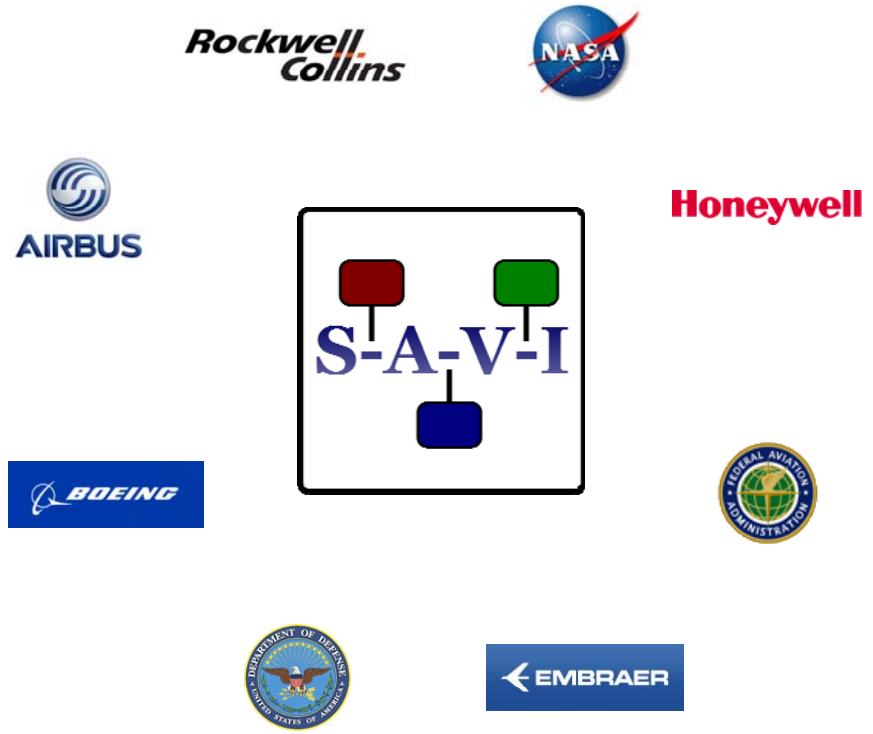
Aerospace Vehicle Systems Institute

Virtual Integration for Model Based Safety Assessment of Complex Systems

System Architecture Virtual Integration Program



David Redman, AVSI Director

Presentation to the 16th Annual NDIA Systems Engineering Conference

29 October 2013

Outline

- Overview of SAVI
- The AADL Error-Model Annex
- Support of Safety Evaluation with AADL
- Case-Study
- Future Work

The Aerospace Vehicle Systems Institute

Full Members

- Airbus
- Boeing
- DoD
- EADS
- Embraer
- GE Aviation
- Goodrich (now UTC)
- Honeywell
- Rockwell Collins
- Rolls Royce
- Saab
- United Technologies

Liaison Members

- FAA
- NASA
- Aerospace Valley

Associate Members

- BAE Systems
- Bombardier
- Gulfstream
- Lockheed Martin

The Aerospace Vehicle Systems Institute

Full Members

- Airbus
- Boeing
- DoD
- EADS
- Embraer
- GE Aviation
- Goodrich (now UTC)
- Honeywell
- Rockwell Collins
- Rolls Royce
- Saab
- United Technologies

Liaison Members

- FAA
- NASA
- Aerospace Valley

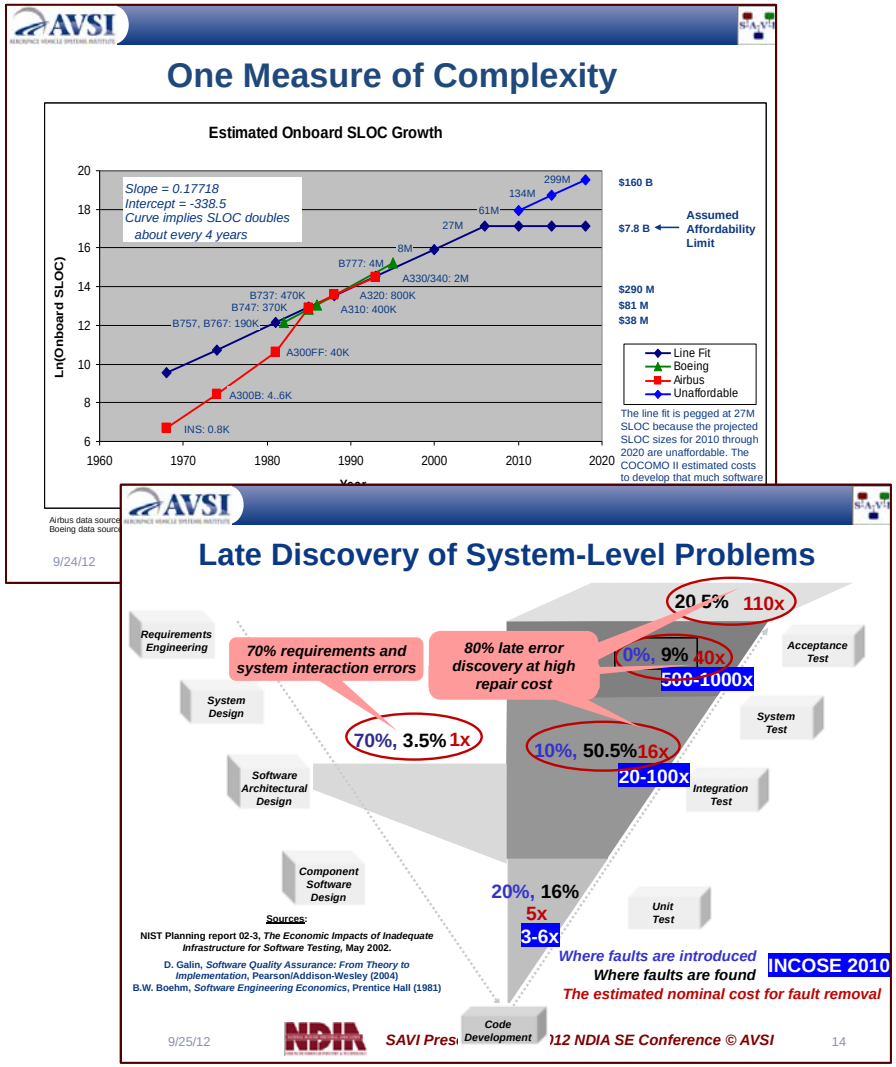
Associate Members

- BAE Systems
- Bombardier
- Gulfstream
- Lockheed Martin

Mission

AVSI addresses issues that impact the aerospace community through international cooperative research and collaboration conducted by industry, government and academia.

The AVSI SAVI Program



- Launched in 2008 to address the problem of growth in complexity of systems leading to cost and schedule overruns
- The objective is to develop a standards-based Virtual Integration Process (VIP) that allows multiple parties to virtually integrate and analyze systems throughout development life cycle
- The result is earlier detection and correction of errors leading to cost savings
- **Highly focused on integration – defining the state of the art in system integration consistency checking**

SAVI Engages Stakeholders

- The SAVI Program has continually sought any and all stakeholders to contribute to the definitions of the standards-based solution
- SAVI has also sought out partners with best-in-class technology that supports the VIP to avoid duplication of effort
- **Current** and past participants include:
  - **Adventium Labs**
  - **Airbus**
  - BAE Systems
  - **Boeing**
  - **US DoD**
  - **Embraer**
  - **Esterel**
  - **Eurostep**
  - **US FAA**
  - GE Aviation
  - **Honeywell**
  - Lockheed Martin
  - **NASA**
  - **Rockwell Collins**
  - **SEI at CMU**
  - **Texas A&M**

