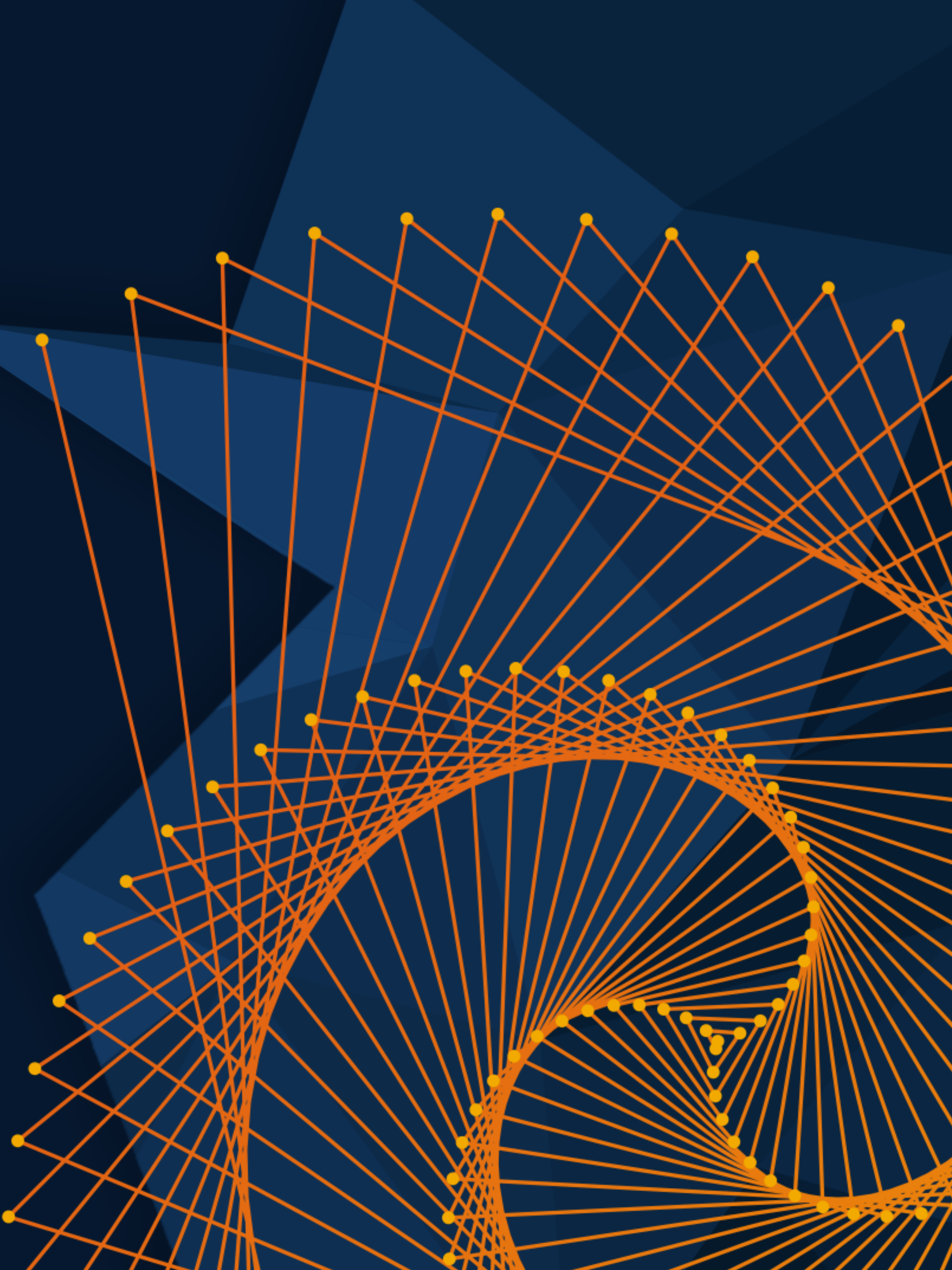
MATLAB EXPO
UNITED KINGDOM

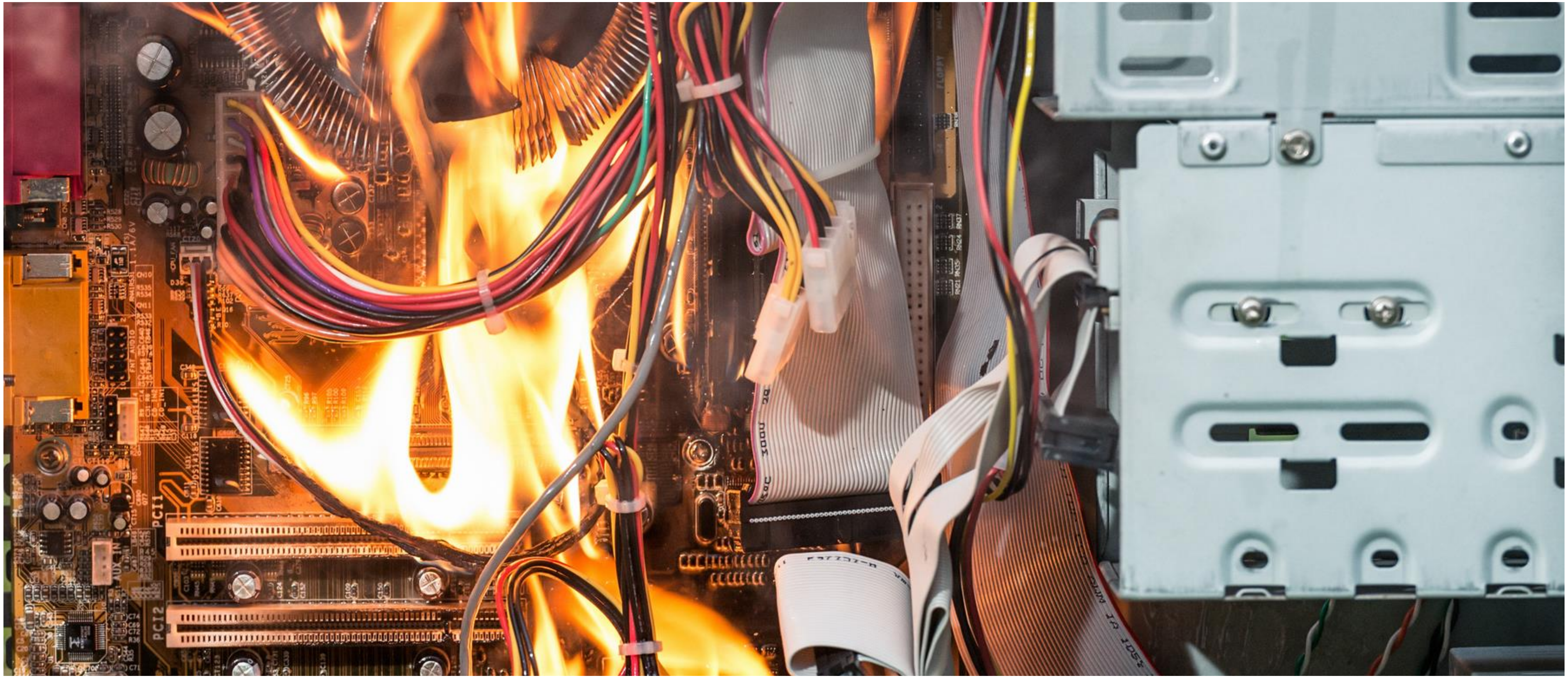
Simulation-Driven Safety Analysis through Fault Injection Testing

Fredrik Håbring, MathWorks

MathWorks®

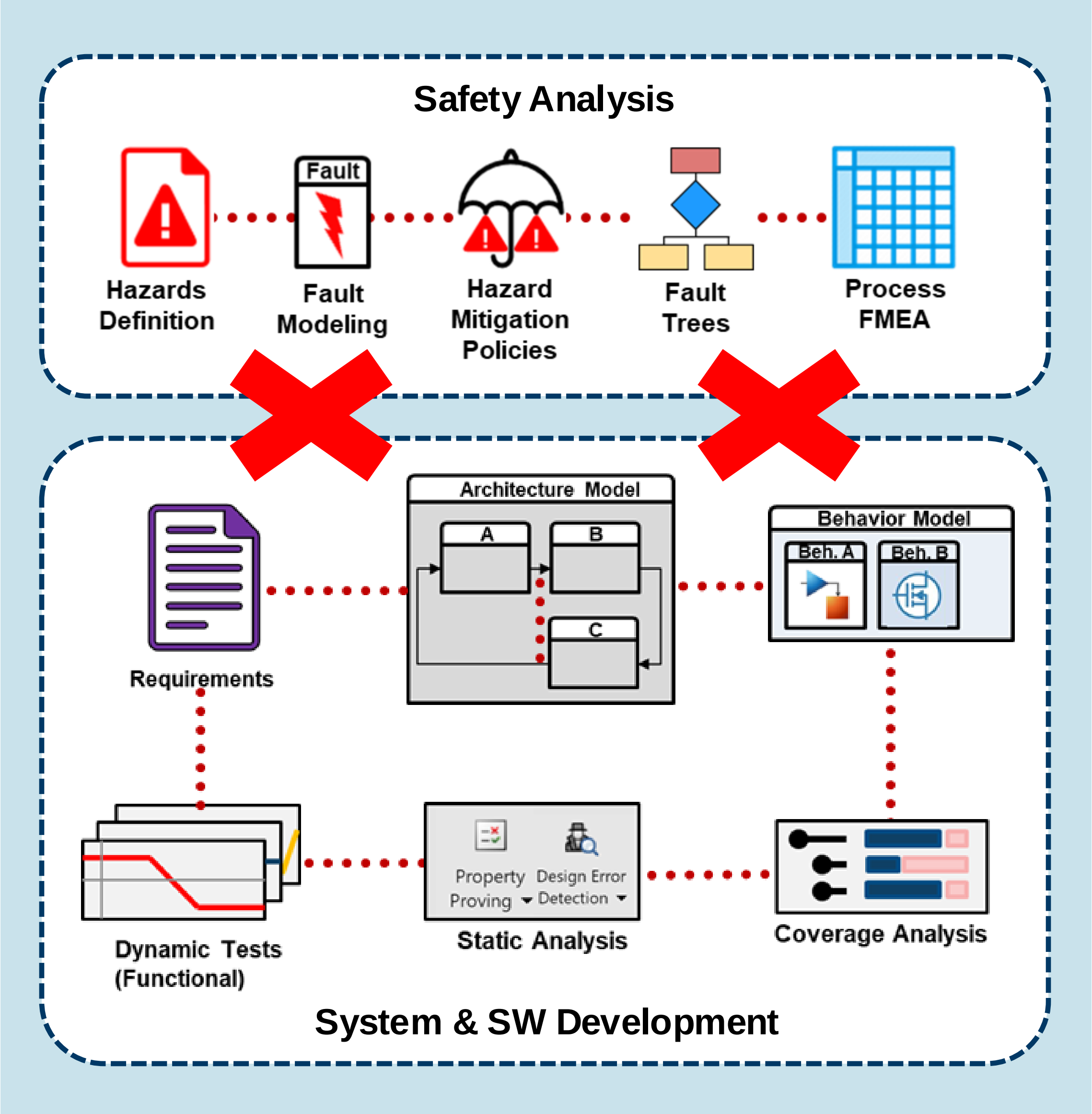


We need to verify that our developed system is safe and can handle faults in a safe way to not cause harm



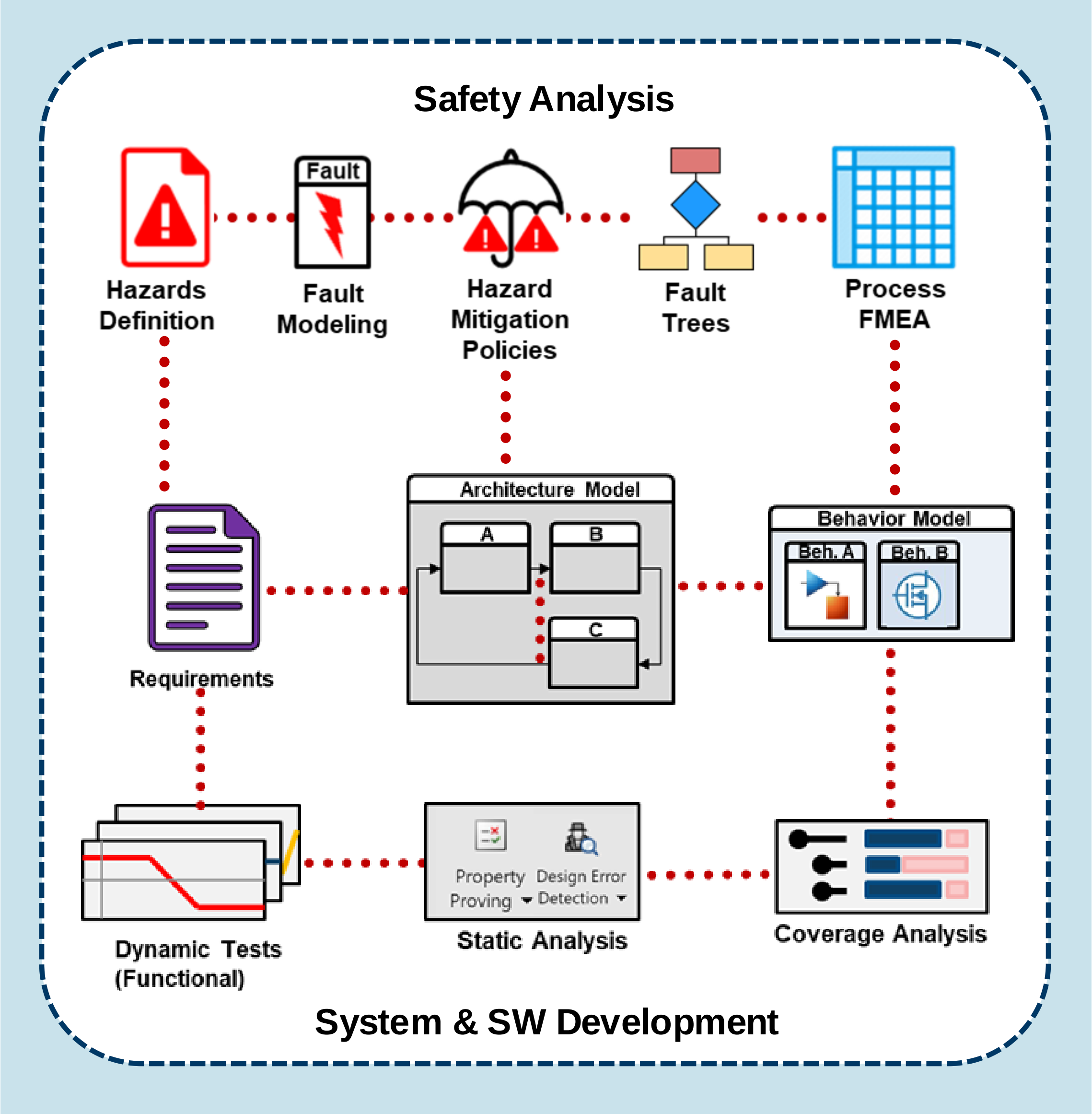
Key Takeaways

- **Traditional Safety Analysis is**
  - Decoupled from design work
  - Complex and complicated
  - Error-prone



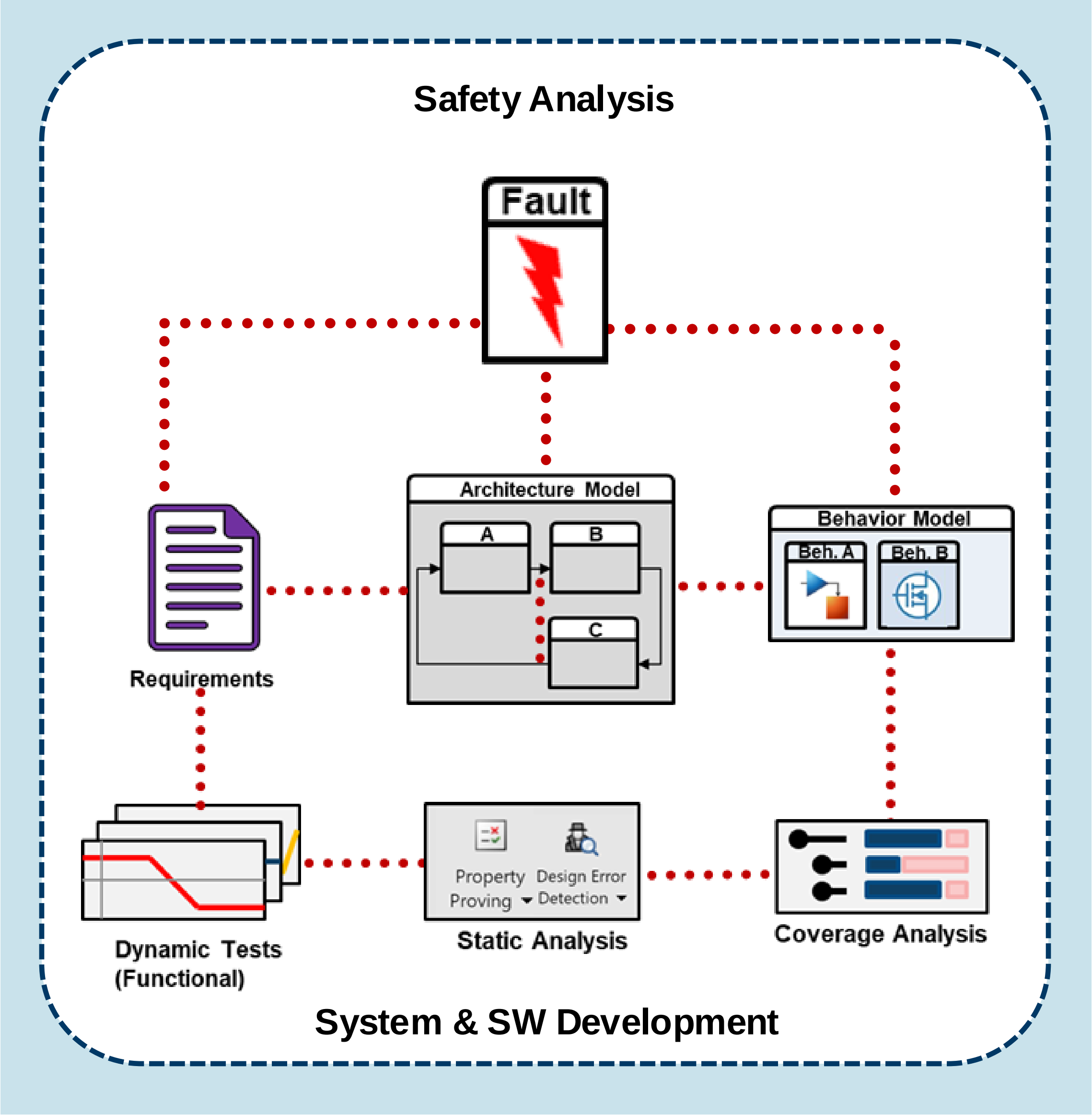
Key Takeaways

- **Model-Based Safety Analysis is**
  - **Fully integrated** with design
  - **Fully traceable** w.r.t. changes
  - **Consistent**
  - **Validated** by simulation

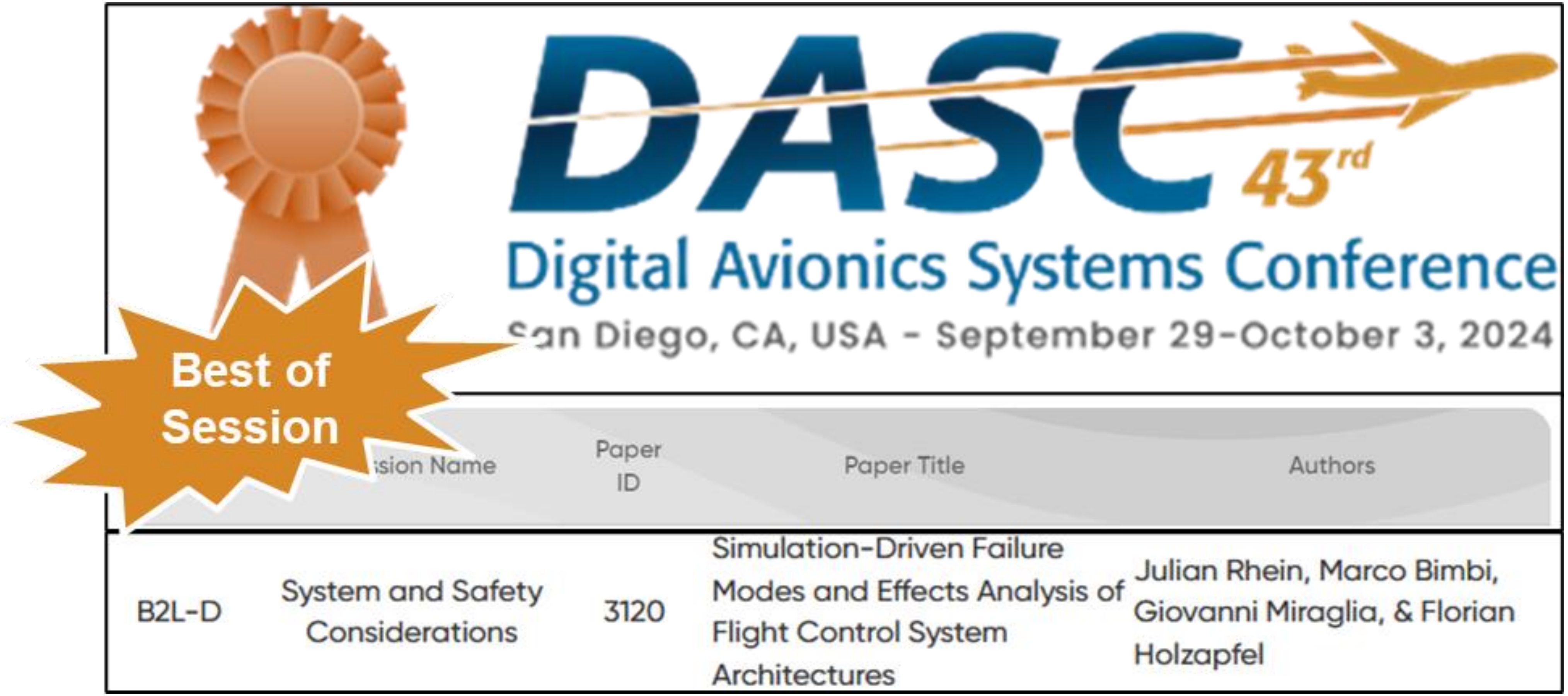


Key Takeaways

- **Enhanced Fault Modeling**
  - **Separated** from design
  - Supports **complex** faults
  - **Analyze** fault effects
  - **Connected** to hazards



