Importance of Consistency Checking in the SAVI Virtual Integration Process (VIP)

Dr. David Redman
Director
Aerospace Vehicle Systems Institute (AVSI)
Outline

• Brief intro to AVSI
• Motivation for SAVI
• Overview of SAVI Concepts
• Results for 2013
• Progress in 2014
• Conclusions and Open Discussion
# The Aerospace Vehicle Systems Institute (AVSI)

## Global Product Data Interoperability Summit | 2014

### Full Members
- Airbus
- Boeing
- DoD
- Airbus Group
- Embraer
- GE Aviation

### Liaison Members
- FAA
- NASA
- Aerospace Valley
- SEI

### Associate Members
- BAE Systems
- Bombardier
- Gulfstream
- Lockheed Martin

### Current SAVI member
- Current SAVI member

### Joining SAVI now
- Joining SAVI now

### Discussing rejoining SAVI
- Discussing rejoining SAVI

### Participated earlier in SAVI
- Participated earlier in SAVI
MOTIVATION FOR VIRTUAL INTEGRATION
Systems Are Becoming More Complex

Estimated Onboard SLOC Growth

Slope: 0.1778  Intercept: -338.5
(commercial airliners only)
Curve implies SLOC doubles about every 4 years

This line fit is pegged at 27.5 M SLOC because the SLOC sizes for 2010-2020 are not affordable. The COCOMO II estimated costs to develop that much software is in excess of $10B

Airbus data source: J. P. Potocki De Montalk, "Computer Software in Civil Aircraft," Sixth Annual Conference on Software Assurance (Compass '91), Gaithersburg, MD, June 24-27, 1991
Boeing data source: J. J. Chilenski, 2009
...with complex Development Ecosystems

Global Product Data Interoperability Summit | 2014
... using dated SE methods

Global Product Data Interoperability Summit | 2014

Silo’ed Organizations

“pi”

\[ \pi = 3.14, \quad 3.14159265, \quad 3.141592653589793 \]

Written Requirements

Mismatched Assumptions
... that drive SCHEDULE DELAYS
... and COST GROWTH

Global Product Data Interoperability Summit | 2014
The impact is documented

High-level Req's in RFP

High-level Design

RFP Response

PDR

Req's Defined

Sys Design

Detailed Design

Sys Re-Design

Sys Development

Sys Integration

V&V

Target Completion

70% errors

3.5% detected

1x cost

10% errors

80% detected

16-100x cost

500-1000x (INCOSE 2011)

Sources:


COST GROWTH

SCHEDULE DELAY
Current Means of Managing Complexity Have Issues

Global Product Data Interoperability Summit | 2014

- Operational Models
- System Models
- Component Models
- Functional/Behavior Model
- Performance Model
- Structural/Component Model
- Cost Model
- Safety Model
- Security Model
- Reliability Model
- Maintainability Model
- Sustainability Model
- Model Abstractions
- Indeterminate Change Impact
- Multiple Truths

MODEL EXPLOSION

- Modeling Domains
  - Ops/Mission Analysis
  - System Design
  - Algorithm Hardware Software Integration
  - Manufacturing
  - Verification & Testing Simulation
  - Systems Engineering Analysis
  - System Integration
- System Architecture Model (Integration Framework)
- Analysis Models
- Hardware Models
- Software Models
- Verification Models
SAVI CONCEPTS
SAVI Goals and Approach

• Reduce costs/development time through early and continuous model-based virtual integration
  • Distributed inter-domain/inter-model consistency checks throughout development - (start integrated, stay integrated)
  • Protect intellectual property (IP)
  • Capture incremental evidence for safety analysis and for certification Approach

• Capture Requirements and Use Cases that define the following:
  • SAVI Data Exchange Layer
  • SAVI Model Repository
  • SAVI Virtual Integration Process
  • SAVI distributed inter-domain/inter-model dependencies and consistency checks
SAVI Objective and Themes

Global Product Data Interoperability Summit | 2014

- 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”
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

Global Product Data Interoperability Summit | 2014

- Each dependency needs to be identified, tracked and checked throughout the life cycle.
Dependencies Are Key

Global Product Data Interoperability Summit | 2014

When an element is changed, links and relationships are traced to find affected elements.

The SAVI Repository stores the links.

Industry wide, 50% of requirements will change between CDR & delivery into service.
Inter-Model Consistency Checking

Global Product Data Interoperability Summit | 2014

- 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
  - Topology of system must be equivalent in all models
What is SAVI Consistency?