Past Results

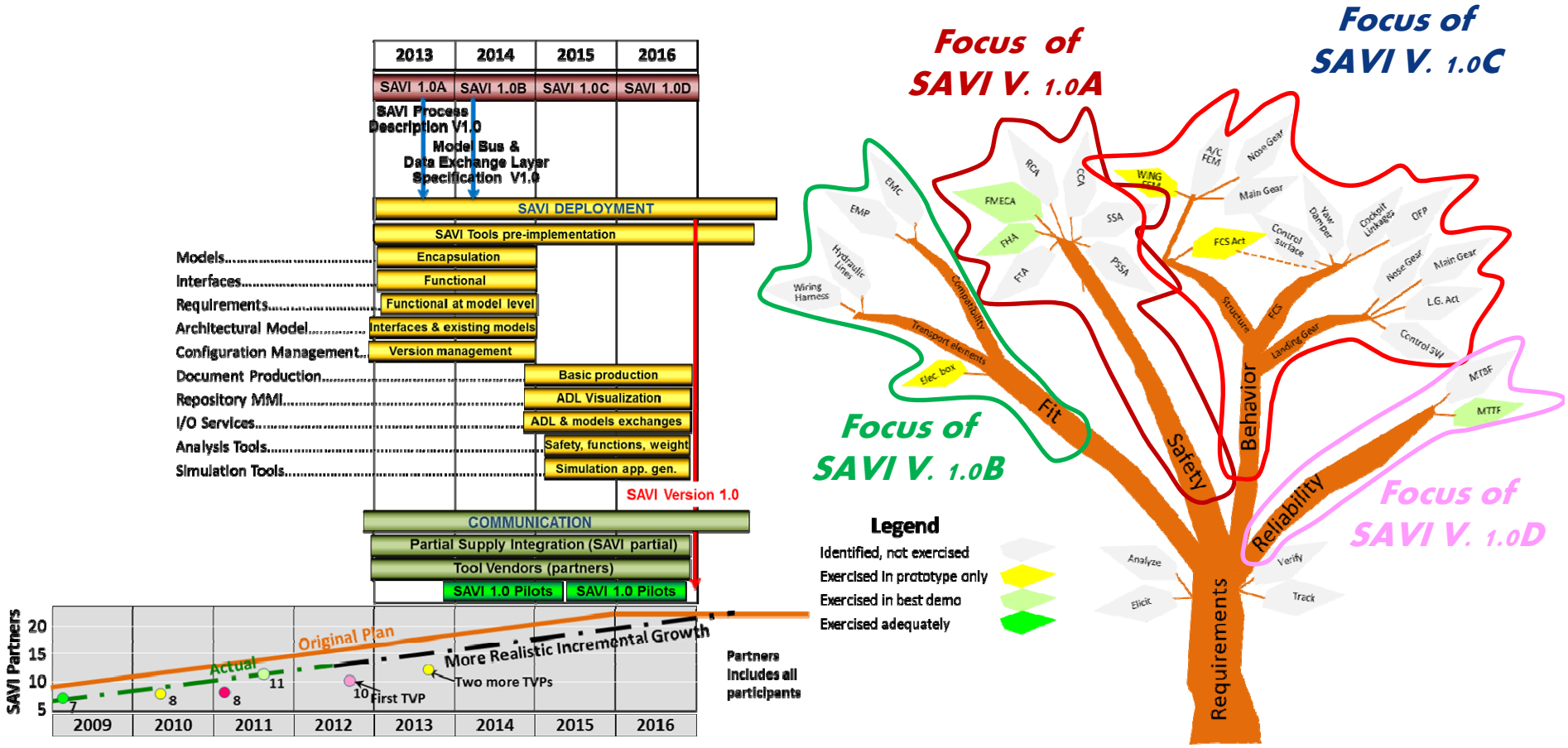
- Several proof of concept phases have researched the feasibility of the SAVI VIP, exploring topics including:
  - Model-based vs. document based systems acquisition
  - SAVI return on investment (RoI)
  - Architectural description language capabilities and extensions
  - Inter-domain tool integration
  - Model repository
  - attributes for virtual integration
  - Model data exchange protocols and technologies
  - IP protection in an integrated, multi-participant modeling environment
  - Assurance methods

Past Results

- Several proof of concept phases have researched the feasibility of the SAVI VIP, exploring topics including:
  - Model-based vs. document based systems acquisition
  - Inter-domain tool integration
  - Model repository attributes for virtual integration
  - Model data exchange
  - environment
  - Assurance methods

SAVI Members have concluded that there is compelling evidence to justify development of the SAVI VIP

Current Project Focus



Safety Demo Focus

- Application on a standardized example (AIR6110)
  - Automated generation of certification documents
  - Compliance with standards requirements
- Highlight the iterative design process
  - First safety evaluation
  - Refinement through system development
- Use of commercial and open-source tools
  - Reproducible at no-cost
  - Adaptation with state-of-the-art analysis tools

THE AADL AND THE ERROR MODEL ANNEX

The Architectural Analysis and Design Language (AADL)

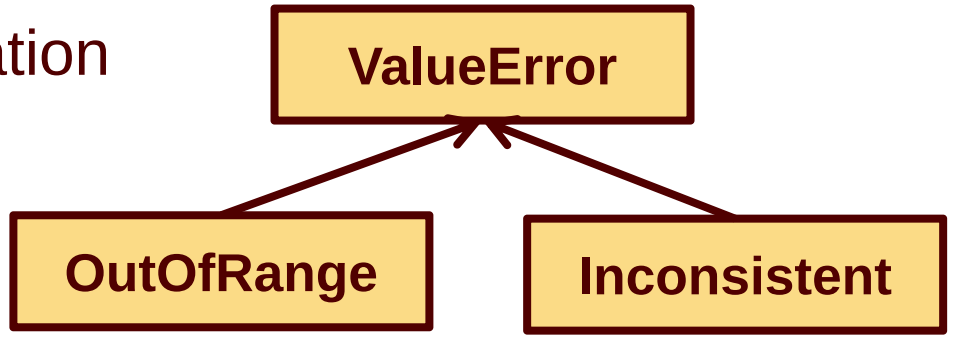
- An SAE standard (AS5506B) maintained by the SAE Aerospace AS-2C Committee
- Semantically precise language suitable for quantitative analyses
- Originally developed for analysis of embedded systems, but language is extensible – standard consists of a core language definition and annexes
- Application of AADL is growing both in the the US and internationally
- Supported by open-source and commercially available tools
- More information at http://www.aadl.info

Overview of Error-Model Annex

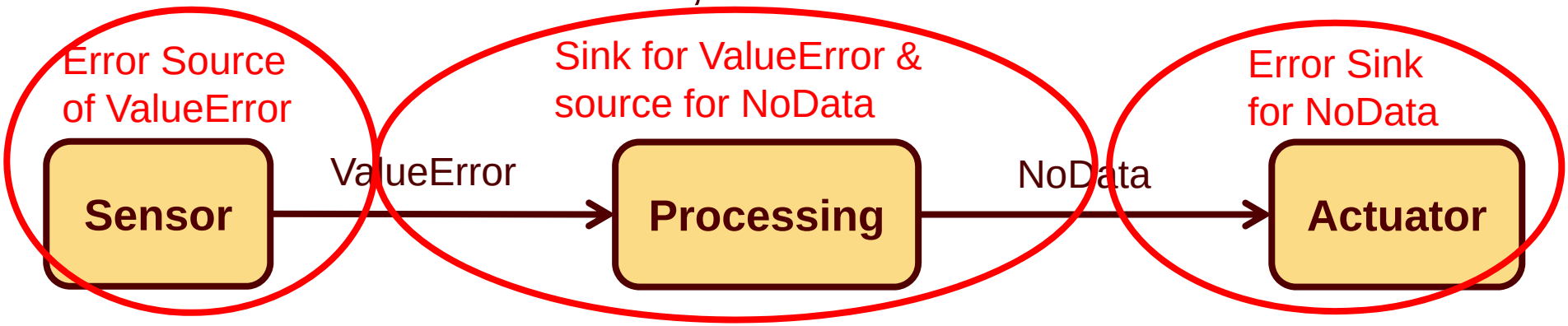
- Extension of AADL for fault description: error events, propagations, etc.
- Integration with current models by extending existing components
- Draft document to be proposed as a standard annex
- Support for Safety Evaluation and Analysis

