<td>Landing</td>
<td>Crew selects a more suitable airport, notifies emergency ground support, and prepares occupants for runway overrun. The crew uses spoilers and thrust reversers to the maximum extent possible.</td>
<td>Hazardous</td>
<td>S18 Aircraft FTA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partial Symmetrical Loss of Wheel Braking</td>
<td>Landing or RTO</td>
<td>See below</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. Unannounced partial symmetrical loss of wheel braking</td>
<td>Landing or RTO</td>
<td>The crew detects the failure when the brakes are opened. Crew uses available wheel braking, spoilers and thrust reversers available to maximum extent to decelerate the aircraft. The temperature on wheels of the loaded aircraft increases and could reach point where wheel/fire failure occurs. Depending on number of brakes lost result could be an overrun.</td>
<td>Major to Hazardous</td>
<td>Additional study required to determine classification</td>
<td>Potentially catastrophic AC to be confirmed by analysis</td>
<td></td>
</tr>
<tr>
<td>b. Announced partial symmetrical loss of wheel braking</td>
<td>Landing</td>
<td>The crew selects a more suitable airport, notifies emergency ground support, and prepares occupants for runway overrun.</td>
<td>Hazardous</td>
<td>S18 Aircraft FTA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asymmetrical Loss of Wheel Braking</td>
<td>Landing or RTO</td>
<td>See below</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. Announced partial asymmetrical loss of wheel braking</td>
<td>Landing or RTO</td>
<td>The crew detects the failure when the brakes are opened. Crew uses available wheel braking, spoilers and thrust reversers available to maximum extent to decelerate the aircraft. The temperature on wheels of the loaded aircraft increases and could reach point where wheel/fire failure occurs. Depending on number of brakes lost result could be an overrun.</td>
<td>Major</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. Announced partial asymmetrical loss of wheel braking</td>
<td>Landing or RTO</td>
<td>The crew selects a more suitable airport, notifies emergency ground support, and prepares occupants for runway overrun.</td>
<td>Hazardous</td>
<td>S18 Aircraft FTA</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

8 Apr 2014 NDIA M&S Committee - Arlington, VA © AVSI
## Publisher/Subscriber Model

### ATA Name
- z24-xx-101 Elec. Pwr. Sys. - L
- z24-xx-102 Elec. Pwr. Dist. Unit - Wheel Well - L
- z24-xx-201 Elec. Pwr. Sys. - R
- z27-xx-101 Rudder Pedal Assembly - L
- z27-xx-104 Rudder Pedal Rudder Position Sensor - L
- z27-xx-201 Rudder Pedal Assembly - R
- z27-xx-204 Rudder Pedal Rudder Position Sensor - R
- z29-xx-102 HPS - L Isolation Valve - L
- z29-xx-103 Selector Valve - L
- z29-xx-104 Accumulator - L

### Publisher/Subscriber Table

<table>
<thead>
<tr>
<th>Publisher ATA</th>
<th>Publisher Name</th>
<th>Connection</th>
<th>Signal</th>
<th>Subscriber ATA</th>
<th>Subscriber Name</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>z29-xx-103</td>
<td>Selector Valve - L</td>
<td>z29-xx-103, z29-xx-104</td>
<td>Hyd. Power (Pressure)</td>
<td>z29-xx-104</td>
<td>Accumulator - L Bi</td>
<td></td>
</tr>
</tbody>
</table>
SysML Model (Early Architecture)
System and SW Architecture with AADL

HW and SW Runtime Architecture with well-defined execution semantics

System Implementation & deployment

Hierarchy of Component Implementations

Textual & Graphical Representation
Architecture Fault Modeling with EMV2

- Error sources, propagation paths & sinks per component
- Fault impact visualization & reports
- Hierarchical fault models
Solid Geometry Model

- Power wire for sensors
- Selector valve
- Accumulator
- Metering valves
- Manual Metering valves
- Hydraulic Pressure sensors
Automation of Safety Analysis Practice

- Use of Error Model EMV2 and ARINC653 annexes
  - Relevance for the avionics community
  - SEI developed simplified public model

- Comparative architecture trade study
  - Federated vs. Integrated Modular Avionics (IMA) architecture

- Support of SAE ARP 4761 System Safety Assessment Practice
  - Hazards (FHA), Fault Trees (FTA), Fault Impact (FMEA)
  - Reliability/Availability Markov Analysis (MA)/Dependence Diagram (DD)
Inter-Model Consistency

- Each group has views/models of the airplane
- Relations/Dependencies exist between the views/models used

- Inconsistent →
  - Possible Problems
  - Not Valuable
Dependencies Are Key

**Software**

**Project Management**

**Systems**

**Electrical**

**Manufacturing**

**Mechanical**

**Test & Evaluation**

**Structures**

**Aerodynamics**

**Propulsion**

Industry wide, 50% of requirements will change between CDR and delivery into service

- The SAVI Repository stores the links
- When an element is changed, links and relationships are traced to find affected elements
- Each dependency must be identified, tracked and checked throughout the life cycle
Inter-Model Consistency Checking

• Consistency between two models exists when the dependence relations between those two models are satisfied
  – Some dependence relations can be detected automatically
    • Some tools are using patterns to assist
  – Some dependence relations will (always) require manual identification
  – Fidelity of consistency is proportional to the effort put into consistency modeling

• Dependence relations exist between entities and attributes
  – The output of one parameter in a model is the input for another model
    • IEEE floating point radar altitude in feet
    • NOT radar altitude on one side and barometric altitude on the other
    • NOT feet on one side and meters on the other
PSSA Video Example
SAVI Version 1.0B - Objectives

• Mature and extend SAVI VIP capabilities to include initial fit and behavioral capabilities
  – Extend WBS example system to include behavioral and fit characteristics (add antiskid and autobraking)
  – Exercise fit and behavioral aspects of the WBS model-based example
  – Carry out consistency checking for the expanded WBS Model

• Implement an ISO10303-239 (PLCS) DEX (or DEXes) into the SAVI Model Repository/Data Exchange Layer (MR/DEL)
Questions?

Contacts:

John Chilenski  
Phone: (425) 237-2624  
john.j.chilenski@boeing.com

Dr. Don Ward  
Phone: (254) 842-5021  
Mobile: (903) 818-3381  
dward@avsi.aero

Dr. Dave Redman  
Office: (979) 862-2316  
Mobile: (979) 218-2272  
dredman@avsi.aero