- Initially identified 6 types of consistency
  - Interface
  - Compositional
  - Constraint
  - Behavioral
  - Version
  - Verification

Physical Geometry

32-bit

64-bit

Ground Proximity Warning System

Avionics Model

Landing Gear Model

Engine Indication and Crew Alerting System

Air/Ground Signal

Radio Altimeter

Weight on Wheels

Speed Indicator

Altimeter

On Ground

In Flight

Global Product Data Interoperability Summit | 2014
What is SAVI Consistency?

Global Product Data Interoperability Summit | 2014

- 6 initial types
  - Interface
  - Compositional
  - Constraint
  - Behavioral
  - Version
  - Verification

- Additional types of consistency
  - Data
    - Value
    - Type
    - Semantics
    - Metadata
  - Model
    - Property
    - Semantics
    - Metadata
    - Behavior

Runtime Consistency: Data Safety, Latencies, Buffer Overflow, Resource Sharing, Data Ordering, etc.

Mathworks 32-bit
Mathworks 64-bit Unix

\[
\pi = 3.1415927
\]

\[
\pi = 3.14159265358979323846
\]

Signal connectivity analysis doesn’t need wiring length but signal latency and jitter analysis does.
SAVI VIP

Global Product Data Interoperability Summit | 2014

- Develop Verification Checks
- Define Dependencies
- Register Dependencies
- Perform Consistency Checks
- Consistent?
- NO
- Resolve Inconsistencies by Consistency Checks
- YES
- Perform Verification Checks
- Compliant?
- NO
- Resolve Non-compliance by
- YES
- Models and Verification Checks sent to Integrator

Incorrect Higher Level Model(s)
Incorrect Model(s)
Incorrect Verification Check(s)
Incorrect Higher Level Verification Check(s)
Incorrect Dependence Definition
Incorrect Dependency Definition
Incorrect Model Refinement
Incorrect Verification Check Refinement
Consistent?
NO
YES

Incorrect Higher Level Models
Refine Model(s)
Lower Level Model(s)

Copyright © 2014 Boeing. All rights reserved.
Copyright © 2014 Northrop Grumman Corporation. All rights reserved.
SAVI Virtual Integration “Vee”

Global Product Data Interoperability Summit | 2014

- Requirements Engineering
- System Design
- Hardware Architectural Design
- Software Architectural Design
- Component Hardware Design
- Component Software Design
- Specify Model-Code Interfaces
- Detailed ADL Model
- High-level ADL Model
- Top-Level Verification Items

Flowchart is inside each of these triangles

- System Test
- Integration Test
- SW Int. Test
- HW Int. Test
- Software Unit Test
- Hardware Unit Test

- Generation of test cases
- Updating models with actual data

Keeping the system continuously integrated!

- Sensitivity analysis for uncertainty
- Confidence in implementation

BOEING is a trademark of Boeing Management Company
Copyright © 2014 Boeing. All rights reserved.
Copyright © 2014 Northrop Grumman Corporation. All rights reserved.
GPDIS_2014.ppt | 22
INITIAL VIP CAPABILITY
VERSION 1.0A - 2013
• Selected as a pathfinder/demonstration for SAVI analysis
  • Existing “S-18 Aircraft” wheel braking system (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
• Enable trade-studies incorporating safety
• Use of commercial and open-source tools
  • Industry standard or low/no cost tools and capabilities in SAVI infrastructure
AFE 61 Model Overview

Global Product Data Interoperability Summit | 2014

- The model set for the AFE 61 WBS PSSA consists of five models for the simplified WBS
  - A set of requirements from AIR 6110 (Spreadsheet)
  - A Publisher/Subscriber model forming the basis for an ICD later in the project (Spreadsheet)
  - A SysML model documenting the architecture at the beginning of the project (Enterprise Architect, SCADE System)
  - An AADL model documenting the refined (final) architecture model at the end of the project (OSATE)
    - Along with the associated Error Model supporting the automated safety analyses
  - A solid geometry model documenting the location of components in 3-space (Solidworks, NX)
### A/C FHA (excerpt)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
<th>Trace From</th>
</tr>
</thead>
<tbody>
<tr>
<td>S18-ACFT-R-0009</td>
<td>Aircraft shall have a means to decelerate on the ground in accordance with 14CFR Part 25.735</td>
<td>Minimum standard required for aircraft certification</td>
</tr>
<tr>
<td>S18-ACFT-R-0110</td>
<td>Aircraft shall have autobrake function</td>
<td>Derived</td>
</tr>
<tr>
<td>S18-ACFT-R-0135</td>
<td>Aircraft shall provide an anti-skid function.</td>
<td>Derived</td>
</tr>
<tr>
<td>S18-ACFT-R-0184</td>
<td>Aircraft shall have hydraulically-driven brake function</td>
<td>Derived</td>
</tr>
<tr>
<td>S18-ACFT-R-0185</td>
<td>The pilot shall be allowed to override the autobrake function.</td>
<td>14CFR 25.735(c)(2)</td>
</tr>
</tbody>
</table>