MathWorks and TUM* won Best of Session award at DASC 2024 for implementing this workflow for an unmanned helicopter


DASC
43rd
Best of
Session

Digital Avionics Systems Conference

San Diego, CA, USA - September 29-October 3, 2024

	sion Name	Paper ID	Paper Title	Authors
B2L-D	System and Safety Considerations	3120	Simulation-Driven Failure Modes and Effects Analysis of Flight Control System Architectures	Julian Rhein, Marco Bimbi, Giovanni Miraglia, & Florian Holzapfel

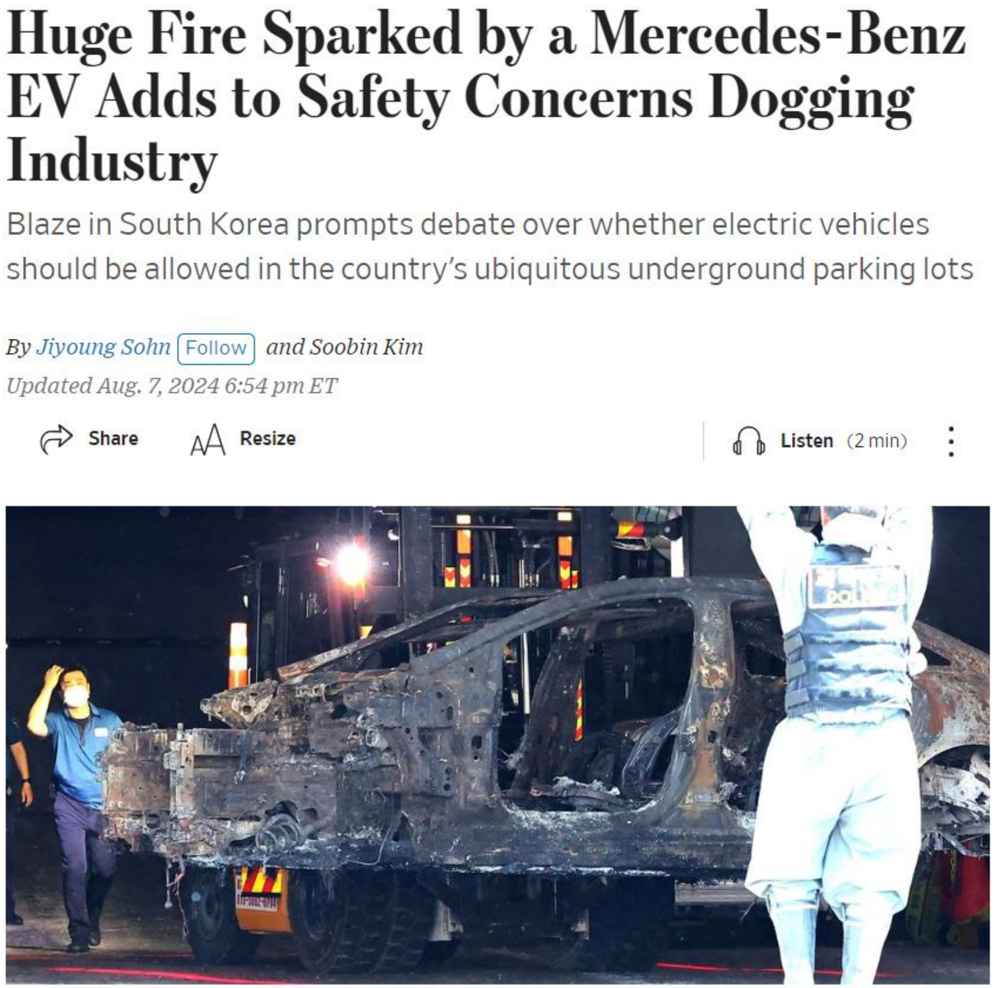
https://2024.dasconline.org/awards/best-paper-awards

*Technical University of Munich

Today’s Agenda

- Importance of safety in product development
- System: Model-based safety analysis workflow
- Component: Fault injection modeling
- Case Study: Aircraft fuel system
- Conclusion

Two recent examples of why safety analysis is paramount for engineered systems



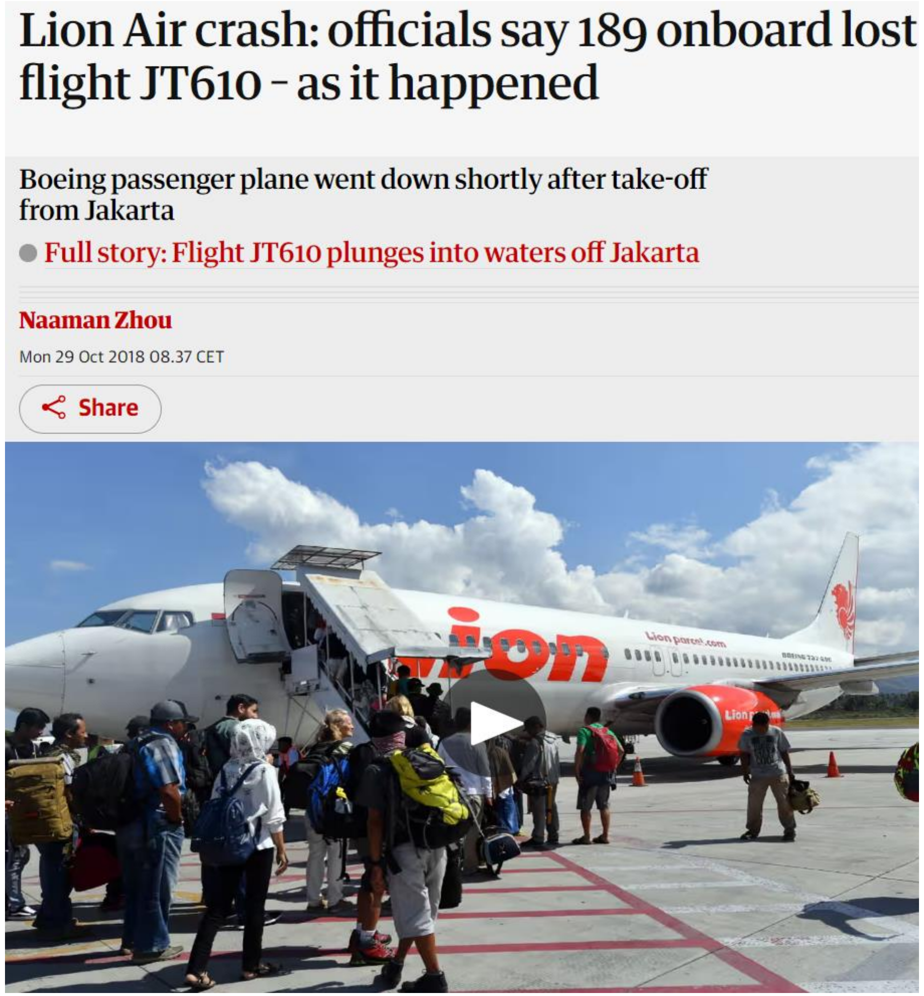
Huge Fire Sparked by a Mercedes-Benz EV Adds to Safety Concerns Dogging Industry

Blaze in South Korea prompts debate over whether electric vehicles should be allowed in the country's ubiquitous underground parking lots

By Jiyoung Sohn *and Soobin Kim*

Updated Aug. 7, 2024 6:54 pm ET

https://www.wsj.com/business/autos/huge-fire-sparked-by-a-mercedes-benz-ev-adds-to-safety-concerns-dogging-industry-8143d058



Lion Air crash: officials say 189 onboard lost flight JT610 – as it happened

Boeing passenger plane went down shortly after take-off from Jakarta

● Full story: Flight JT610 plunges into waters off Jakarta

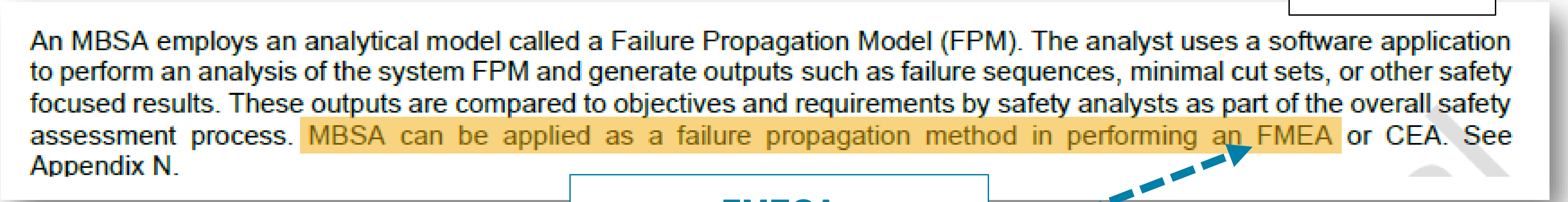
Naaman Zhou

Mon 29 Oct 2018 08.37 CET

https://www.theguardian.com/world/live/2018/oct/29/lion-air-crash-rescue-teams-search-waters-off-jakarta-for-flight-jt610

Functional safety standards recommends activities for system safety analysis: **aerospace example**

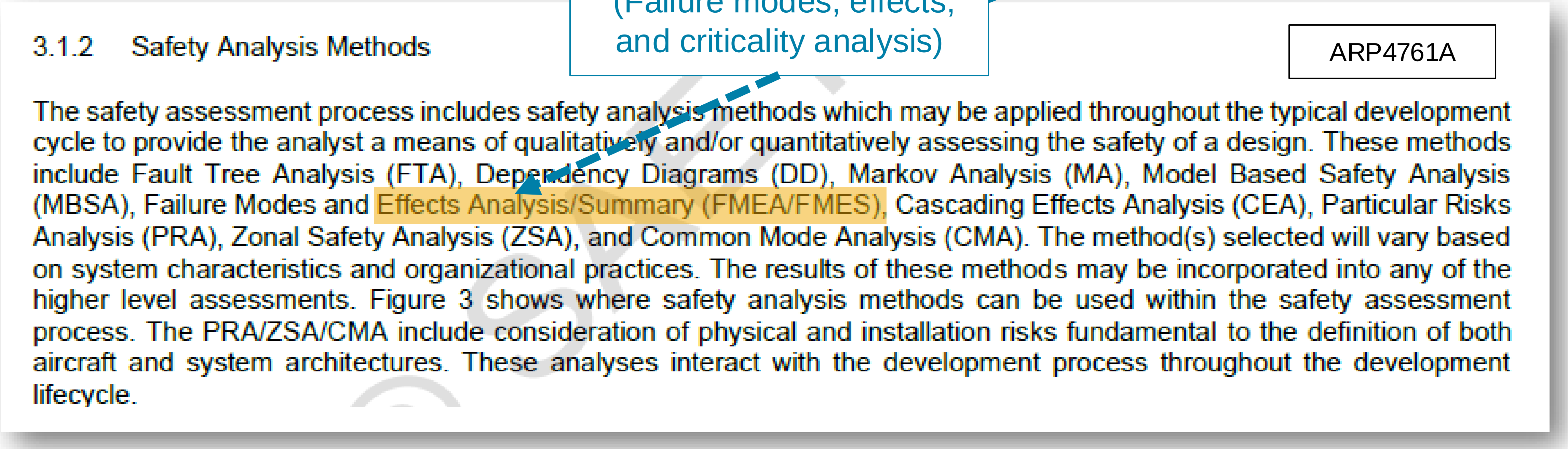
ARP4761A



An MBSA employs an analytical model called a Failure Propagation Model (FPM). The analyst uses a software application to perform an analysis of the system FPM and generate outputs such as failure sequences, minimal cut sets, or other safety focused results. These outputs are compared to objectives and requirements by safety analysts as part of the overall safety assessment process. MBSA can be applied as a failure propagation method in performing an FMEA or CEA. See Appendix N.

FMECA
(Failure modes, effects, and criticality analysis)

ARP4761A



3.1.2 Safety Analysis Methods

The safety assessment process includes safety analysis methods which may be applied throughout the typical development cycle to provide the analyst a means of qualitatively and/or quantitatively assessing the safety of a design. These methods include Fault Tree Analysis (FTA), Dependency Diagrams (DD), Markov Analysis (MA), Model Based Safety Analysis (MBSA), Failure Modes and Effects Analysis/Summary (FMEA/FMES), Cascading Effects Analysis (CEA), Particular Risks Analysis (PRA), Zonal Safety Analysis (ZSA), and Common Mode Analysis (CMA). The method(s) selected will vary based on system characteristics and organizational practices. The results of these methods may be incorporated into any of the higher level assessments. Figure 3 shows where safety analysis methods can be used within the safety assessment process. The PRA/ZSA/CMA include consideration of physical and installation risks fundamental to the definition of both aircraft and system architectures. These analyses interact with the development process throughout the development lifecycle.

Functional safety standards recommends activities for system safety analysis: **automotive example**

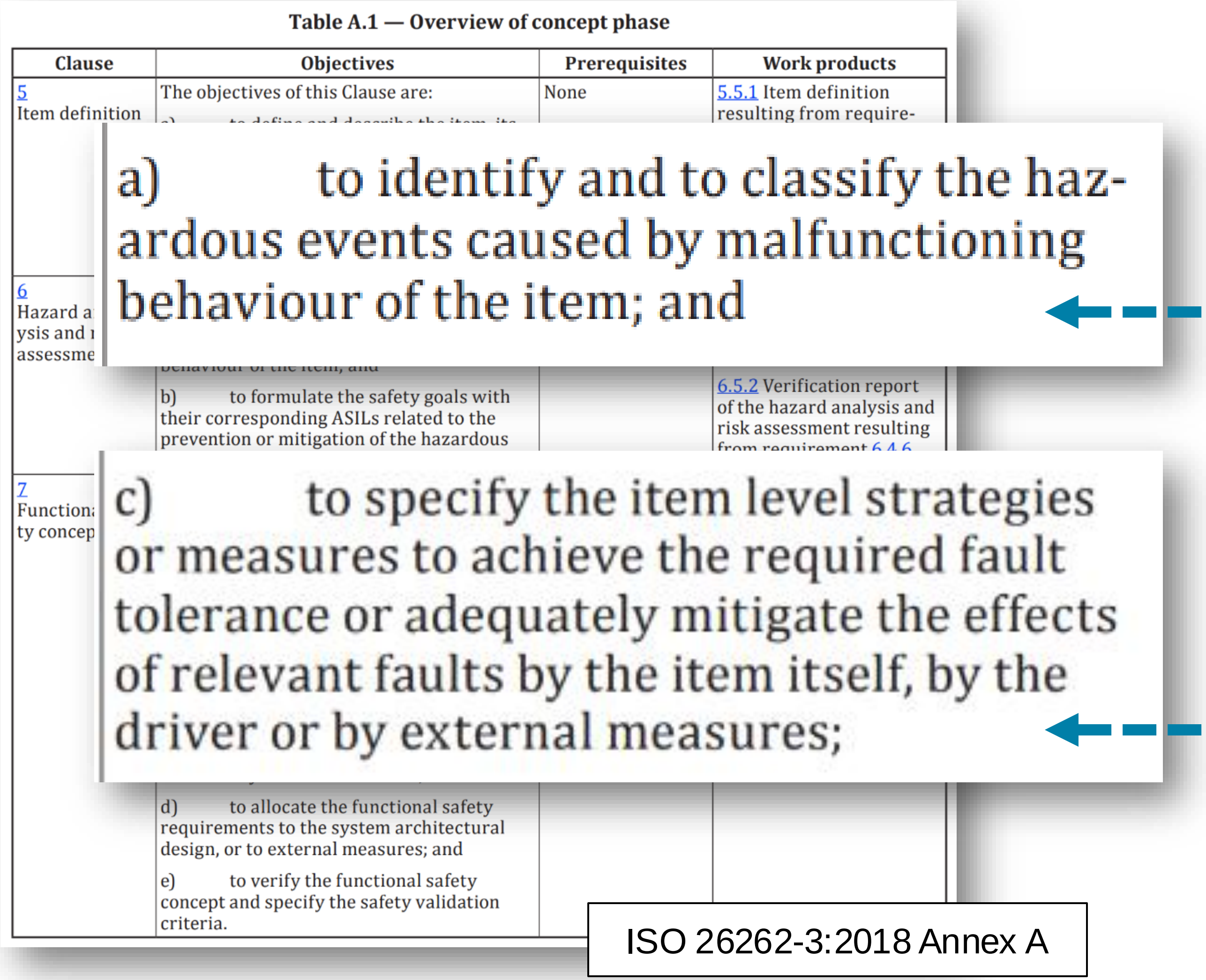


Table A.1 — Overview of concept phase

Clause	Objectives	Prerequisites	Work products
5 Item definition	The objectives of this Clause are: a) to define and describe the item, its	None	5.5.1 Item definition resulting from require-
6 Hazard a ysis and r assessme	behaviour of the item; and b) to formulate the safety goals with their corresponding ASILs related to the prevention or mitigation of the hazardous		6.5.2 Verification report of the hazard analysis and risk assessment resulting from requirement 6.4.6
7 Function ty concep	d) to allocate the functional safety requirements to the system architectural design, or to external measures; and e) to verify the functional safety concept and specify the safety validation criteria.		

a) to identify and to classify the hazardous events caused by malfunctioning behaviour of the item; and

c) to specify the item level strategies or measures to achieve the required fault tolerance or adequately mitigate the effects of relevant faults by the item itself, by the driver or by external measures;

ISO 26262-3:2018 Annex A

Hazard Assessment

FMECA
(Failure modes, effects, and criticality analysis)

Functional safety standards recommends activities for system safety analysis: **automotive example**

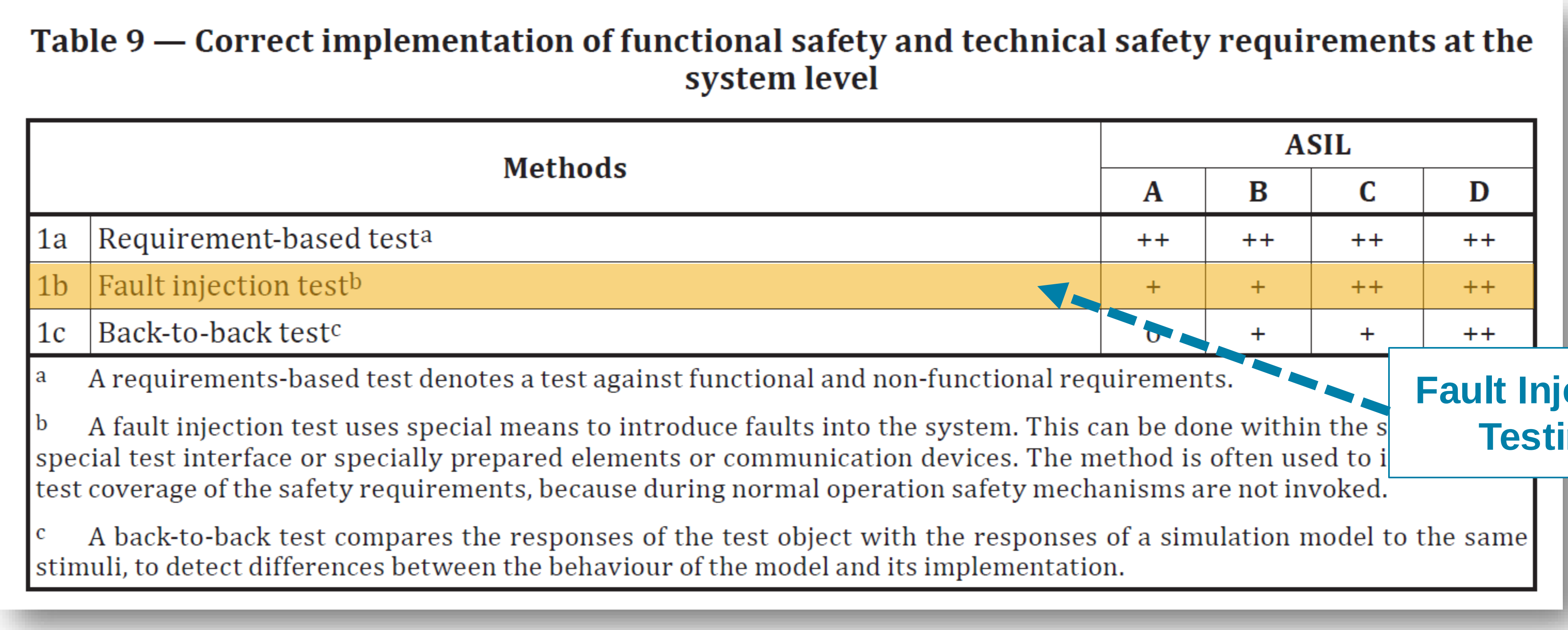


Table 9 — Correct implementation of functional safety and technical safety requirements at the system level

Methods		ASIL			
		A	B	C	D
1a	Requirement-based test[a]	++	++	++	++
1b	Fault injection test[b]	+	+	++	++
1c	Back-to-back test[c]	o	+	+	++

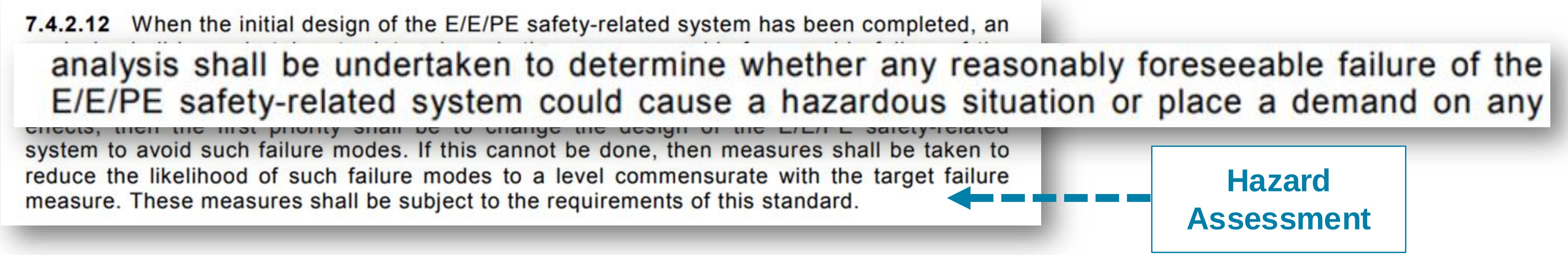
[a] A requirements-based test denotes a test against functional and non-functional requirements.

