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

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

GLOBAL PRODUCT DATA INTEROPERABILITY
SUMMIT
2014

ELYSIUM Parker NORTHROP GRUMMAN BOEING

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)

Full Members

- Airbus
- Boeing
- DoD
- Airbus Group
- Embraer
- GE Aviation
- Honeywell
- Rockwell Collins
- Rolls Royce
- Saab
- United Technologies

Liaison Members

- FAA
- NASA
- Aerospace Valley
- SEI

Current SAVI member

Joining SAVI now

Discussing rejoining SAVI

Participated earlier in SAVI

Associate Members

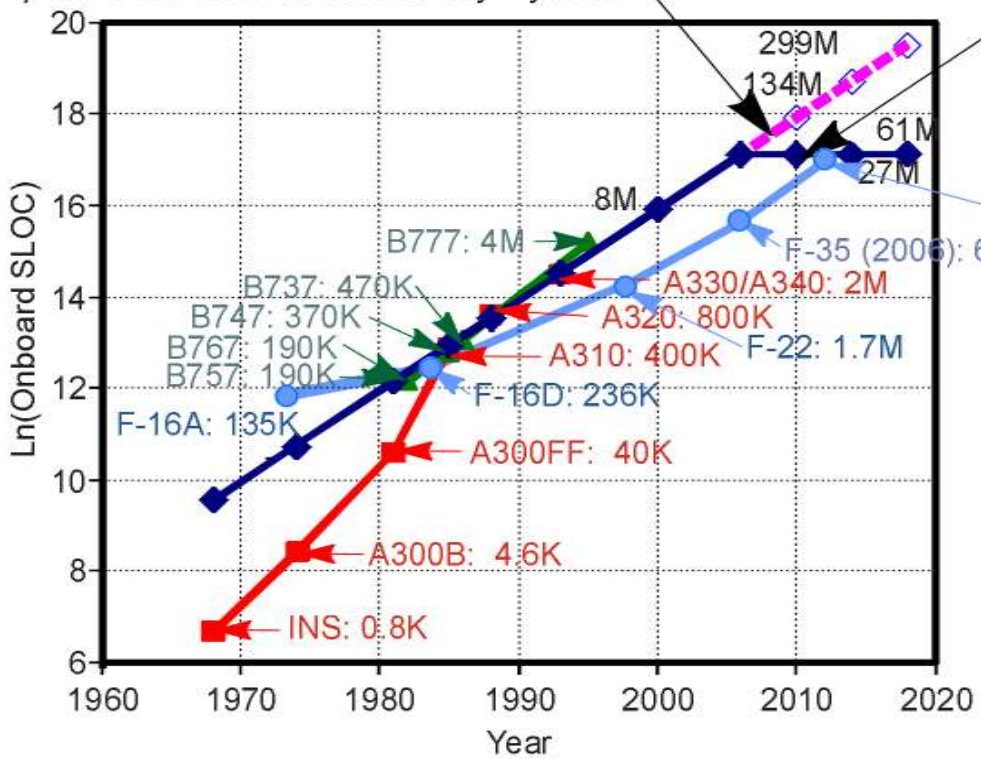
- BAE Systems
- Bombardier
- Gulfstream
- Lockheed Martin

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



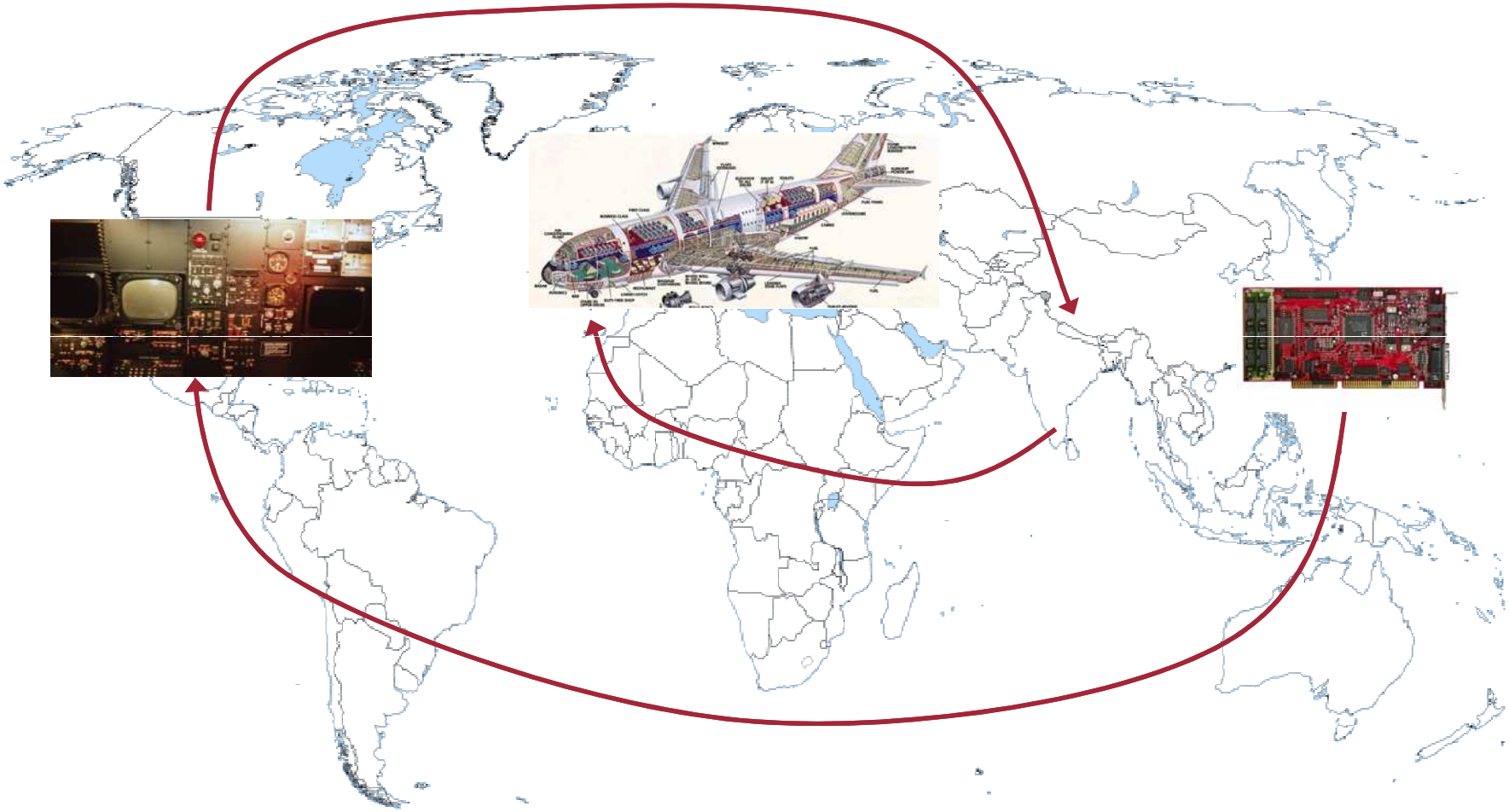
This line fit is pegged at 27.5 M SLOC because the SLOC sizes for 2010 - 2020 are not affordable. The COCOMO II estimated costs to develop that much software is in excess of $10B

- Straight line curve fit
- Boeing aircraft
- Airbus aircraft
- USAF fighter aircraft
- Not affordable extrapolation

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
USAF fighter data source: Hagen and Sorenson, "Delivering Military Software Affordably,: Defense AT&L, March-April 2013

…with complex Development Ecosystems

Global Product Data Interoperability Summit | **2014**



src: http://en.wikipedia.org/wiki/File:Gravis_UltraSound_PNP.jpg

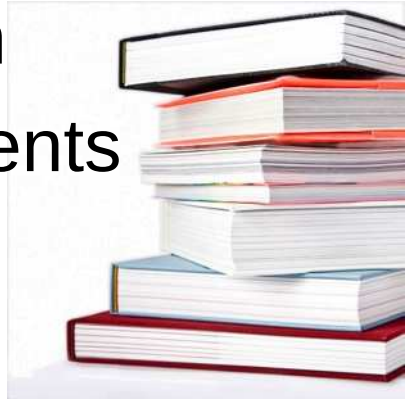
… using dated SE methods

Silo'ed Organizations

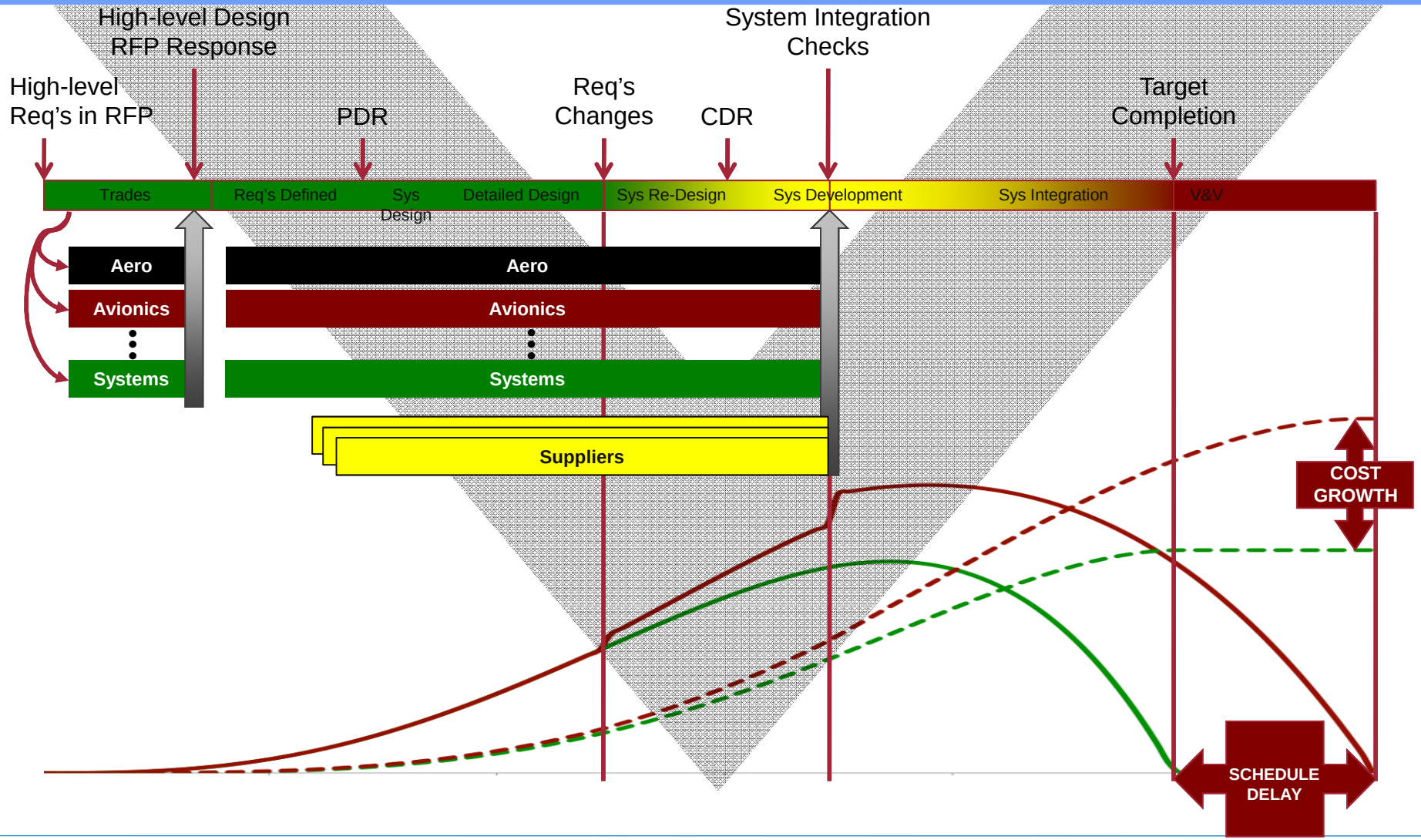
"pi"

