Supporting Safety Evaluation Process using AADL

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

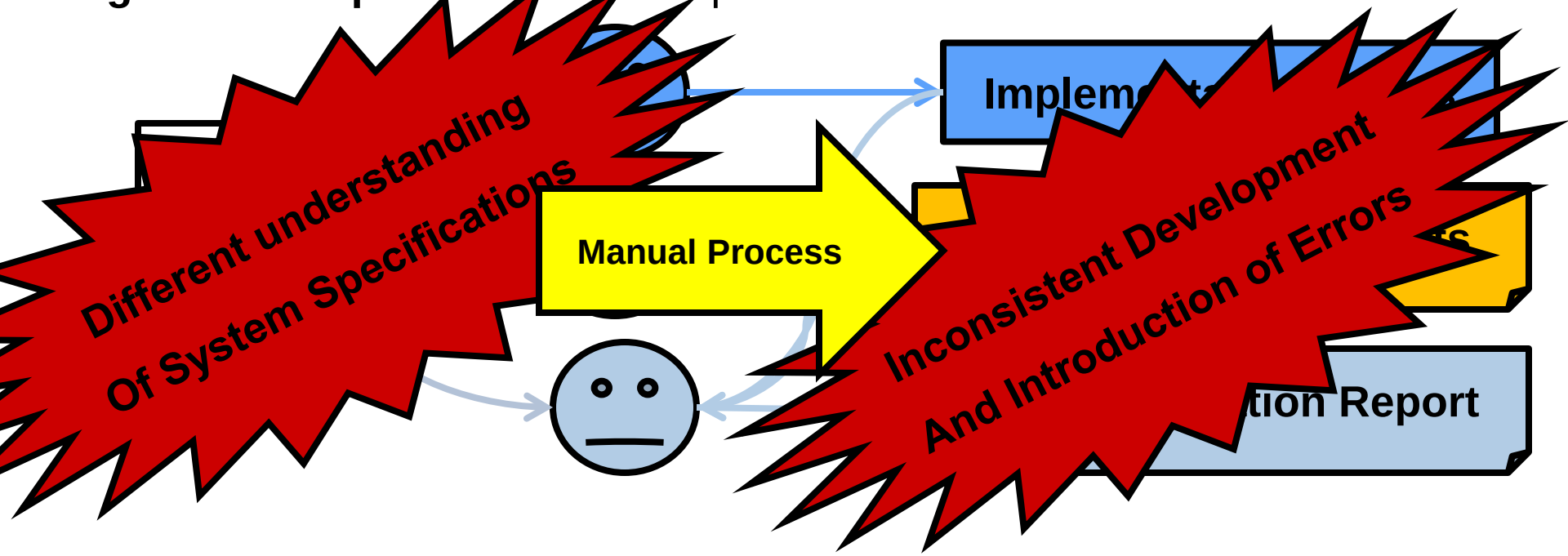
Julien Delange and Peter Feiler
12/09/2013

Safety Analysis issues (aka the problem)

Manual process, **inaccurate** with system implementation

Some errors are **not captured/caught during analysis**

Long and error-prone evaluation process

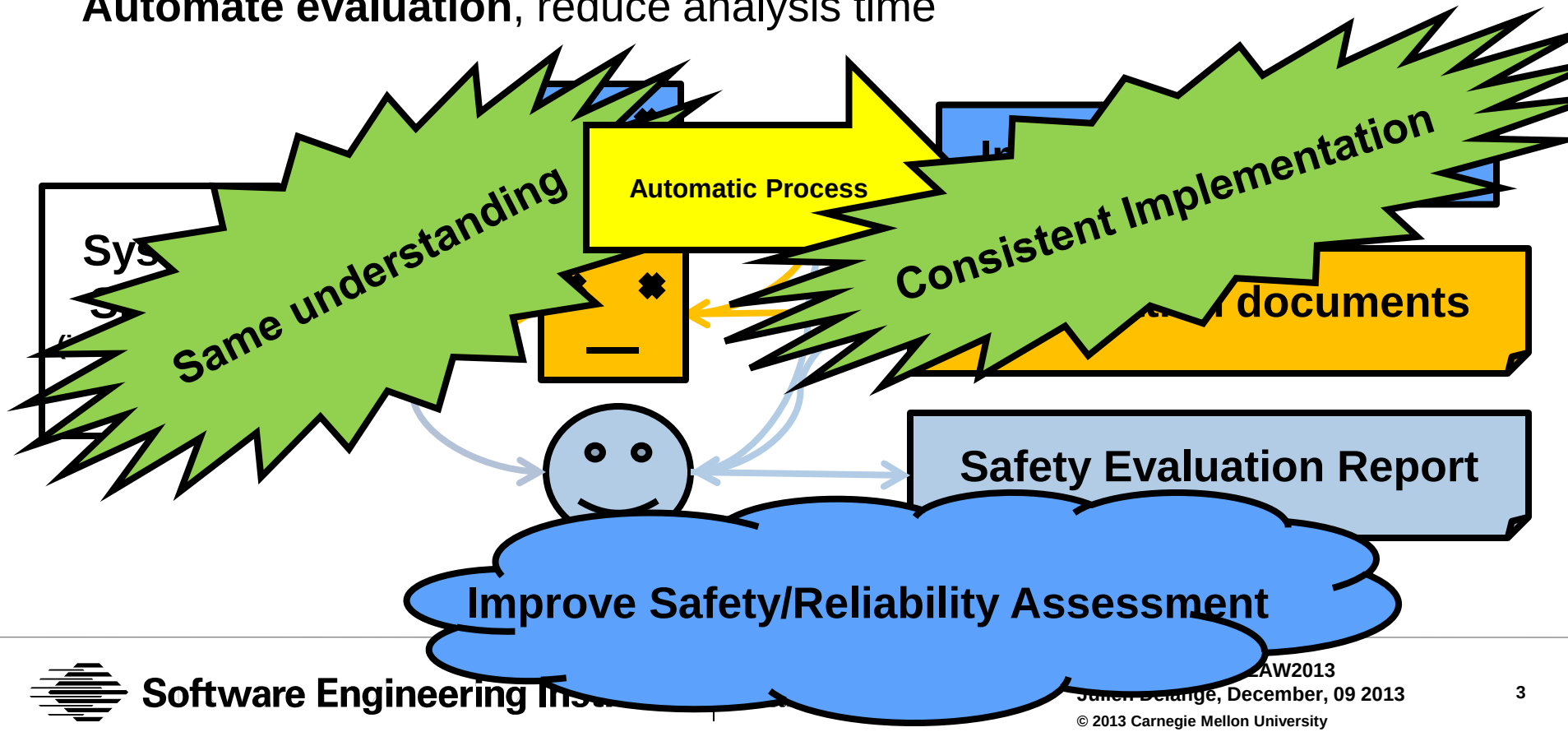


Automate/Improve Evaluation (aka the solution)

Derives materials **from existing artifacts** (i.e. architecture models)

Avoid manual process traps and pitfalls

Automate evaluation, reduce analysis time



Combine existing methods (aka the approach)

Add safety-information to existing models

Automate the evaluation process, **avoid manual efforts**

Generate materials required by safety standards (ARP4761)