### A/C Reqs (excerpt)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S18-ACFT-R-0009</td>
<td>Aircraft shall have a means to decelerate on the ground in accordance with 14CFR Part 25.735</td>
</tr>
<tr>
<td>S18-ACFT-R-0110</td>
<td>Aircraft shall have autobrake function</td>
</tr>
<tr>
<td>S18-ACFT-R-0135</td>
<td>Aircraft shall provide an anti-skid function.</td>
</tr>
<tr>
<td>S18-ACFT-R-0184</td>
<td>Aircraft shall have hydraulically-driven brake function.</td>
</tr>
<tr>
<td>S18-ACFT-R-0185</td>
<td>The pilot shall be allowed to override the autobrake function.</td>
</tr>
</tbody>
</table>

### WBS FHA (excerpt)

<table>
<thead>
<tr>
<th>Function</th>
<th>Failure Condition (Hazard Description)</th>
<th>Phase</th>
<th>Effect of Failure Condition 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>Hazardous</td>
<td>S18-ACFT-R-0009</td>
<td></td>
</tr>
<tr>
<td>a. Unannunciated loss of wheel braking</td>
<td>Crew detects the failure when the brakes are operated. The crew uses spoilers and thrust reversers to the maximum extent possible. This may result in a runway overrun.</td>
<td>Landing or RTO</td>
<td>See Below</td>
<td>Hazardous</td>
<td>S18 Aircraft FTA</td>
<td></td>
</tr>
<tr>
<td>b. Annunciated loss of wheel braking</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>Landing</td>
<td>See Below</td>
<td>Hazardous</td>
<td>Crew procedures for loss of normal and reserve modes</td>
<td>S18 Aircraft FTA</td>
</tr>
<tr>
<td>Partial Symmetrical Loss of Wheel Braking</td>
<td>Loss of wheel braking</td>
<td>Landing or RTO</td>
<td>See below</td>
<td>Major</td>
<td>Additional study required to determine classification</td>
<td>Potentially catastrophic at 40&quot; to be confirmed by analysis</td>
</tr>
<tr>
<td>a. Unannunciated partial symmetrical loss of wheel braking</td>
<td>The crew detects the failure when the brakes are used. Crew uses available wheel braking, spoilers and thrust reversers available to maximum extent to decelerate the aircraft. The temperature on wheels of the loaded brakes increases and could reach point where wheel/fire failure occurs. Depending on number of brakes lost result could be an overrun.</td>
<td>Landing or RTO</td>
<td>See below</td>
<td>Hazardous</td>
<td>Additional study required to determine classification</td>
<td>Potentially catastrophic at 40&quot; to be confirmed by analysis</td>
</tr>
<tr>
<td>b. Annunciated partial symmetrical loss of wheel braking</td>
<td>The crew is aware that there is a partial loss of braking before landing. Crew uses wheel braking, spoilers and thrust reversers available to maximum extent to decelerate the aircraft. The temperature on wheels of the loaded brakes increases and could reach point where wheel/fire failure occurs. Depending on number of brakes lost result could be an overrun.</td>
<td>Landing</td>
<td>See below</td>
<td>Major</td>
<td>Additional study required to determine classification</td>
<td>Potentially catastrophic at 40&quot; to be confirmed by analysis</td>
</tr>
<tr>
<td>Asymmetrical Loss of Wheel Braking</td>
<td>Loss of wheel braking</td>
<td>Landing or RTO</td>
<td>See below</td>
<td>Hazardous</td>
<td>Additional study required to determine classification</td>
<td>Potentially catastrophic at 40&quot; to be confirmed by analysis</td>
</tr>
<tr>
<td>a. Asymmetrical loss of wheel braking</td>
<td>The crew is aware that there is a partial loss of braking before landing. Crew uses wheel braking, spoilers and thrust reversers available to maximum extent to decelerate the aircraft. The temperature on wheels of the loaded brakes increases and could reach point where wheel/fire failure occurs. Depending on number of brakes lost result could be an overrun.</td>
<td>Landing or RTO</td>
<td>See below</td>
<td>Hazardous</td>
<td>Additional study required to determine classification</td>
<td>Potentially catastrophic at 40&quot; to be confirmed by analysis</td>
</tr>
<tr>
<td>b. Asymmetrical loss of wheel braking</td>
<td>The crew is aware that there is a partial loss of braking before landing. Crew uses wheel braking, spoilers and thrust reversers available to maximum extent to decelerate the aircraft. The temperature on wheels of the loaded brakes increases and could reach point where wheel/fire failure occurs. Depending on number of brakes lost result could be an overrun.</td>
<td>Landing or RTO</td>
<td>See below</td>
<td>Hazardous</td>
<td>Additional study required to determine classification</td>
<td>Potentially catastrophic at 40&quot; to be confirmed by analysis</td>
</tr>
<tr>
<td>c. Unannunciated loss of Deceleration Capability</td>
<td>Taxi</td>
<td>Major</td>
<td>Crew is unable to decelerate the aircraft, resulting in low speed contact with terminal, aircraft, or vehicles.</td>
<td>Major</td>
<td>Additional study required to determine classification</td>
<td>Potentially catastrophic at 40&quot; to be confirmed by analysis</td>
</tr>
<tr>
<td>d. Annunciated loss of Deceleration Capability</td>
<td>Taxi</td>
<td>No Safety Effect</td>
<td>Crew steers the aircraft clear of any obstacles and calls for a tug or portable stairs.</td>
<td>No Safety Effect</td>
<td>Additional study required to determine classification</td>
<td>Potentially catastrophic at 40&quot; to be confirmed by analysis</td>
</tr>
</tbody>
</table>
System and SW Architecture with AADL