Mismatched Assumptions

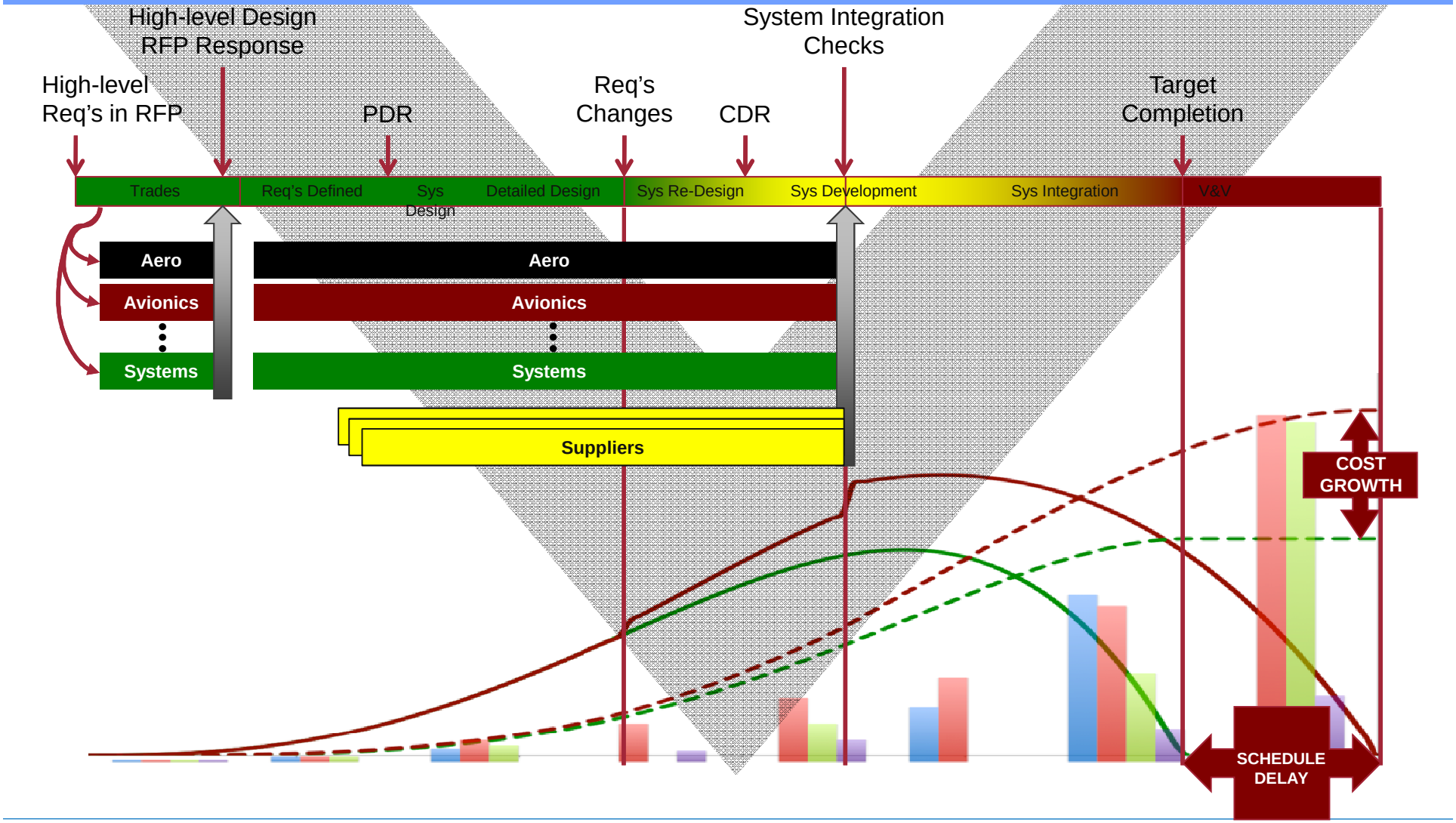
Written Requirements



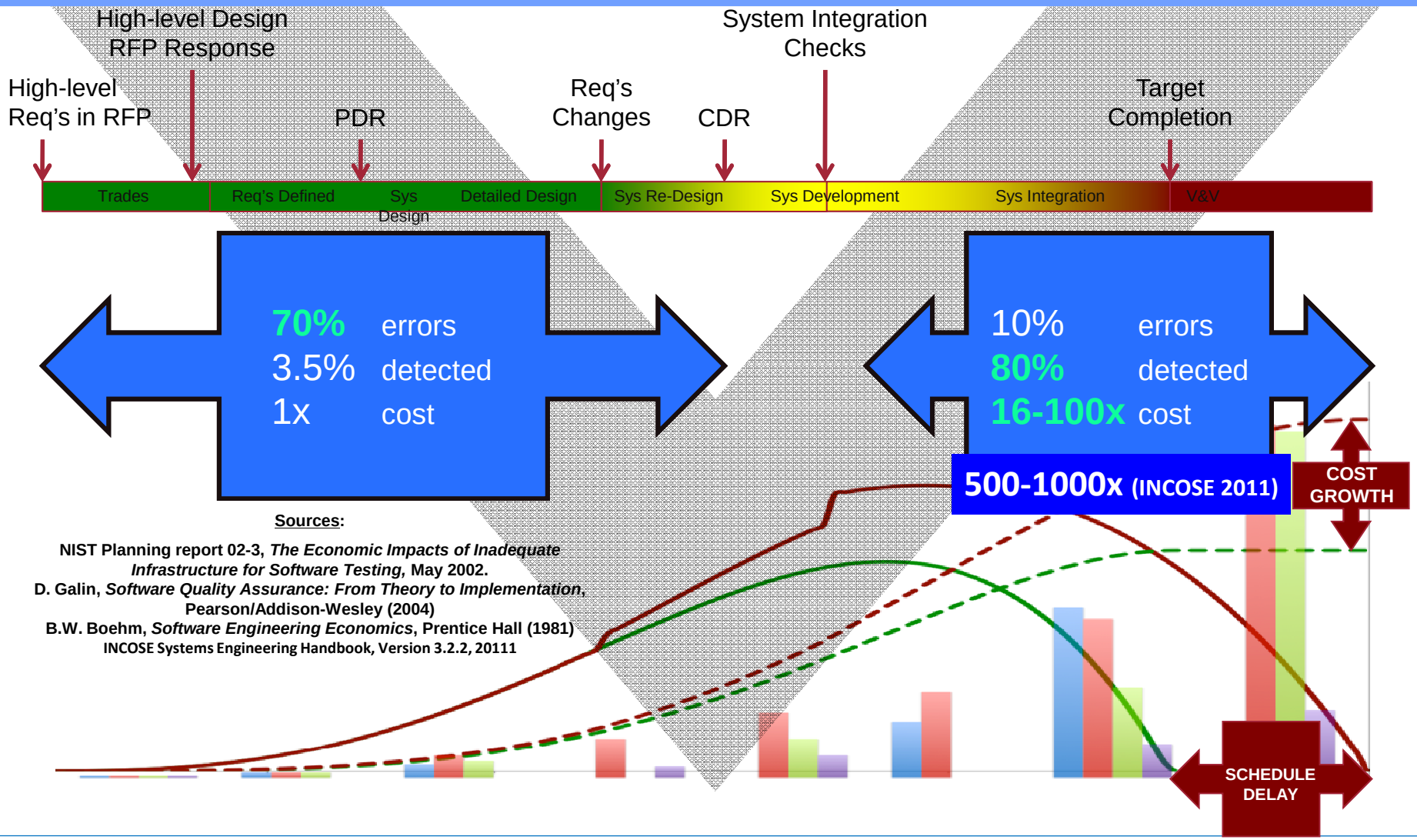
… that drive SCHEDULE DELAYS



… and COST GROWTH



The impact is documented



Sources:

NIST Planning report 02-3, *The Economic Impacts of Inadequate Infrastructure for Software Testing*, May 2002.
D. Galin, *Software Quality Assurance: From Theory to Implementation*, Pearson/Addison-Wesley (2004)
B.W. Boehm, *Software Engineering Economics*, Prentice Hall (1981)
INCOSE Systems Engineering Handbook, Version 3.2.2, 20111

Current Means of Managing Complexity Have Issues

- [illegible]dels
- [illegible]
- Fu[illegible]avio[illegible] Mode[illegible]
- Performance Model
- Structural/Compo[illegible] Model
- Cost Model
- Safety Model
- Security Model
- Reliability Model
- Maintai[illegible]abil[illegible]y Mode[illegible]
- St[illegible]
- M[illegible]del
- M[illegible]s

Indeterminate Change Impact

Incompatible Abstractions

MODEL EXPLOSION

- Modeling Domains
  - Ops/Missi[illegible] An[illegible]
  - System Desi[illegible]
  - Algorith[illegible]
  - Hardware [illegible]
  - [illegible]ftware [illegible]
  - [illegible]tics Sup[illegible]
  - [illegible]ufacturing
  - [illegible]ration & Te[illegible]
  - [illegible]ance Simulation
  - [illegible]eering Analysis
  - [illegible]System Integration

Multiple Truths

- [illegible]em Architecture [illegible]el (Integration Fra[illegible]mework)
  - Analysis Models
  - Hardware Models
  - Software Models
  - Verification Models