Agenda

Overview of AADL & Error-Model Annex

Overview of ARP4761 and Safety Evaluation

Support of Safety Evaluation with AADL

Case-Study

On-Going Work

Discussion

Agenda

Overview of AADL/Error-Model Annex

Overview of ARP4761 & Safety Evaluation

Support of Safety Evaluation with AADL

Case-Study

On-Going Work

Discussion

Architecture Analysis Design Language

Modeling language standardized by SAE

- Inherit MetaH concepts
- Initiated in 2003; revised in 2008

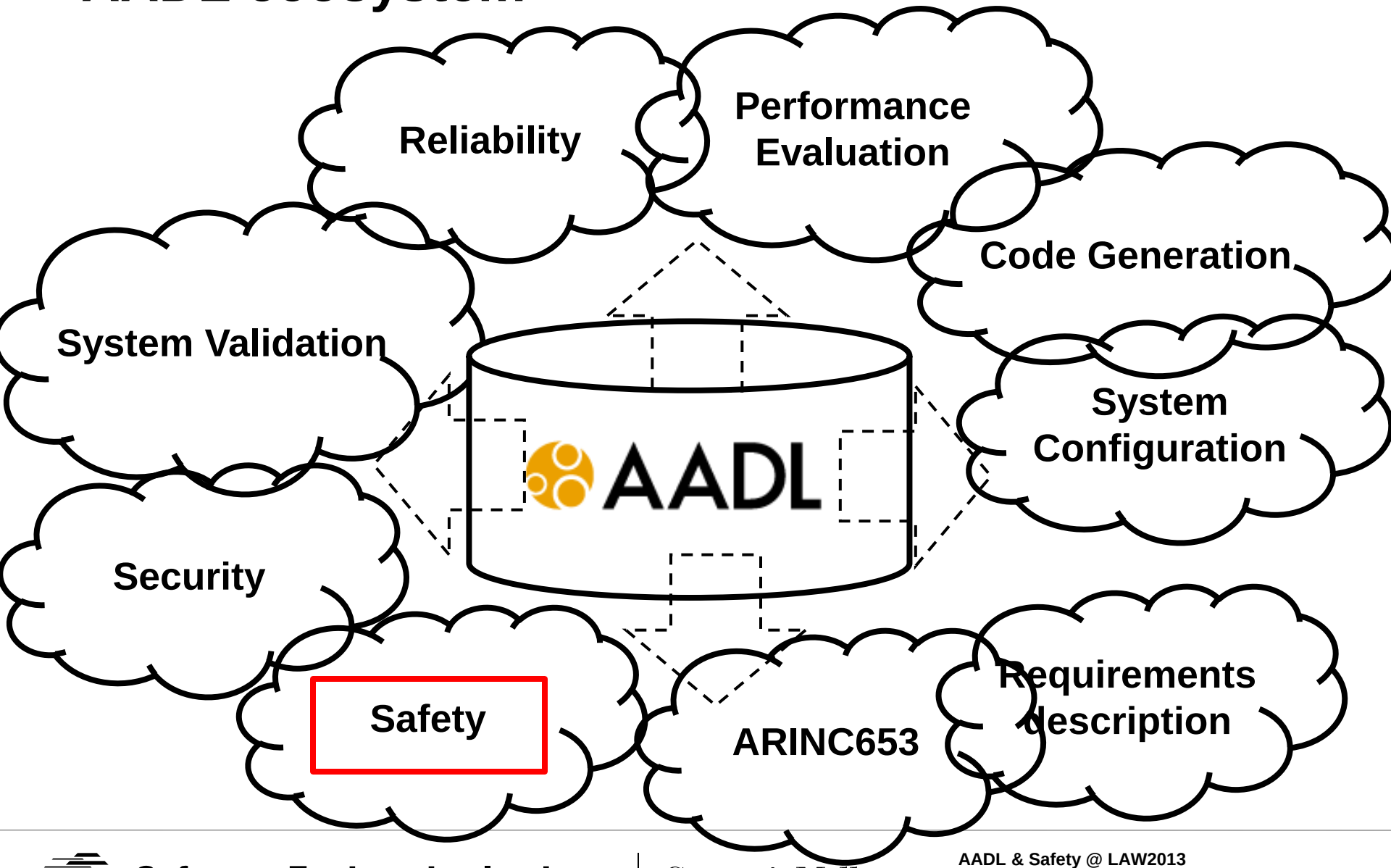
Design of hardware and software

- Analysis of different criteria (performance, safety, security, etc.)
- Tool support: OSATE, Ocarina, MASIW

Evaluation during research projects

- SAVI: avionics community
- ASSERT: aerospace community

AADL ecosystem



Overview of Error-Model Annex

Extension of AADL for fault description: error events, propagations, etc.

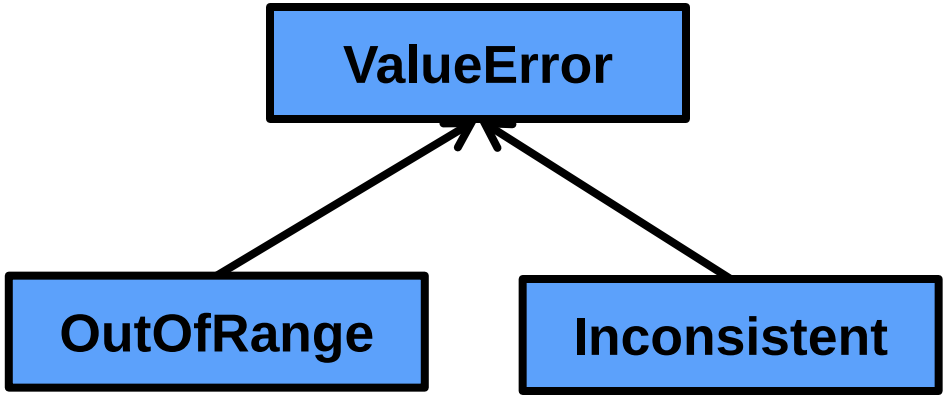
Integration with current models by extending existing components

Draft document to be proposed as a standard annex

Support for Safety Evaluation and Analysis

Error Types and propagations

Error types: error classification

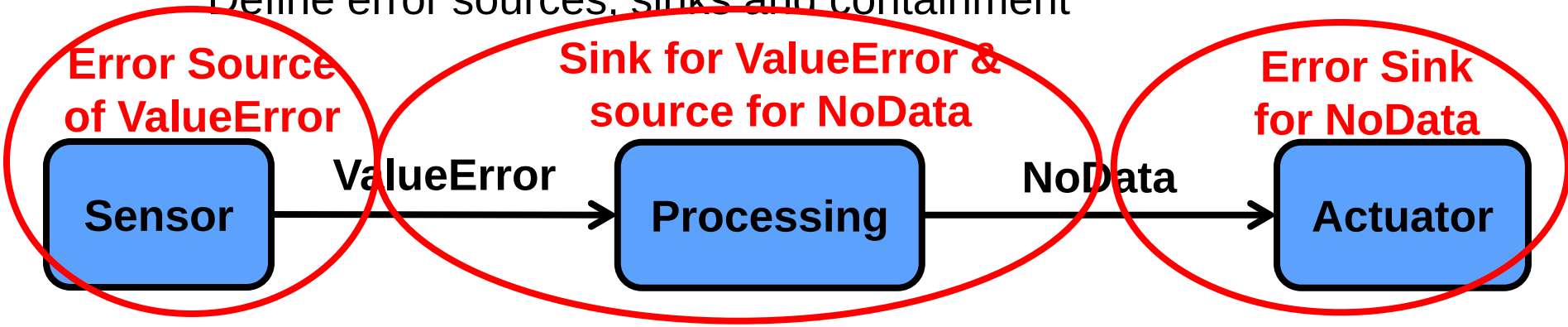


Extensions and **renaming**

Error propagations across components

Associate errors with system connections

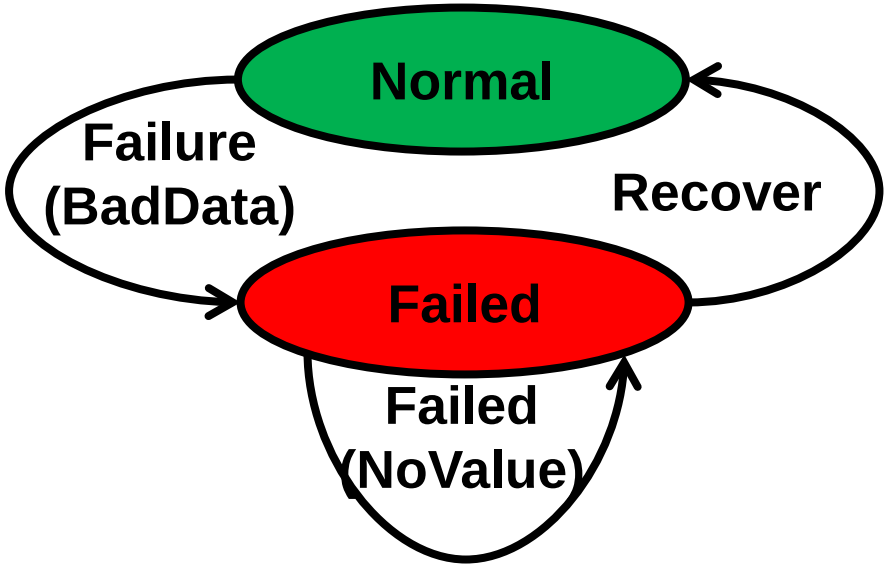
Define error sources, sinks and containment



Error behavior

States machines

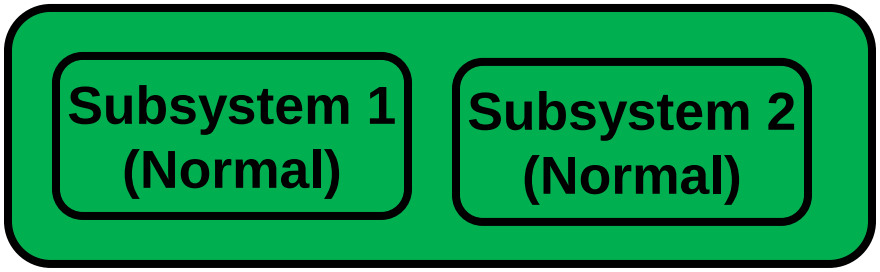
Error-related transitions
Propagation rules
Use of error types