Error Types and Propagations

- Error types: error classification

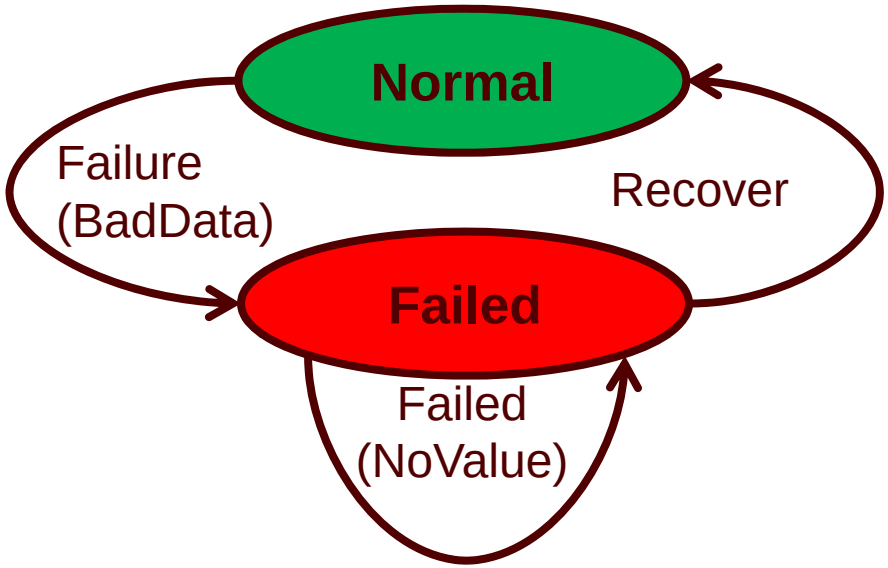


- Extensions and renaming
- Error propagations across components
  - Associate errors with system connections
  - Define error sources, sinks and containment

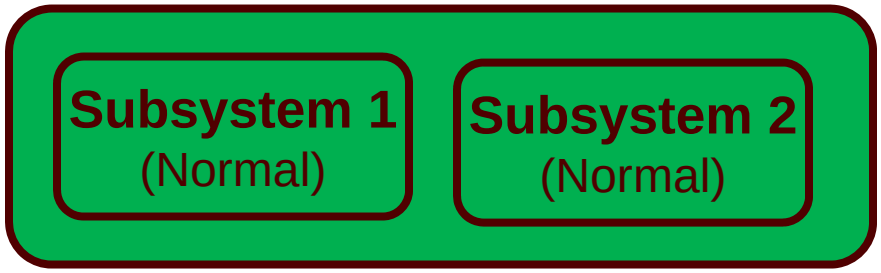


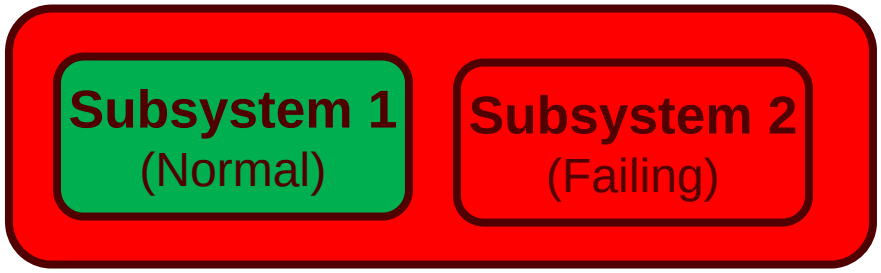
Error behavior

- States machines
  - Error-related transitions
  - Propagation rules
  - Use of error types



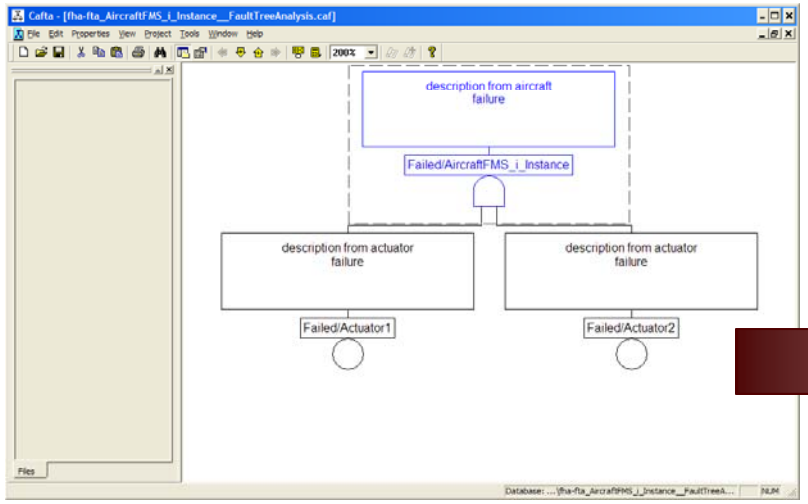
- Composite behavior
  - Define system states according to its parts
  - ex: “I am failing if one of my component is failing”





Specific Error-Model Properties

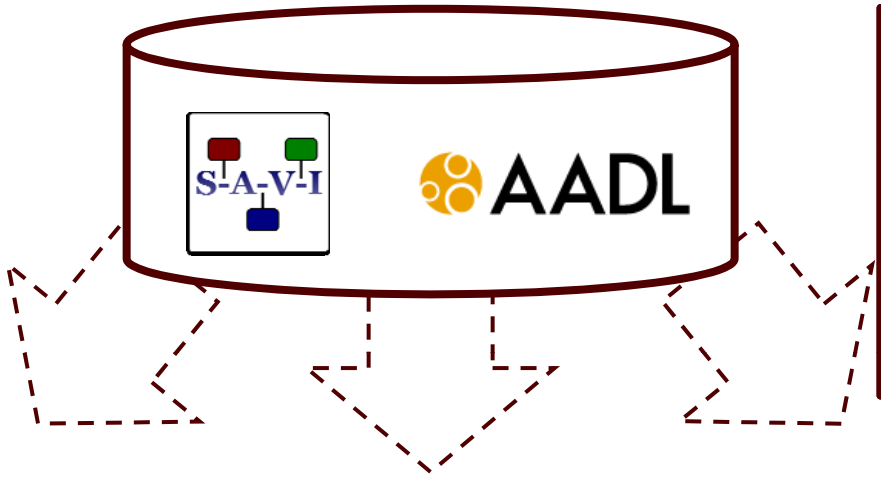
- Severity, likelihood, error description
- Support for generating validation documentation
- Tailoring for safety standards (ARP4761, MIL-STD-882)




```
ARP4761::severity => Catastrophic  applies to InadvertentBrake;
ARP4761::likelihood => ExtremelyImprobable applies to InadvertentBrake;
EMV2::hazard =>
    [   crossreference => "AIR6110 page 37 figure 17";
        failure => "Inadvertent wheel brake application";
        phase => "Takeoff";
        description => "Undetected inadvertent wheel brake on one wheel
                        without locking the wheel.";
        comment => "Crew cannot detect the failure by the asymmetry which is very small.
                    Brake temperature can reach very high temperature.";
    ]
    applies to Inadverte
```

SUPPORT OF SAFETY EVALUATION WITH AADL

AADL & Safety Evaluation – Tool Overview



Architecture centricity enables generative technologies to support analyses

FHA	FTA	Markov Chain	SPN/SANs	FMEA
• Spreadsheet • Use error propagations	• CAFTA OpenFTA • Use composite behavior • Error flows	• PRISM • Use error flow • Error behavior	• Stochastic Petri Nets and Activity Nets • Use error flow • Error behavior	• Spreadsheet • Error behavior • Propagations

"traditional" methodologies (a la ARP 4754/4761)

Safety Analysis & AADL

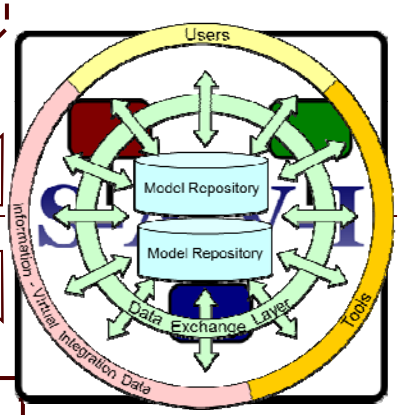
- Preliminary System Safety Assessment (PSSA) support
  - High-level component, interfaces from the OEM
  - Automatic generation of validation materials (FHA, FTA)
- System Safety Assessment (SSA) support
  - Use refined models from suppliers
  - Enhancement of error specifications
  - Support of quantitative safety analysis (FTA, FMEA, MA)

Evolution of Safety Analysis process with AADL

Preliminary System Safety Assessment

Component types (system interfaces)

AADL



Validation Materials (FHA, FTA)

Check PSSA and SSA consistencies

AADL

Component implementation

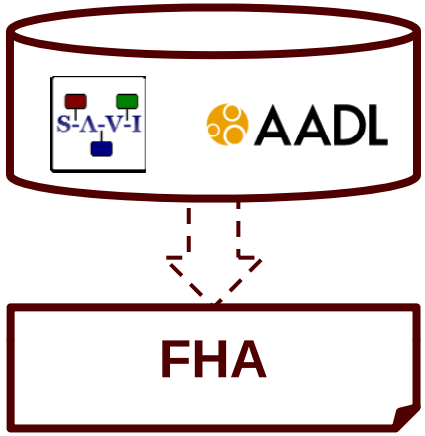
Validation with quantitative fault rates (FMEA, FTA, DD, MA)