SAVI CONCEPTS

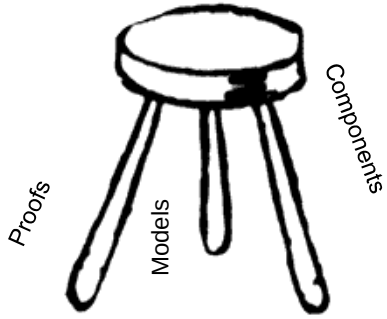
SAVI Goals and Approach

- **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**

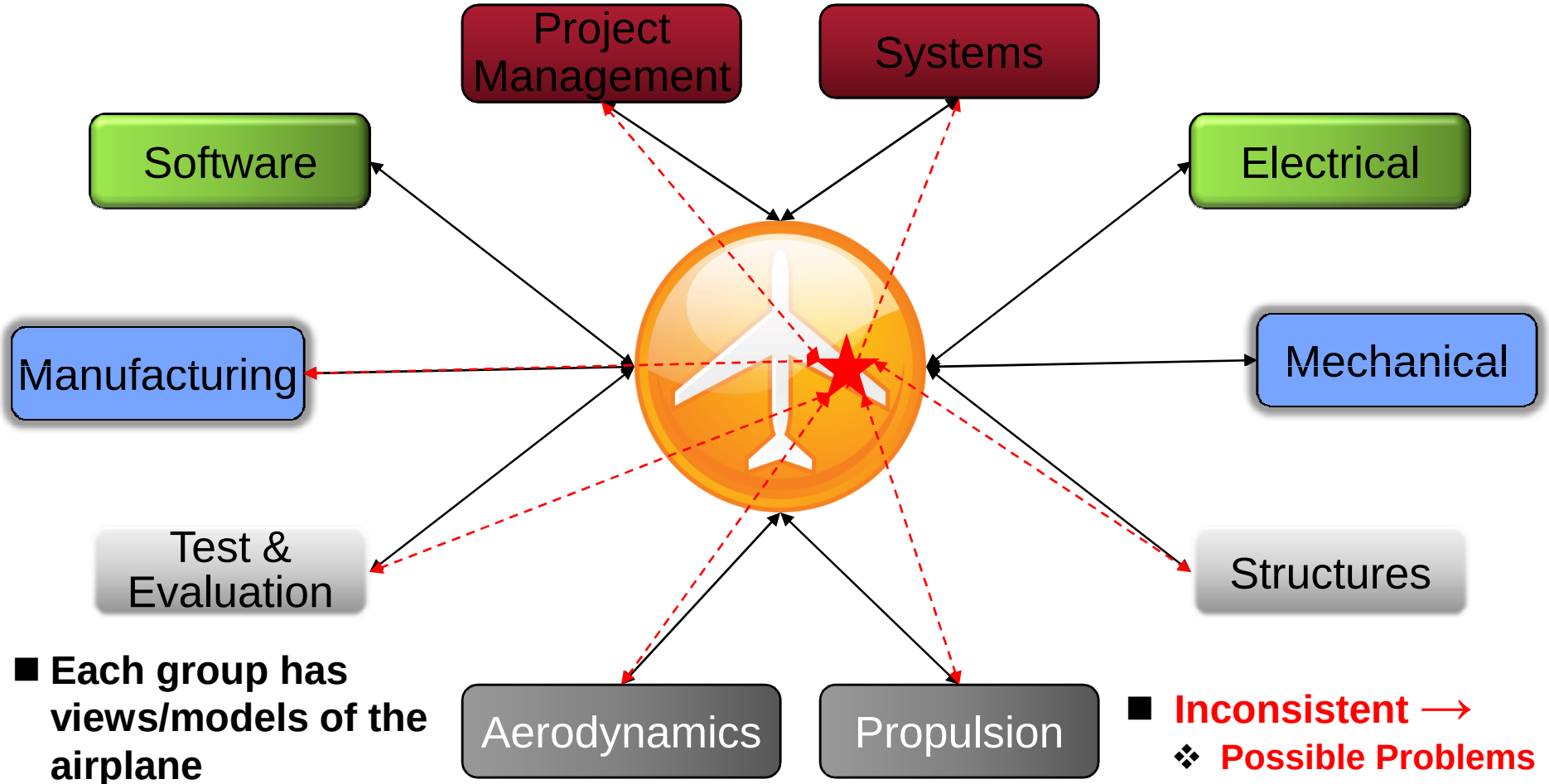
SAVI Objective and Themes

- **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"

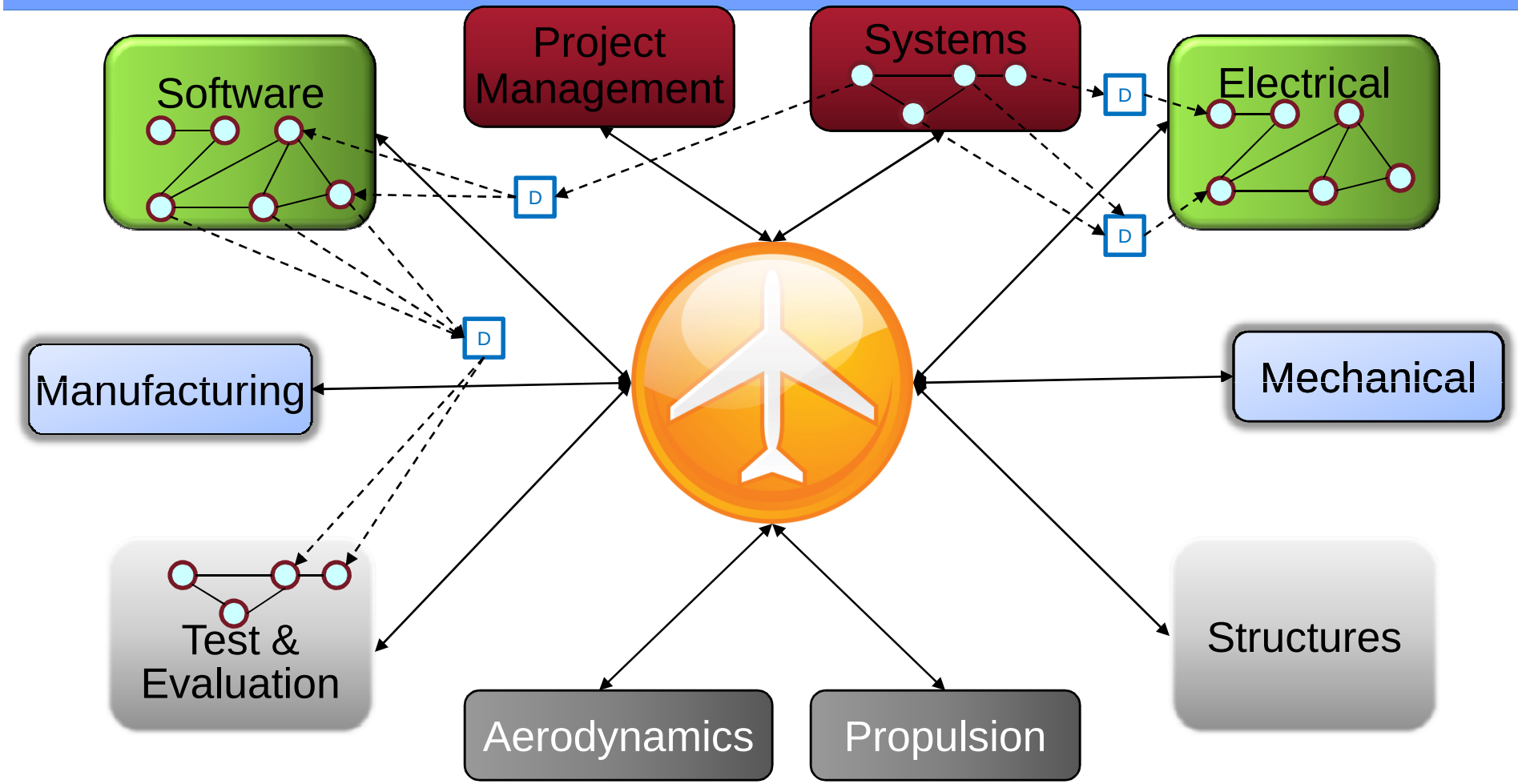


Inter-Model Consistency



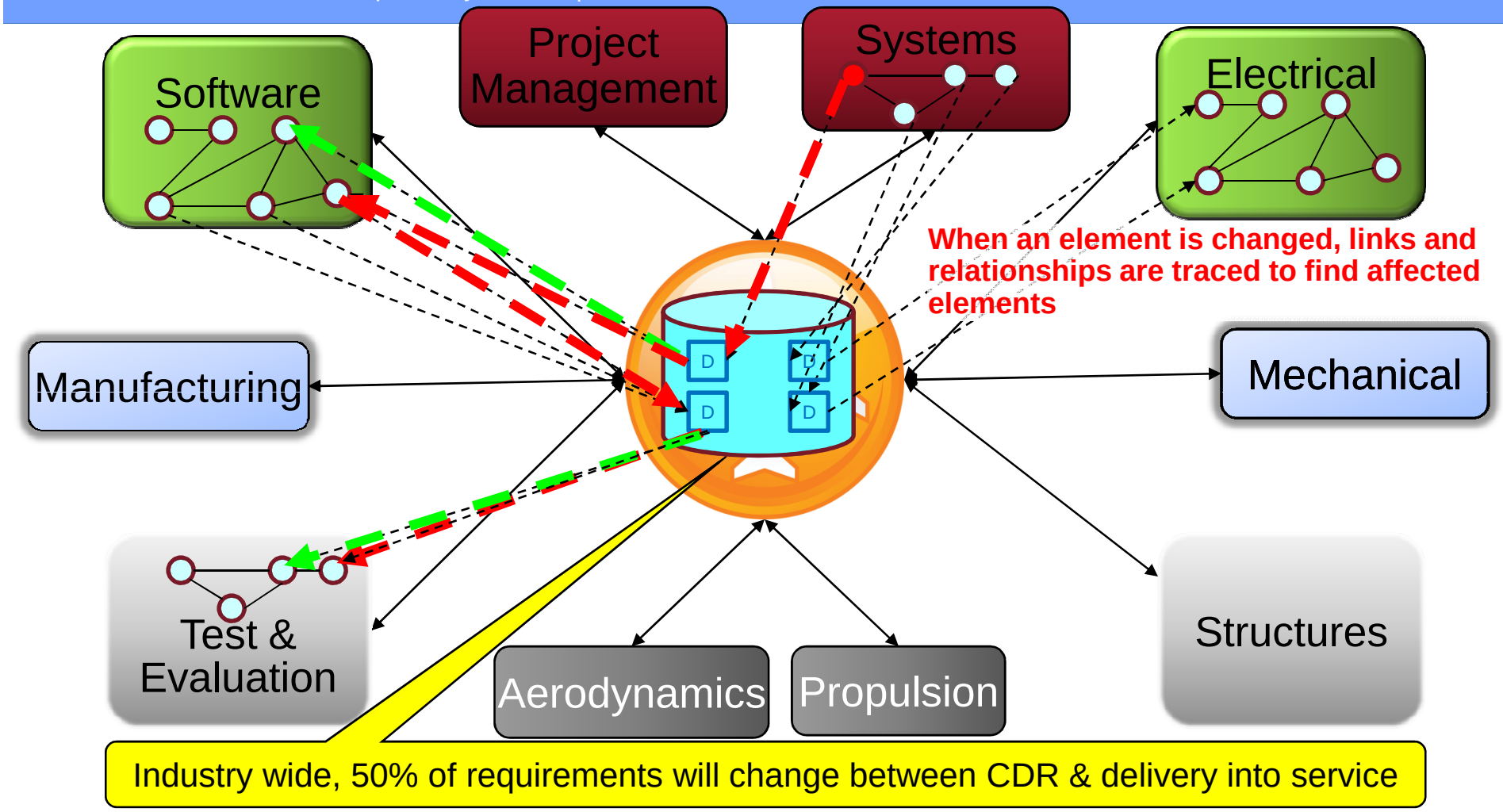
- **Each group has views/models of the airplane**
- **Relations/Dependencies exist between the views/models used**
- **Inconsistent →**
  - **Possible Problems**
  - **Not Valuable**

Dependencies Are Key



- **Each dependency needs to be identified, tracked and checked throughout the life cycle**

Dependencies Are Key



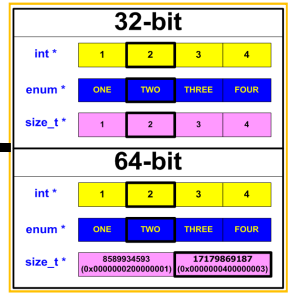
- **The SAVI Repository stores the links**

Inter-Model Consistency Checking

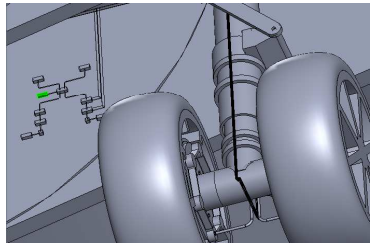
- **Consistency between two models exists when the dependence relations between those two models are satisfied**
  - **Some dependence relations can be detected automatically**
    - **Some tools are using patterns to assist**
  - **Some dependence relations will (always) require manual identification**
  - **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**
  - **Topology of system must be equivalent in all models**

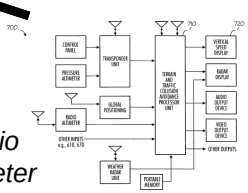
What is SAVI Consistency?