[b] A fault injection test uses special means to introduce faults into the system. This can be done within the s special test interface or specially prepared elements or communication devices. The method is often used to i test coverage of the safety requirements, because during normal operation safety mechanisms are not invoked.

[c] A back-to-back test compares the responses of the test object with the responses of a simulation model to the same stimuli, to detect differences between the behaviour of the model and its implementation.

Fault Injection Testing

Functional safety standards recommends activities for system safety analysis: **industrial example**

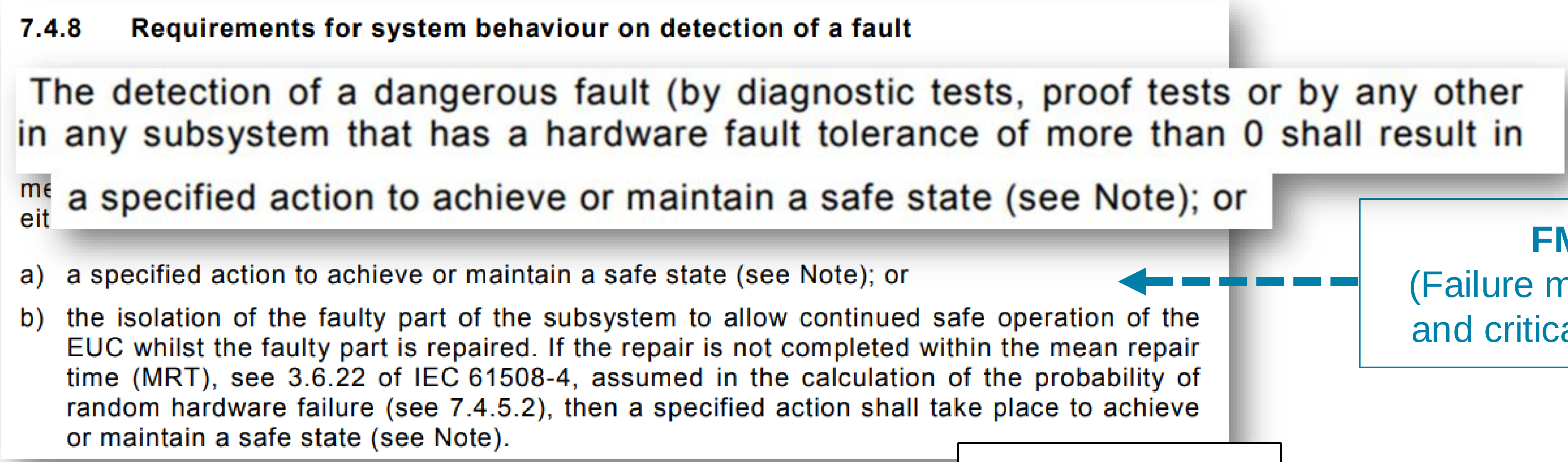


7.4.2.12 When the initial design of the E/E/PE safety-related system has been completed, an

analysis shall be undertaken to determine whether any reasonably foreseeable failure of the E/E/PE safety-related system could cause a hazardous situation or place a demand on any

effects, then the first priority shall be to change the design of the E/E/PE safety-related system to avoid such failure modes. If this cannot be done, then measures shall be taken to reduce the likelihood of such failure modes to a level commensurate with the target failure measure. These measures shall be subject to the requirements of this standard.

Hazard Assessment



7.4.8 Requirements for system behaviour on detection of a fault

The detection of a dangerous fault (by diagnostic tests, proof tests or by any other in any subsystem that has a hardware fault tolerance of more than 0 shall result in

me
eit

a specified action to achieve or maintain a safe state (see Note); or

a) a specified action to achieve or maintain a safe state (see Note); or

b) the isolation of the faulty part of the subsystem to allow continued safe operation of the EUC whilst the faulty part is repaired. If the repair is not completed within the mean repair time (MRT), see 3.6.22 of IEC 61508-4, assumed in the calculation of the probability of random hardware failure (see 7.4.5.2), then a specified action shall take place to achieve or maintain a safe state (see Note).

FMECA
(Failure modes, effects, and criticality analysis)

IEC 61508-2:2010

Functional safety standards recommends activities for system safety analysis: **industrial example**

IEC 61508-2:2010

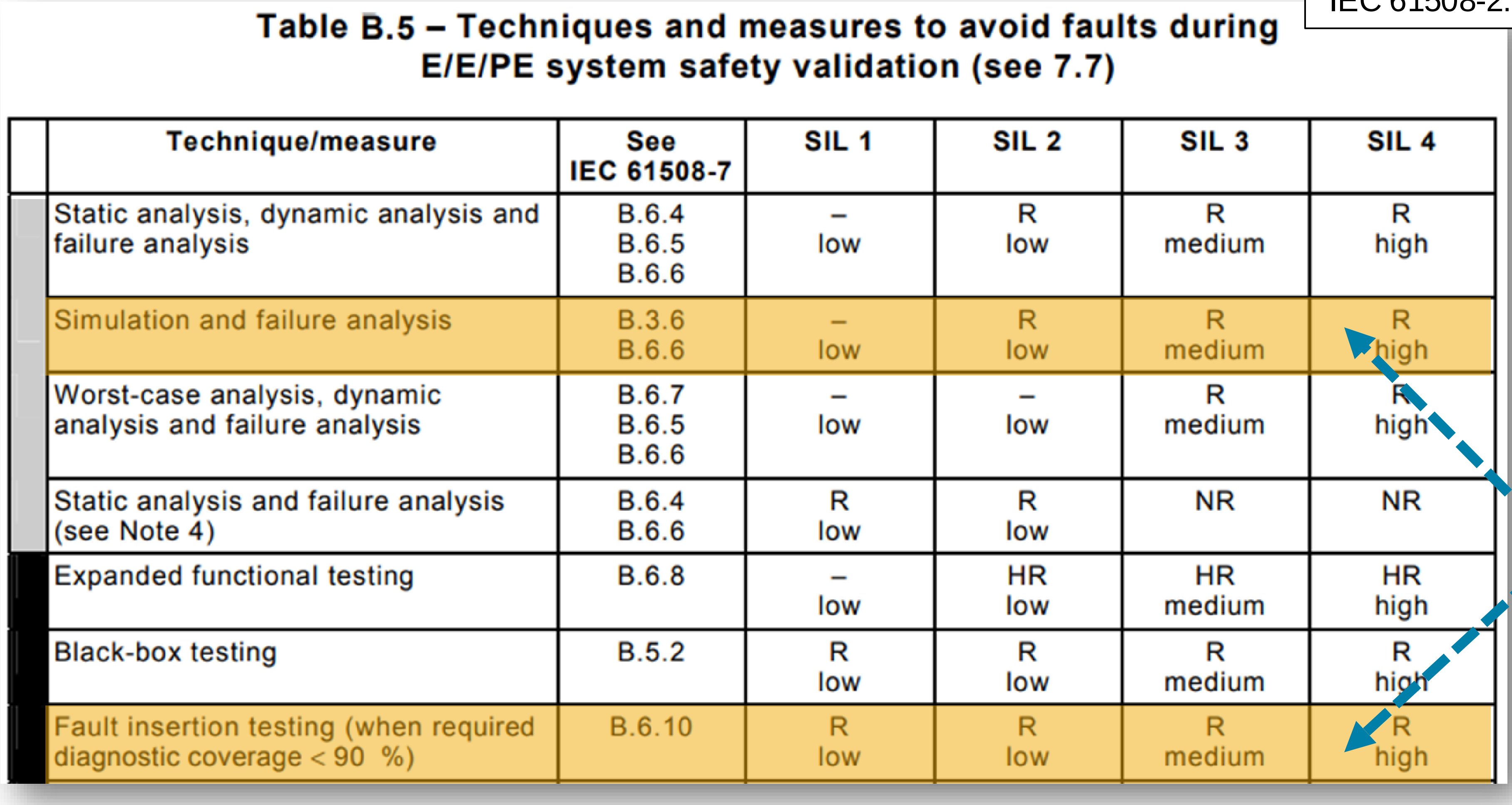
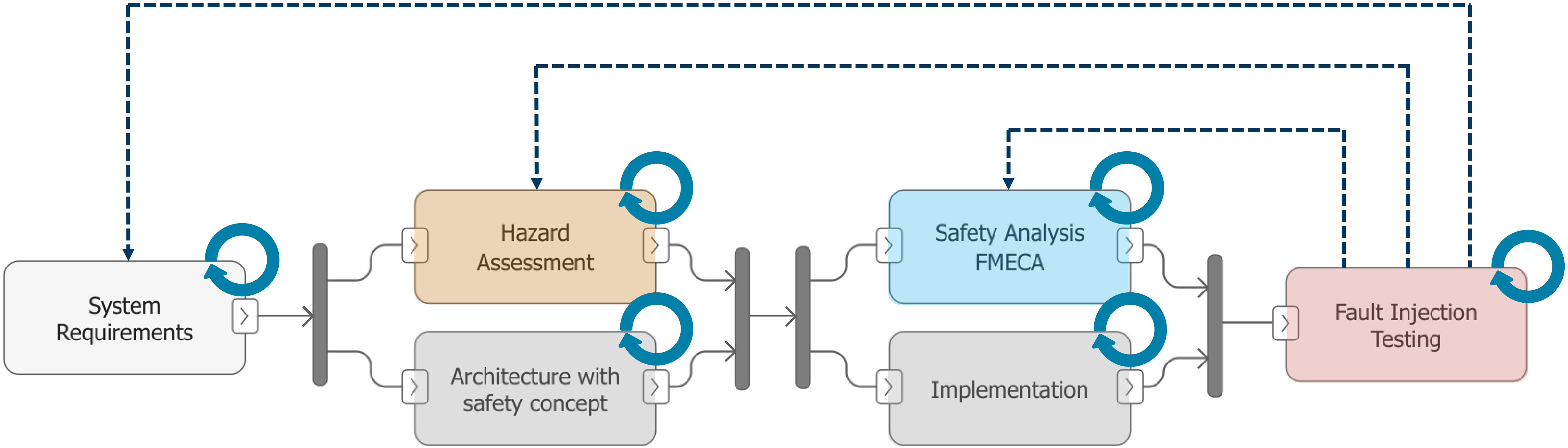


Table B.5 – Techniques and measures to avoid faults during E/E/PE system safety validation (see 7.7)

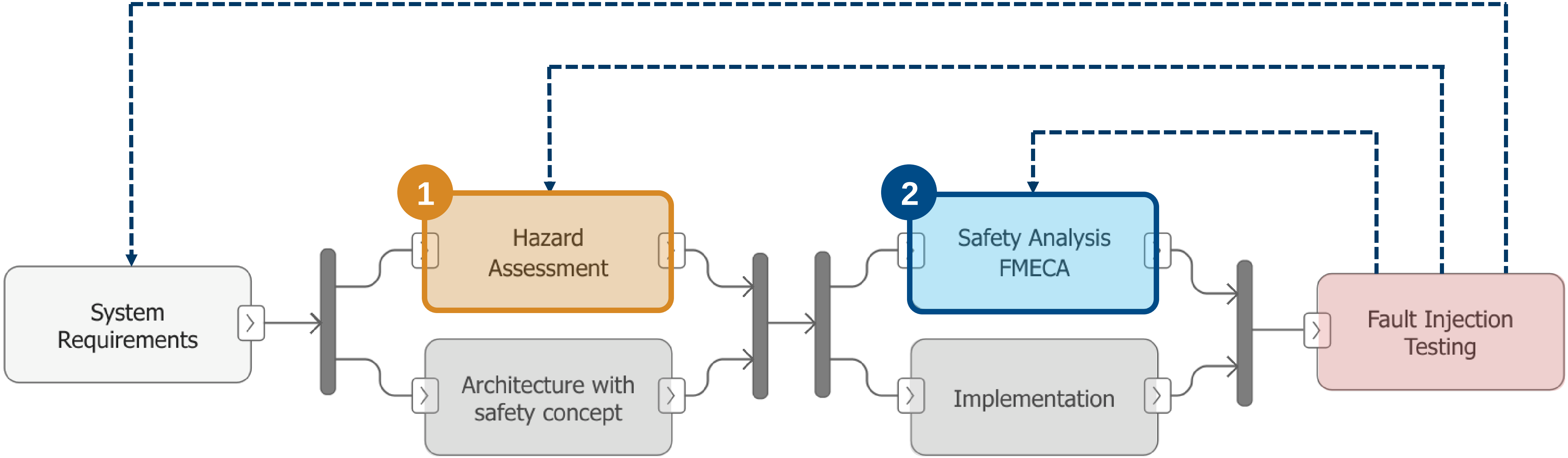
	Technique/measure	See IEC 61508-7	SIL 1	SIL 2	SIL 3	SIL 4
	Static analysis, dynamic analysis and failure analysis	B.6.4 B.6.5 B.6.6	– low	R low	R medium	R high
	Simulation and failure analysis	B.3.6 B.6.6	– low	R low	R medium	R high
	Worst-case analysis, dynamic analysis and failure analysis	B.6.7 B.6.5 B.6.6	– low	– low	R medium	R high
	Static analysis and failure analysis (see Note 4)	B.6.4 B.6.6	R low	R low	NR	NR
	Expanded functional testing	B.6.8	– low	HR low	HR medium	HR high
	Black-box testing	B.5.2	R low	R low	R medium	R high
	Fault insertion testing (when required diagnostic coverage < 90 %)	B.6.10	R low	R low	R medium	R high

Fault Injection Testing

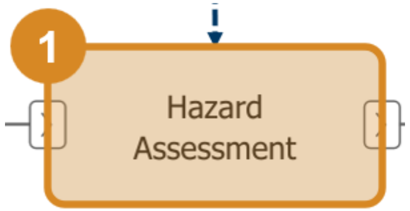
Safety analysis is a highly **iterative** workflow involving detection, mitigation, and verification



Safety analysis is a highly **iterative** workflow involving detection, mitigation, and verification



Let’s make an example of a Hazard Assessment
Electric Car Battery



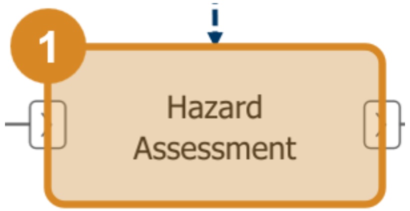
Thermal Runaway

- **Description**: Uncontrolled increase in temperature within the battery cells.
- **Potential Consequences**: Fire, explosion, damage to the vehicle, injury to occupants.
- **Severity**: High
- **Likelihood**: Medium
- **Risk Level**: High

Overcharging

- **Description**: Battery cells receive more charge than their maximum capacity.
- **Potential Consequences**: Degradation of battery life, thermal runaway, fire.
- **Severity**: Medium
- **Likelihood**: Medium
- **Risk Level**: Medium

Let’s make an example of a Hazard Assessment
Electric Car Battery

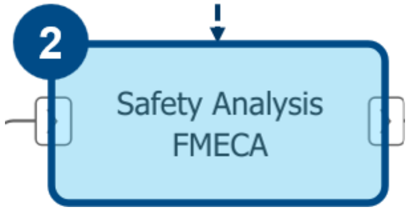


Hazard	Description	Potential Consequences	Severity	Likelihood	Risk Level	Mitigation Measures
Thermal Runaway	Uncontrolled increase in temperature within battery cells	Fire, explosion, damage to vehicle, injury to occupants	High	Medium	High	Advanced thermal management system, redundant temperature sensors
Overcharging	Battery cells receive more charge than their maximum capacity	Degradation of battery life, thermal runaway, fire	Medium	Medium	Medium	Battery Management System (BMS), overcharge protection circuits

Let’s make an example of a Hazard Assessment
Electric Car Battery

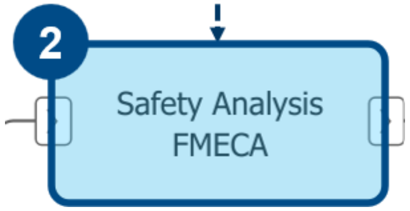
Hazard	Description	Potential Consequences	Severity	Likelihood	Risk Level	Mitigation Measures
Thermal Runaway	Uncontrolled increase in temperature within battery cells	Fire, explosion, damage to vehicle, injury to occupants	High	Medium	High	Advanced thermal management system, redundant temperature sensors
Overcharging	Battery cells receive more charge than their maximum capacity	Degradation of battery life, thermal runaway, fire	Medium	Medium	Medium	Battery Management System (BMS), overcharge protection circuits
Short Circuit	Electrical short circuit within battery pack or connections	Loss of power, thermal runaway, fire	High	Low	Medium	Insulation, circuit breakers, regular maintenance
Mechanical Damage	Physical damage to battery pack due to impact or vibration	Short circuit, thermal runaway, fire, reduced battery performance	High	Medium	High	Robust battery enclosure, impact sensors
Overheating During Charging	Excessive heat generated during the charging process	Thermal runaway, fire, reduced battery lifespan	High	Low	Medium	Advanced thermal management system, pressure sensor for coolant leakage detection
Software Malfunction	Failure of battery management system (BMS) software	Incorrect battery monitoring and control, overcharging, deep discharging, thermal runaway	High	Low	Medium	Software validation, redundancy in control system

Failure modes, effects, and criticality analysis (FMECA)
Electric Car Battery



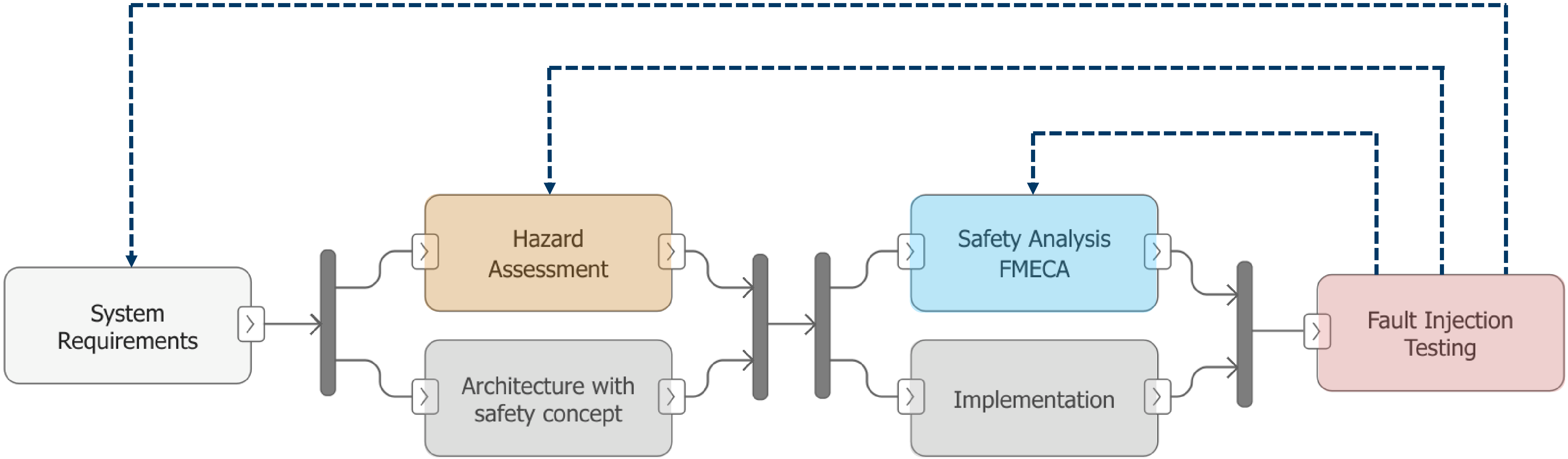
Component	Potential Failure Mode	Potential Effect(s)	Severity (S)	Potential Cause(s)	Occurrence (O)	Current Control(s)	Detection (D)	Risk Priority Number
Cooling Medium	Leakage	Loss of cooling efficiency, overheating	8	Puncture, poor sealing	3	Regular maintenance, robust design	3	72
	Contamination	Reduced heat transfer efficiency	6	Impurities in coolant	2	Filtration system	3	36