Refinement & development evolution

System Safety Assessment

Functional Hazard Analysis Support

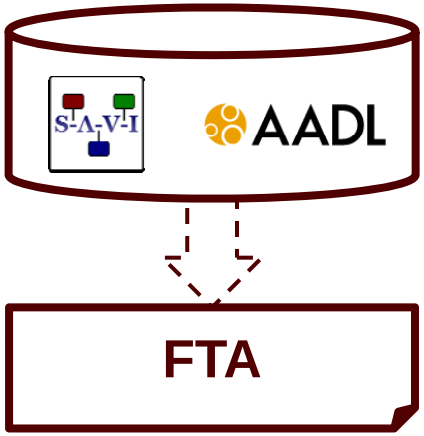
- Use of component error behavior
  - Error propagations rules
  - Internal error events
- Specify initial failure mode



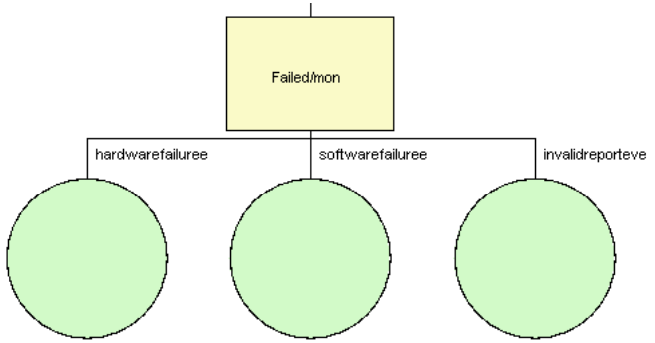
- Define error description and related information
- Create spreadsheet containing FHA elements
  - To be reused by commercial or open-source tools

Fault-Tree Analysis Support

- Use of composite error behavior
  - FTA nodes
- Use of component error behavior
  - Incoming error events



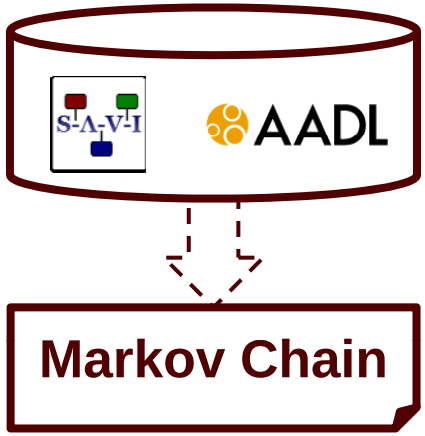
- Walk through the components hierarchy
  - Generate the complete fault-tree
  - Focus on specific AADL subcomponents

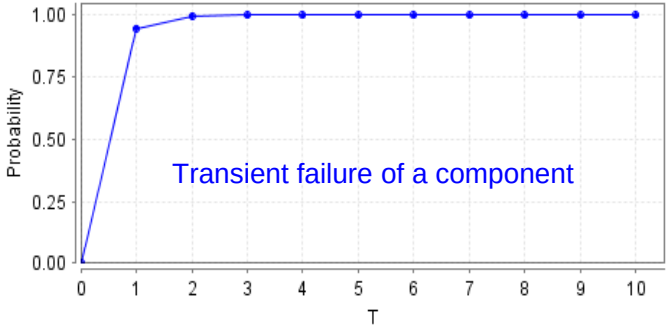


- Export to several tools
  - Commercial: CAFTA
  - Open-Source: OpenFTA – http://www.openfta.com

Markov-Chain Support

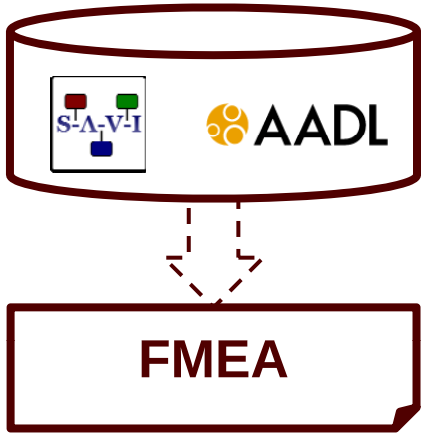
- Use of component error behavior
  - Error propagations rules
  - Error transitions
- Map states and error types into specific values
  - Tool-specific approach
- Ability to evaluate system state over time
  - What is the probability my system is failing within 30 days ?
- Export to open-source tools
  - PRISM http://www.prismmodelchecker.org/





Failure Mode and Effects Support

- Use of component error behavior
  - Error propagations rules (source, sink, etc.)
  - Internal error events
- Traverse all error paths
  - Record impact over the components hierarchy
- Use error description and related information
- Create spreadsheet containing FHA elements
  - To be reused by commercial or open-source tools



AVSI

CASE STUDY

Safety Analysis Overview and Demo Sequence

- Demonstrate a select set of PSSA analyses in the context of the Wheel Braking System (WBS) example
- Potential scenarios
  - Baseline design (pre-RFP)
  - Competing Architectures (RFP responses)
  - Architecture refinement (iteration on RFP selection)
  - Safety property specification refinement
- Preconditions
  - Aircraft and higher-level safety artifacts provided to PSSA – following progression of AIR 6110 (be specific)
  - WBS model(s) and supporting environment models configured with ARP property sets
  - Consistency check scenarios confirm model consistency
  - Reminder: “Per ARP 4761 the PSSA is the method for determining how failures can lead to the functional hazards identified by the FHA, and how the FHA requirements can be met.”

Wheel Brake System

- Development of a public model to complement the models developed in the SAVI Program
  - https://wiki.sei.cmu.edu/aadl/index.php/ARP4761_-_Wheel_Brake_System_%28WBS%29_Example
- Use of Error-Model and ARINC annexes
  - Relevance for the avionics community
- Apply the technology/toolset on a known example
  - Generation of FHA, FTA, MA & FMEA