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



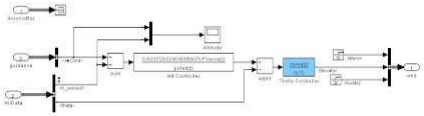
Physical Geometry





Ground Proximity Warning System

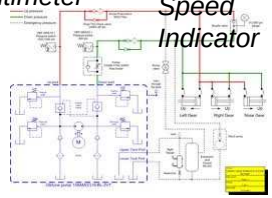
Radio Altimeter



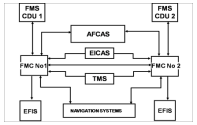
Weight on Wheels

Altimeter

Speed Indicator



Avionics Model



Engine Indication and Crew Alerting System

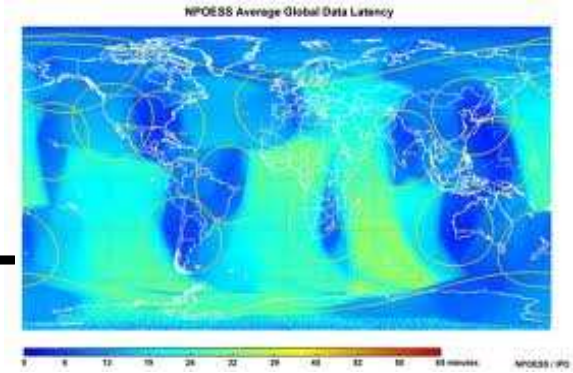
Air/Ground Signal

In Flight

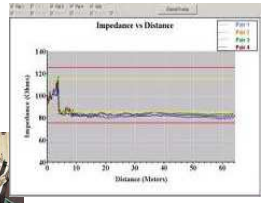
What is SAVI Consistency?

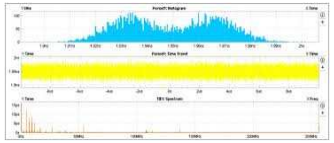
- **6 initial types**
  - **Interface**
  - **Compositional**
  - **Constraint**
  - **Behavioral**
  - **Version**
  - **Verification**

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



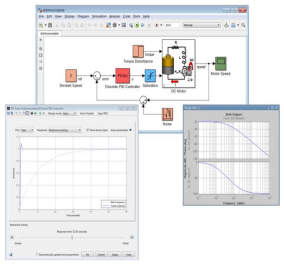
- **Additional types of consistency**
  - **Data**
    - **Value**
    - **Type**
    - **Semantics**
    - **Metadata**
  - **Model**
    - **Property**
    - **Semantics**
    - **Metadata**
    - **Behavior**





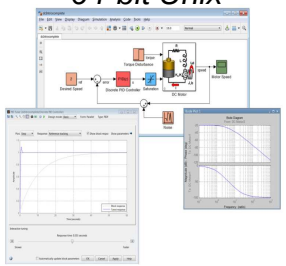
Signal connectivity *analysis doesn't need wiring length but* ***signal latency*** *and jitter analysis does.*

Mathworks
32-bit

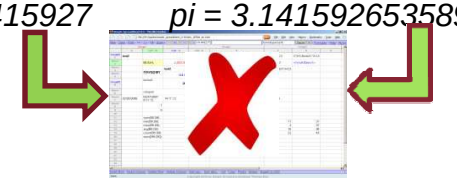


pi = 3.1415927

Mathworks
64-bit Unix

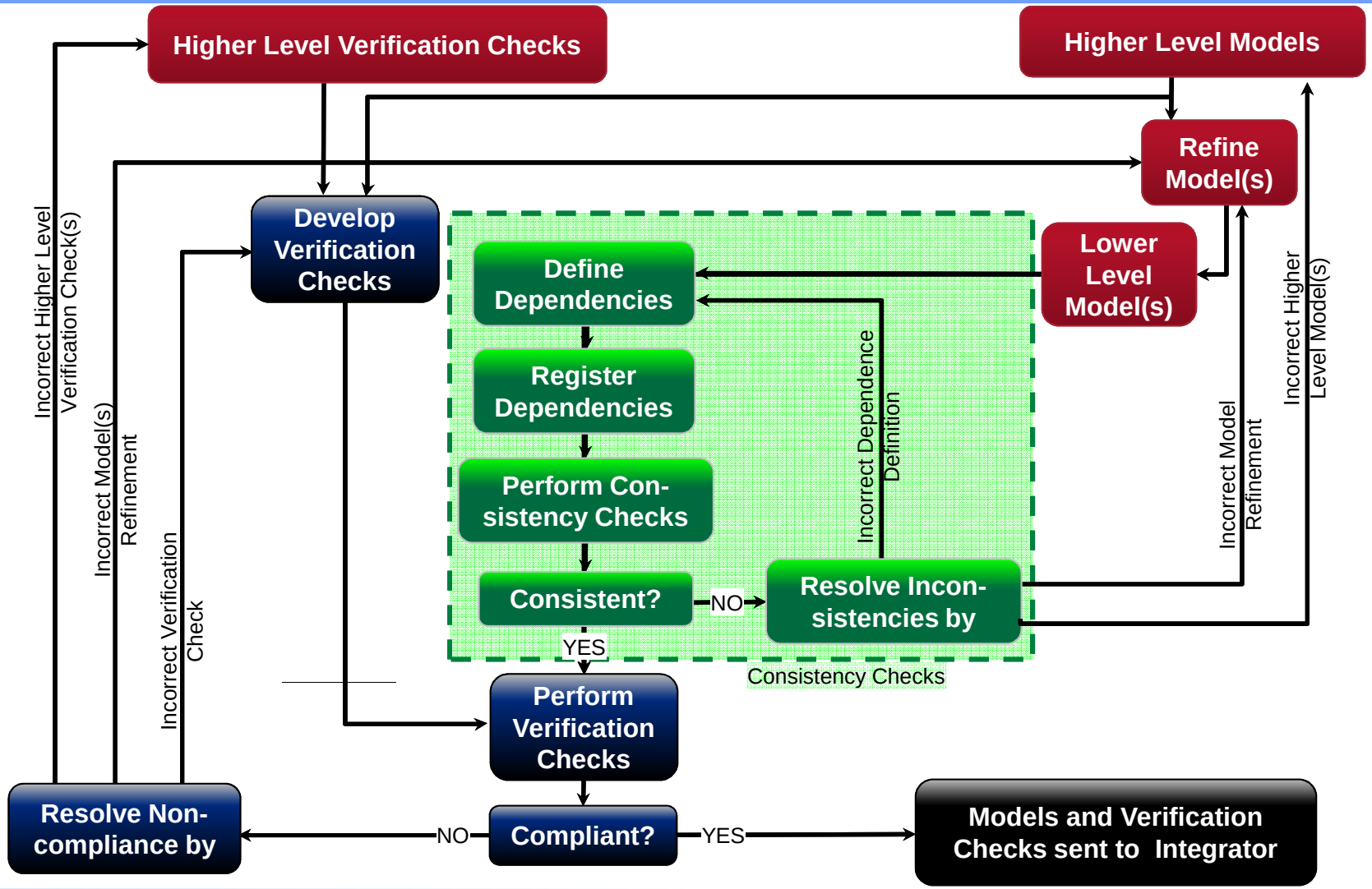


pi = 3.14159265358979323846



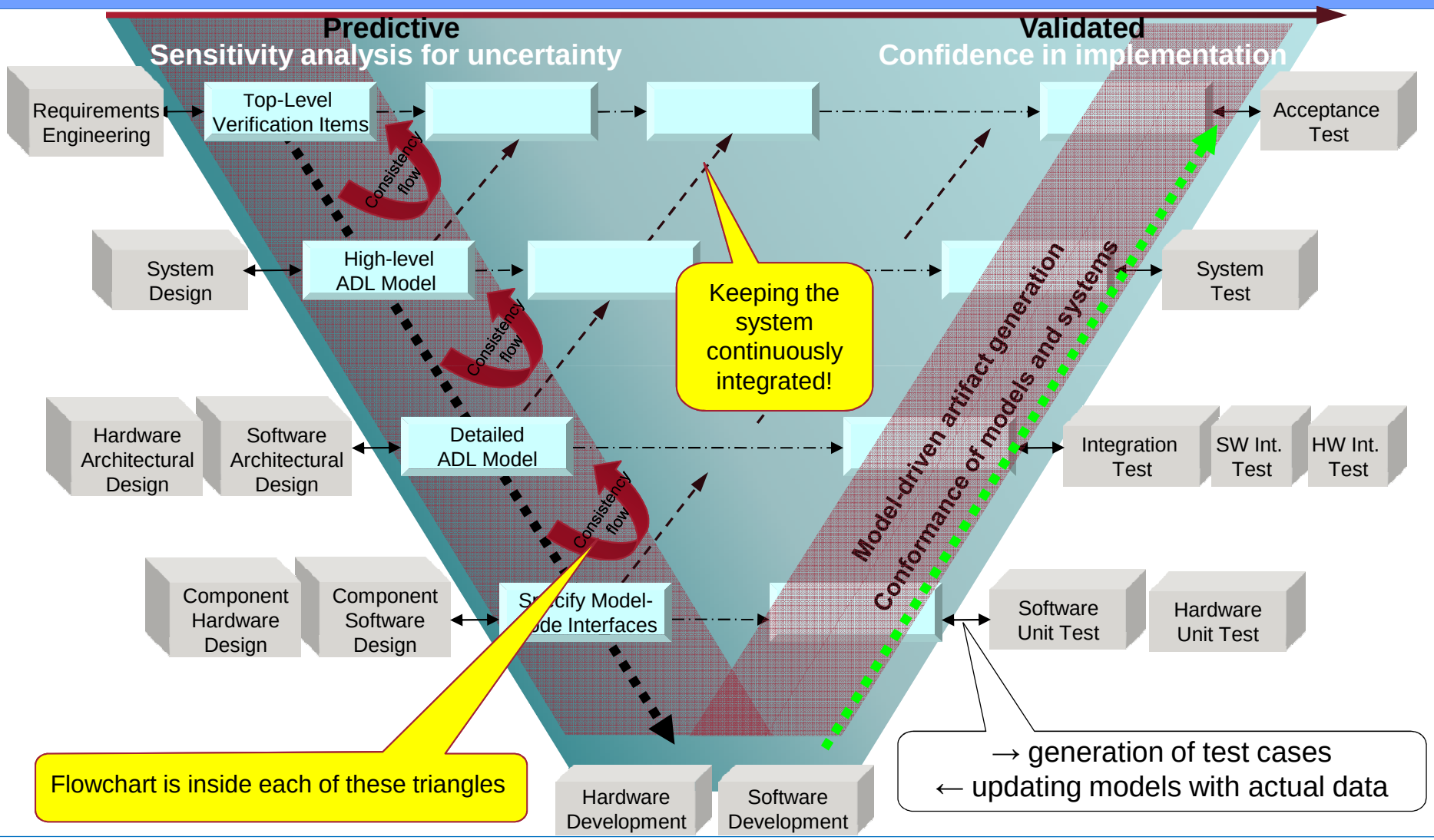
SAVI VIP

Global Product Data Interoperability Summit | **2014**



SAVI Virtual Integration "Vee"

Global Product Data Interoperability Summit | **2014**



INITIAL VIP CAPABILITY

VERSION 1.0A - 2013

WBS Safety Analysis

- **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

- **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)**

Requirements Model

Global Product Data Interoperability Summit | **2014**

A/C Reqts (excerpt)

Requirement	Description	Derived	Traced From
S18-ACFT-R-0009	Aircraft shall have a means to decelerate on the ground in accordance with 14CFR 25.735	14 CFR Part 25.735	Minimum standard required for aircraft certification
S18-ACFT-R-0110	Aircraft shall have autobrake function	Derived	Technological improvements in CAT IIIb auto-landing capability and market research, (report MRS18- XXX) about the customer needs
S18-ACFT-R-0135	Aircraft shall provide an anti-skid function.	Derived	
S18-ACFT-R-0184	Aircraft shall have hydraulically-driven brake function	Derived	
S18-ACFT-R-0185	The pilot shall be allowed to override the autobrake function.	14CFR 25.735(c)(2)	

A/C FHA (excerpt)

Failure Condition (Hazard Description)	Phase	Effect of Failure Condition on Aircraft/Crew	Classification
Loss of Deceleration Capability	Landing, RTO, Taxi	See Below	See Below
a. Unannunciated loss of Deceleration Capability	Landing, RTO	Catastrophic	Crew is unable to decelerate the aircraft,resulting in a high speed overrun
b. Annunciated loss of Deceleration Capability	Landing	Hazardous	Crew selects a more suitable runway,notifies emergency ground support, and prepares occupants for runway overrun.
c. Unannunciated loss of Deceleration Capability	Taxi	Major	Crew is unable to stop the aircraft on the taxi way or gate resulting in low speed contact with terminal, aircraft, or vehicles.
d. Annunciated loss of Deceleration Capability	Taxi	No Safety Effect	Crew steers the aircraft clear of any obstacles and calls for a tug or portable stairs.