Failure modes, effects, and criticality analysis (FMECA)
Electric Car Battery

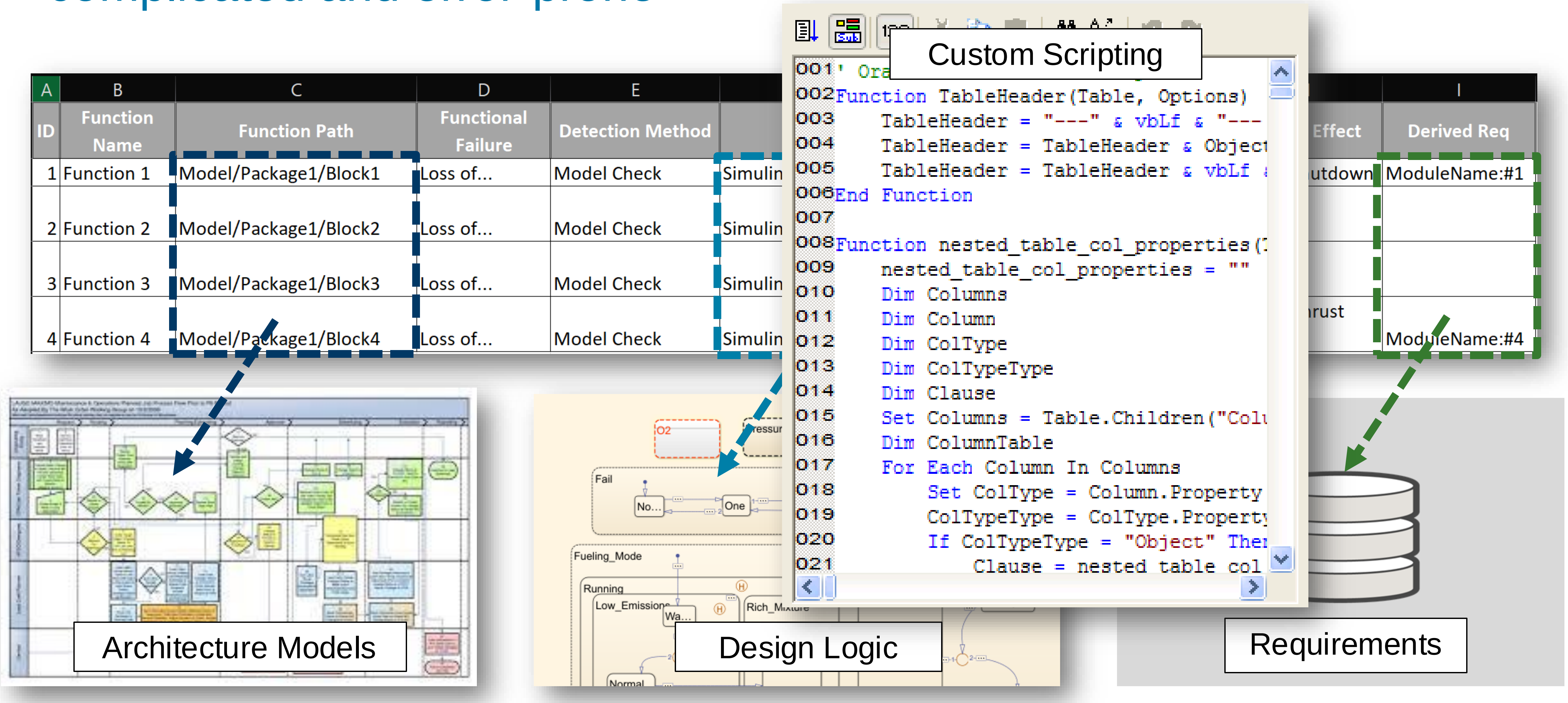


Component	Potential Failure Mode	Potential Effect(s)	Severity (S)	Potential Cause(s)	Occurrence (O)	Current Control(s)	Detection (D)	Risk Priority Number
Cooling Medium	Leakage	Loss of cooling efficiency, overheating	8	Puncture, poor sealing	3	Regular maintenance, robust design	3	72
	Contamination	Reduced heat transfer efficiency	6	Impurities in coolant	2	Filtration system	3	36
Heat Exchanger	Blockage	Reduced cooling efficiency, overheating	8	Debris, corrosion	2	Regular inspection and cleaning	3	48
	Corrosion	Leakage, reduced heat transfer	7	Poor material quality, harsh environment	3	Use of corrosion-resistant materials	4	84
Coolant Pump	Mechanical Failure	Loss of coolant flow, overheating	9	Wear and tear, motor failure	3	Regular maintenance, quality components	3	81
	Electrical Failure	Pump stops working, overheating	9	Electrical faults	2	Electrical system checks	3	54
Control Unit	Software Malfunction	Incorrect system operation, overheating	9	Software bugs, control logic errors	2	Software validation, redundancy	3	54
	Hardware Failure	System stops working, overheating	9	Component failure	2	Quality control, redundancy	3	54

Safety analysis is a highly **iterative** workflow involving detection, mitigation, and verification



Traditional safety analysis is decoupled from design, complex, complicated and error-prone



A	B	C	D	E			I
ID	Function Name	Function Path	Functional Failure	Detection Method		Effect	Derived Req
1	Function 1	Model/Package1/Block1	Loss of...	Model Check	Simulin	utdown	ModuleName:#1
2	Function 2	Model/Package1/Block2	Loss of...	Model Check	Simulin		
3	Function 3	Model/Package1/Block3	Loss of...	Model Check	Simulin		
4	Function 4	Model/Package1/Block4	Loss of...	Model Check	Simulin	rust	ModuleName:#4

Custom Scripting

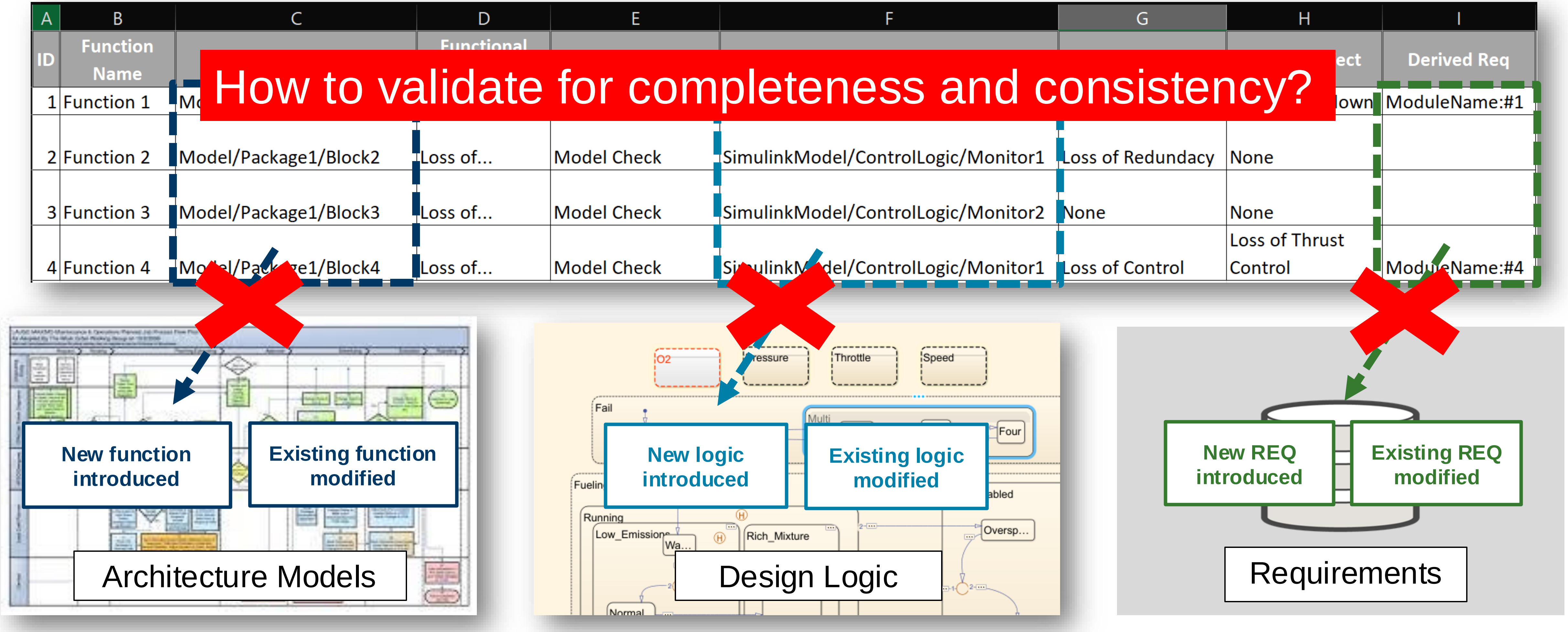
```
' Ora
Function TableHeader(Table, Options)
    TableHeader = "---" & vbLf & "---
    TableHeader = TableHeader & Object
    TableHeader = TableHeader & vbLf &
End Function

Function nested_table_col_properties(
    nested_table_col_properties = ""
    Dim Columns
    Dim Column
    Dim ColType
    Dim ColTypeType
    Dim Clause
    Set Columns = Table.Children("Colu
    Dim ColumnTable
    For Each Column In Columns
        Set ColType = Column.Property
        ColTypeType = ColType.Property
        If ColTypeType = "Object" Then
            Clause = nested_table_col
```

Architecture Models

Design Logic

Requirements

Traditional safety analysis is inherently difficult to validate for completeness and consistency



How to validate for completeness and consistency?

A	B	C	D	E	F	G	H	I
ID	Function Name		Functional				ect	Derived Req
1	Function 1	Mo					own	ModuleName:#1
2	Function 2	Model/Package1/Block2	Loss of...	Model Check	SimulinkModel/ControlLogic/Monitor1	Loss of Redundacy	None	
3	Function 3	Model/Package1/Block3	Loss of...	Model Check	SimulinkModel/ControlLogic/Monitor2	None	None	
4	Function 4	Model/Package1/Block4	Loss of...	Model Check	SimulinkModel/ControlLogic/Monitor1	Loss of Control	Loss of Thrust Control	ModuleName:#4

New function introduced

Existing function modified

Architecture Models

New logic introduced

Existing logic modified

Design Logic

New REQ introduced

Existing REQ modified

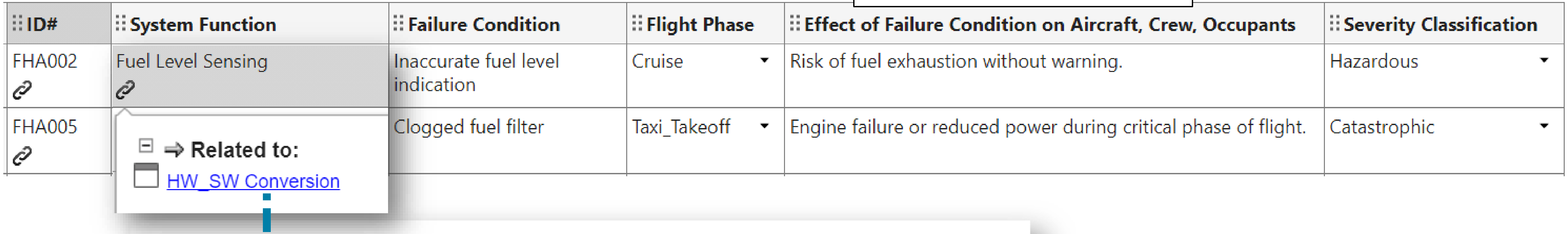
Requirements

Today’s Agenda

- Importance of safety in product development
- System: Model-based safety analysis workflow
- Component: Fault injection modeling
- Case Study: Aircraft fuel system
- Conclusion

Model-Based Safety Analysis is fully integrated and traceable with respect to changes

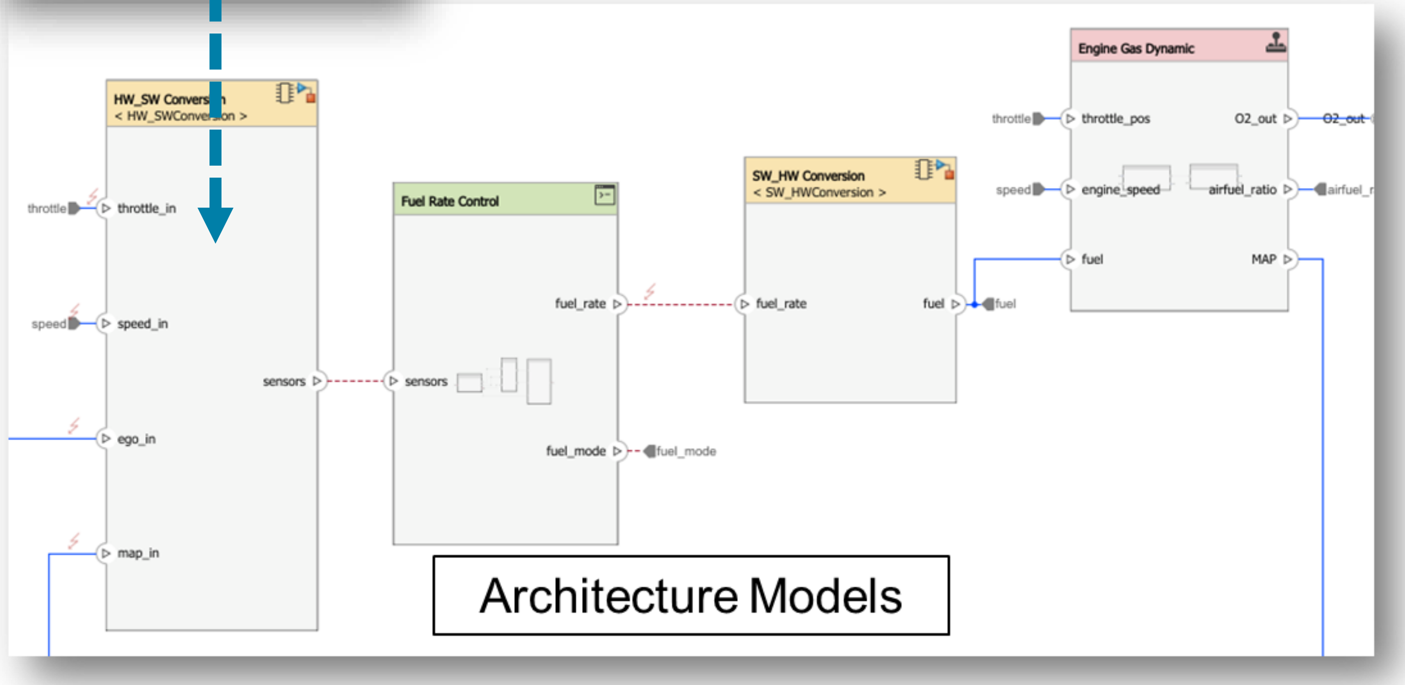
Hazard Assessment



ID#	System Function	Failure Condition	Flight Phase	Effect of Failure Condition on Aircraft, Crew, Occupants	Severity Classification
FHA002	Fuel Level Sensing	Inaccurate fuel level indication	Cruise	Risk of fuel exhaustion without warning.	Hazardous
FHA005		Clogged fuel filter	Taxi_Takeoff	Engine failure or reduced power during critical phase of flight.	Catastrophic

⇒ Related to:

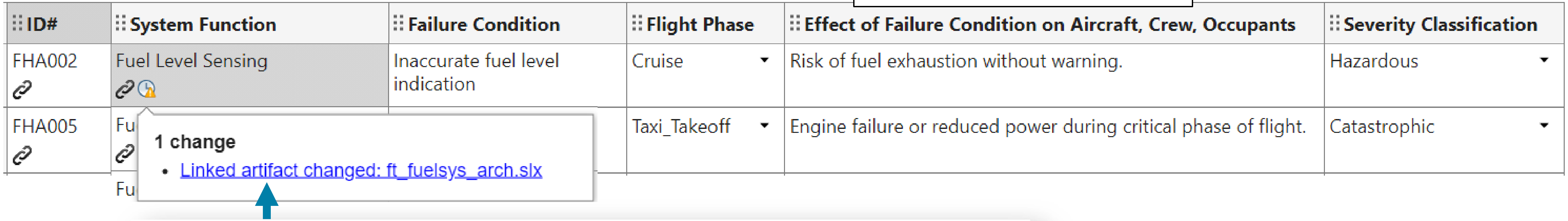
HW_SW Conversion



Architecture Models

Model-Based Safety Analysis is fully integrated and traceable with respect to changes

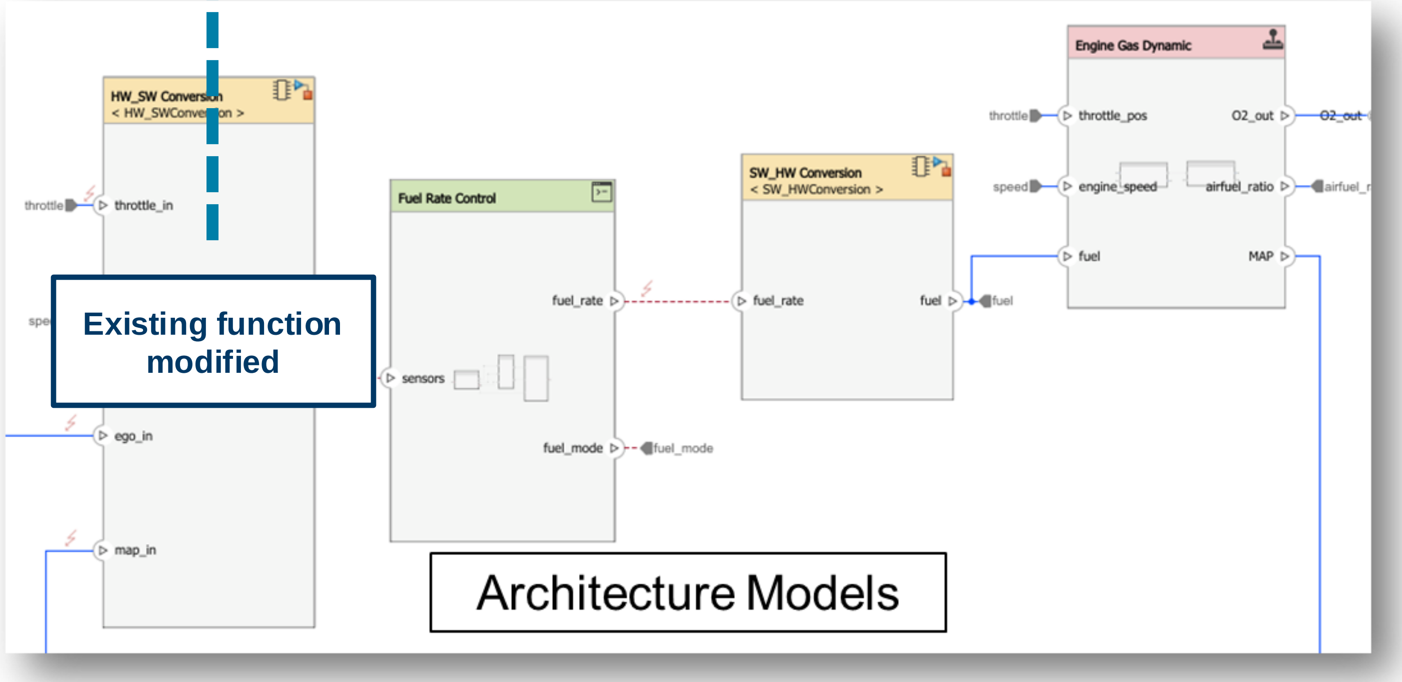
Hazard Assessment



ID#	System Function	Failure Condition	Flight Phase	Effect of Failure Condition on Aircraft, Crew, Occupants	Severity Classification
FHA002	Fuel Level Sensing	Inaccurate fuel level indication	Cruise	Risk of fuel exhaustion without warning.	Hazardous
FHA005	Fu		Taxi_Takeoff	Engine failure or reduced power during critical phase of flight.	Catastrophic
	Fu				