AADL model Parent System

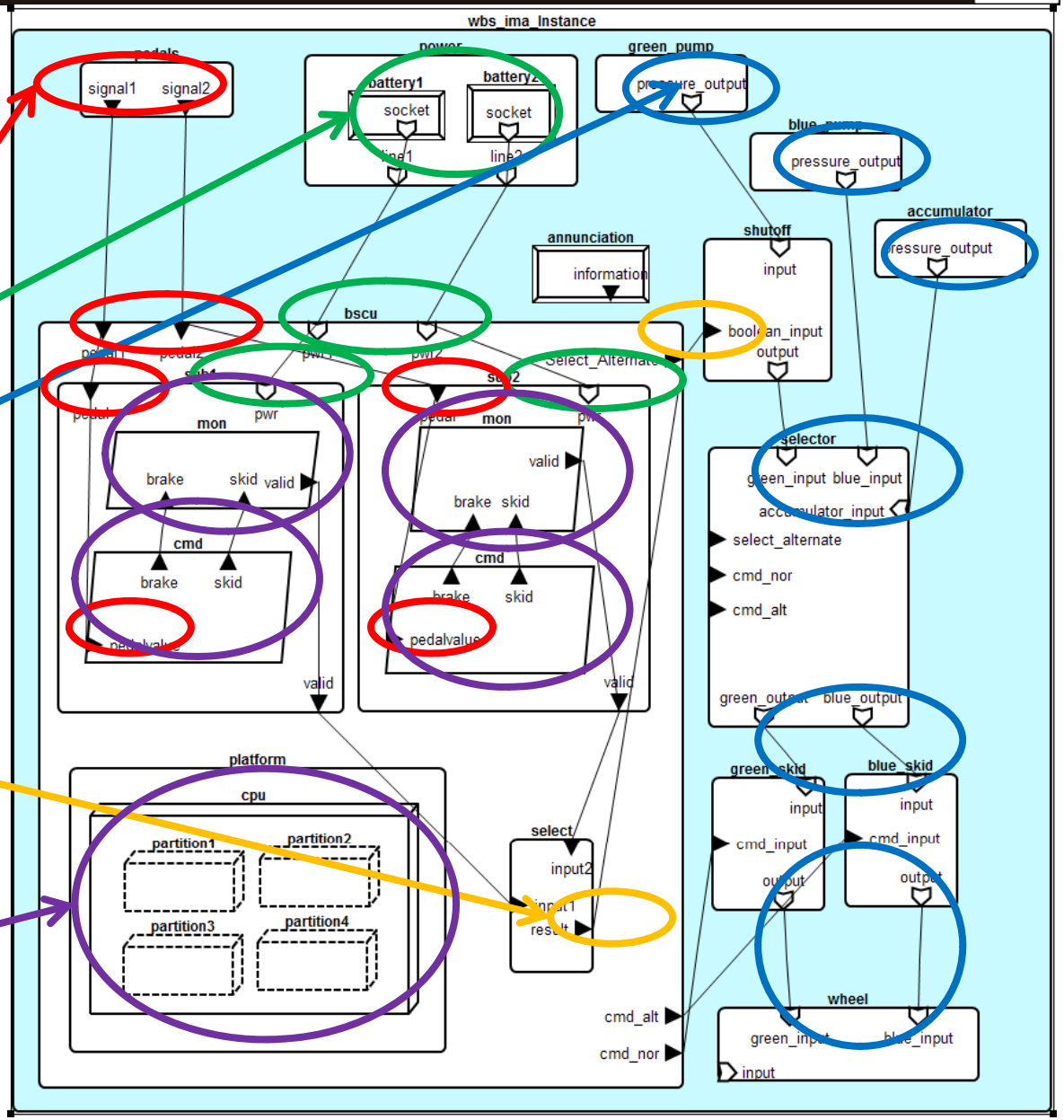
NoService

NoPower

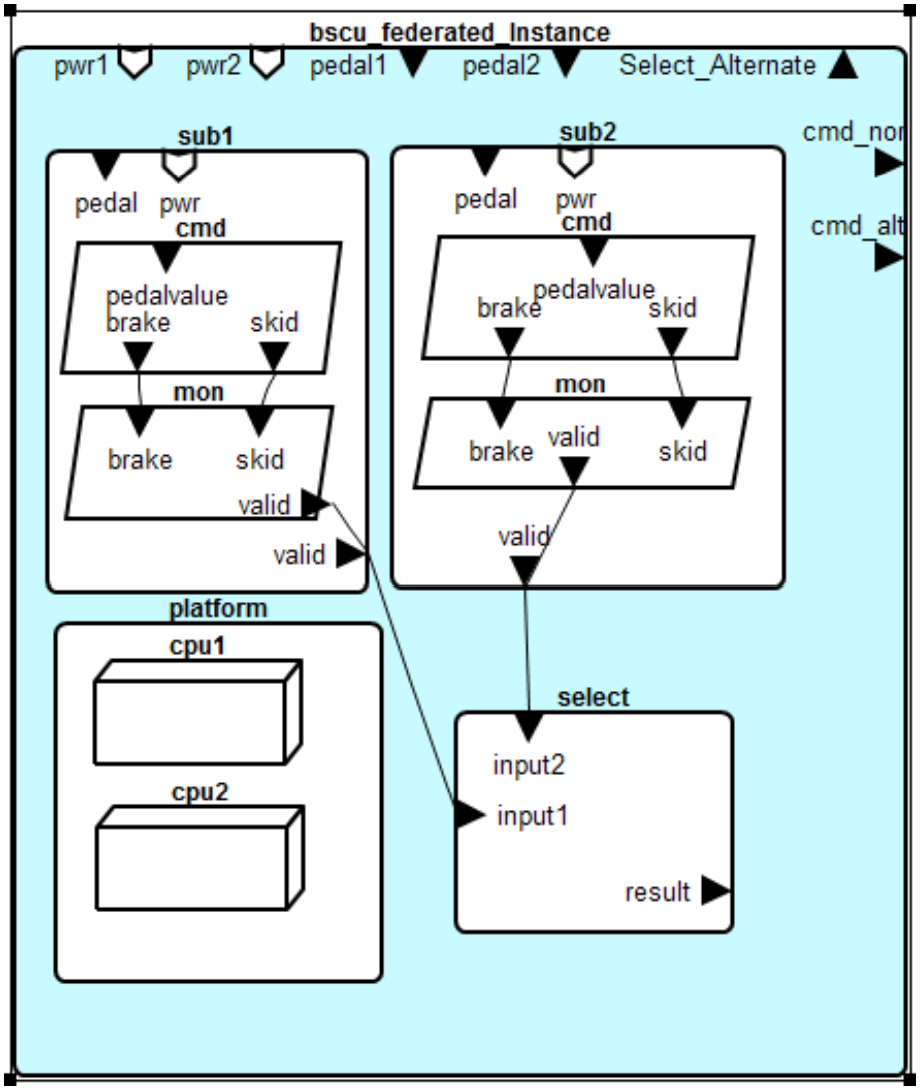
NoPressure

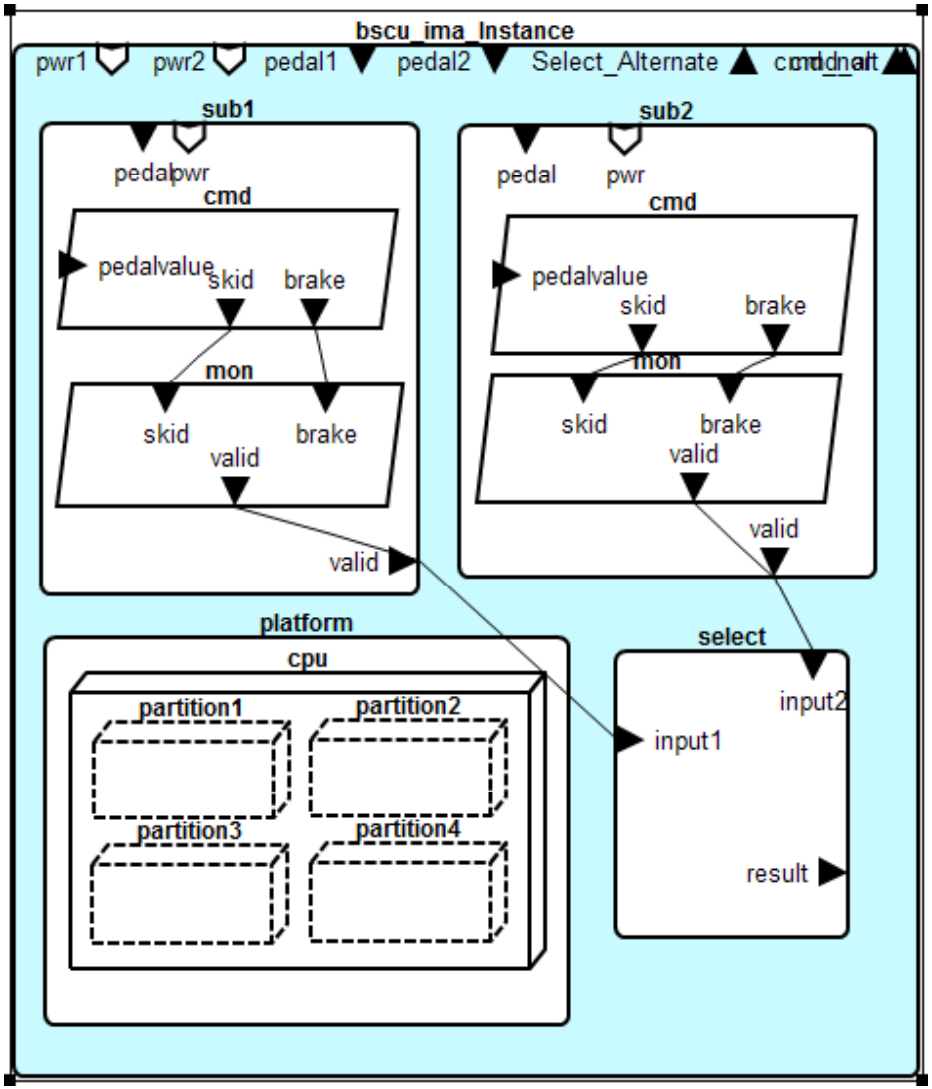
InvalidReport

Software and/or RuntimeError



AADL model, BSCU variations



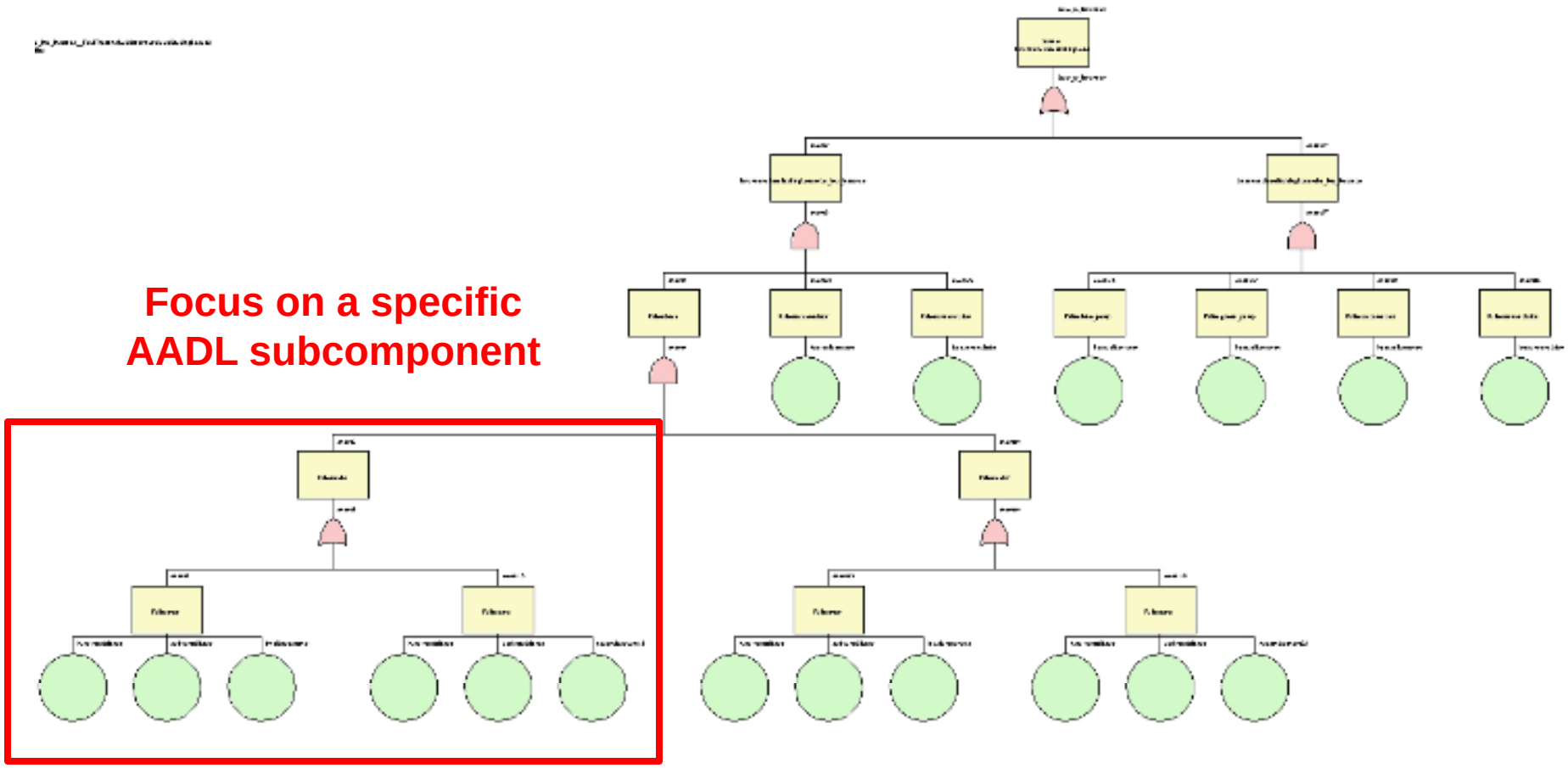


FHA of the Parent System

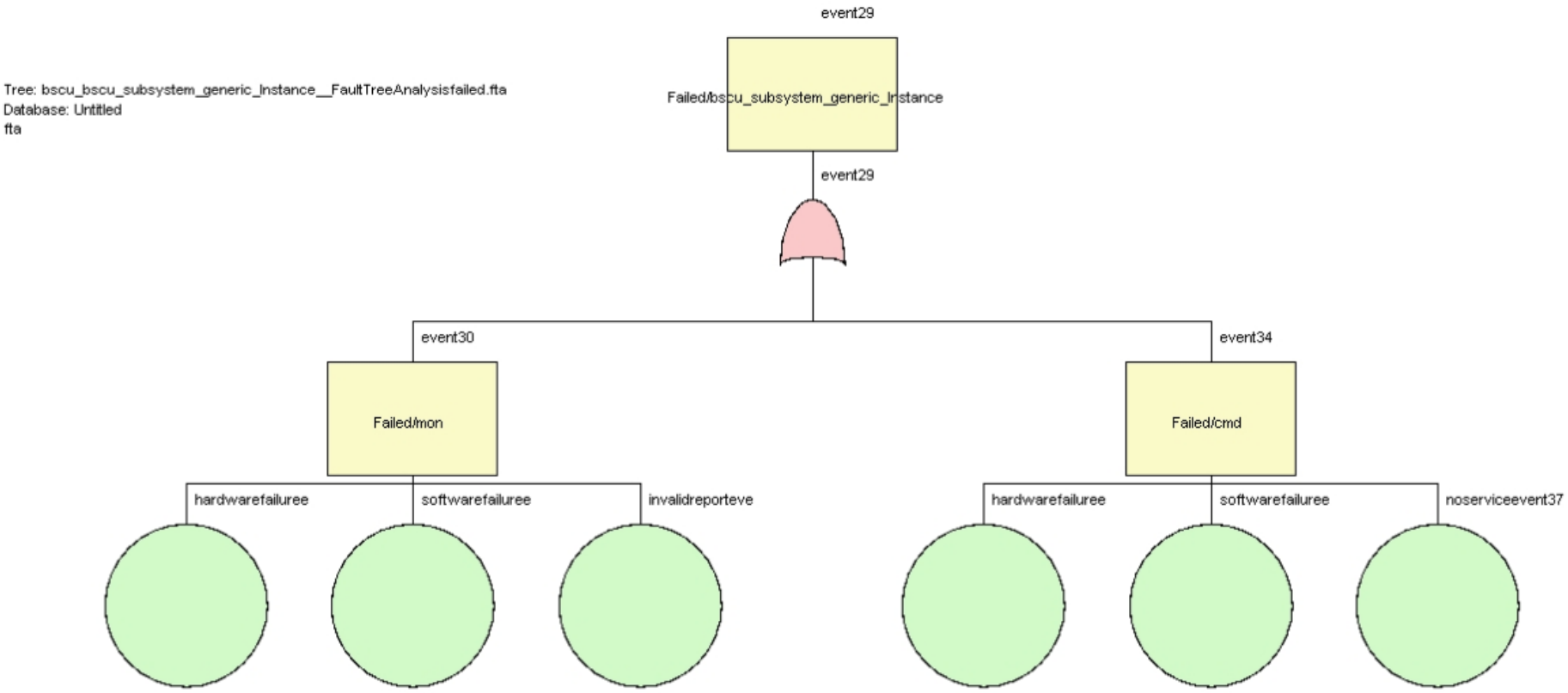
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	Component	Error	Crossreference	Functiona	Operational Phase		Effects of	Severity	Criticality	Verificati	Comment				
2	Root system	AsymmetricLoss	AIR6110 page 36 figure 17	Partial Sy	Landing or RTO		Asymmet	Catastrop	Extremel		Decrease in braking performance. Tendency to veer off the runway.				
3	Root system	InadvertentBrake	AIR6110 page 37 figure 17	Inadverte	Takeoff		Undetect	Catastrop	Extremel		Crew cannot detect the failure by the asymmetry which is very small. Bra				
4	Root system	AnnunciatedBrakingLoss	AIR6110 page 35 figure 17	Crew det	Landing or RTO		Total Loss	Hazardou	Extremel		Reference to crew procedures for loss of normal and reserve modes				
5	Root system	UnannunciatedBrakingLoss	AIR6110 page 35 figure 17	Crew det	Landing or RTO		Total Loss	Hazardou	Extremel		Reference to crew procedures for loss of normal and reserve modes				
6	Root system	PartialBrakingLoss	AIR6110 page 35 figure 17	Crew det	Landing or RTO		Partial Sy	Hazardou	Extremel		Additional study required to determine classification				
7	annunciation	LossAnnunciation	AIR6110 and ARP4761 - see ARP4	Loss of Ar	all		The syste	Catastrop	Extremel						
8	pedals	NoService on signal1	TBD	No signal	TBD		No signal				Would be critical if both power supplies are lost				
9	pedals	NoService on signal2	TBD	No signal	TBD		No signal				Would be critical if both power supplies are lost				
10	power/battery1	Depleted	TBD	Battery D	all		No more	Major	Probable		Can be an issue if redundant battery is failing also				
11	power/battery1	Explode	TBD	Battery Ex	all		Battery Ex	Catastrop	Extremel		Have a physical impact on the surrounding components				
12	power/battery1	NoPower on socket	ARP4761 page 277 figure 9	Loss of or	Landing/RTO		Loss of El	Major	Probable		Major hazard if both power are lost				