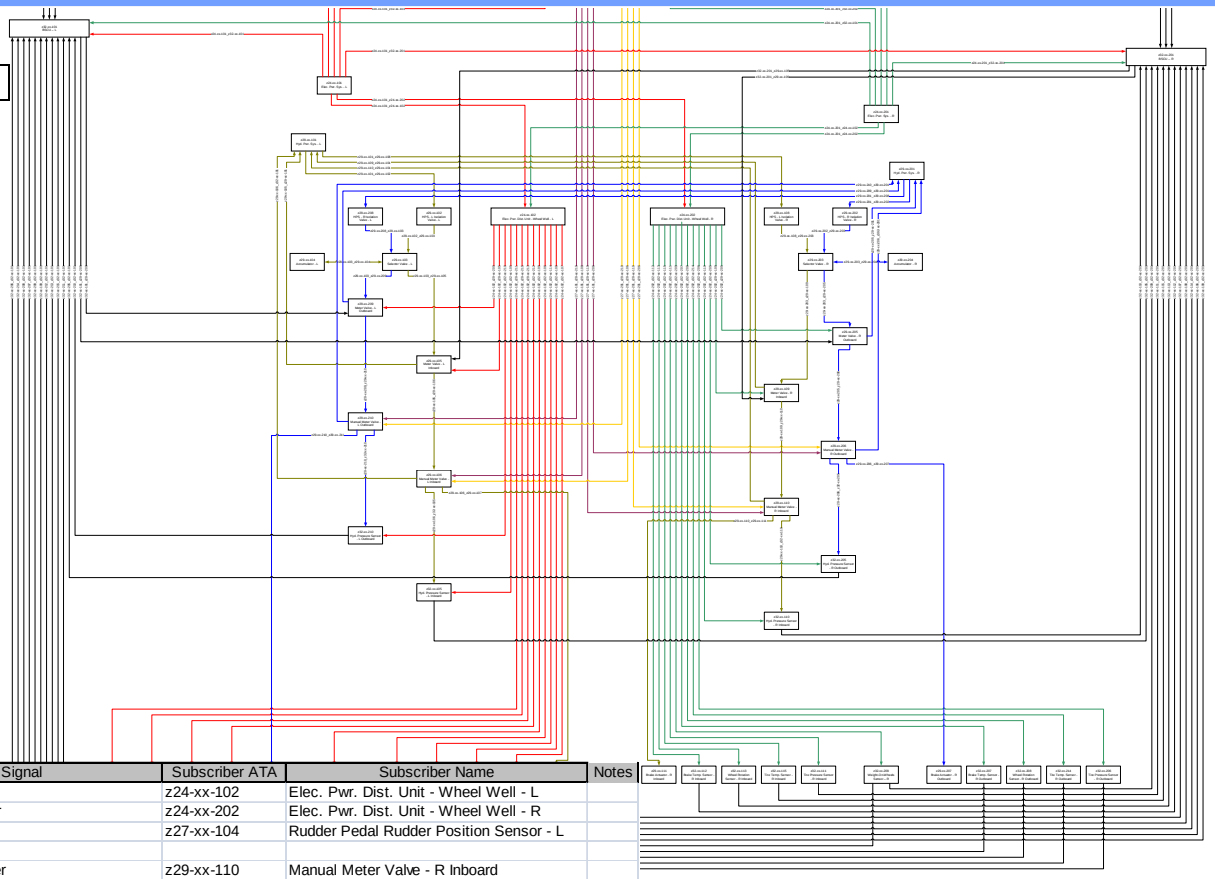
WBS FHA (excerpt)

Function	Failure Condition (Hazard Description)	Phase	Effect of Failure Condition on Aircraft/Crew	Classification	Reference to Supporting Material	Verification
Decelerate Aircraft using Wheel Braking	Total Loss of wheel braking	Landing or RTO	See Below			
	a. Unannunciated loss of wheel braking	Landing or RTO	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.	Hazardous		S18 Aircraft FTA
	b. Annunciated loss of wheel braking	Landing	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.	Hazardous	Crew procedures for loss of normal and reserve modes	S18 Aircraft FTA
	Partial Symmetrical Loss of Wheel Braking	Landing or RTO	See below			
	a. Unannunciated partial symmetrical loss of wheel braking	Landing or RTO	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.	Major to Hazardous	Additional study required to determine classification	Potentially catastrophic â€" to be confirmed by analysis
	b. Annunciated partial symmetrical loss of wheel braking	Landing	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.	Major		
	Asymmetrical Loss of Wheel Braking	Landing or RTO	See below			
	a. Asymmetrical loss of wheel braking â€" brake system failure only	Landing or RTO	Decrease in braking performance. Tendency to veer off the runway. For braking performance and brake temperature the effects are the same as partial brake loss above. The crew keeps the aircraft on the runway by using rudder at high speed and nose wheel steering at low speed. Consequences are TBD pending results of the justification studies	Potentially catastrophic â€" to be confirmed by analysis	Additional studies required to determine classification.	

Publisher/Subscriber Model

Global Product Data Interoperability Summit | **2014**

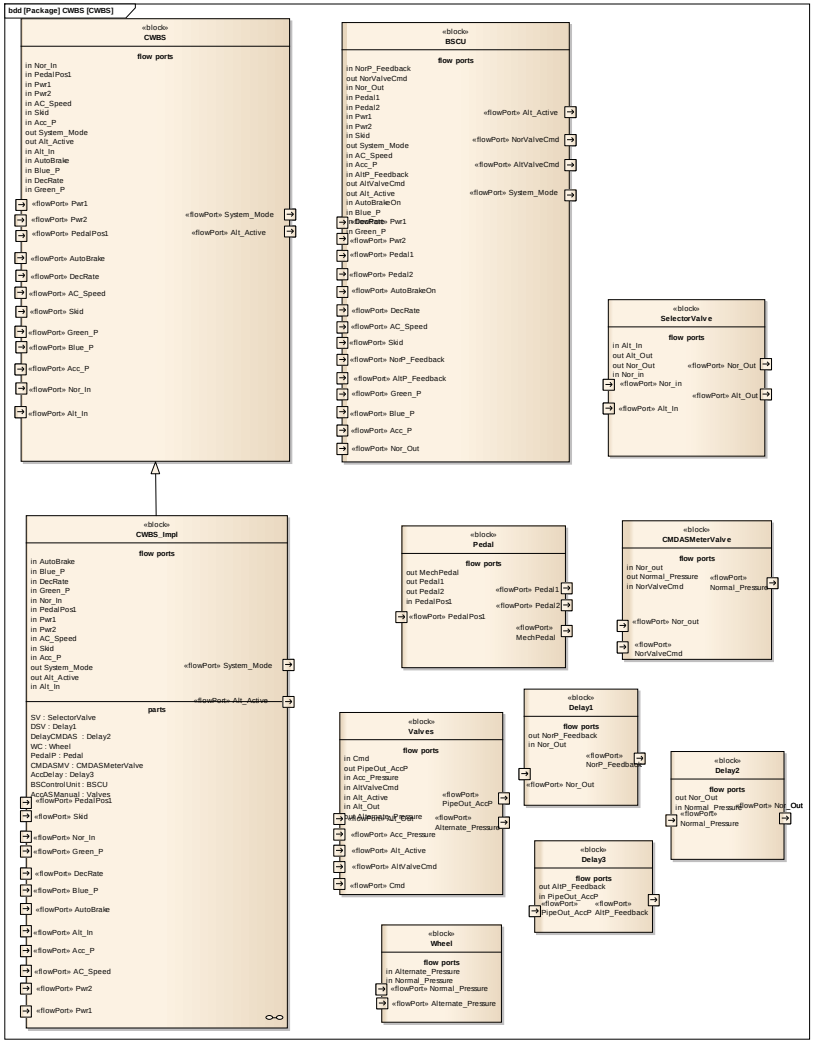
ATA	Name
z24-xx-101	Elec. Pwr. Sys. - L
z24-xx-102	Elec. Pwr. Dist. Unit - Wheel Well - L
z24-xx-201	Elec. Pwr. Sys. - R
z24-xx-202	Elec. Pwr. Dist. Unit - Wheel Well - R
z27-xx-101	Rudder Pedal Assembly - L
z27-xx-104	Rudder Pedal Rudder Position Sensor - L
z27-xx-201	Rudder Pedal Assembly - R
z27-xx-204	Rudder Pedal Rudder Position Sensor - R
z29-xx-101	Hyd. Pwr. Sys. - L
z29-xx-102	HPS - L Isolation Valve - L
z29-xx-103	Selector Valve - L
z29-xx-104	Accumulator - L