1 change

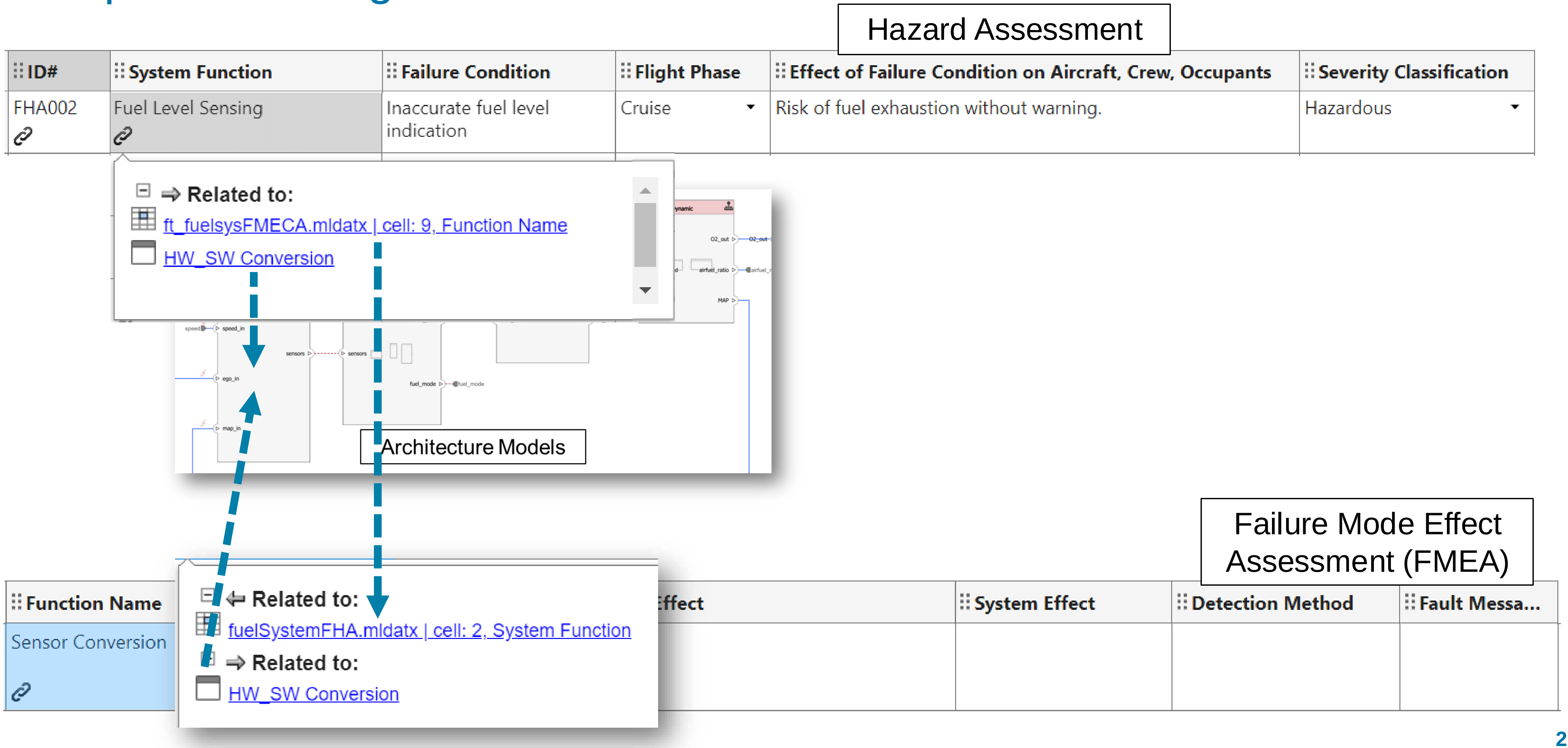
- Linked artifact changed: ft_fuelsys_arch.slx



Existing function modified

Architecture Models

Model-Based Safety Analysis is fully integrated and traceable with respect to changes



Hazard Assessment

ID#	System Function	Failure Condition	Flight Phase	Effect of Failure Condition on Aircraft, Crew, Occupants	Severity Classification
FHA002	Fuel Level Sensing	Inaccurate fuel level indication	Cruise	Risk of fuel exhaustion without warning.	Hazardous

Related to:
ft_fuelsysFMECA.mldatx | cell: 9, Function Name
HW_SW Conversion

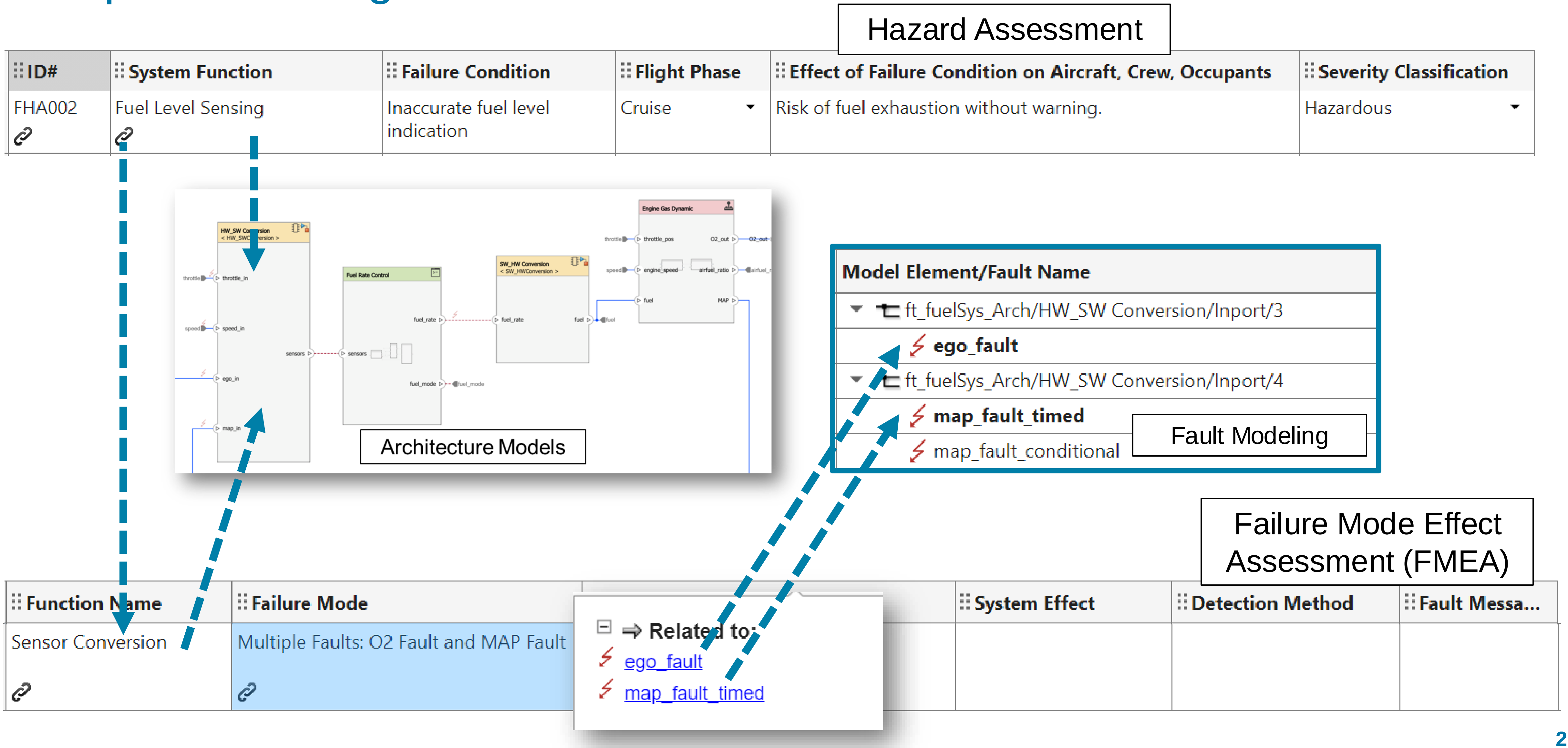
Architecture Models

Failure Mode Effect Assessment (FMEA)

Related to:
fuelSystemFHA.mldatx | cell: 2, System Function
Related to:
HW_SW Conversion

Function Name	ffect	System Effect	Detection Method	Fault Messa...
Sensor Conversion				

Model-Based Safety Analysis is fully integrated and traceable with respect to changes



Hazard Assessment

ID#	System Function	Failure Condition	Flight Phase	Effect of Failure Condition on Aircraft, Crew, Occupants	Severity Classification
FHA002	Fuel Level Sensing	Inaccurate fuel level indication	Cruise	Risk of fuel exhaustion without warning.	Hazardous

Architecture Models

Fault Modeling

Model Element/Fault Name
ft_fuelSys_Arch/HW_SW Conversion/Inport/3
ego_fault
ft_fuelSys_Arch/HW_SW Conversion/Inport/4
map_fault_timed
map_fault_conditional

Failure Mode Effect Assessment (FMEA)

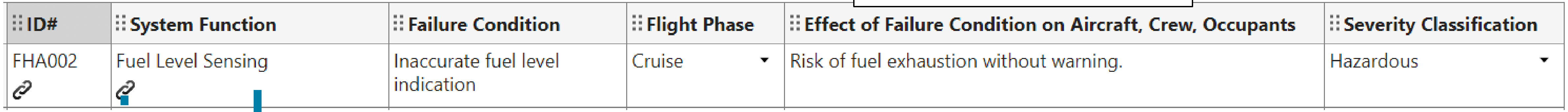
Function Name	Failure Mode	System Effect	Detection Method	Fault Messa...
Sensor Conversion	Multiple Faults: O2 Fault and MAP Fault			

⇒ Related to:
ego_fault

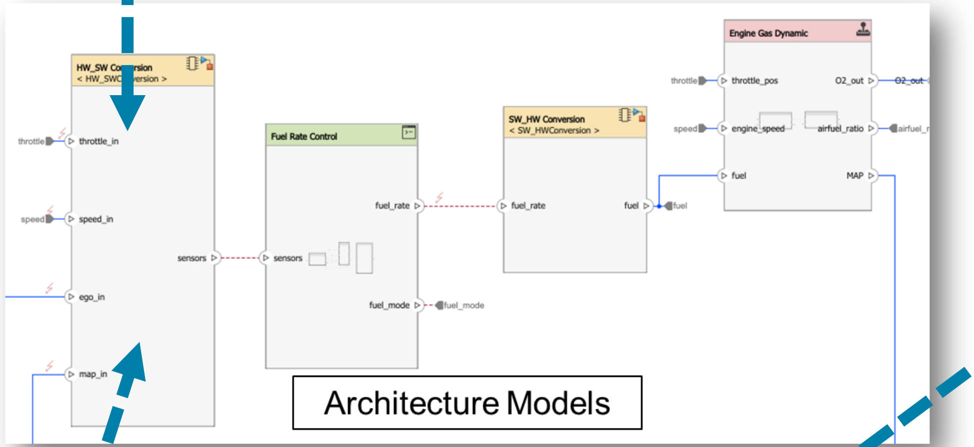
map_fault_timed

Model-Based Safety Analysis is fully integrated and traceable with respect to changes

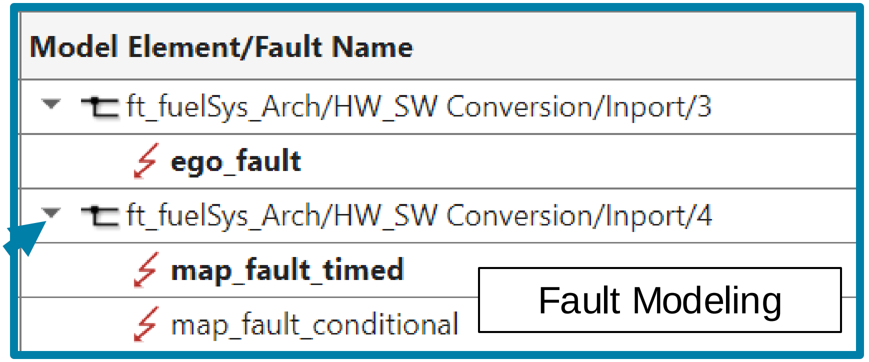
Hazard Assessment



ID#	System Function	Failure Condition	Flight Phase	Effect of Failure Condition on Aircraft, Crew, Occupants	Severity Classification
FHA002	Fuel Level Sensing	Inaccurate fuel level indication	Cruise	Risk of fuel exhaustion without warning.	Hazardous



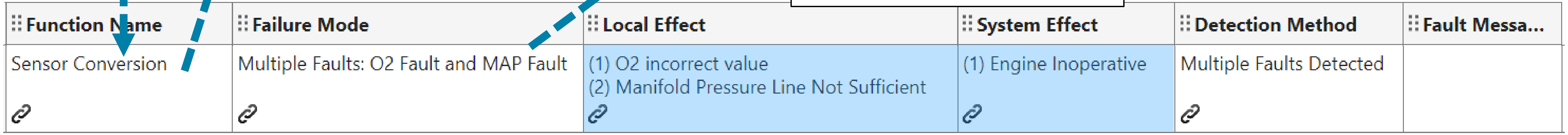
Architecture Models



Model Element/Fault Name
ft_fuelSys_Arch/HW_SW Conversion/Inport/3
ego_fault
ft_fuelSys_Arch/HW_SW Conversion/Inport/4
map_fault_timed
map_fault_conditional

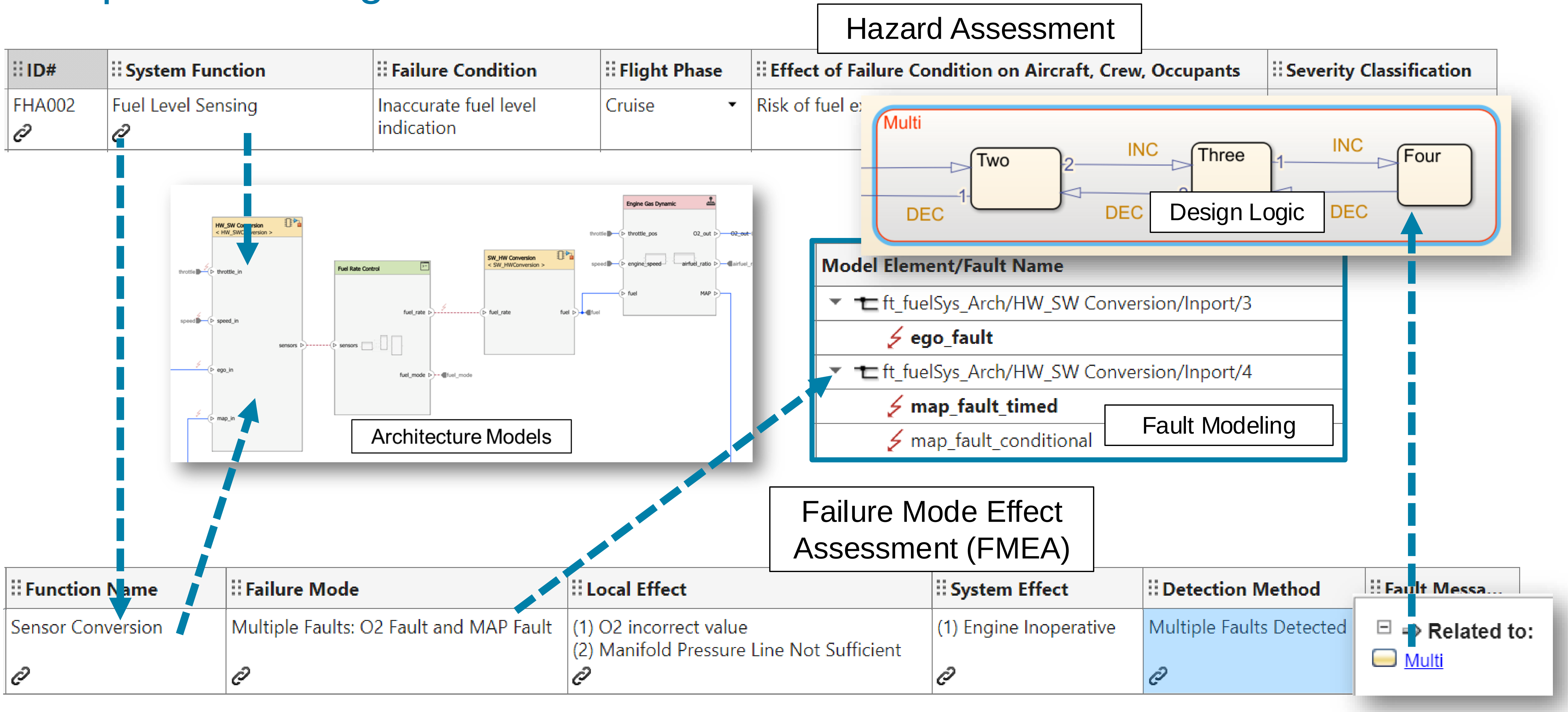
Fault Modeling

Failure Mode Effect Assessment (FMEA)



Function Name	Failure Mode	Local Effect	System Effect	Detection Method	Fault Messa...
Sensor Conversion	Multiple Faults: O2 Fault and MAP Fault	(1) O2 incorrect value (2) Manifold Pressure Line Not Sufficient	(1) Engine Inoperative	Multiple Faults Detected	

Model-Based Safety Analysis is fully integrated and traceable with respect to changes



Hazard Assessment

ID#	System Function	Failure Condition	Flight Phase	Effect of Failure Condition on Aircraft, Crew, Occupants	Severity Classification
FHA002	Fuel Level Sensing	Inaccurate fuel level indication	Cruise	Risk of fuel ex	

Design Logic

Architecture Models

Model Element/Fault Name
ft_fuelSys_Arch/HW_SW Conversion/Inport/3
ego_fault
ft_fuelSys_Arch/HW_SW Conversion/Inport/4
map_fault_timed
map_fault_conditional

Fault Modeling

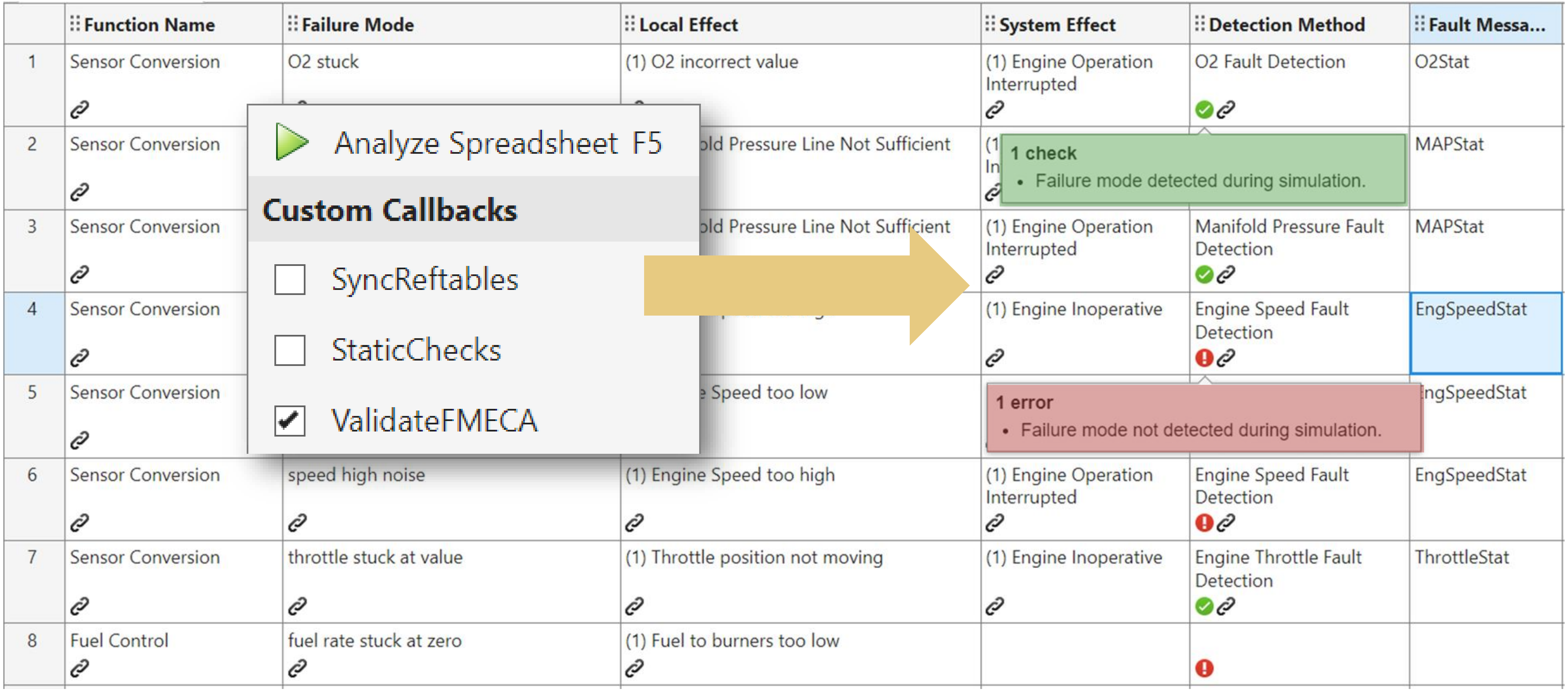
Failure Mode Effect Assessment (FMEA)

Function Name	Failure Mode	Local Effect	System Effect	Detection Method	Fault Messa...
Sensor Conversion	Multiple Faults: O2 Fault and MAP Fault	(1) O2 incorrect value (2) Manifold Pressure Line Not Sufficient	(1) Engine Inoperative	Multiple Faults Detected	

Related to:

Multi

FMEA is validated by simulating the system architecture with fault-injections using implementation models



	Function Name	Failure Mode	Local Effect	System Effect	Detection Method	Fault Messa...
1	Sensor Conversion 🔗	O2 stuck	(1) O2 incorrect value	(1) Engine Operation Interrupted 🔗	O2 Fault Detection ✓🔗	O2Stat
2	Sensor Conversion 🔗		old Pressure Line Not Sufficient	(1 In 🔗		MAPStat
3	Sensor Conversion 🔗		old Pressure Line Not Sufficient	(1) Engine Operation Interrupted 🔗	Manifold Pressure Fault Detection ✓🔗	MAPStat
4	Sensor Conversion 🔗			(1) Engine Inoperative 🔗	Engine Speed Fault Detection ❗🔗	EngSpeedStat
5	Sensor Conversion 🔗		e Speed too low			ngSpeedStat
6	Sensor Conversion 🔗	speed high noise 🔗	(1) Engine Speed too high 🔗	(1) Engine Operation Interrupted 🔗	Engine Speed Fault Detection ❗🔗	EngSpeedStat
7	Sensor Conversion 🔗	throttle stuck at value 🔗	(1) Throttle position not moving 🔗	(1) Engine Inoperative 🔗	Engine Throttle Fault Detection ✓🔗	ThrottleStat
8	Fuel Control 🔗	fuel rate stuck at zero 🔗	(1) Fuel to burners too low 🔗		❗	

1 check

- Failure mode detected during simulation.