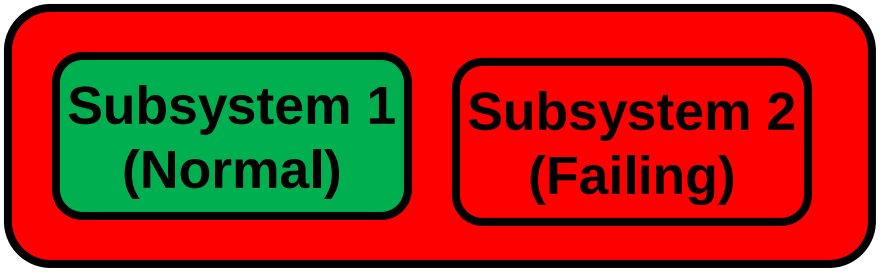


Composite behavior

Define system states according to its parts

ex: "I am failing if one of my component is failing"





Support of AADL textual syntax

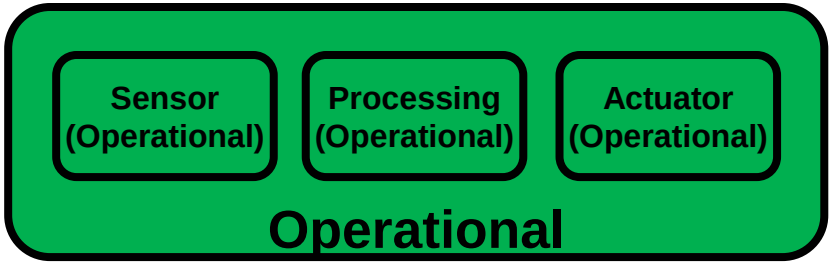
Error types mechanism w/ extensions

```
error types
    ValueError          : type;
    OutOfRange          : type extends ValueError;
    Inconsistent        : type extends ValueError;
end types;
```

Error propagations


```
system sensor
features
    valueout: out data port d;
annex EMV2 {**
    use types error_library;
    use behavior error_library::Simple;
    error propagations
        valueout : out propagation {ValueError};
    flows
        f1 : error source valueout{ValueError};
    end propagations;
**};
end sensor;
```

Composite error state Machine




```
system main
end main;

system implementation main.impl
subcomponents
    s : system sensor;
    p : system processing;
    a : system actuator;
annex EMV2 {**
    use types error_library;
    use behavior error_library::Simple;
    composite error behavior
    states
        [s.Failed or p.Failed or a.Failed ]-> Failed;
        [s.Operational and p.Operational and a.Operational ]-> Operational;
    end composite;
**};
end main.impl;
```