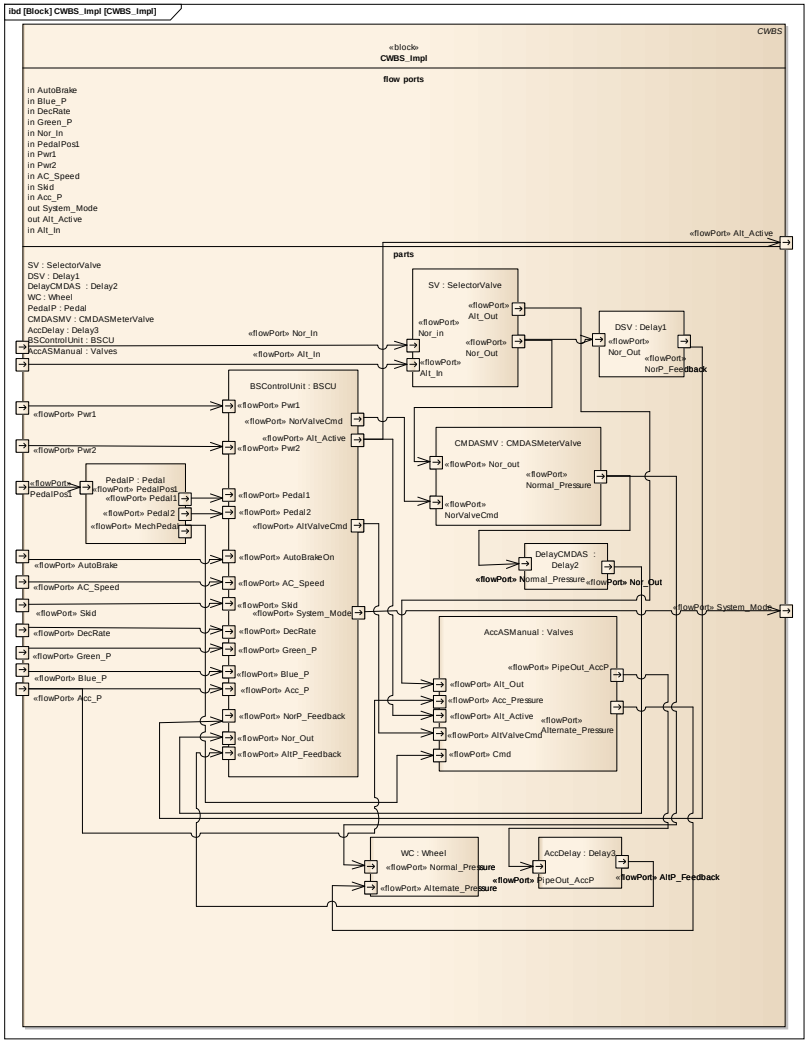


Publisher ATA	Publisher Name	Connection	Signal	Subscriber ATA	Subscriber Name	Notes
z24-xx-101	Elec. Pwr. Sys. - L	z24-xx-101_z24-xx-102	Primary Power	z24-xx-102	Elec. Pwr. Dist. Unit - Wheel Well - L	
z24-xx-101	Elec. Pwr. Sys. - L	z24-xx-101_z24-xx-202	Secondary Power	z24-xx-202	Elec. Pwr. Dist. Unit - Wheel Well - R	
z24-xx-101	Elec. Pwr. Sys. - L	z24-xx-101_z27-xx-104	Main Power	z27-xx-104	Rudder Pedal Rudder Position Sensor - L	
z27-xx-101	Rudder Pedal Assembly - L	z27-xx-101_z29-xx-110	Mechanical Power	z29-xx-110	Manual Meter Valve - R Inboard	
z27-xx-101	Rudder Pedal Assembly - L	z27-xx-101_z29-xx-206	Mechanical Power	z29-xx-206	Manual Meter Valve - R Outboard	
z29-xx-101	Hyd. Pwr. Sys. - L	z29-xx-101_z29-xx-102	Hyd. Power (Pressure)	z29-xx-102	HPS - L Isolation Valve - L	
z29-xx-103	Selector Valve - L	z29-xx-103_z29-xx-104	Hyd. Power (Pressure)	z29-xx-104	Accumulator - L	Bi
z29-xx-105	Meter Valve - L Inboard	z29-xx-105_z29-xx-101	Hyd. Power (Return)	z29-xx-101	Hyd. Pwr. Sys. - L	
z32-xx-101	BSCU - L	z32-xx-101_z29-xx-205	Meter Valve – R Outboard Command	z29-xx-205	Meter Valve - R Outboard	
z32-xx-101	BSCU - L	z32-xx-101_z29-xx-209	Meter Valve – L Outboard Command	z29-xx-209	Meter Valve - L Outboard	
z32-xx-109	Weight-On-Wheels Sensor - L	z32-xx-109_z32-xx-101	Weight-On-Weels Sensor – L Reading	z32-xx-101	BSCU - L	
z32-xx-109	Weight-On-Wheels Sensor - L	z32-xx-109_z32-xx-201	Weight-On-Weels Sensor – L Reading	z32-xx-201	BSCU - R	

SysML Model (Early Architecture)

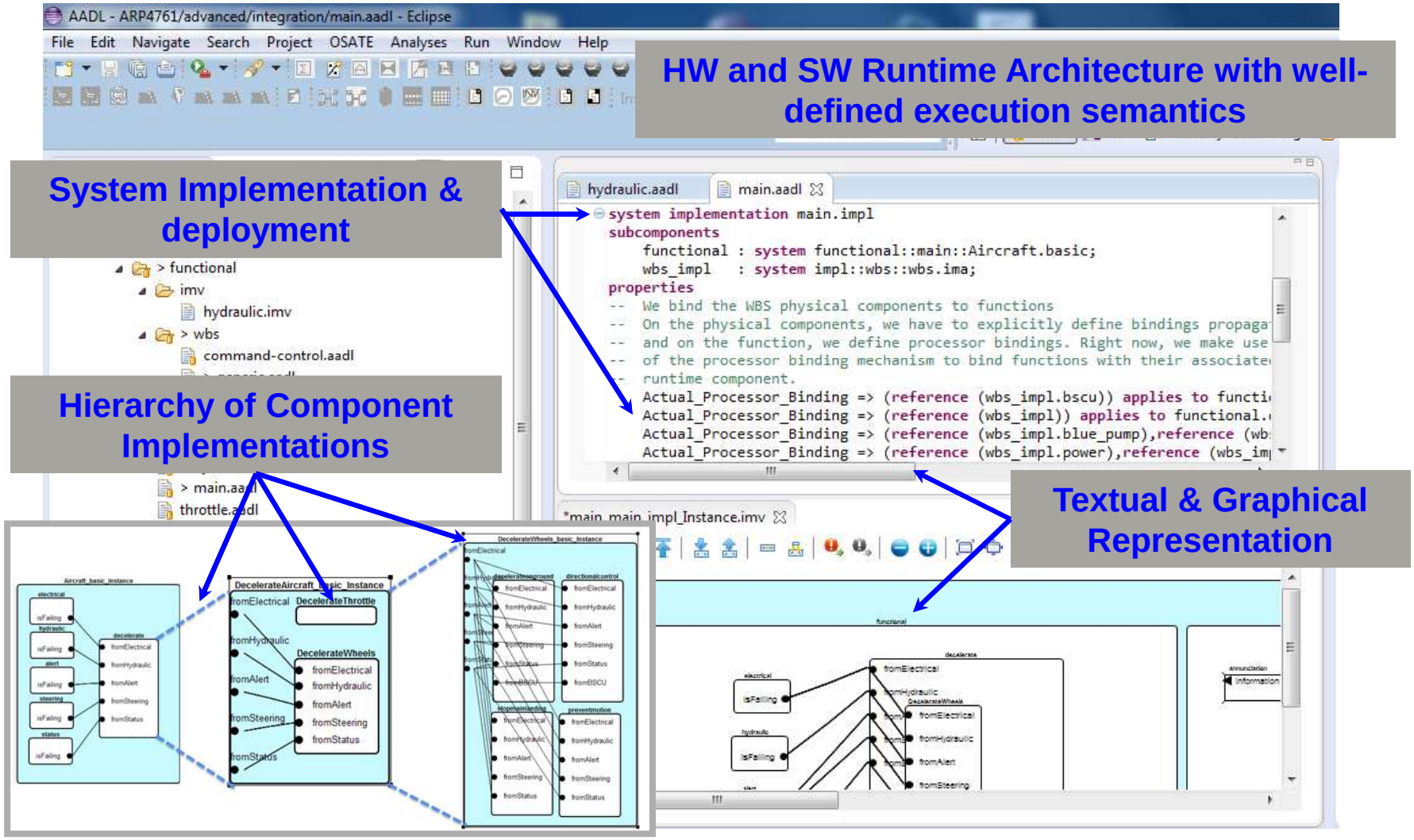
Global Product Data Interoperability Summit | **2014**