13	power/battery2	Depleted	TBD	Battery D	all		No more	Major	Probable		Can be an issue if redundant battery is failing also				
14	power/battery2	Explode	TBD	Battery Ex	all		Battery Ex	Catastrop	Extremel		Have a physical impact on the surrounding components				
15	power/battery2	NoPower on socket	ARP4761 page 277 figure 9	Loss of or	Landing/RTO		Loss of El	Major	Probable		Major hazard if both power are lost				
16	blue_pump	HydraulicError	ARP4761 page 275 figure L9	Hydraulic	TBD		Loss of or	Major	Probable		Major hazard if both pumps are lost				
17	green_pump	HydraulicError	ARP4761 page 275 figure L9	Hydraulic	TBD		Loss of or	Major	Probable		Major hazard if both pumps are lost				
18	accumulator	HydraulicError	ARP4761 page 275 figure L9	Hydraulic	TBD		Loss of or	Major	Probable		Major hazard if both pumps are lost				
19	bscu/sub1	Failed	ARP4761 figure L4 page 215	Failure of	all		Failure of	Major	Probable		Would be critical if two subsystem (primary and redundant) are deffectiv				
20	sub1/mon	InvalidReport	TBD	Invalid Re	TBD		Report fr	Minor	Probable		Minor Hazard				
21	bscu/sub2	Failed	ARP4761 figure L4 page 215	Failure of	all		Failure of	Major	Probable		Would be critical if two subsystem (primary and redundant) are deffectiv				
22	sub2/mon	InvalidReport	TBD	Invalid Re	TBD		Report fr	Minor	Probable		Minor Hazard				
23	bscu/select	InternalError	ARP4761 figure L4 page 215		all		BSCU vali	Hazardou	Extremel						
24	platform/cpu	HardwareFailure	TBD		all		Hardware	Major	Probable		Impact all software components associated to the hardware				
25	cpu/partition1	SoftwareFailure	TBD		all		Software	Major	Probable		Impact all components that are controlled by this software				
26	cpu/partition2	SoftwareFailure	TBD		all		Software	Major	Probable		Impact all components that are controlled by this software				
27	cpu/partition3	SoftwareFailure	TBD		all		Software	Major	Probable		Impact all components that are controlled by this software				
28	cpu/partition4	SoftwareFailure	TBD		all		Software	Major	Probable		Impact all components that are controlled by this software				