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 InadvertentBrake;
```

Agenda

Overview of AADL & Error-Model Annex

Overview of ARP4761 & Safety Evaluation

Analysis of System Safety with AADL

Case-Study

On-Going Work

Discussion

ARP4761 Safety Standard

SAE standard for Safety Assessment

Avionics Community mostly (relation with DO178B)

Assurance of System Safety

Define Safety Evaluation Process Materials & Methodology

Iterative process, follow development workflow

Inter-connection between documents (cross checks)

Use in the SAE AIR6110 standard

Example of safety evaluation process

Wheel-Brake System Example

Safety Analysis Workflow

Aircraft-level (functions)

- Define failure conditions
- Allocate failure to system functions

Preliminary System Safety Assessment

- System Functional Hazard Analysis (FHA)
- System Fault-Tree Analysis (FTA)

System Safety Assessment

- Failure Mode and Effect Analysis
- Refined FTA with Quantitative Failures Rates

System Development Cycle

Functional Hazard Analysis

ARP4761, section 3

Identify and classify functions failure conditions

Aircraft or System Level

- Aircraft, High-Level View
- Refinement at System Level

1 Function	2 Failure Condition (Hazard Description)	3 Phase	4 Effect of Failure Condition on Aircraft/Crew	5 Classification	6 Reference to Supporting Material	7 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	The crew detects the failure when the brakes are operated. The crew uses spoilers and thrust reversers 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 landing overrun. 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			