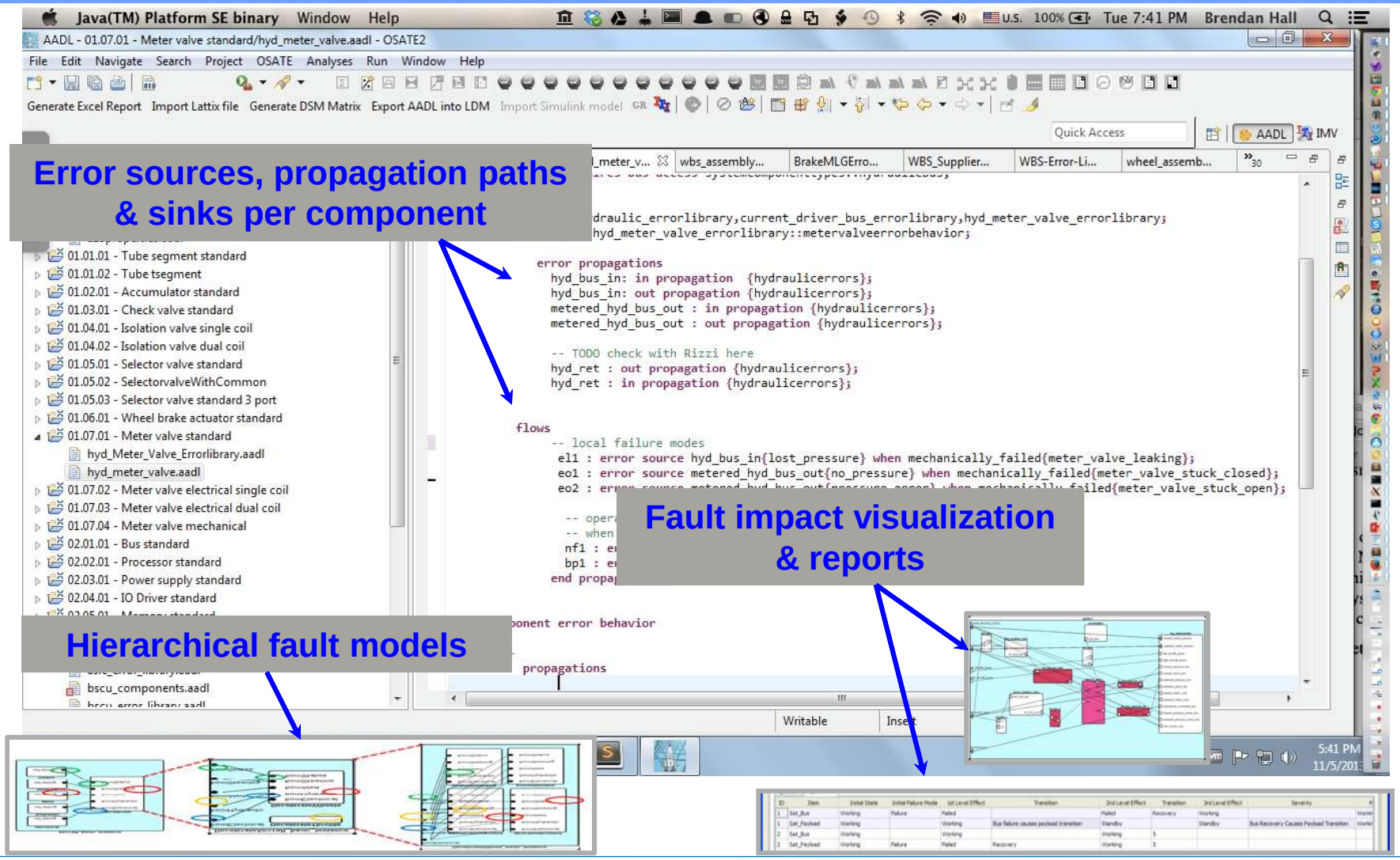
System and SW Architecture with AADL

Global Product Data Interoperability Summit | **2014**

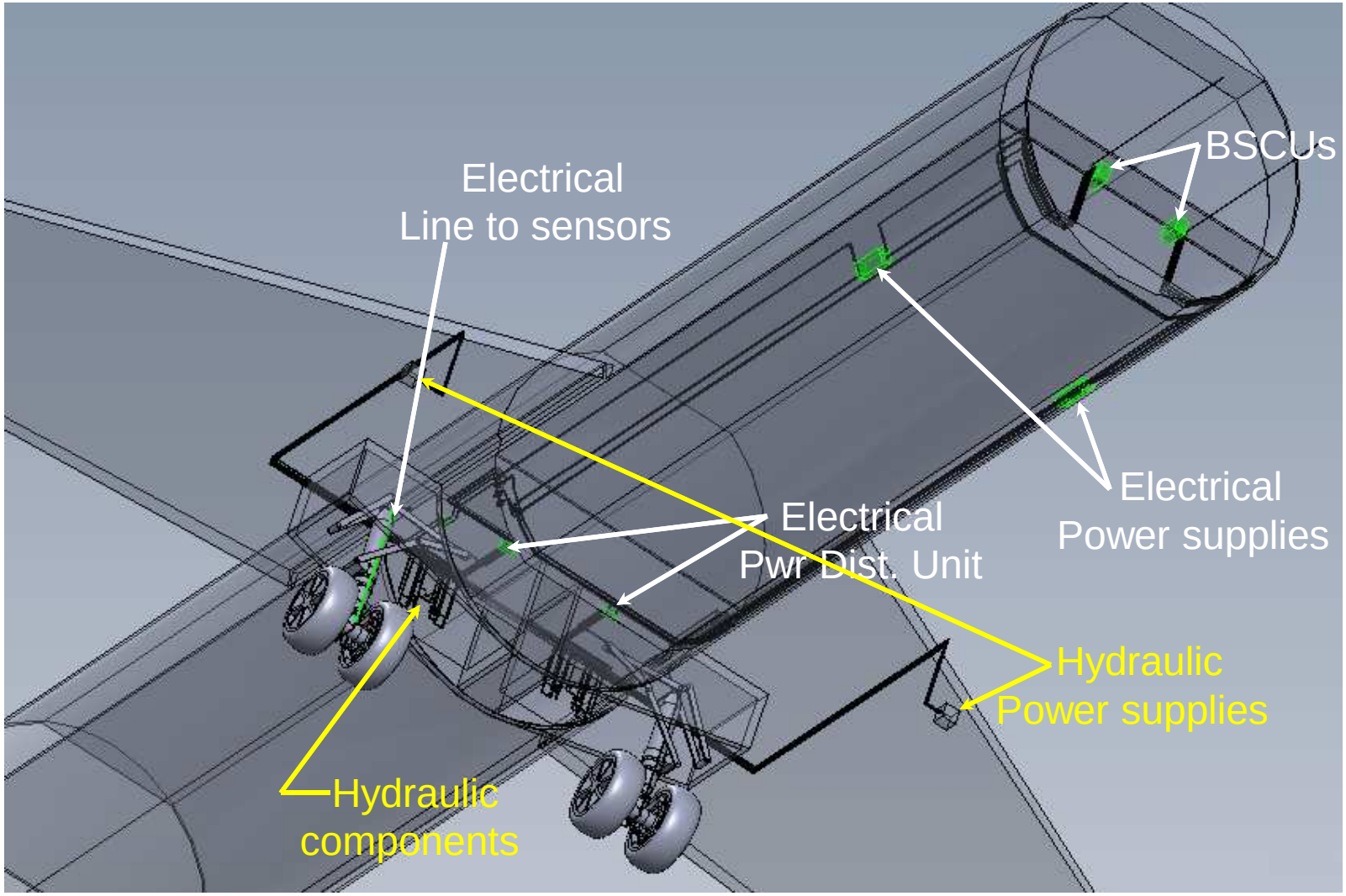


Architecture Fault Modeling with EMV2

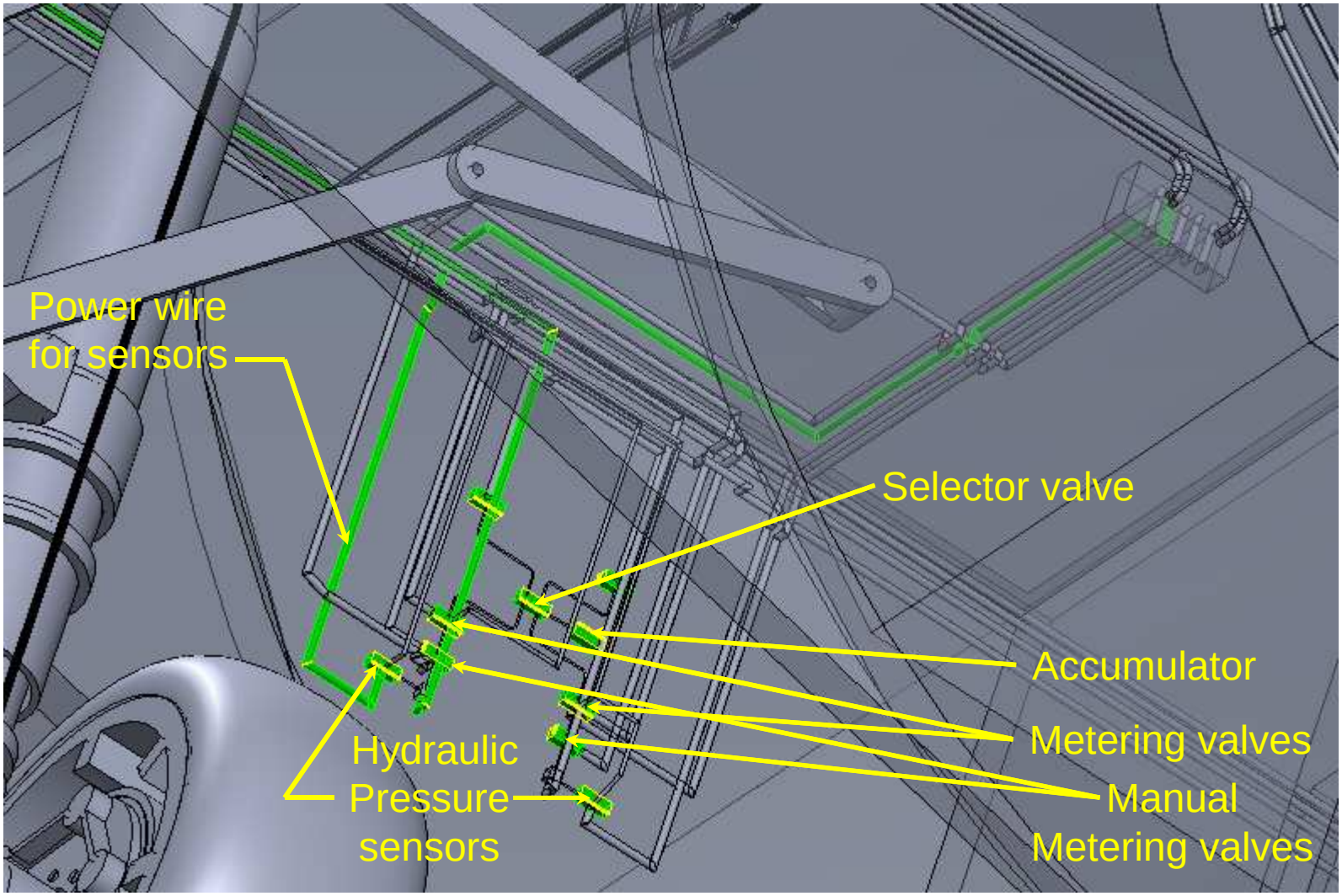
Global Product Data Interoperability Summit | **2014**



Solid Geometry Model

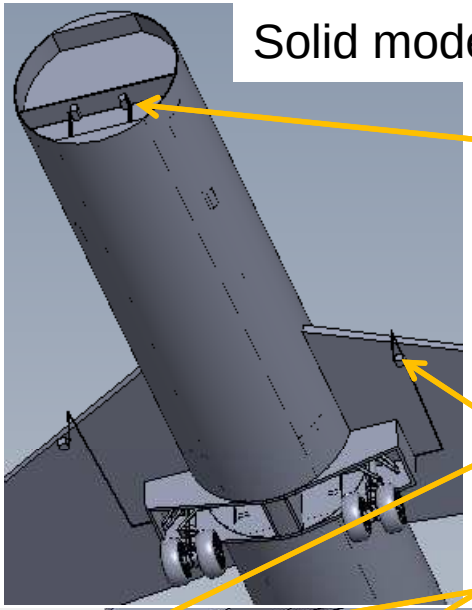


Solid Geometry Model



Inter-Model Consistency Checks

Global Product Data Interoperability Summit | **2014**

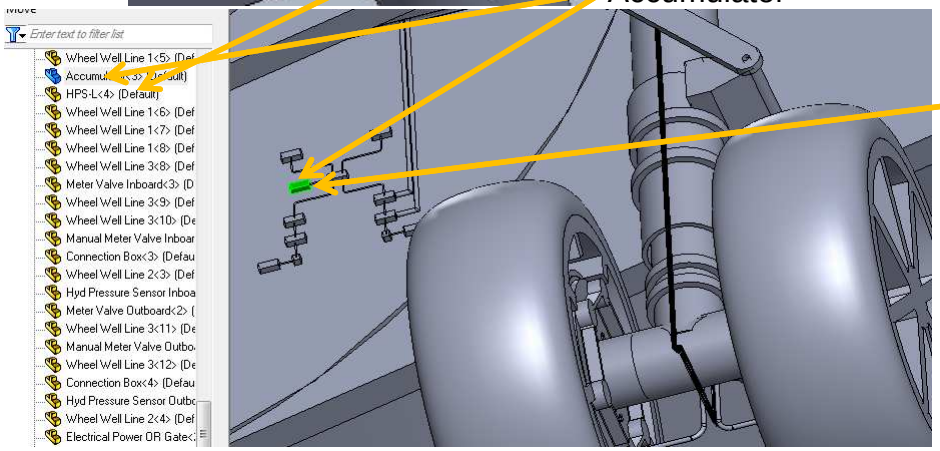


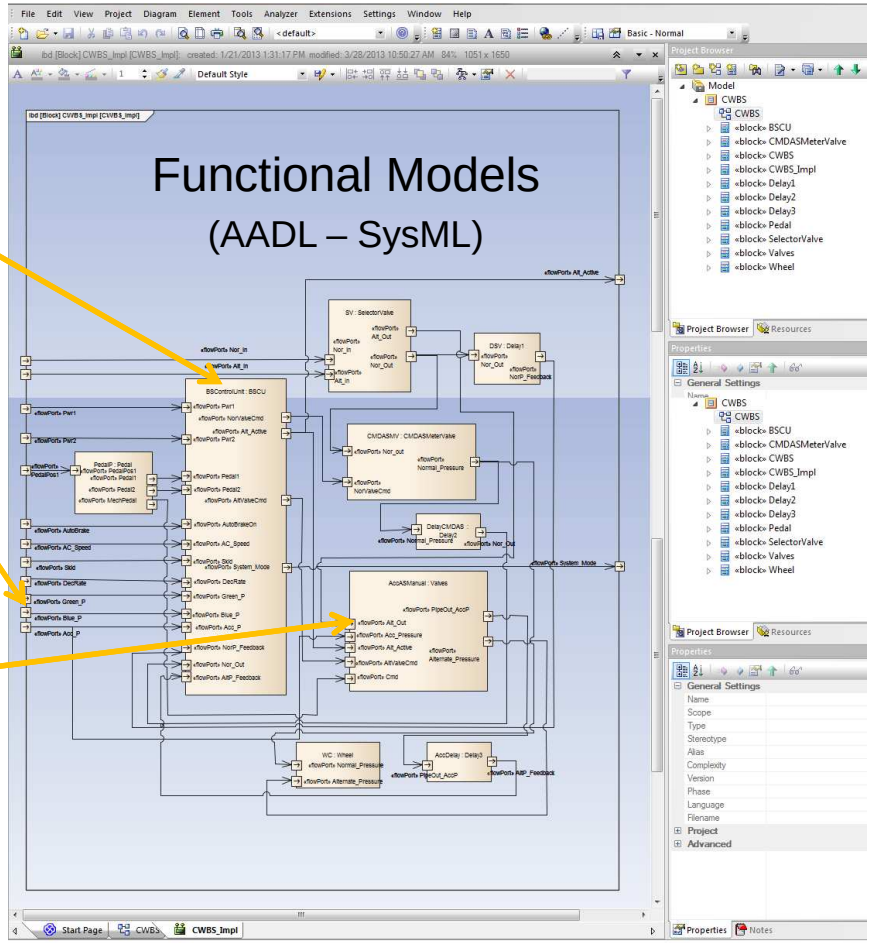
Solid models

BSCU

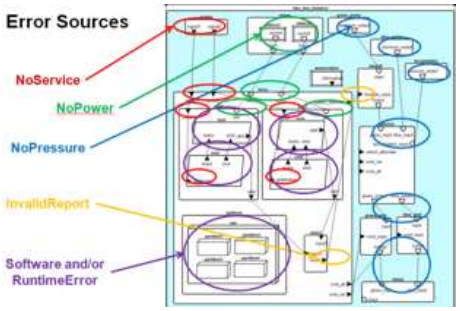
Hyd power supply

Accumulator

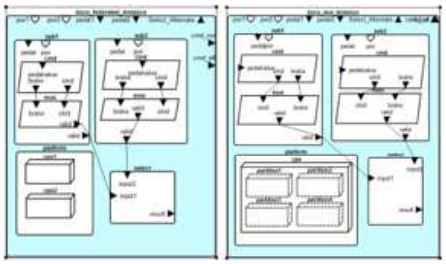




Automation of Safety Analysis Practice

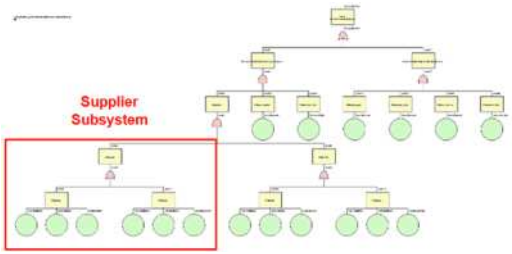


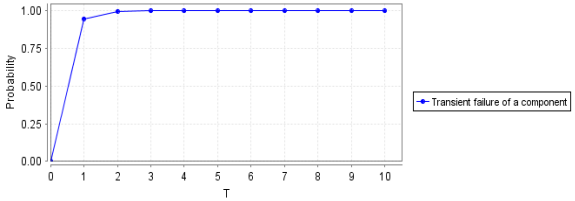
- **Use of Error Model EMV2 and ARINC653 annexes**
  - **Relevance for the avionics community**
- **Comparative architecture trade study**
  - **Federated vs. Integrated Modular Avionics (IMA) architecture**