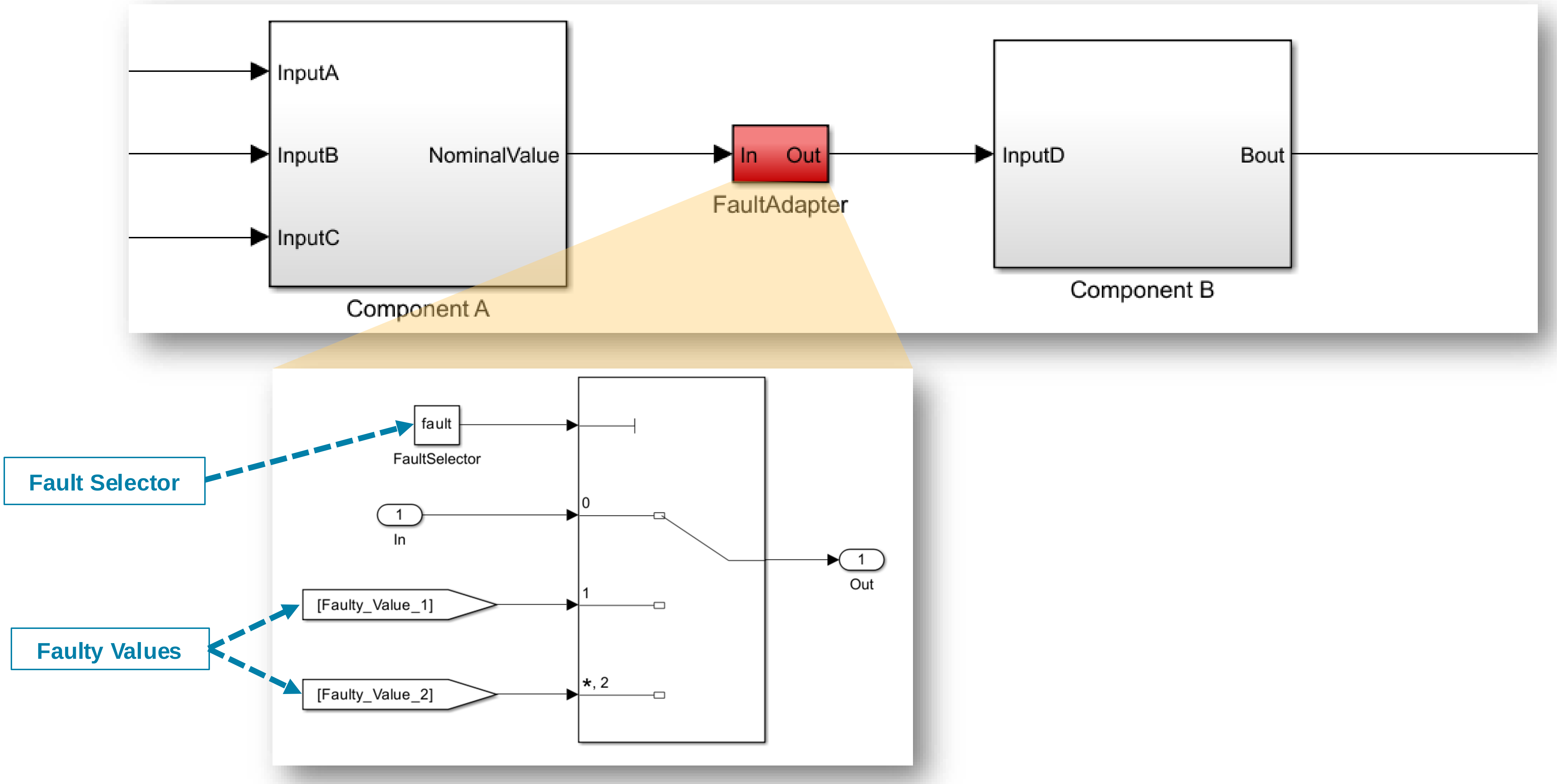
1 error

- Failure mode not detected during simulation.

Today’s Agenda

- Importance of safety in product development
- System: Model-based safety analysis workflow
- Component: Fault injection modeling
- Case Study: Aircraft fuel system
- Conclusion

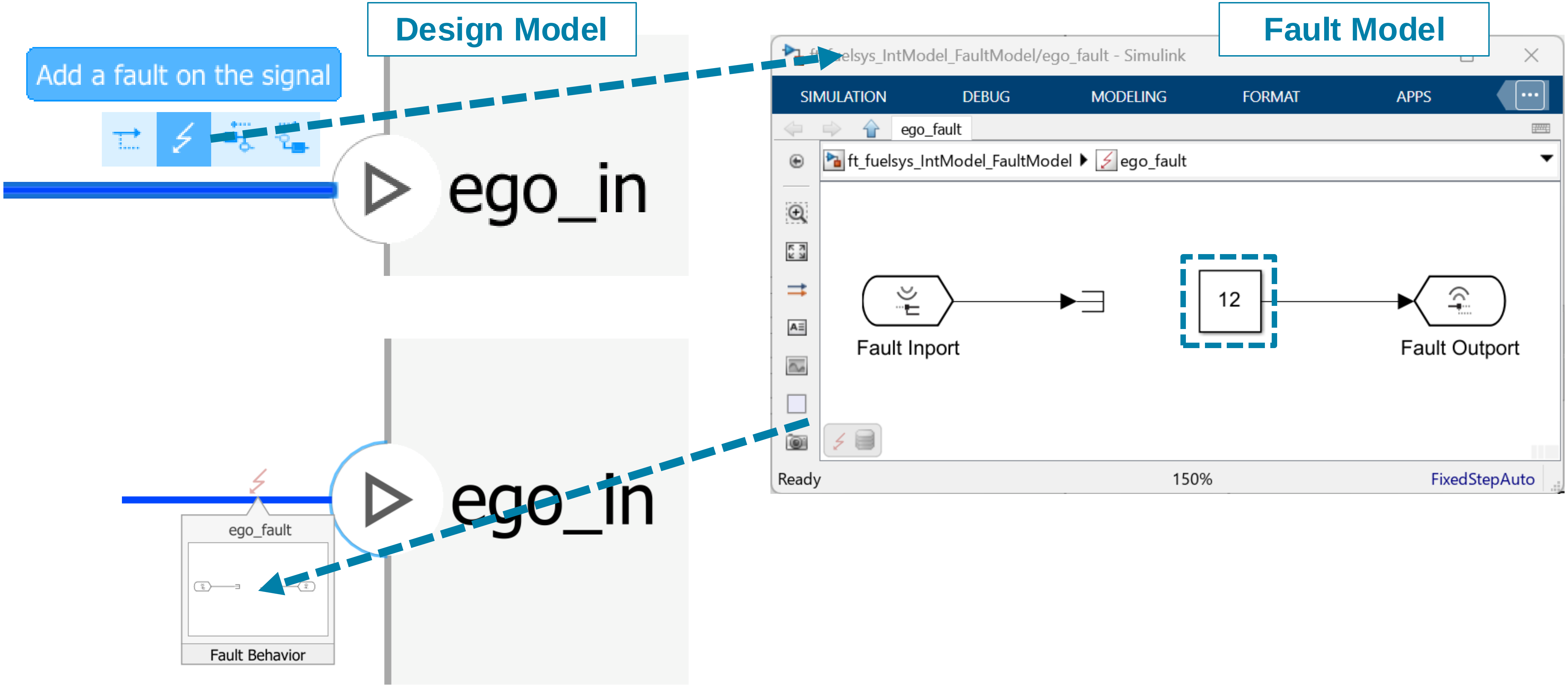
Fault modeling today modifies the design, makes it difficult to analyze effects and is not connected to hazards



Fault Selector

Faulty Values

New enhanced fault modeling is separated from the design, makes it easy to analyze effects and is connected to hazards

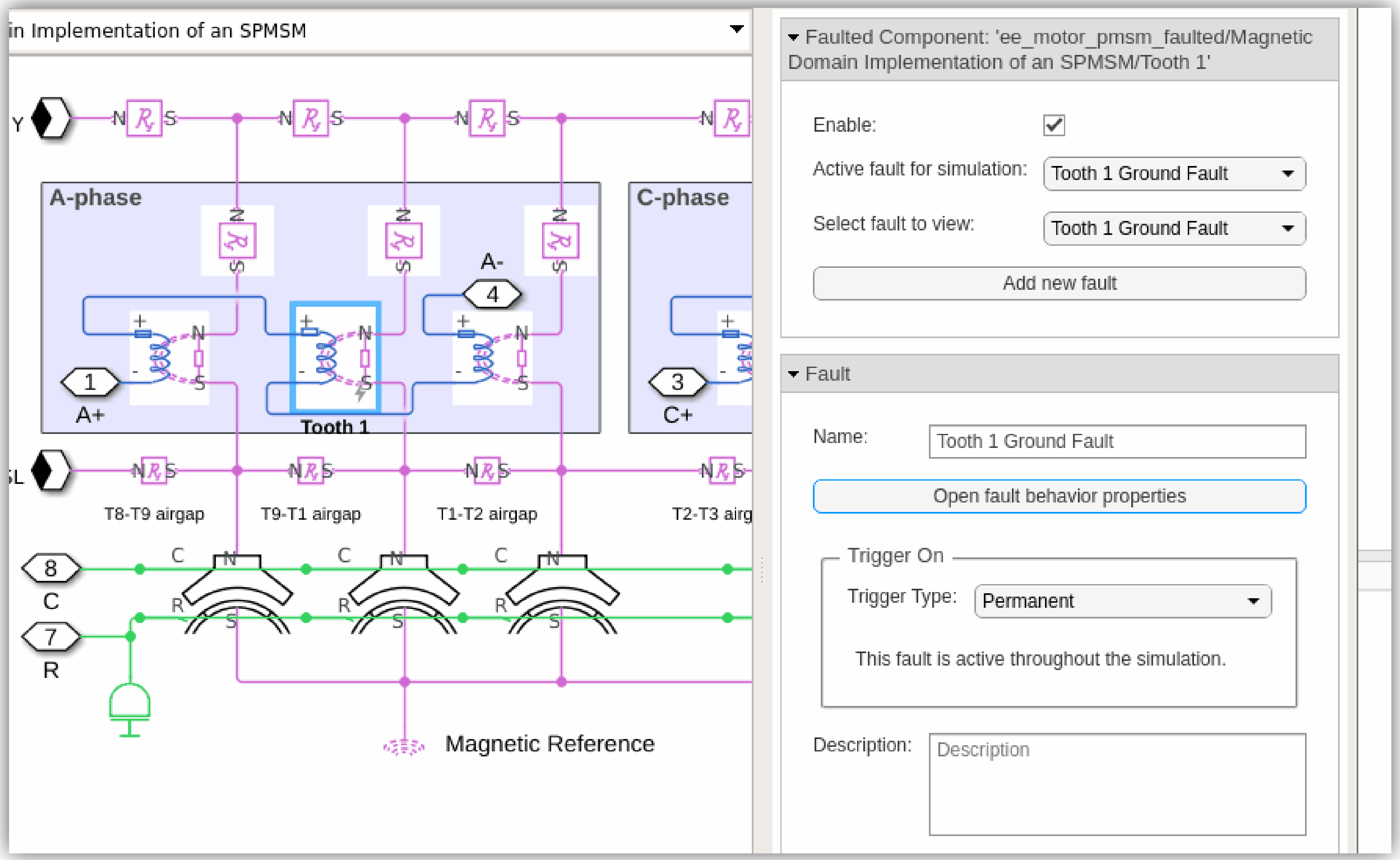


Design Model

Fault Model

Add a fault on the signal

New enhanced fault modeling is separated from the design, makes it easy to analyze effects and is connected to hazards



▾ Faulted Component: 'ee_motor_pmsm_faulted/Magnetic Domain Implementation of an SPMSM/Tooth 1'

Enable: ☑

Active fault for simulation: Tooth 1 Ground Fault

Select fault to view: Tooth 1 Ground Fault

▾ Fault

Name: Tooth 1 Ground Fault

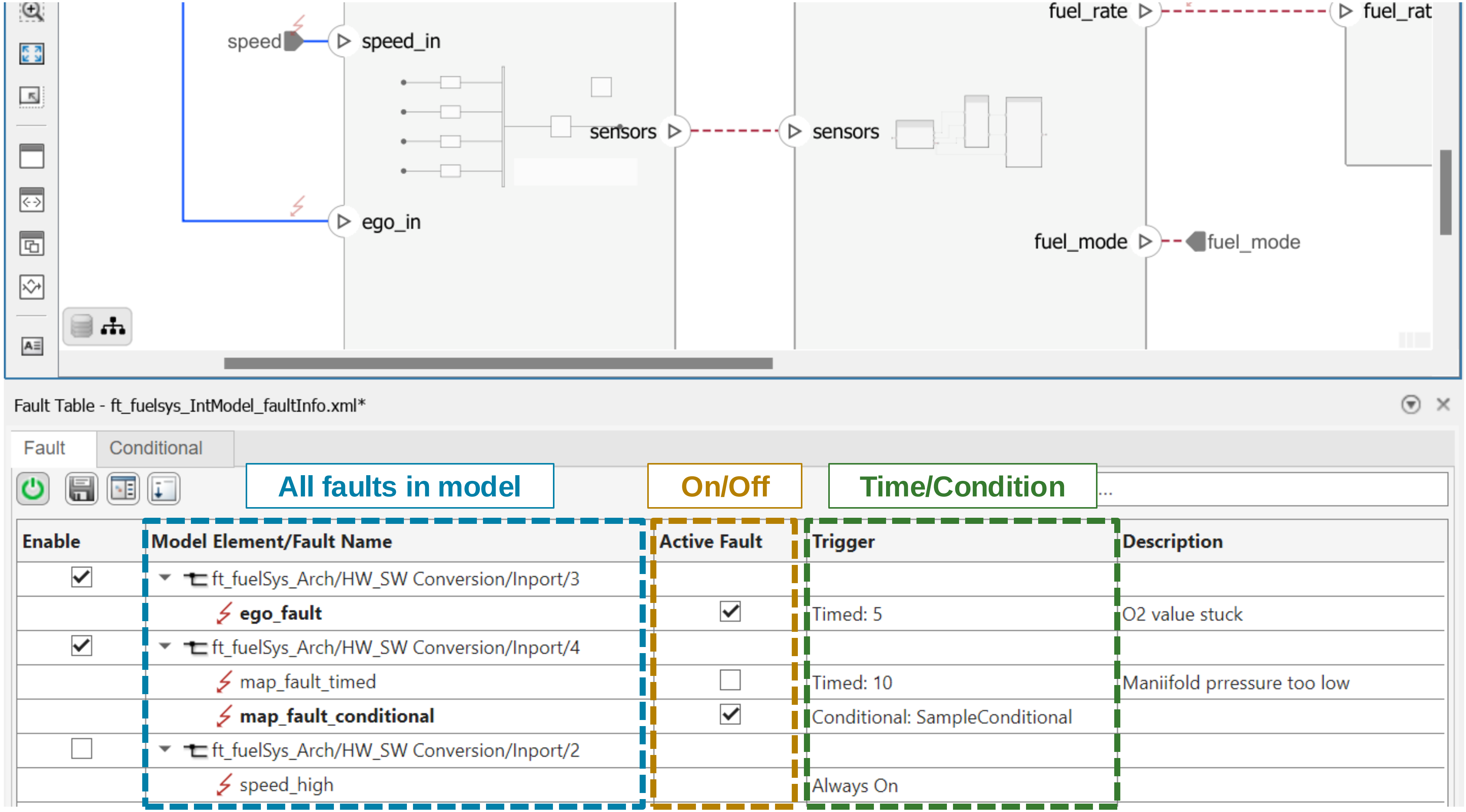
Trigger On

Trigger Type: Permanent

This fault is active throughout the simulation.

Description: Description

New enhanced fault modeling is separated from the design, makes it easy to analyze effects and is connected to hazards



Fault Table - ft_fuelsys_IntModel_faultInfo.xml*

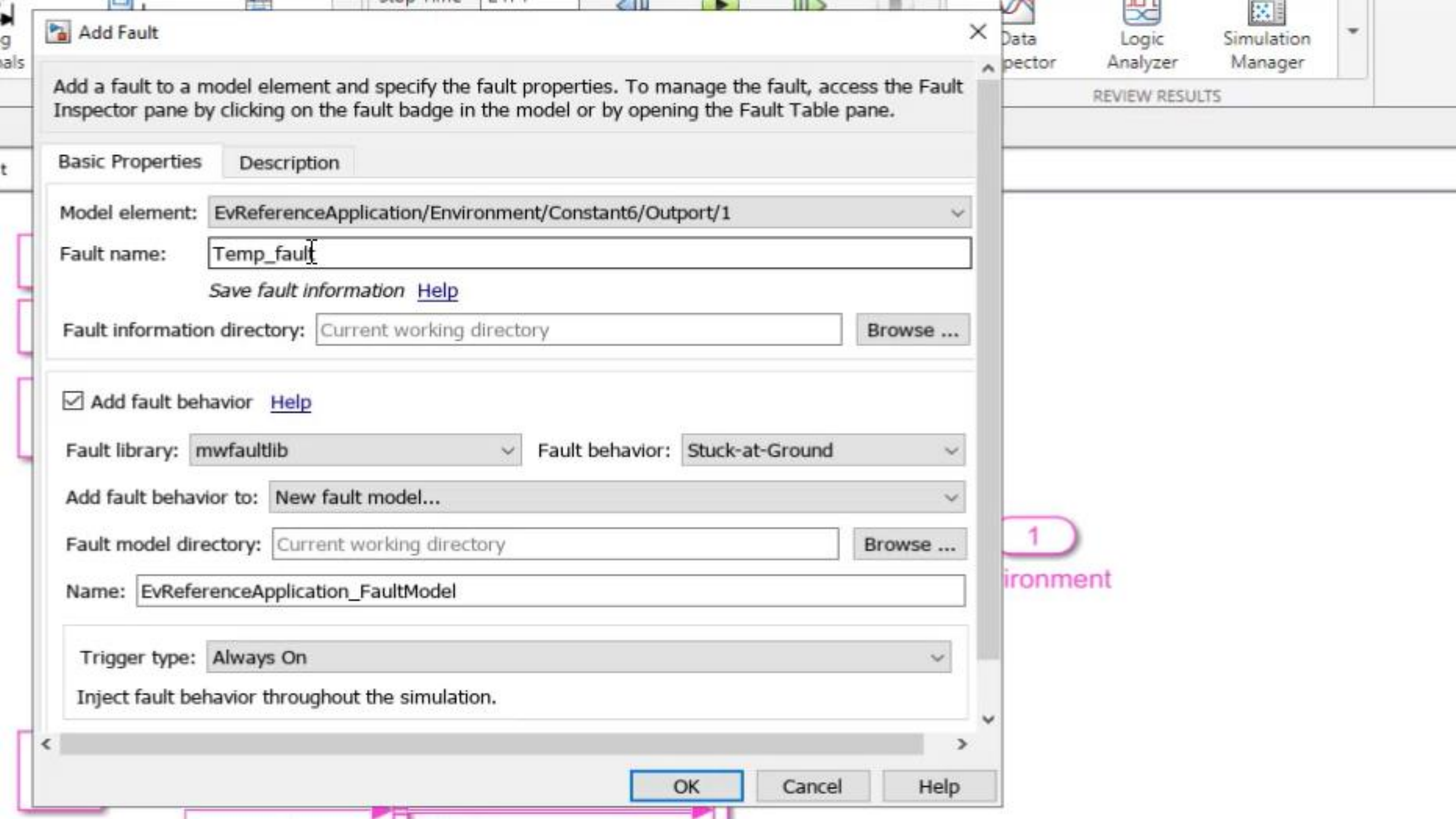
All faults in model

On/Off

Time/Condition

Enable	Model Element/Fault Name	Active Fault	Trigger	Description
☑	ft_fuelSys_Arch/HW_SW Conversion/Inport/3			
	ego_fault	☑	Timed: 5	O2 value stuck
☑	ft_fuelSys_Arch/HW_SW Conversion/Inport/4			
	map_fault_timed	☐	Timed: 10	Maniifold prressure too low
	map_fault_conditional	☑	Conditional: SampleConditional	
☐	ft_fuelSys_Arch/HW_SW Conversion/Inport/2			
	speed_high		Always On	

Modelling Faults without Modifying the Design



Add Fault

Add a fault to a model element and specify the fault properties. To manage the fault, access the Fault Inspector pane by clicking on the fault badge in the model or by opening the Fault Table pane.