Input for safety requirements specification

- Description and specification in FTA, DD or MA
- Reference of Aircraft Low-Level to System FHA

Spreadsheet with reference to functions failures description

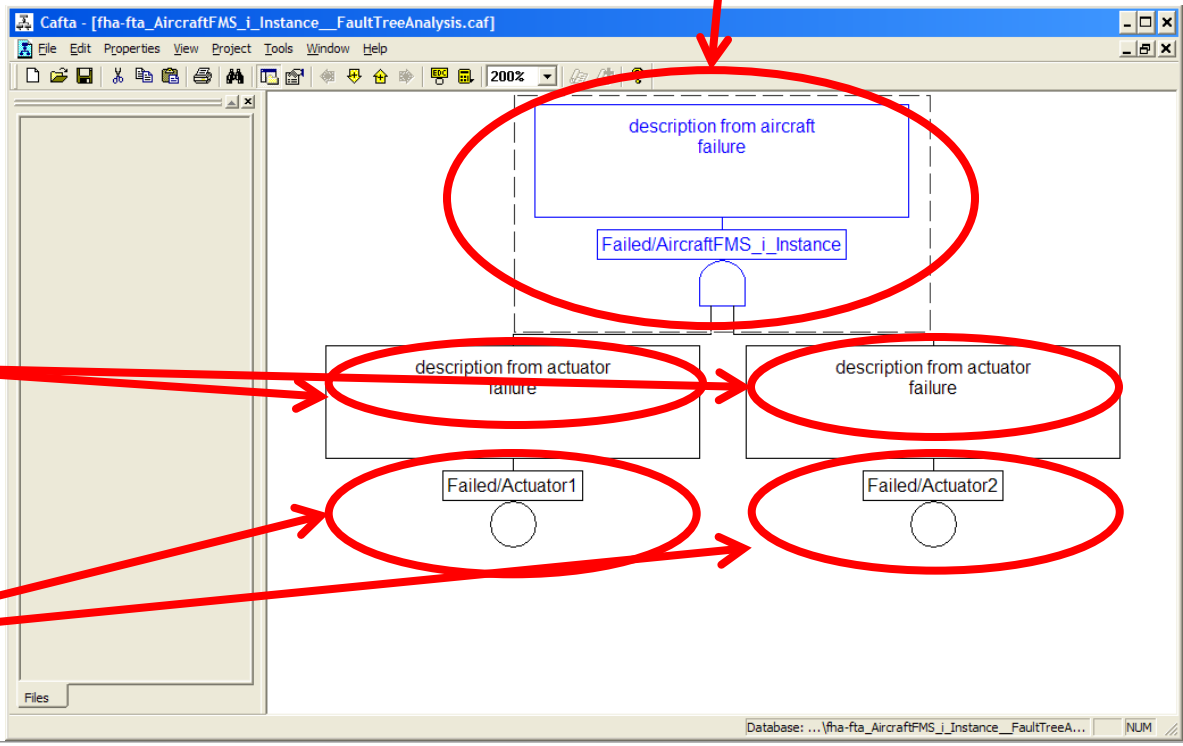
Fault-Tree Analysis

ARP4761, section 4.1

Relationship of failure effects and failure modes

Reference to system hierarchy

Support with Open-Source and Commercial Tools



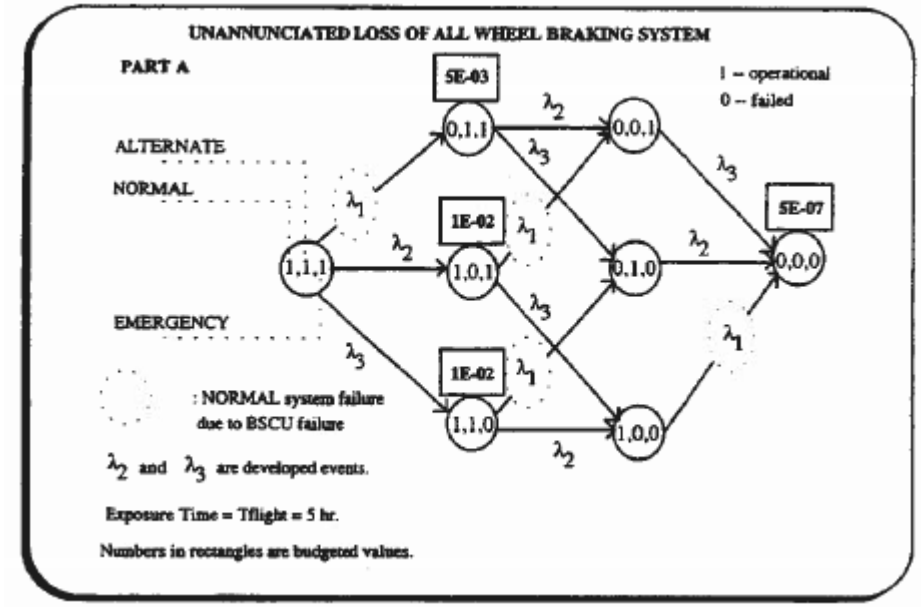
Markov Chain

ARP4761, section 4.1

Evaluation of system behavior over time

Probability of being in particular states

Analysis and evaluation of fault states



Support with Commercial and Open-Source Tools

Failure Mode and Effect Analysis

ARP4761, section 4.2

Impact of Fault at a Higher Levels

Start from Function Level to System/Aircraft Level

Spreadsheet/textual document

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				

Agenda

Overview of AADL & Error-Model Annex

Overview of ARP4761 & Safety Evaluation

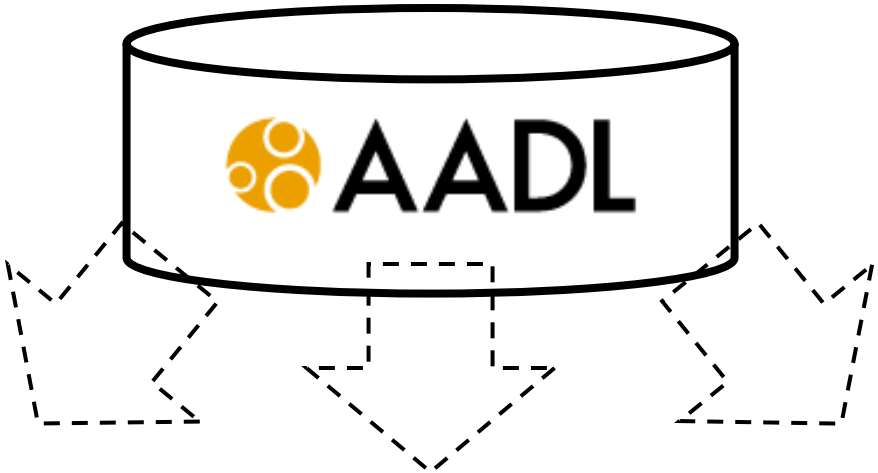
Support of Safety Evaluation with AADL

Case-Study

On-Going Work

Discussion

AADL & Safety Evaluation – Tool Overview



FHA

- Spreadsheet
- Use error propagations

FTA

- CAFTA
  OpenFTA
- Use composite behavior
- Error flows

Markov Chain

- PRISM
- Use error flow
- Error behavior

FMEA

- Spreadsheet
- Error behavior
- Propagations

Safety Analysis & AADL

Preliminary System Safety Assessment (PSSA) support

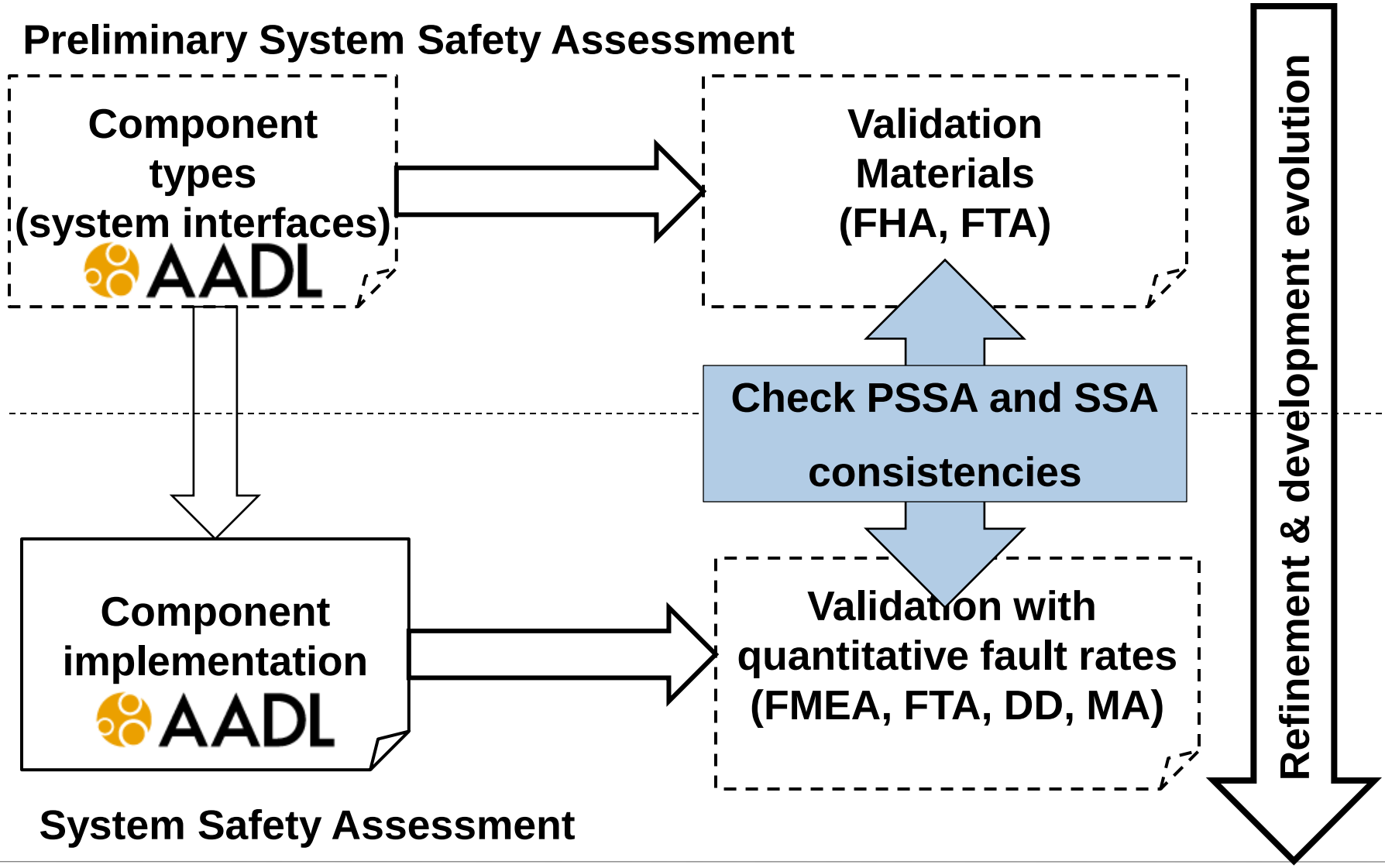
- High-level component, interfaces from the OEM
- Automatic generation of validation materials (FHA, FTA)

System Safety Assessment (SSA) support