- **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)**

Function Name	Failure Mode	Failure Rate (E-6)	Flight Phase	Failure Effect	Detection Method	Comments
+5 Volt	+5V out of spec.	0.2143	All	Possible P/S shutdown	Power Supply Monitor trips, shuts down supply and passes "invalid power supply (P/S)" to other BSCU system	BSCU channel fails
	+5V short to ground	0.2857	All	P/S shutdown	Power supply monitor passes invalid P/S to other BSCU system	BSCU channel fails
	Loss of / reduced filtering	0.3571	All	Increase Ripple	May pass out of spec voltage to rest of BSCU if ripple is such that it is not detected by the P/S monitor	May cause spurious P/S monitor trip
	+5V open	0.5714	All	P/S shutdown	Power supply monitor passes invalid P/S to other BSCU system	BSCU channel fails
	No Effect	0.1429	All	No Effect	None/No Effect	No Effect
Total Failure Rate of +5V Supply		1.5714				



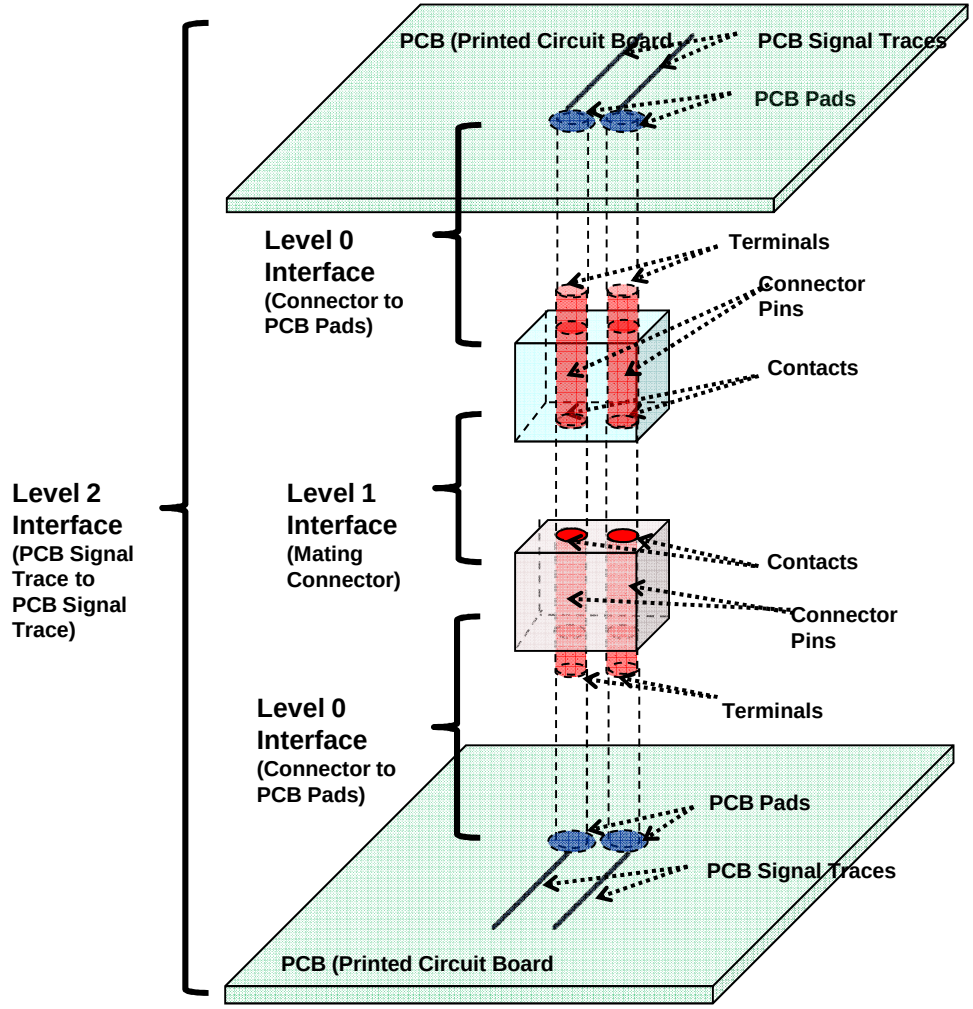


CAPABILITIES BEING ADDED

VERSION 1.0B - 2014

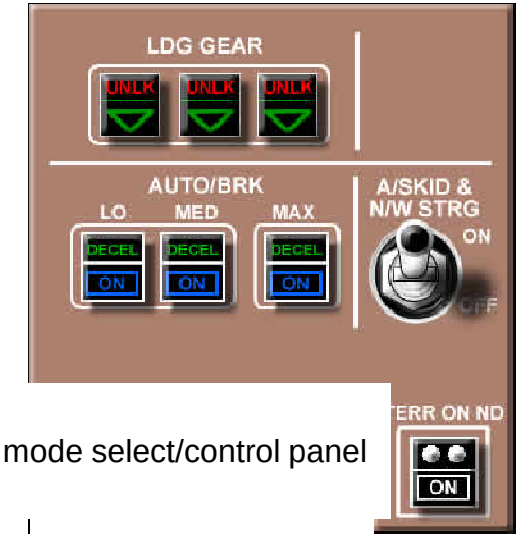
AFE 61S1 (2014) Use Cases

- **Printed Circuit Board Interconnect**
  - **Prove physical implementation matches (is consistent with) the logical design (schematic)**
- **Future: expand use case to include wiring harnesses**

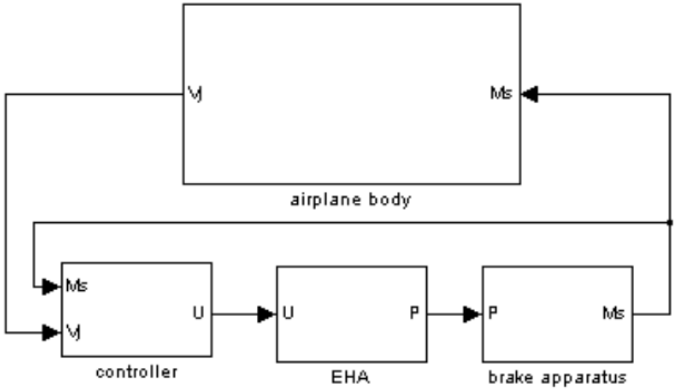


AFE 61S1 (2014) Use Cases

- **Autobrake/antiskid enabled**
  - **Multiple communicating state machines**
  - **Multiple communicating control laws**
- **Electro-mechanical braking system**
  - **Adds multi-physics simulation models to the mix**

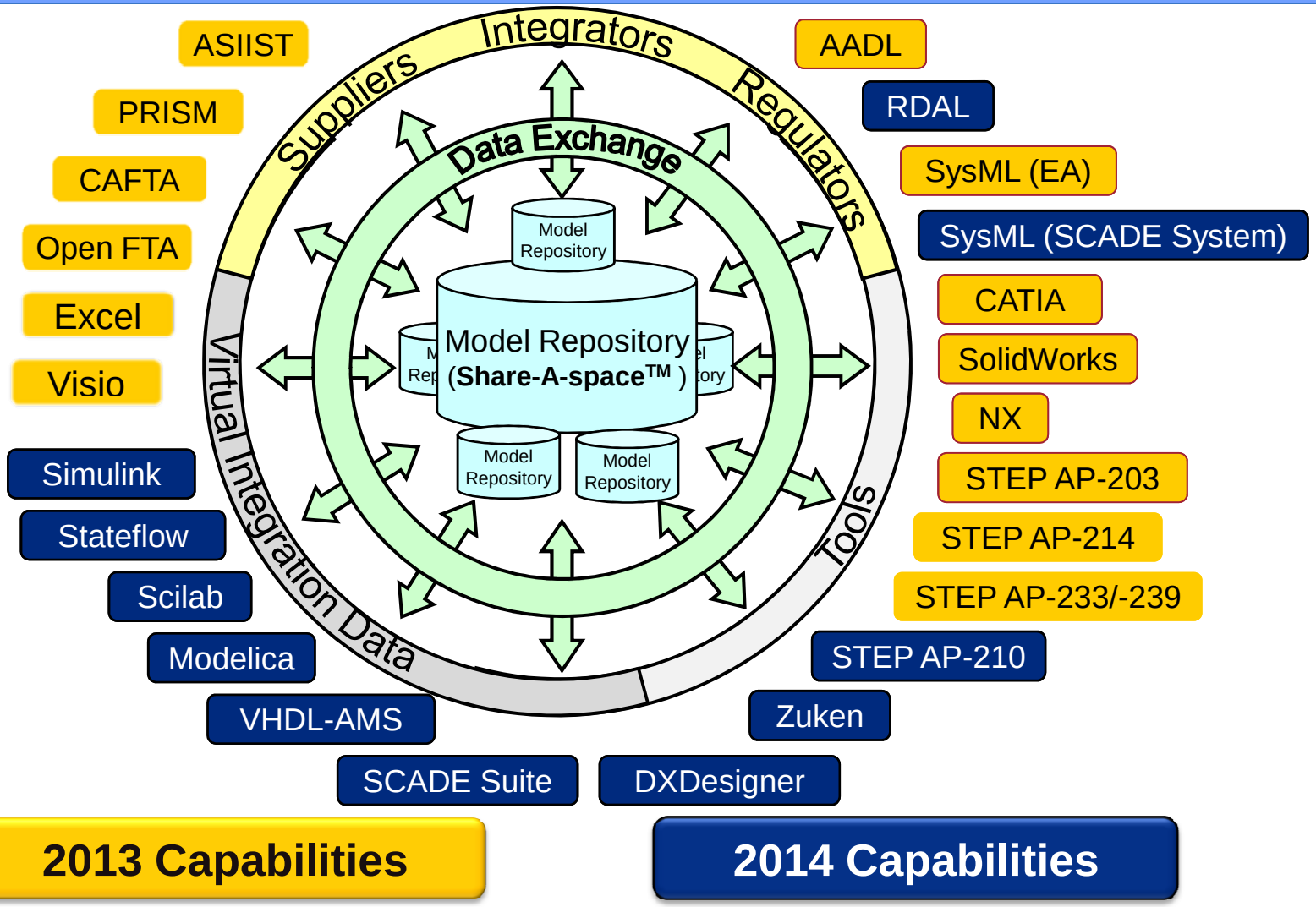


Typical mode select/control panel



AFE 61S1 Model Map

Global Product Data Interoperability Summit | **2014**



CONCLUSION

Summary

- **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?

- **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

- **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**