Basic Properties | Description

Model element: EvReferenceApplication/Environment/Constant6/Outport/1

Fault name: Temp_fault

Save fault information Help

Fault information directory: Current working directory Browse ...

☑ Add fault behavior Help

Fault library: mwfaultlib Fault behavior: Stuck-at-Ground

Add fault behavior to: New fault model...

Fault model directory: Current working directory Browse ...

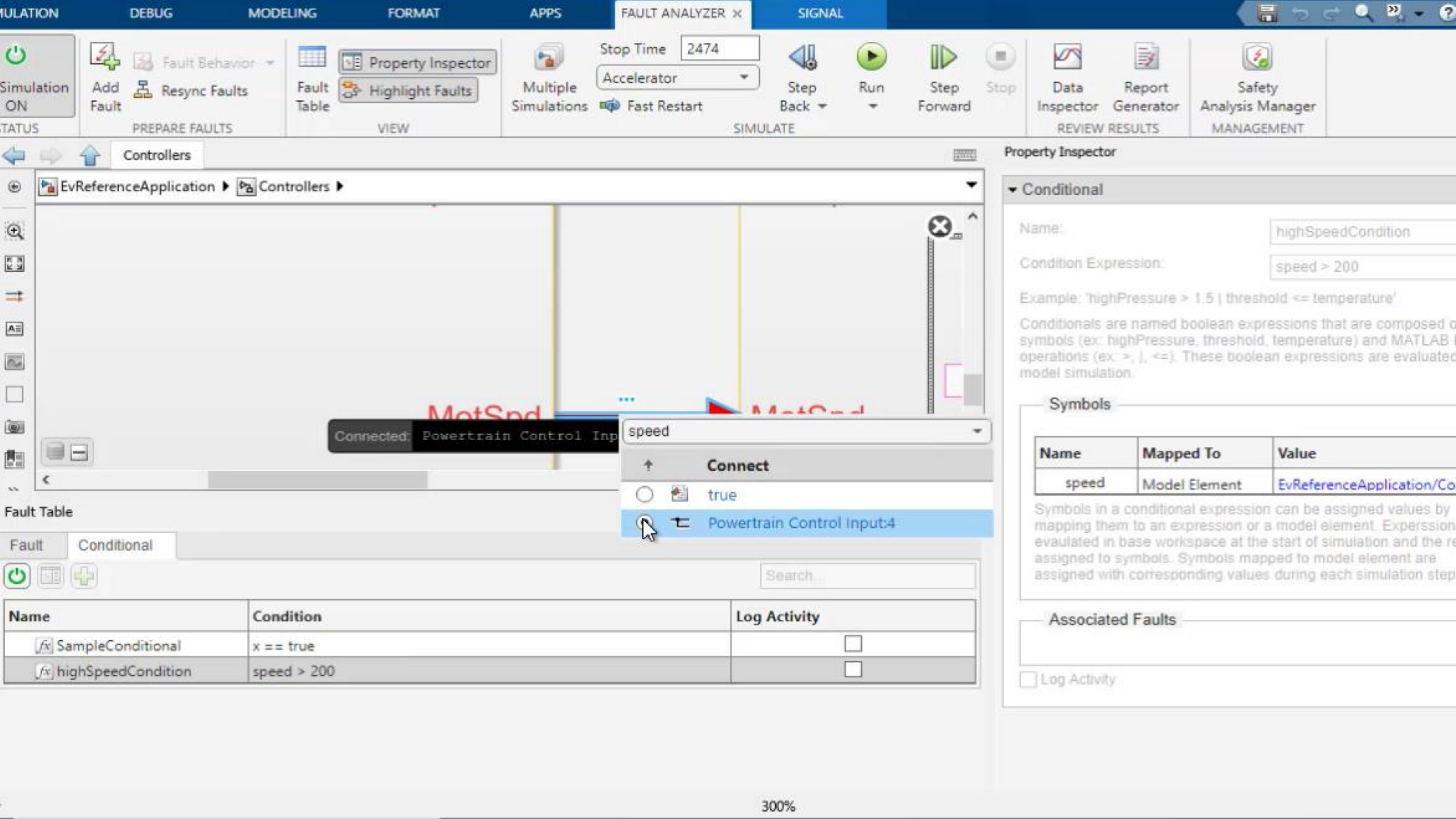
Name: EvReferenceApplication_FaultModel

Trigger type: Always On

Inject fault behavior throughout the simulation.

OK | Cancel | Help

Modelling Conditional Fault Injections



Stop Time 2474

Accelerator

Connected: Powertrain Control Inp

speed

		Connect
○		true
○		Powertrain Control Input:4

Property Inspector

Conditional

Name: highSpeedCondition

Condition Expression: speed > 200

Example: 'highPressure > 1.5 | threshold <= temperature'

Conditionals are named boolean expressions that are composed o symbols (ex: highPressure, threshold, temperature) and MATLAB operations (ex: >, |, <=). These boolean expressions are evaluated model simulation.

Symbols

Name	Mapped To	Value
speed	Model Element	EvReferenceApplication/Co

Symbols in a conditional expression can be assigned values by mapping them to an expression or a model element. Expression evaluated in base workspace at the start of simulation and the re assigned to symbols. Symbols mapped to model element are assigned with corresponding values during each simulation step

Associated Faults

□ Log Activity

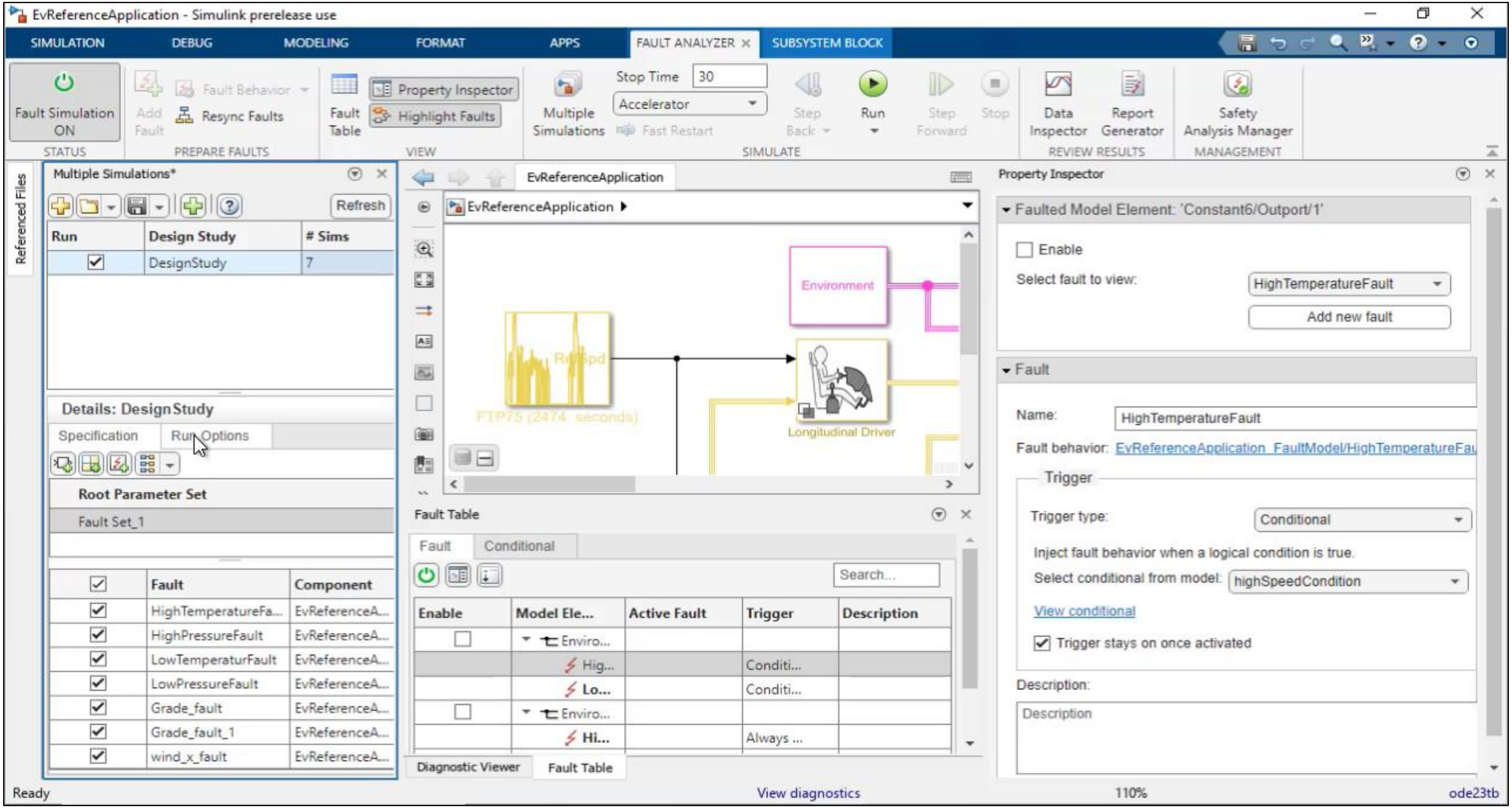
Fault Table

Fault | Conditional

Search...

Name	Condition	Log Activity
SampleConditional	x == true	□
highSpeedCondition	speed > 200	□

Analyzing Fault Effects using Batch Simulations



EvReferenceApplication - Simulink prerelease use

Stop Time: 30

Accelerator

Multiple Simulations*

Run	Design Study	# Sims
☑	DesignStudy	7

Details: DesignStudy

Root Parameter Set

Fault Set_1

☑	Fault	Component
☑	HighTemperatureFa...	EvReferenceA...
☑	HighPressureFault	EvReferenceA...
☑	LowTemperaturFault	EvReferenceA...
☑	LowPressureFault	EvReferenceA...
☑	Grade_fault	EvReferenceA...
☑	Grade_fault_1	EvReferenceA...
☑	wind_x_fault	EvReferenceA...

EvReferenceApplication ▸

Fault Table

Fault | Conditional

Enable	Model Ele...	Active Fault	Trigger	Description
☐	▾ Enviro...			
	Hig...		Conditi...	
	Lo...		Conditi...	
☐	▾ Enviro...			
	Hi...		Always ...	

Property Inspector

Faulted Model Element: 'Constant6/Outport/1'

☐ Enable

Select fault to view: HighTemperatureFault

Fault

Name: HighTemperatureFault

Fault behavior: EvReferenceApplication_FaultModel/HighTemperatureFau

Trigger

Trigger type: Conditional

Inject fault behavior when a logical condition is true.

Select conditional from model: highSpeedCondition

☑ Trigger stays on once activated

Description:

Description

Ready | View diagnostics | 110% | ode23tb

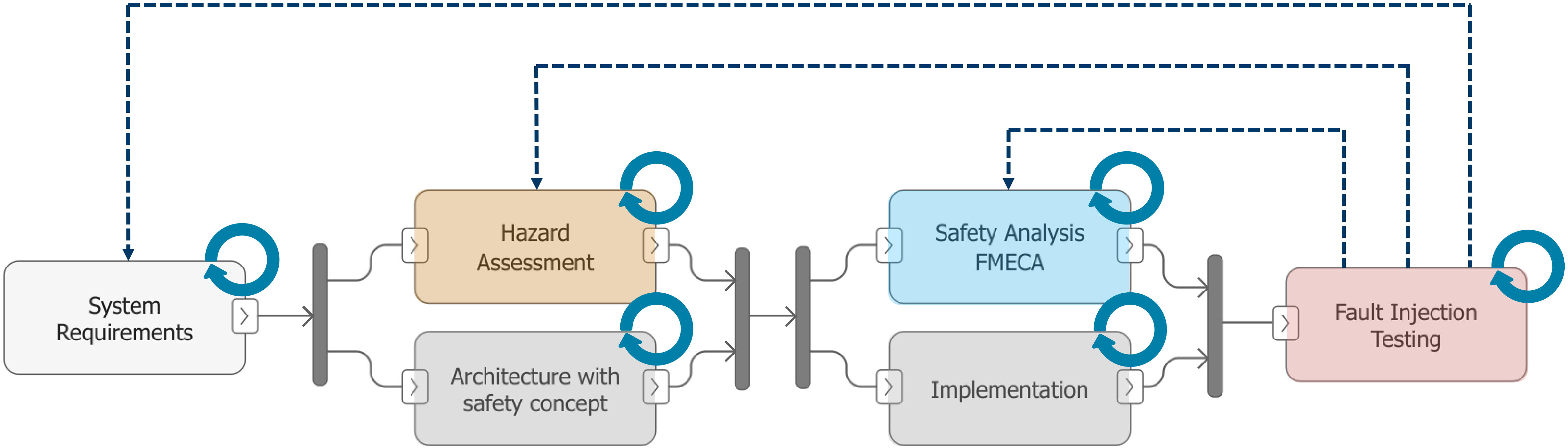
Today’s Agenda

- Importance of safety in product development
- System: Model-based safety analysis workflow
- Component: Fault injection modeling
- Case Study: Aircraft fuel system
- Conclusion

Model-Based Safety Analysis Example:

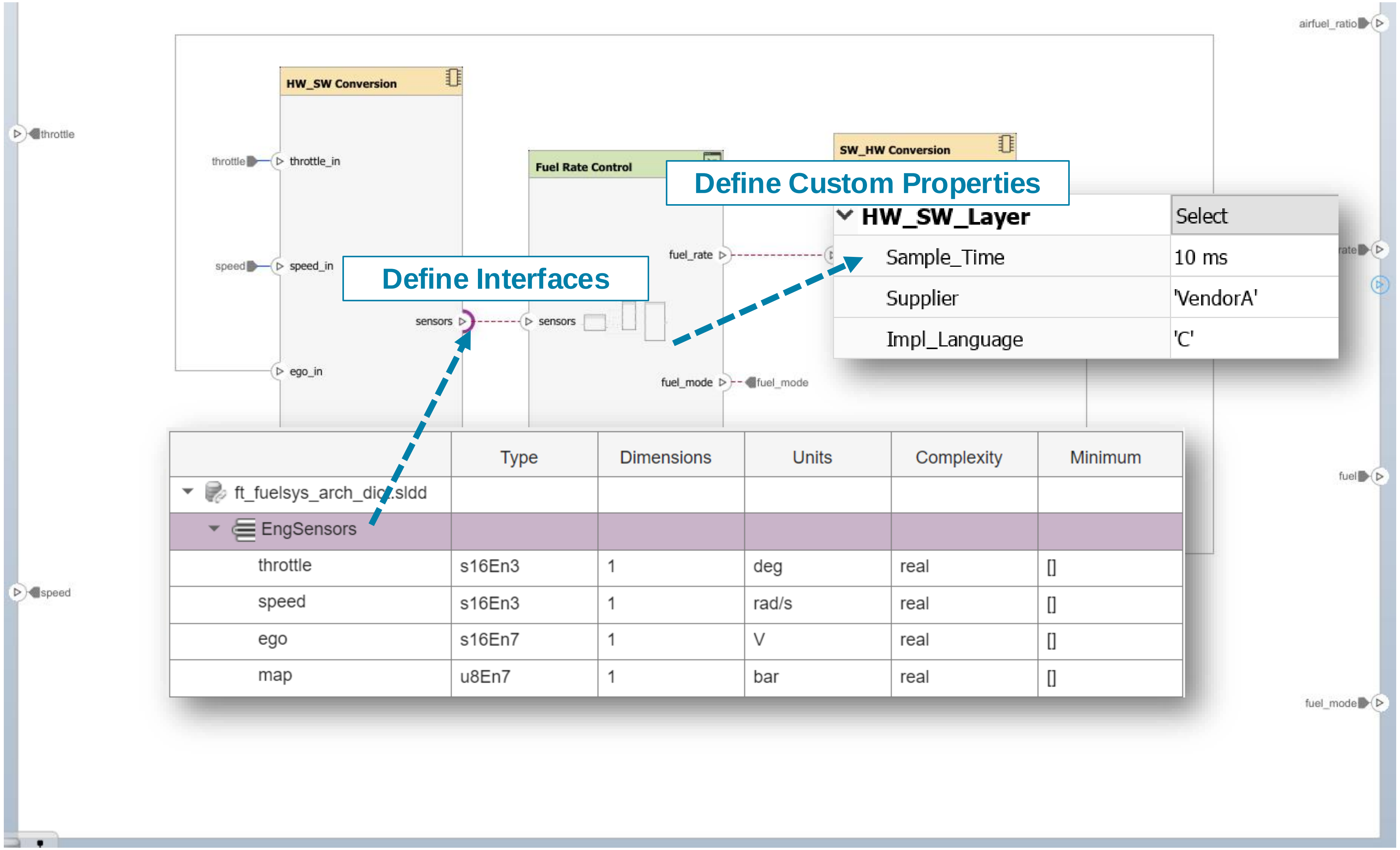
Aircraft Fuel System

Safety analysis is a highly **iterative** workflow involving detection, mitigation, and verification



- **» Develop Architecture**
- Perform Hazard Analysis
- Link Analysis to Design Artifacts
- Characterize Faults
- Static Checks
- Inject Faults & Explore Effects
- Validate through Simulation

Develop your system and software architecture, incl. interfaces and custom properties



Define Custom Properties

HW_SW_Layer	Select
Sample_Time	10 ms
Supplier	'VendorA'
Impl_Language	'C'

Define Interfaces

	Type	Dimensions	Units	Complexity	Minimum
ft_fuelsys_arch_dict.sldd					
EngSensors					
throttle	s16En3	1	deg	real	[]
speed	s16En3	1	rad/s	real	[]
ego	s16En7	1	V	real	[]
map	u8En7	1	bar	real	[]

Develop Architecture

» **Perform Hazard Analysis**

Link Analysis to Design Artifacts

Characterize Faults

Static Checks

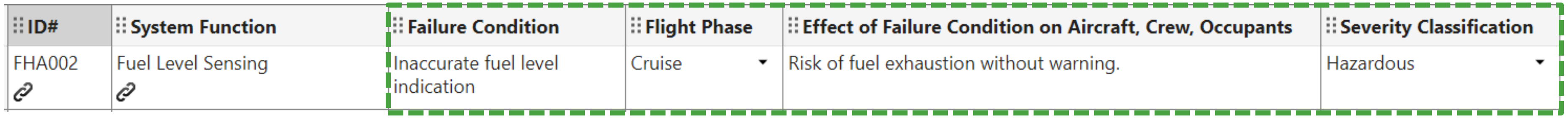
Inject Faults & Explore Effects

Validate through Simulation

Identify potential hazards that could arise during the system's operation and assess the risks of each one

Hazard Assessment

User Defined



ID#	System Function	Failure Condition	Flight Phase	Effect of Failure Condition on Aircraft, Crew, Occupants	Severity Classification
FHA002	Fuel Level Sensing	Inaccurate fuel level indication	Cruise	Risk of fuel exhaustion without warning.	Hazardous

Develop Architecture

Perform Hazard Analysis

» **Link Analysis to Design Artifacts**

Characterize Faults

Static Checks

Inject Faults & Explore Effects

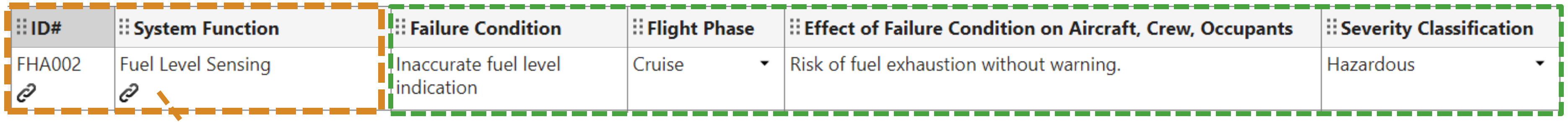
Validate through Simulation

Link hazards to system architecture for ensuring consistency and completeness of analysis

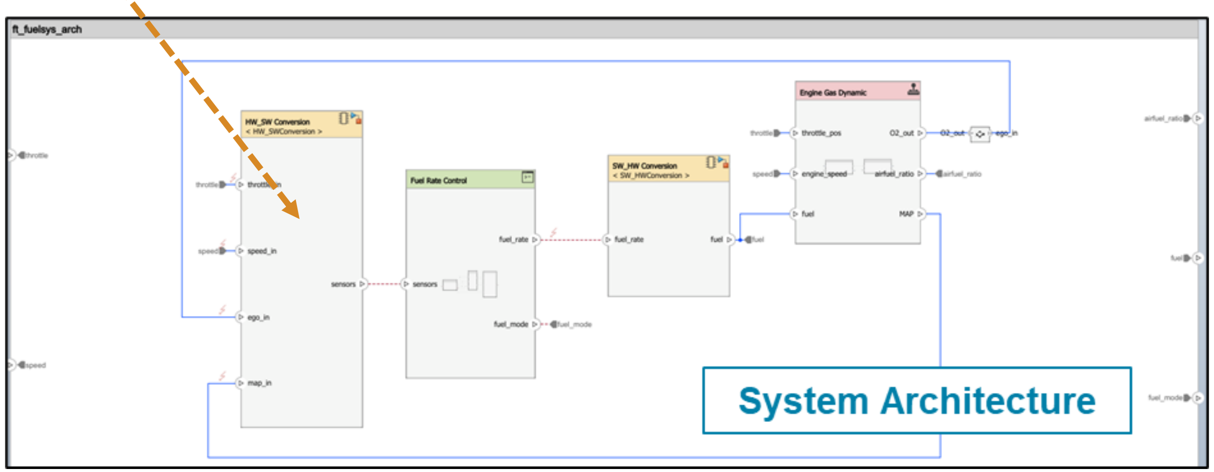
Synchronized with Model

Hazard Assessment

User Defined



ID#	System Function	Failure Condition	Flight Phase	Effect of Failure Condition on Aircraft, Crew, Occupants	Severity Classification
FHA002	Fuel Level Sensing	Inaccurate fuel level indication	Cruise	Risk of fuel exhaustion without warning.	Hazardous