FTA of the Parent System

Focus on a specific AADL subcomponent

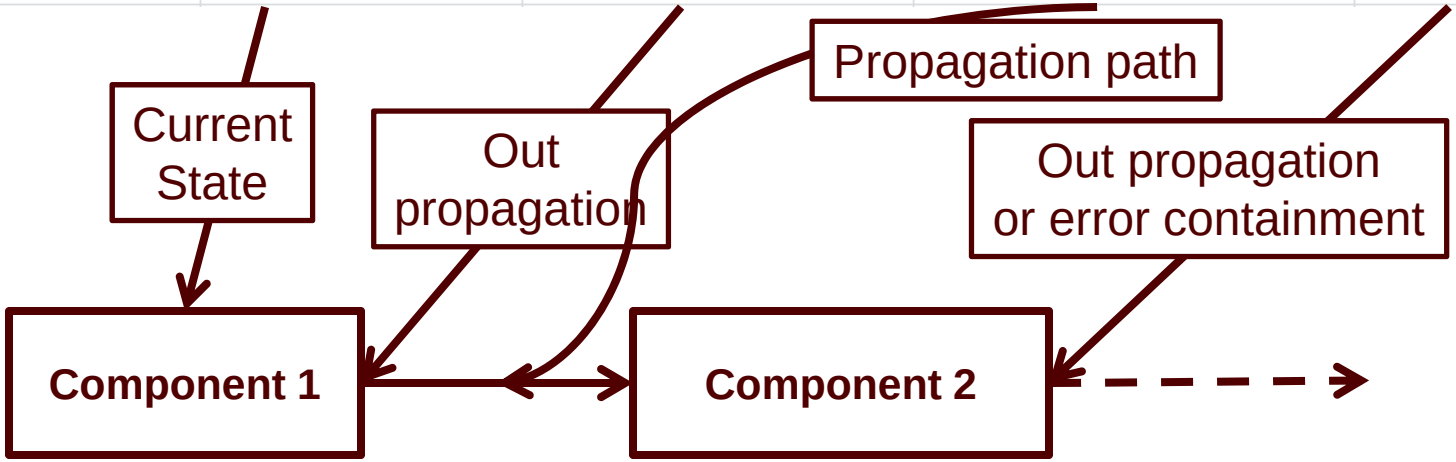


FTA of the BSCU subcomponent



FMEA of the Parent System

Component	Initial Failure Mode	1st Level Effect	Failure Mode	second Level Effect
pedals	{NoService}	pedals.signal1:{NoService}	pedals{NoService}->sub1/cmd	sub1/cmd: {NoService} Masked
pedals	{NoService}	pedals.signal2:{NoService}	pedals{NoService}->sub2/cmd	sub2/cmd: {NoService} Masked
pedals	internal event InternalFault	pedals.signal2:{NoService}	pedals{NoService}->sub2/cmd	sub2/cmd: {NoService} Masked
pedals	internal event InternalFault	pedals.signal1:{NoService}	pedals{NoService}->sub1/cmd	sub1/cmd: {NoService} Masked
power/battery1	{NoPower}	power/battery1.socket:{NoPower}	power/battery1{NoPower}->bscu/sub1	bscu/sub1: {NoPower} Masked
power/battery1	internal event Depleted	power/battery1.socket:{NoPower}	power/battery1{NoPower}->bscu/sub1	bscu/sub1: {NoPower} Masked
power/battery1	internal event Explode	power/battery1.socket:{NoPower}	power/battery1{NoPower}->bscu/sub1	bscu/sub1: {NoPower} Masked
power/battery2	{NoPower}	power/battery2.socket:{NoPower}	power/battery2{NoPower}->bscu/sub2	bscu/sub2: {NoPower} Masked
power/battery2	internal event Depleted	power/battery2.socket:{NoPower}	power/battery2{NoPower}->bscu/sub2	bscu/sub2: {NoPower} Masked
power/battery2	internal event Explode	power/battery2.socket:{NoPower}	power/battery2{NoPower}->bscu/sub2	bscu/sub2: {NoPower} Masked



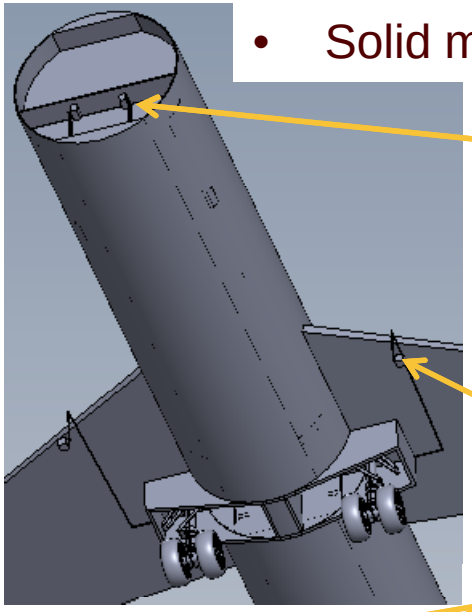
FUTURE WORK

Safety Analysis Consistency Checks

- Consistency at integration time
  - Consistency between models from different suppliers
  - Strengthen the Virtual Integration promoted by SAVI
- Consistency of the internal model
  - ex: Can I propagate this error according to my actual state ?
- Consistency across error models specifications
  - Component Error Behavior with Composite Error Behavior
  - Correctness of a state according to subcomponents
- Error information with Behavior information