- Use refined models from suppliers
- Enhancement of error specifications
- Support of quantitative safety analysis (FTA, FMEA, MA)

System Development Cycle

Evolution of Safety Analysis process with AADL



Safety Analyses on Refined Architecture

Aircraft-Level Safety Analysis

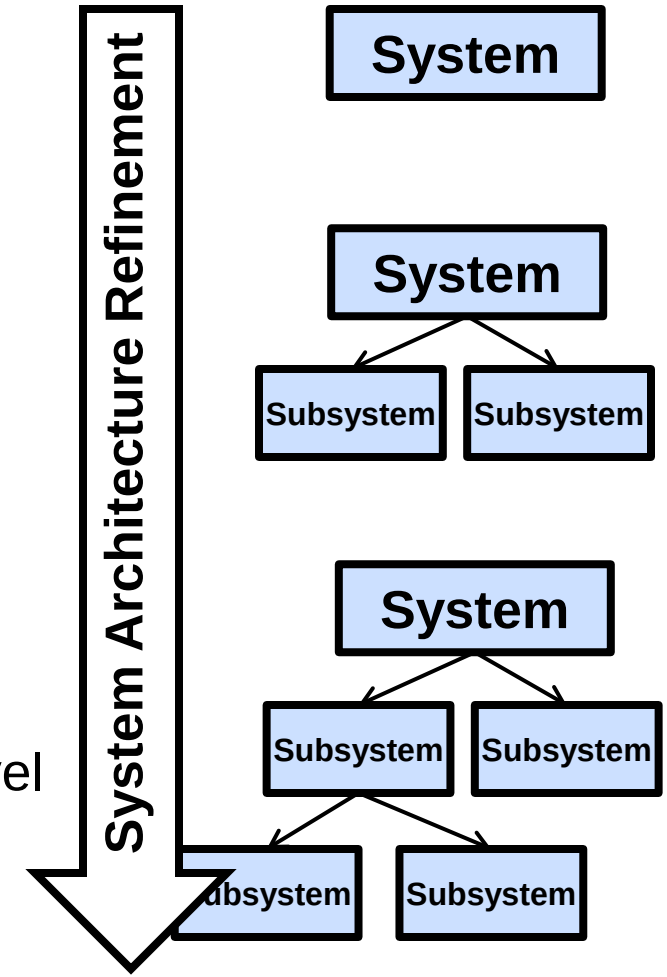
- Define aircraft failure conditions
- Allocate failure to system functions
- Perform PSSA and SSA

Avionics Subsystem Level Safety Analysis

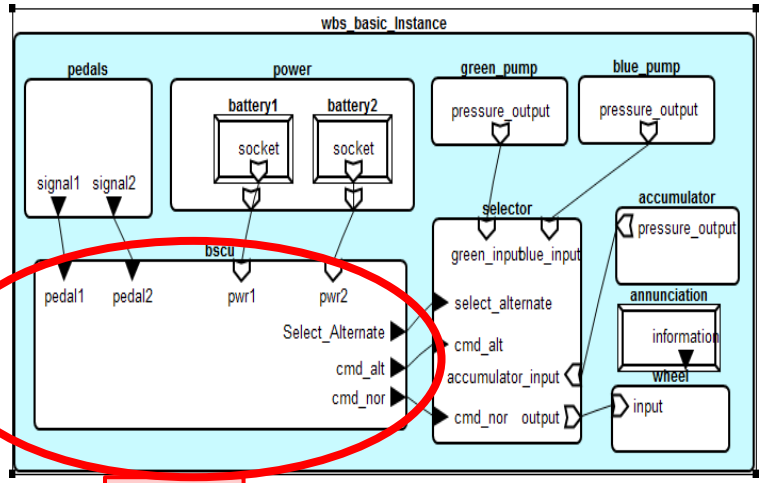
- Perform PSSA and SSA at subsystem level
- Ensure consistency with aircraft level analysis

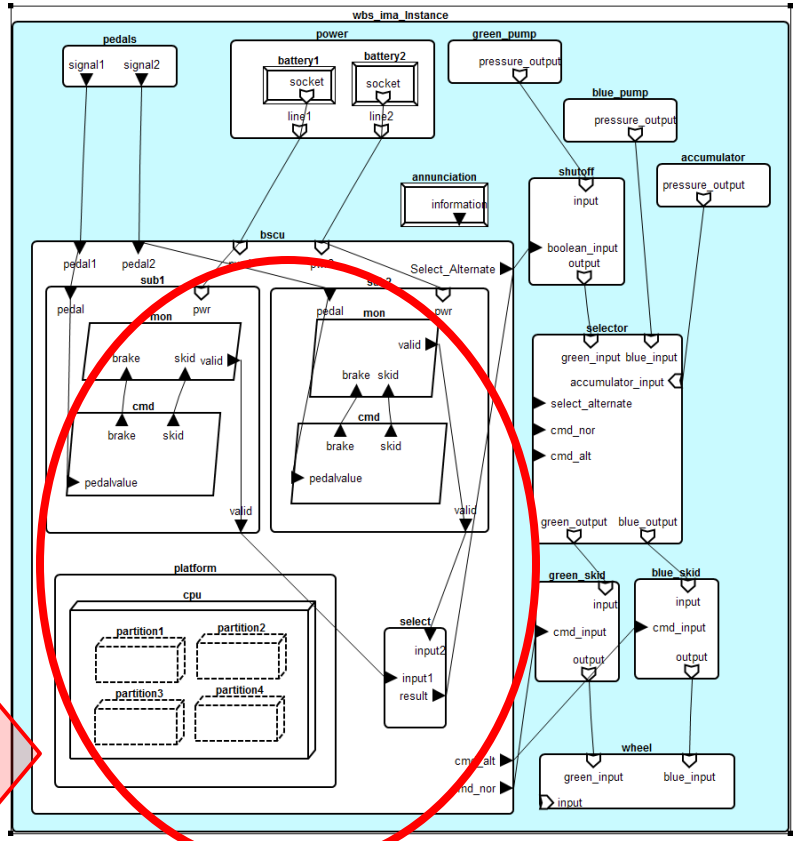
Navigation Sub-Subsystem Level Safety Analysis

- Perform PSSA and SSA at sub-subsystem level
- Ensure consistency with aircraft level analysis



Evolution of the AADL model





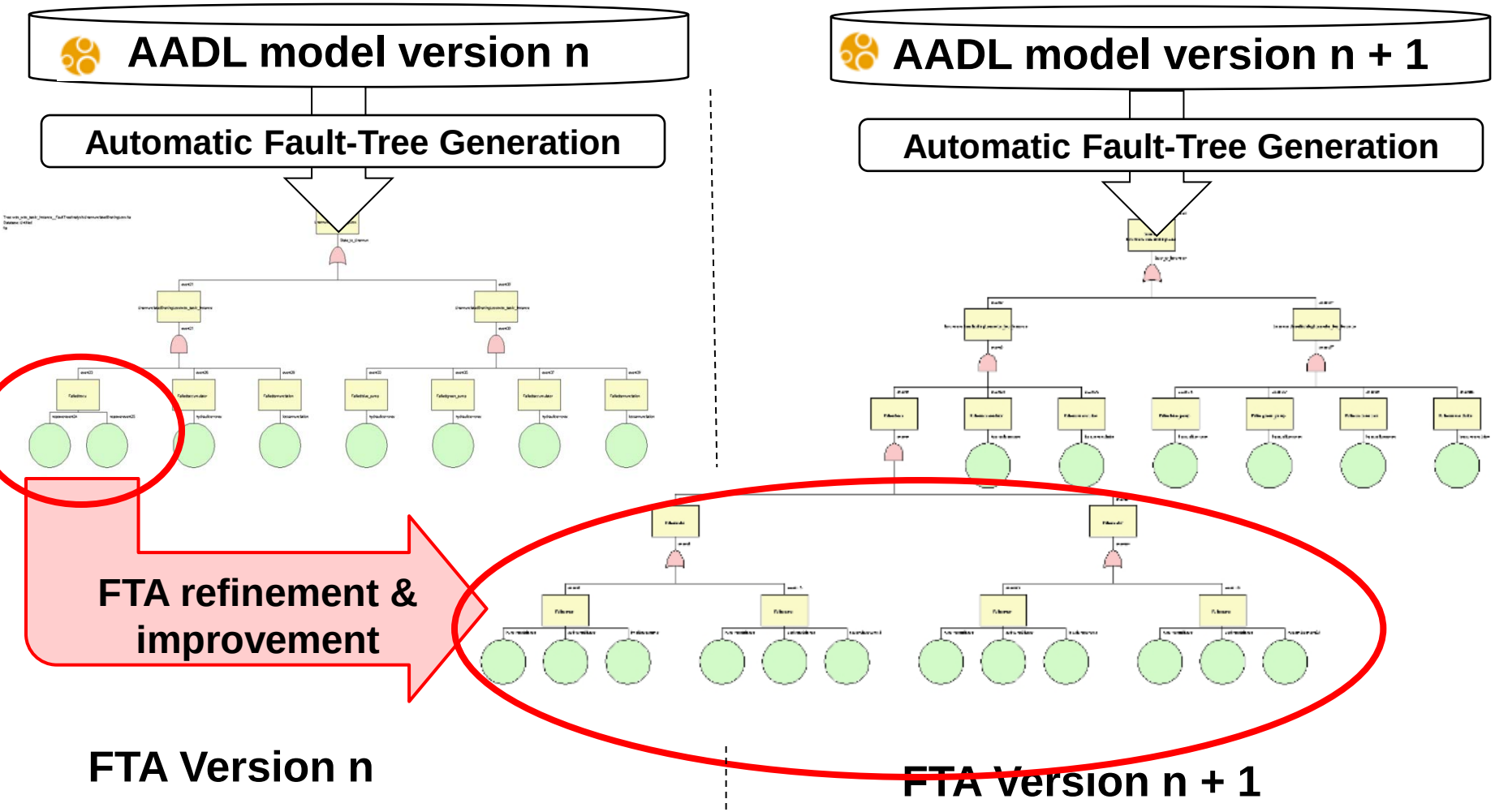
Component extension, refinement & implementation

AADL model Version n

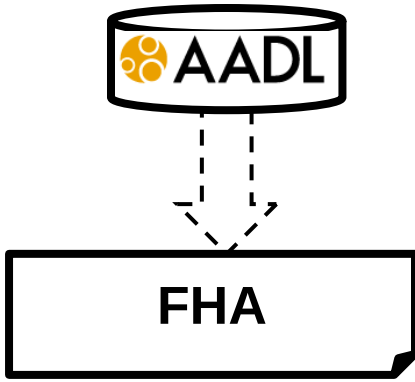
AADL model Version n + 1

Development Process

Evolution of Safety Assessment with AADL



Functional Hazard Analysis Support



Use of **component error behavior**

- Error propagations rules
- Internal error events

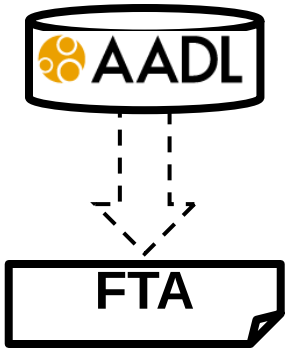
Specify initial failure mode

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

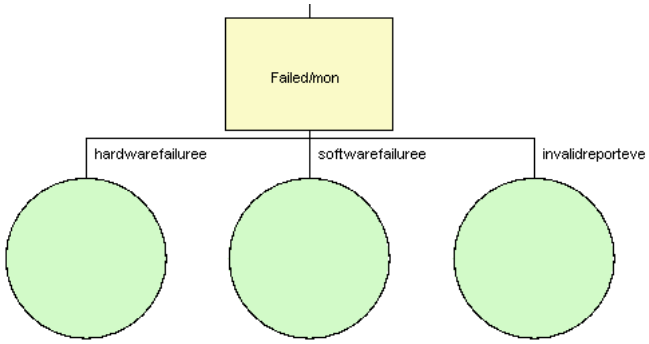
Use of **component error behavior**

Incoming error events

Walk through the components hierarchy

Generate the complete fault-tree

Focus on specific AADL subcomponents

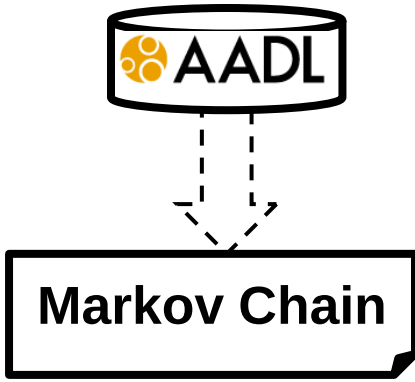


Export to several tools

Commercial: CAFTA

Open-Source: OpenFTA – http://www.openfta.com