Global Product Data Interoperability Summit | 2014

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

Global Product Data Interoperability Summit | 2014

- BSCUs
- Electrical Line to sensors
- Electrical Power supplies
- Hydraulic Power supplies
- Hydraulic components
Solid Geometry Model

Global Product Data Interoperability Summit | 2014

- Power wire for sensors
- Selector valve
- Accumulator
- Metering valves
- Manual Metering valves
- Hydraulic Pressure sensors
Inter-Model Consistency Checks

Global Product Data Interoperability Summit | 2014

Solid models

BSCU

Hyd power supply

Accumulator

Functional Models

(AADL – SysML)
Automation of Safety Analysis Practice

Global Product Data Interoperability Summit | 2014

- Use of Error Model EMV2 and ARINC653 annexes
  - Relevance for the avionics community

- 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)
CAPABILITIES BEING ADDED
VERSION 1.0B - 2014
• **Printed Circuit Board Interconnect**
  • Prove physical implementation matches (is consistent with) the logical design (schematic)
  • Future: expand use case to include wiring harnesses
**AFE 61S1 (2014) Use Cases**

Global Product Data Interoperability Summit | 2014

- **Autobrake/antiskid enabled**
  - Multiple communicating state machines
  - Multiple communicating control laws

- **Electro-mechanical braking system**
  - Adds multi-physics simulation models to the mix

Typical mode select/control panel
Summary

Global Product Data Interoperability Summit | 2014

- **SAVI target/goals (summary)**
  Reduce costs/development time through early and continuous model-based virtual integration
  - Distributed inter-domain/inter-model consistency checks throughout development - (start integrated, stay integrated)
  - Protect intellectual property (IP)
  - Capture incremental evidence for safety analysis and for certification

- **Approach**
  Capture Requirements and Use Cases that define the following:
  - SAVI Data Exchange Layer
  - SAVI Model Repository
  - SAVI Virtual Integration Process
  - SAVI distributed inter-domain/inter-model dependencies and consistency checks
Questions or Comments?

Global Product Data Interoperability Summit | 2014

• For more information
  
  • SAVI Program Manager: Dr. Don Ward (dward@avsi.aero)
  
  • AVSI Director: Dr. Dave Redman (dredman@avsi.aero)
  
  • Web: savi.avsi.aero
Acronyms

Global Product Data Interoperability Summit | 2014

- AFE – Authority For Expenditure
- AIR – Aerospace Information report
- AVSI – Aerospace Vehicle Systems Institute
- BSCU – Braking System Control Unit or Brake and Steering Control Unit
- IMA – Integrated Modular Avionics
- IP – Intellectual Property
- PCB – Printed Circuit Board
- PSSA – Preliminary Systems Safety Assessment
- SAVI – Systems Architecture Virtual Integration
- SE – Systems Engineering
- VIP – Virtual Integration Process
- WBS – Wheel Braking System
- CFDIU – Centralized Fault Display Interface Unit