SAVI Consistency Checks

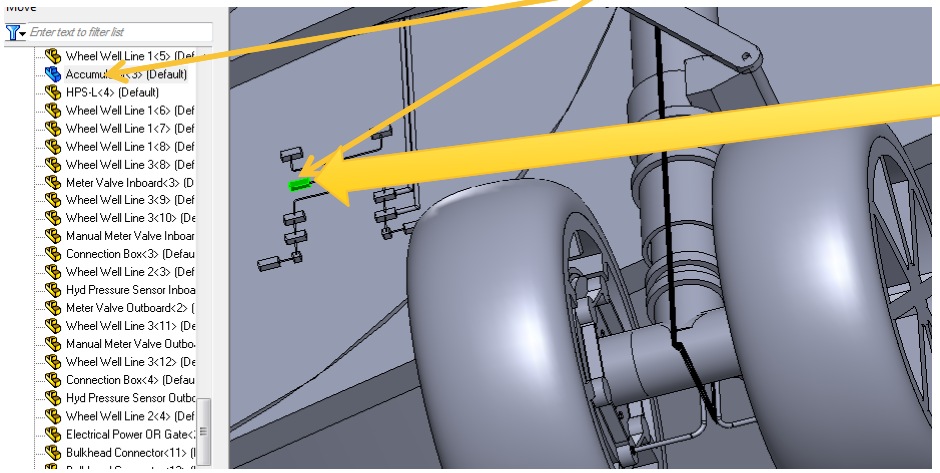
- Solid models



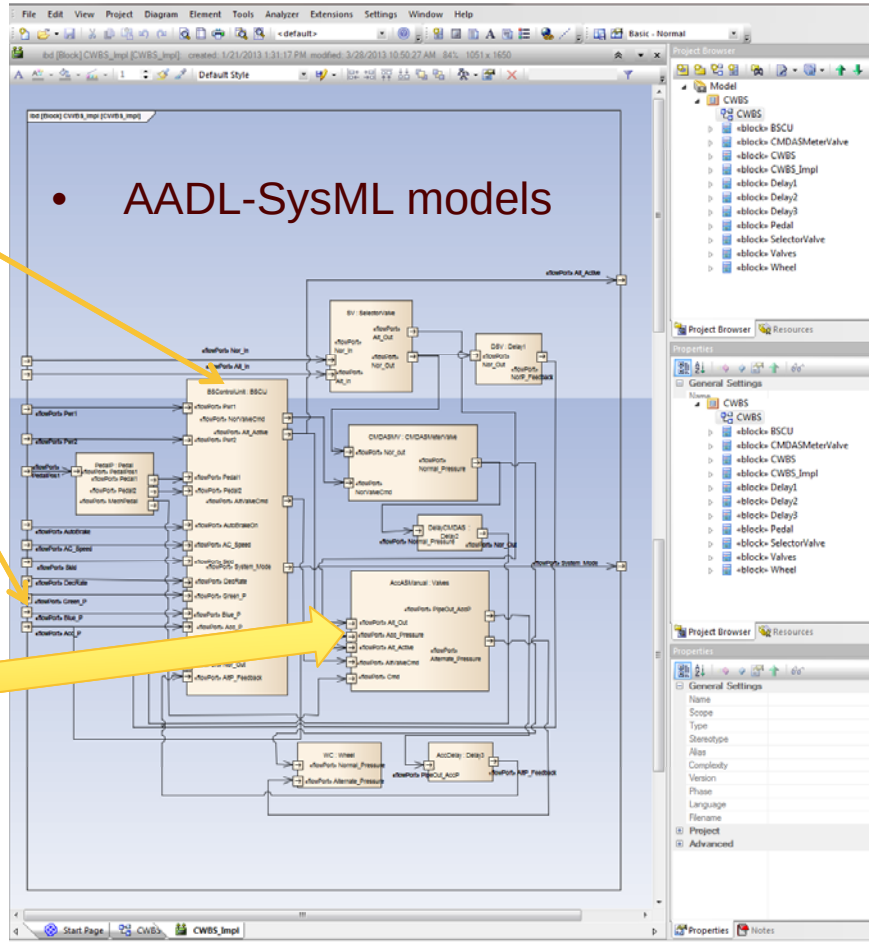
BSCU

Hyd power supply

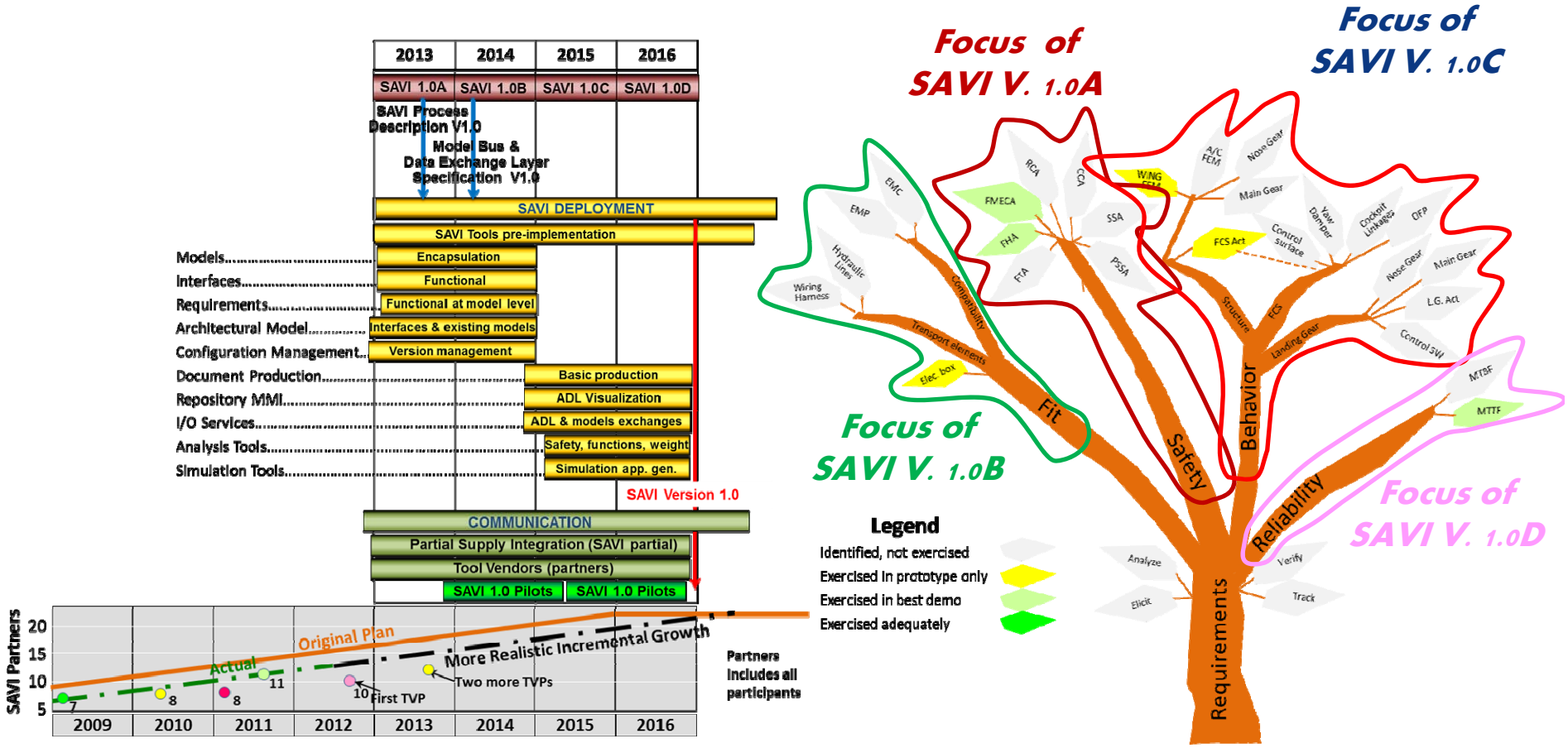
Accumulator



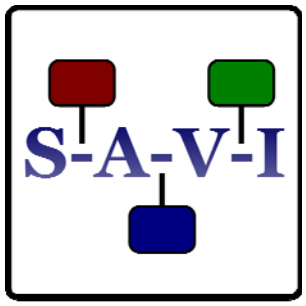
- AADL-SysML models



Current Project Focus



Questions?



Contacts:

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

Dr. Julien Delange
Office: (412) 268-9652
jdelange@sei.cmu.edu