Markov-Chain Support

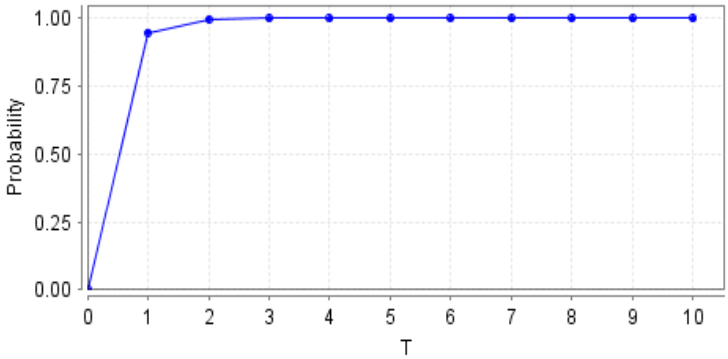


Use of **component error behavior**

- Error propagations rules
- Error transitions

Map states and error types into specific values

- Tool-specific approach

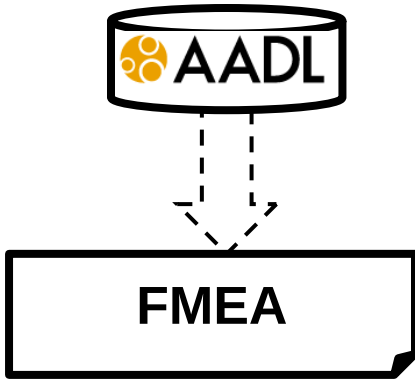


Ability to evaluate system state over time

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

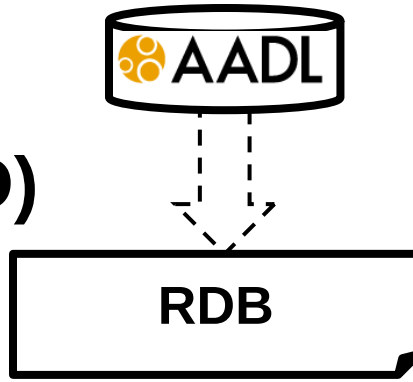
- Record impact over the components hierarchy

Use error description and related information

Create spreadsheet containing FHA elements

- To be reused by commercial or open-source tools

Reliability Block Diagram
aka ARP4761 Dependence Diagram (DD)



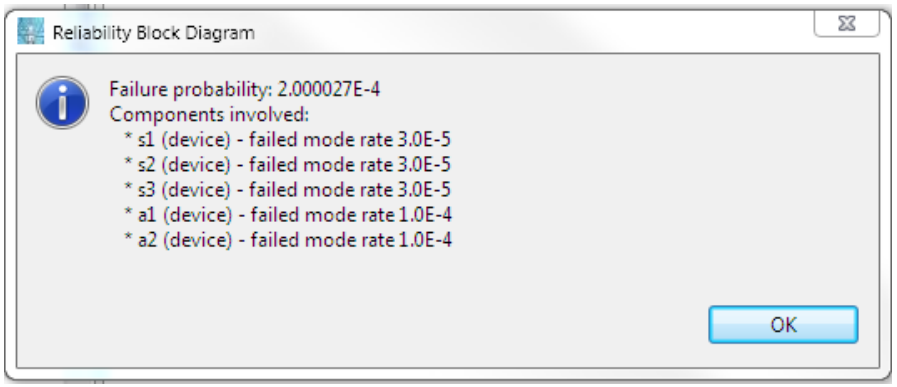
Use of **composite error behavior**

- Error propagations rules (source, sink, etc.)
- Internal error events

Compute reliability of the Dependence Diagram

- Use of recover and failure events
- Overall probability of system failure

Support in OSATE (built-in)



Agenda

Overview of AADL & Error-Model Annex

Approach for Safety Evaluation

Support of Safety Evaluation with AADL

Case-Study

On-Going Work

Discussion

Wheel Brake System

Development of a **public model**

Available on AADL public wiki

Use of core and additions of AADL

Error-Model (safety) + ARINC653 annexes (specific architecture)

Demonstration for the System Architecture Virtual Integration consortium

Relevance for the avionics domain

Apply the technology/toolset on a known example

Generation of FHA, FTA, MA & FMEA

AADL model root system

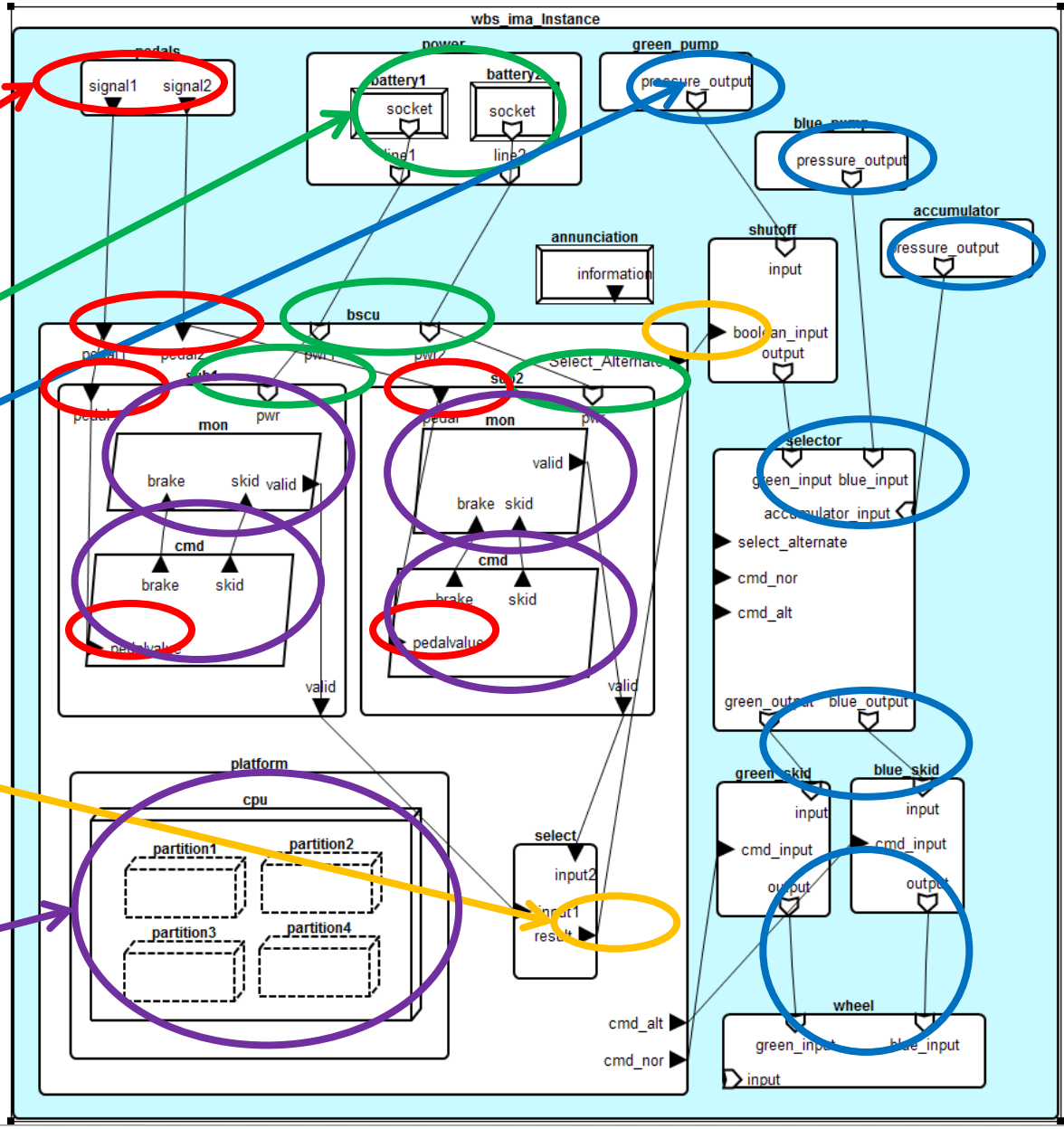
NoService

NoPower

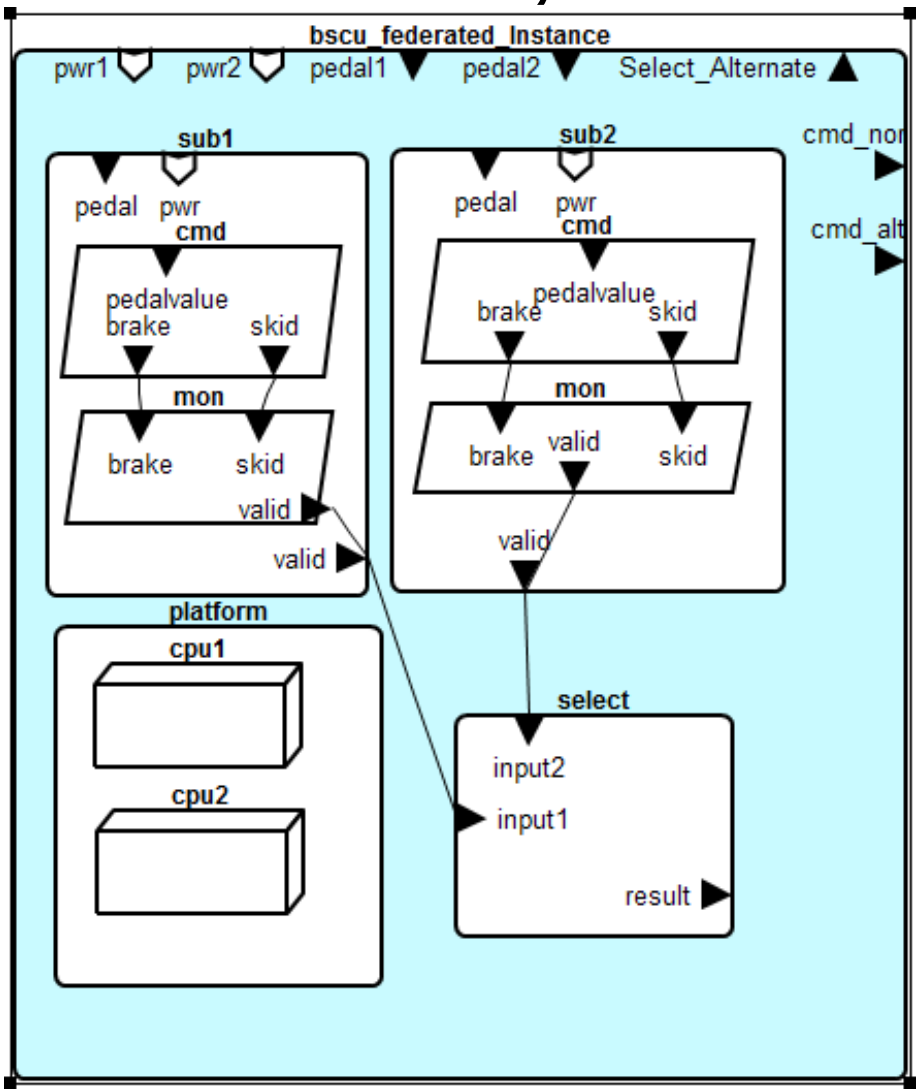
NoPressure

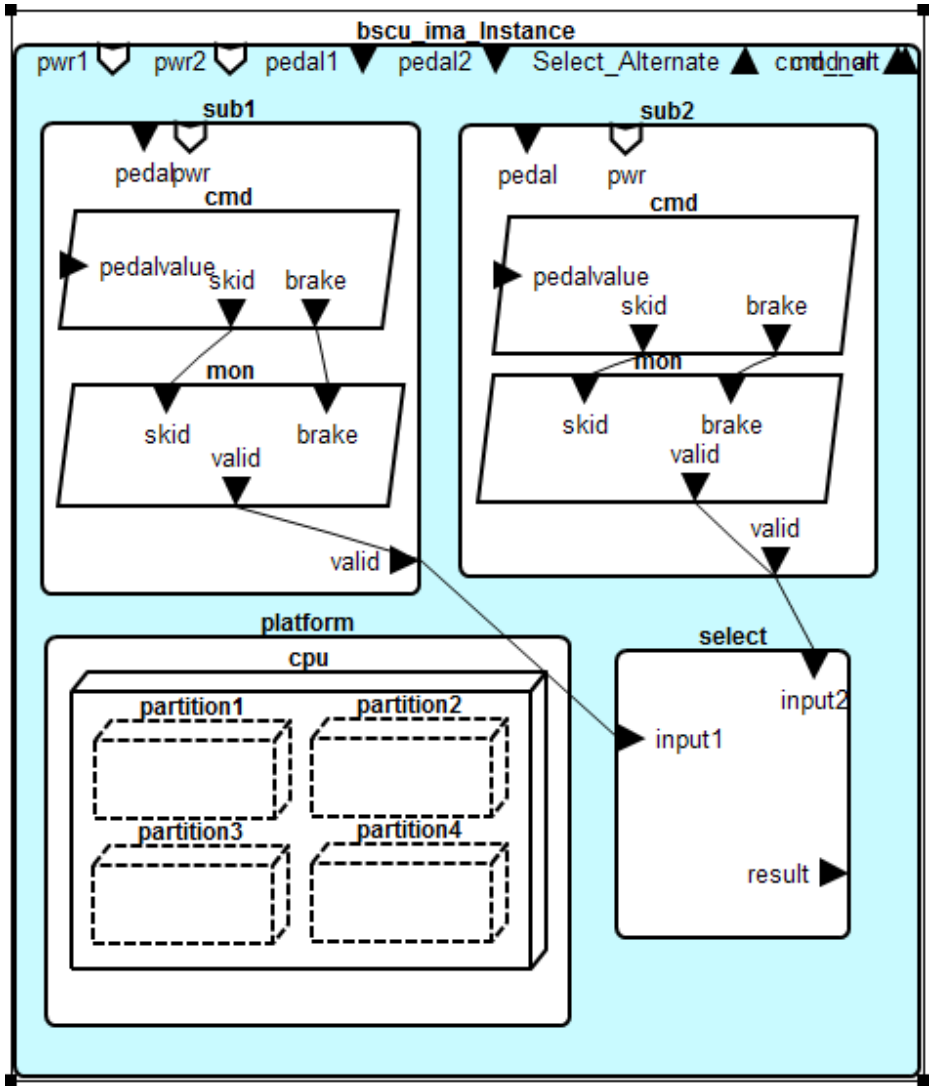
InvalidReport

Software and/or RuntimeError



AADL model, BSCU variations

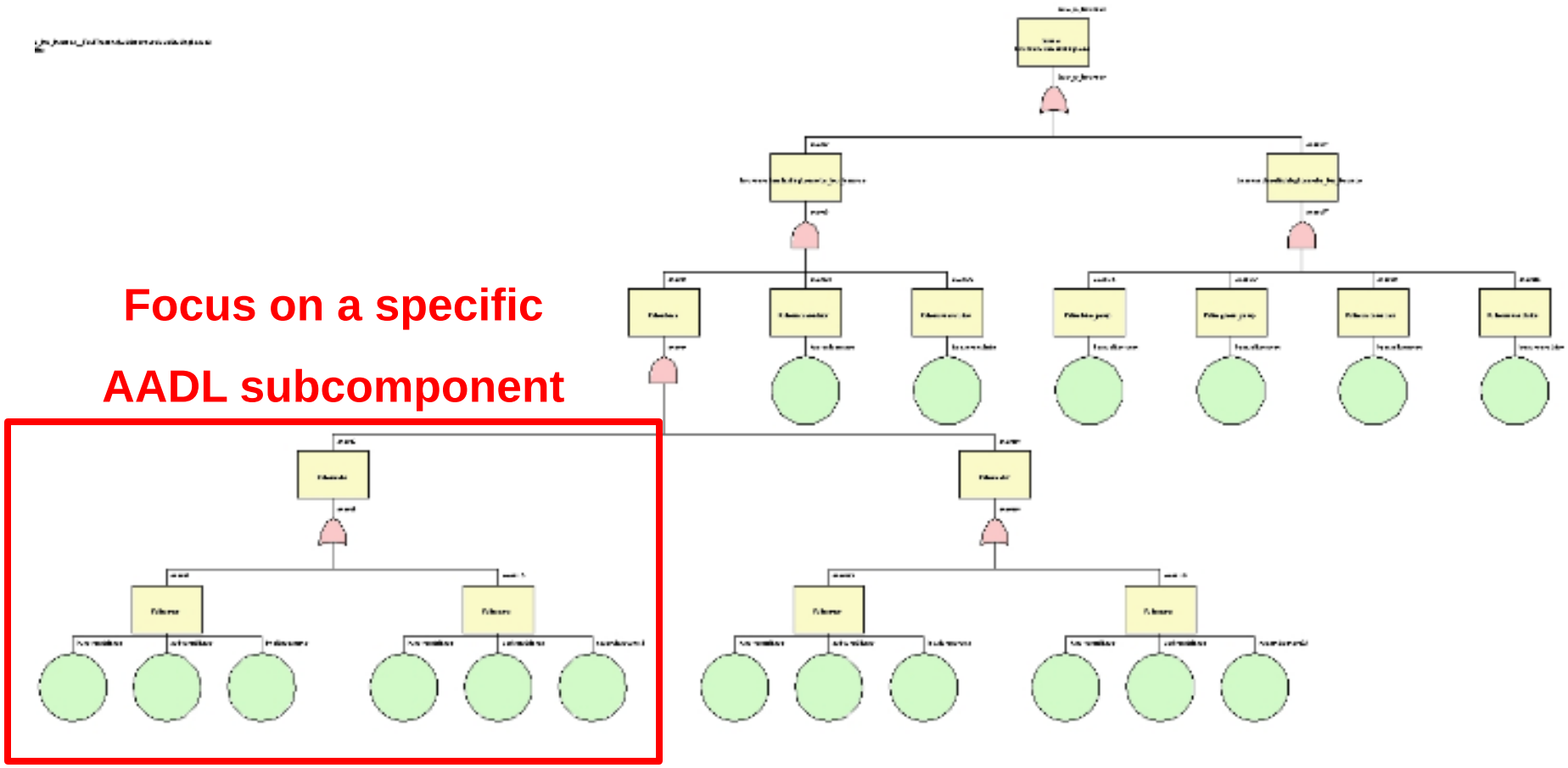




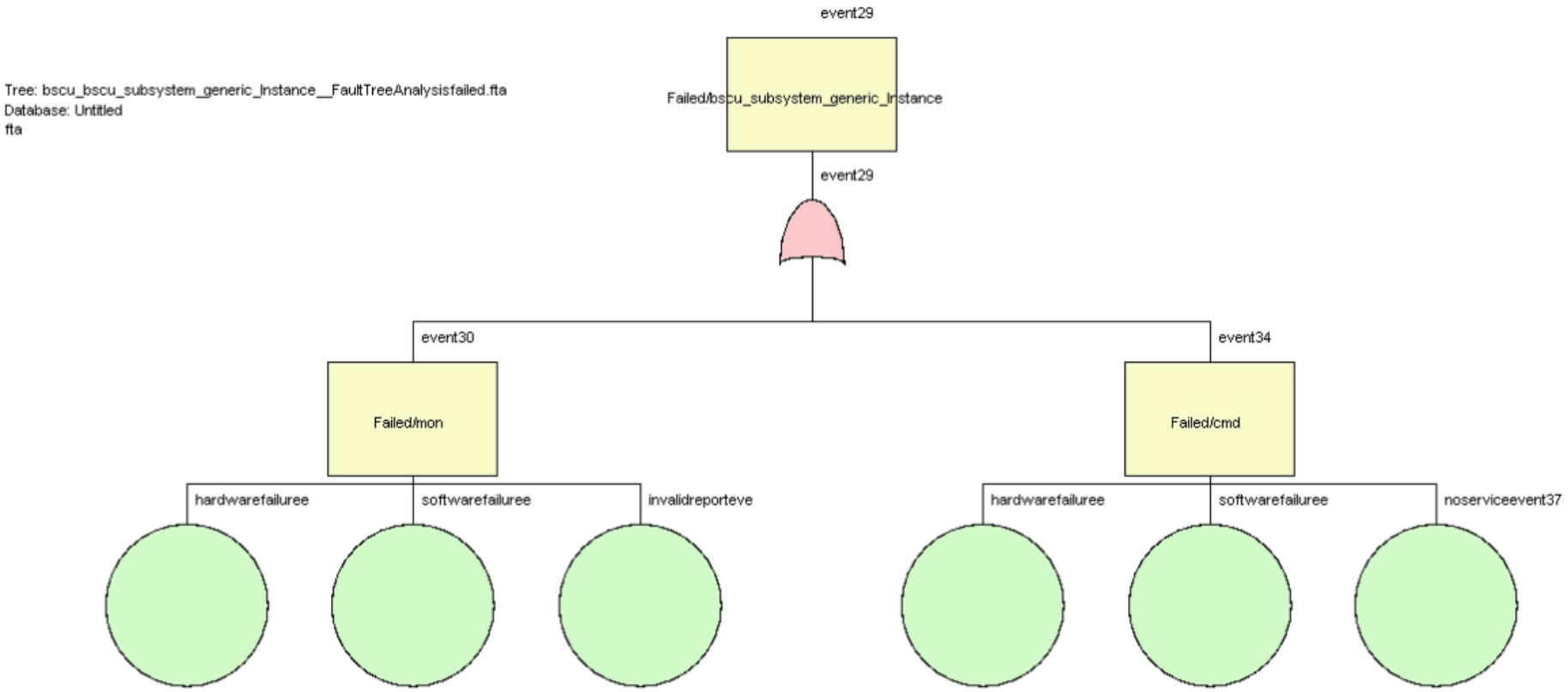
FHA of the root system

	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 E	all		Battery E	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 E	all		Battery E	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 root system

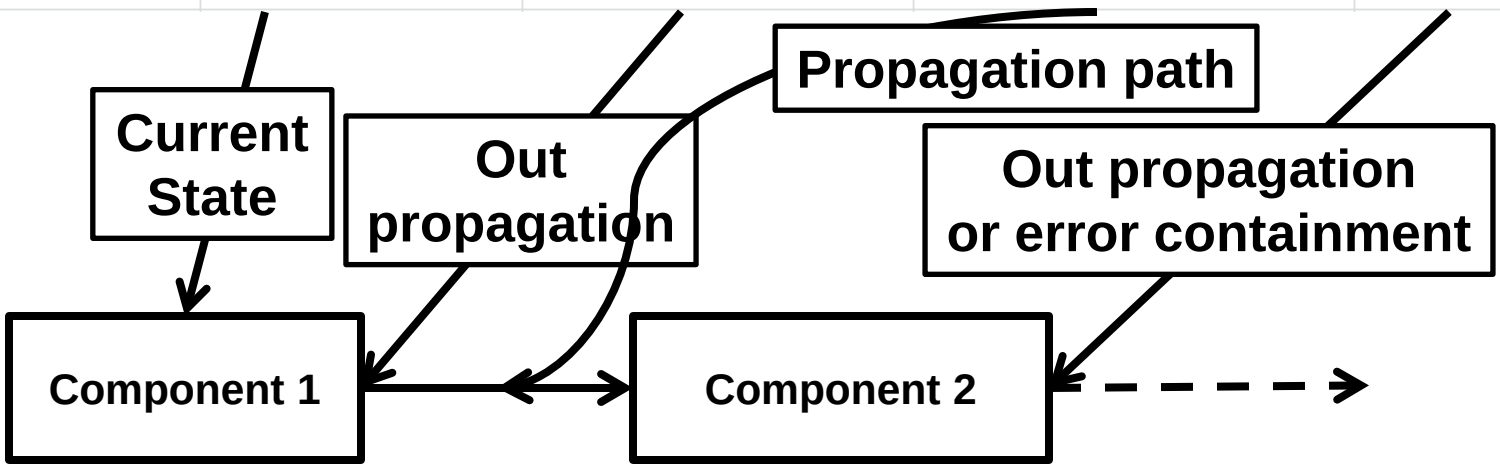


FTA of the BSCU subcomponent



FMEA of the root 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



Agenda

Overview of AADL & Error-Model Annex

Overview of ARP4761 & Safety Evaluation

Support of Safety Evaluation with AADL

Case-Study

Conclusion

Discussion

Conclusion

Facilitate Safety Evaluation

- Derives safety materials from existing assets
- Automate evaluation & check architecture consistency
- Improve evaluation reliability & robustness
- Support for incremental evaluation

Investigate interaction with other system characteristics

- Behavior specification

Agenda

Overview of AADL & Error-Model Annex

Approach for Safety Evaluation

Support of Safety Evaluation with AADL

Case-Study

Case-Study

Discussion

Contact

Presenter / Point of Contact

Dr. Julien Delange

Telephone: +1 412-268-9652

Email: jdelange@sei.cmu.edu

U.S. Mail

Software Engineering Institute

Customer Relations

4500 Fifth Avenue

Pittsburgh, PA 15213-2612

USA

Web

www.aadl.info

www.sei.cmu.edu

www.sei.cmu.edu/contact.cfm

Customer Relations

Email: info@sei.cmu.edu

Telephone: +1 412-268-5800

SEI Phone: +1 412-268-5800

SEI Fax: +1 412-268-6257