System Architecture

Develop Architecture

Perform Hazard Analysis

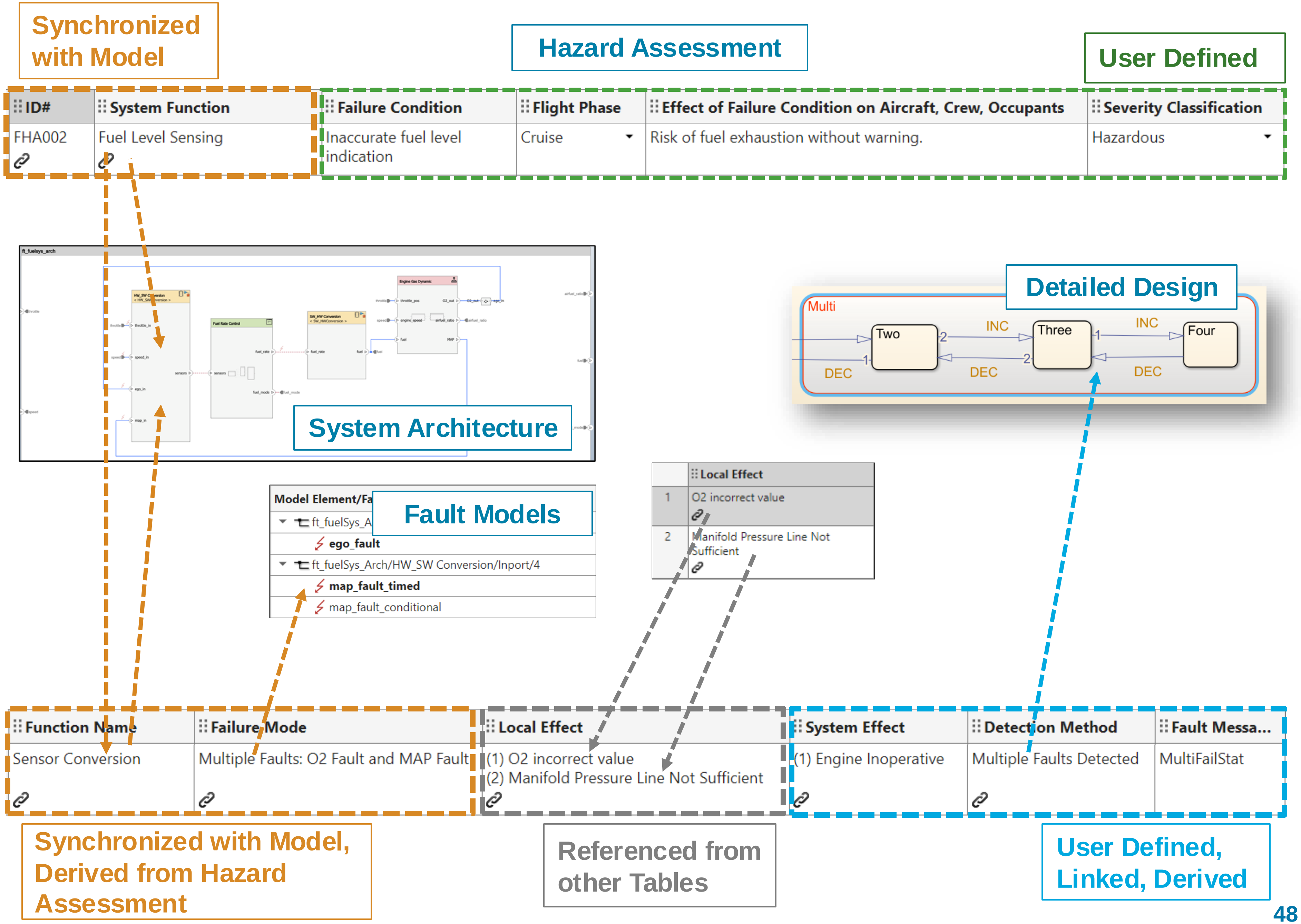
» **Link Analysis to Design Artifacts**

Characterize Faults

Static Checks

Inject Faults & Explore Effects

Validate through Simulation



Synchronized with Model

Hazard Assessment

User Defined

ID#	System Function	Failure Condition	Flight Phase	Effect of Failure Condition on Aircraft, Crew, Occupants	Severity Classification
FHA002	Fuel Level Sensing	Inaccurate fuel level indication	Cruise	Risk of fuel exhaustion without warning.	Hazardous

System Architecture

Detailed Design

Fault Models

Model Element/Fa
ft_fuelSys_A
ego_fault
ft_fuelSys_Arch/HW_SW Conversion/Inport/4
map_fault_timed
map_fault_conditional

	Local Effect
1	O2 incorrect value
2	Manifold Pressure Line Not Sufficient

Function Name	Failure Mode	Local Effect	System Effect	Detection Method	Fault Messa...
Sensor Conversion	Multiple Faults: O2 Fault and MAP Fault	(1) O2 incorrect value (2) Manifold Pressure Line Not Sufficient	(1) Engine Inoperative	Multiple Faults Detected	MultiFailStat

Synchronized with Model, Derived from Hazard Assessment

Referenced from other Tables

User Defined, Linked, Derived

Develop Architecture

Perform Hazard Analysis

» **Link Analysis to Design Artifacts**

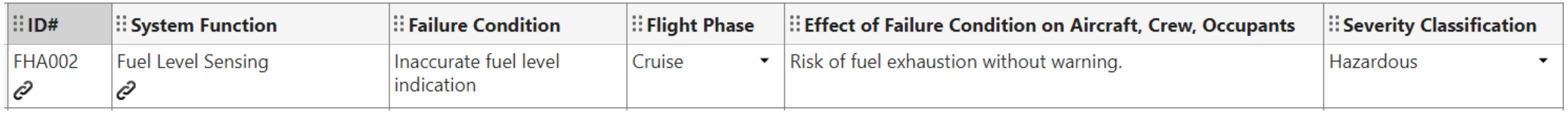
Characterize Faults

Static Checks

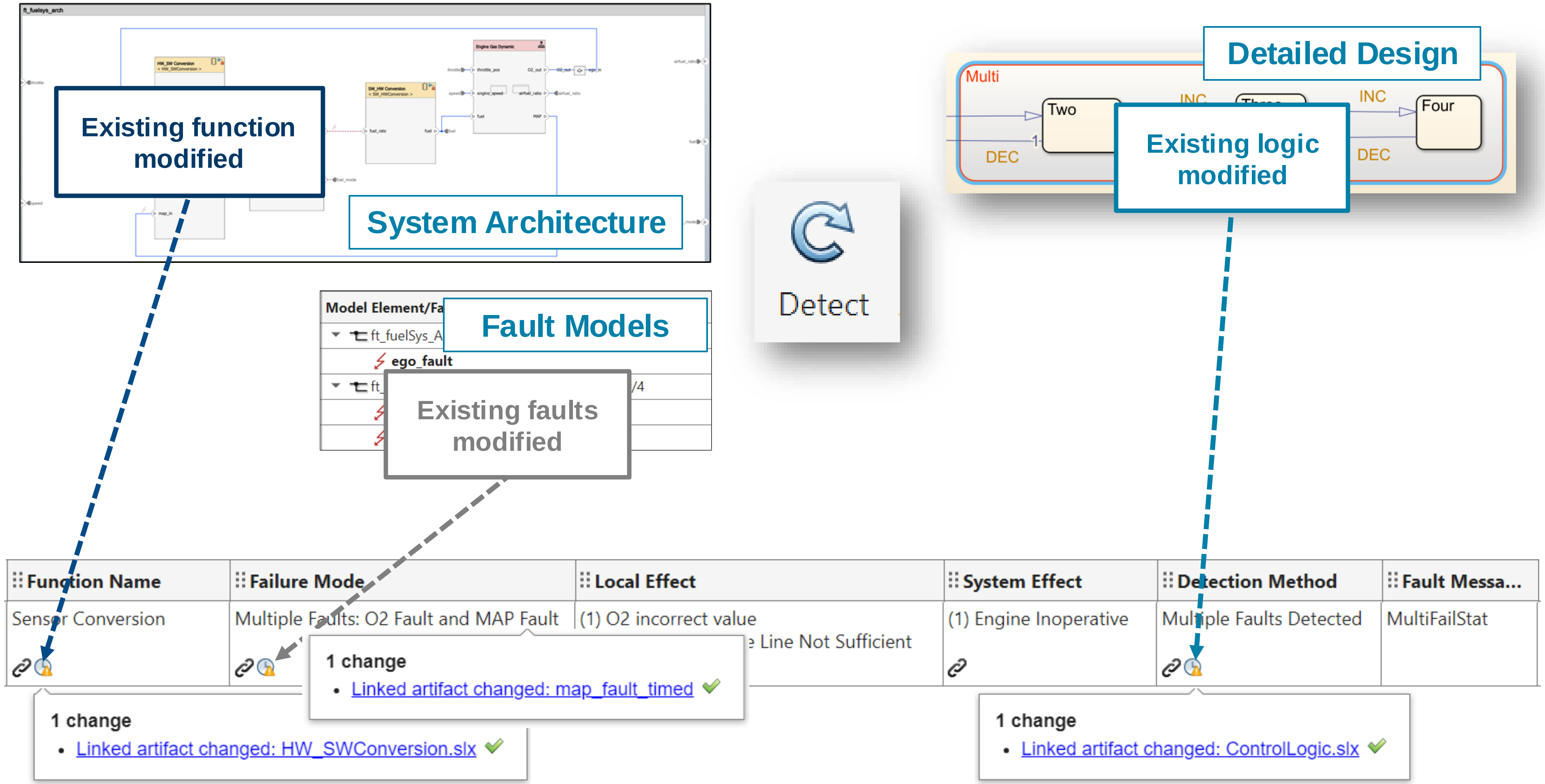
Inject Faults & Explore Effects

Validate through Simulation

Manage changes using suspect links and reviews



ID#	System Function	Failure Condition	Flight Phase	Effect of Failure Condition on Aircraft, Crew, Occupants	Severity Classification
FHA002	Fuel Level Sensing	Inaccurate fuel level indication	Cruise	Risk of fuel exhaustion without warning.	Hazardous



Existing function modified

System Architecture

Fault Models

Existing faults modified

Detailed Design

Existing logic modified

Function Name	Failure Mode	Local Effect	System Effect	Detection Method	Fault Messa...
Sensor Conversion	Multiple Faults: O2 Fault and MAP Fault	(1) O2 incorrect value e Line Not Sufficient	(1) Engine Inoperative	Multiple Faults Detected	MultiFailStat

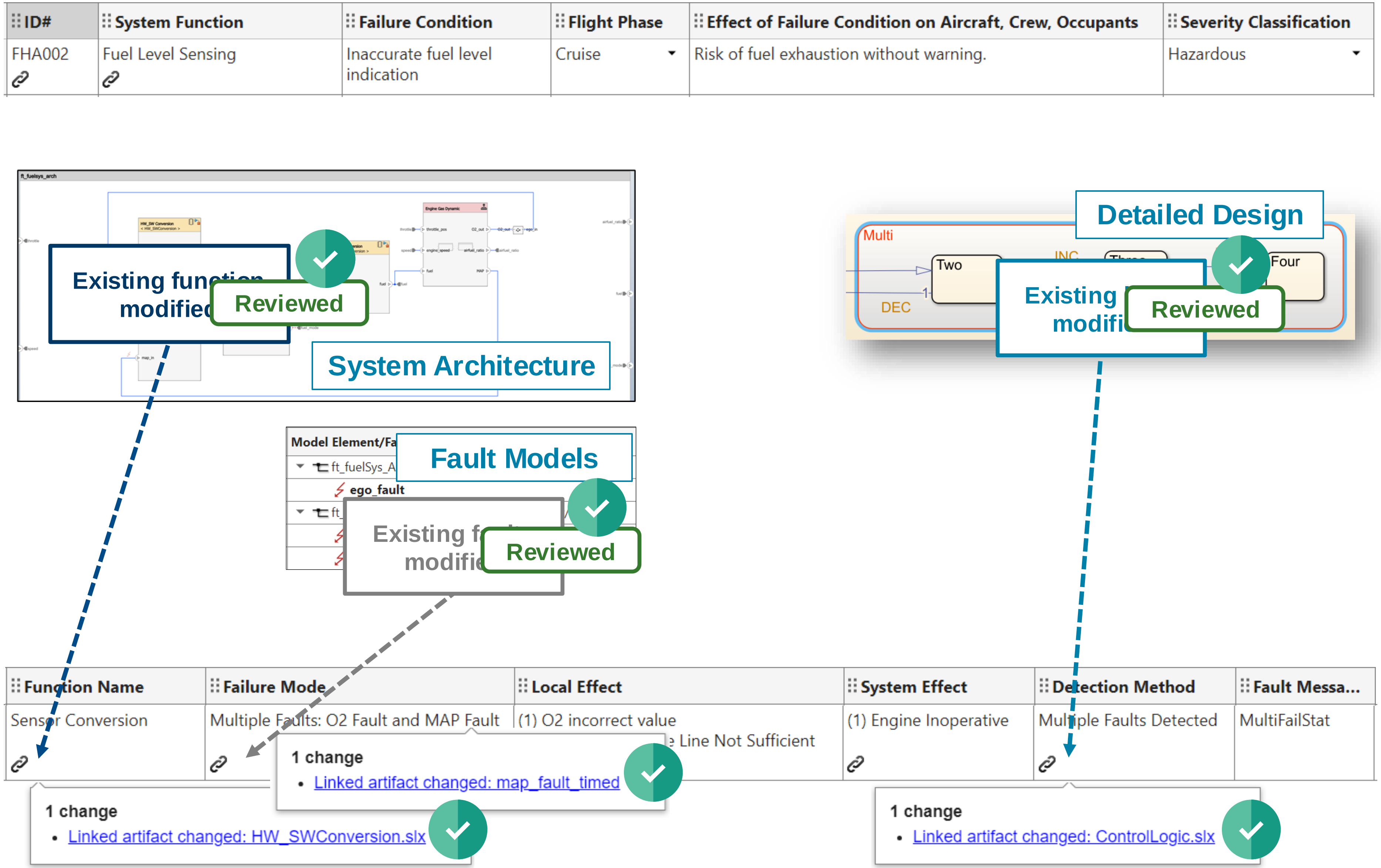
1 change
- Linked artifact changed: HW_SWConversion.slx ✓

1 change
- Linked artifact changed: map_fault_timed ✓

1 change
- Linked artifact changed: ControlLogic.slx ✓

- Develop Architecture
- Perform Hazard Analysis
- » **Link Analysis to Design Artifacts**
- Characterize Faults
- Static Checks
- Inject Faults & Explore Effects
- Validate through Simulation

Manage changes using suspect links and reviews



ID#	System Function	Failure Condition	Flight Phase	Effect of Failure Condition on Aircraft, Crew, Occupants	Severity Classification
FHA002	Fuel Level Sensing	Inaccurate fuel level indication	Cruise	Risk of fuel exhaustion without warning.	Hazardous

System Architecture

Existing fun
modified
Reviewed

Fault Models

Existing f
modifie
Reviewed

Detailed Design

Existing
modifi
Reviewed

Function Name	Failure Mode	Local Effect	System Effect	Detection Method	Fault Messa...
Sensor Conversion	Multiple Faults: O2 Fault and MAP Fault	(1) O2 incorrect value e Line Not Sufficient	(1) Engine Inoperative	Multiple Faults Detected	MultiFailStat

1 change
- Linked artifact changed: HW_SWConversion.slx

1 change
- Linked artifact changed: map_fault_timed

1 change
- Linked artifact changed: ControlLogic.slx

Develop Architecture

Perform Hazard Analysis

» **Link Analysis to Design Artifacts**

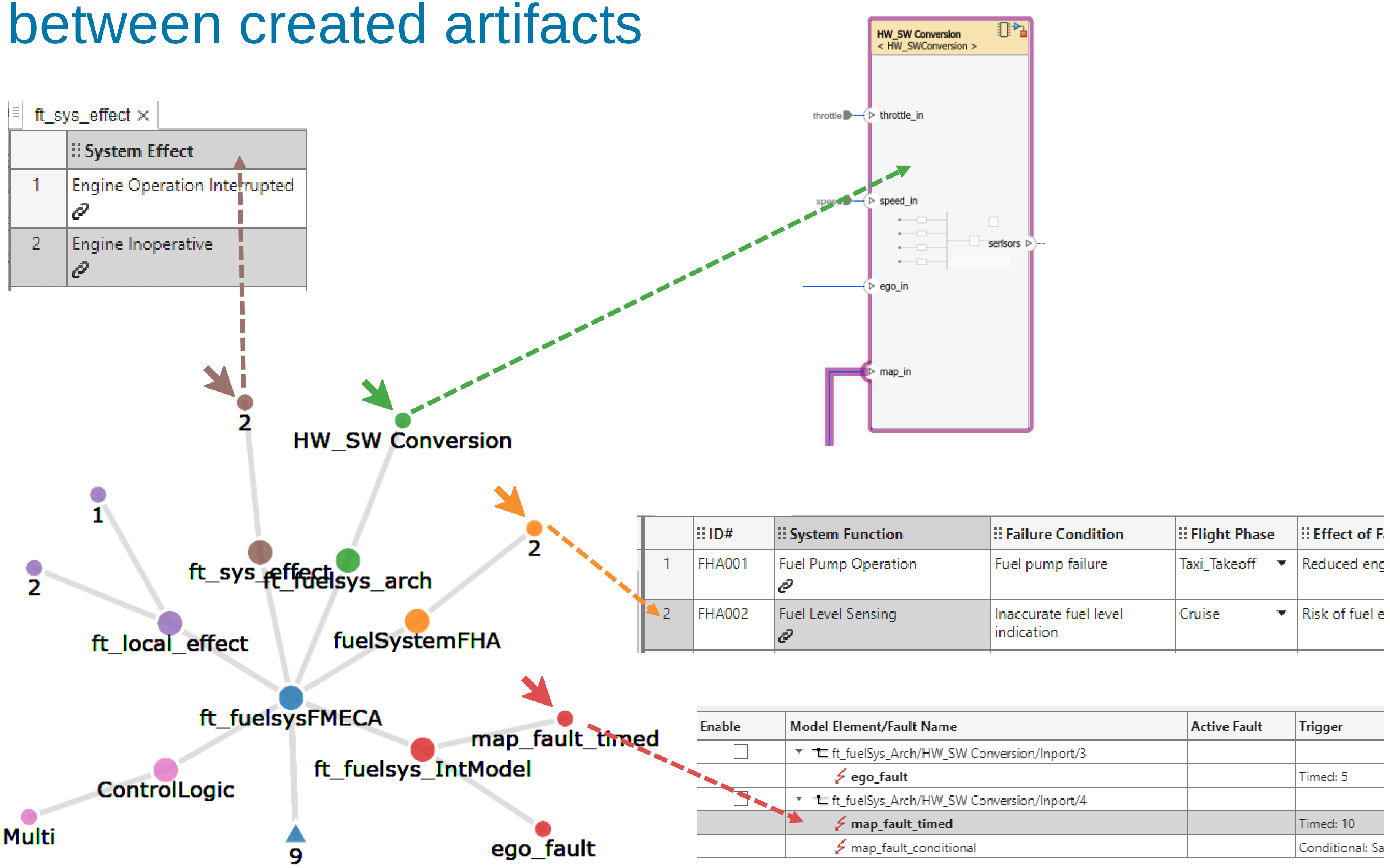
Characterize Faults

Static Checks

Inject Faults & Explore Effects

Validate through Simulation

You can build dependency graphs to ease navigation between created artifacts



ft_sys_effect ×

	System Effect
1	Engine Operation Interrupted
2	Engine Inoperative

	ID#	System Function	Failure Condition	Flight Phase	Effect of F
1	FHA001	Fuel Pump Operation	Fuel pump failure	Taxi_Takeoff	Reduced eng
2	FHA002	Fuel Level Sensing	Inaccurate fuel level indication	Cruise	Risk of fuel e

Enable	Model Element/Fault Name	Active Fault	Trigger
□	ft_fuelSys_Arch/HW_SW Conversion/Inport/3		
	ego_fault		Timed: 5
□	ft_fuelSys_Arch/HW_SW Conversion/Inport/4		
	map_fault_timed		Timed: 10
	map_fault_conditional		Conditional: Sa

Develop Architecture

Perform Hazard Analysis

Link Analysis to Design Artifacts

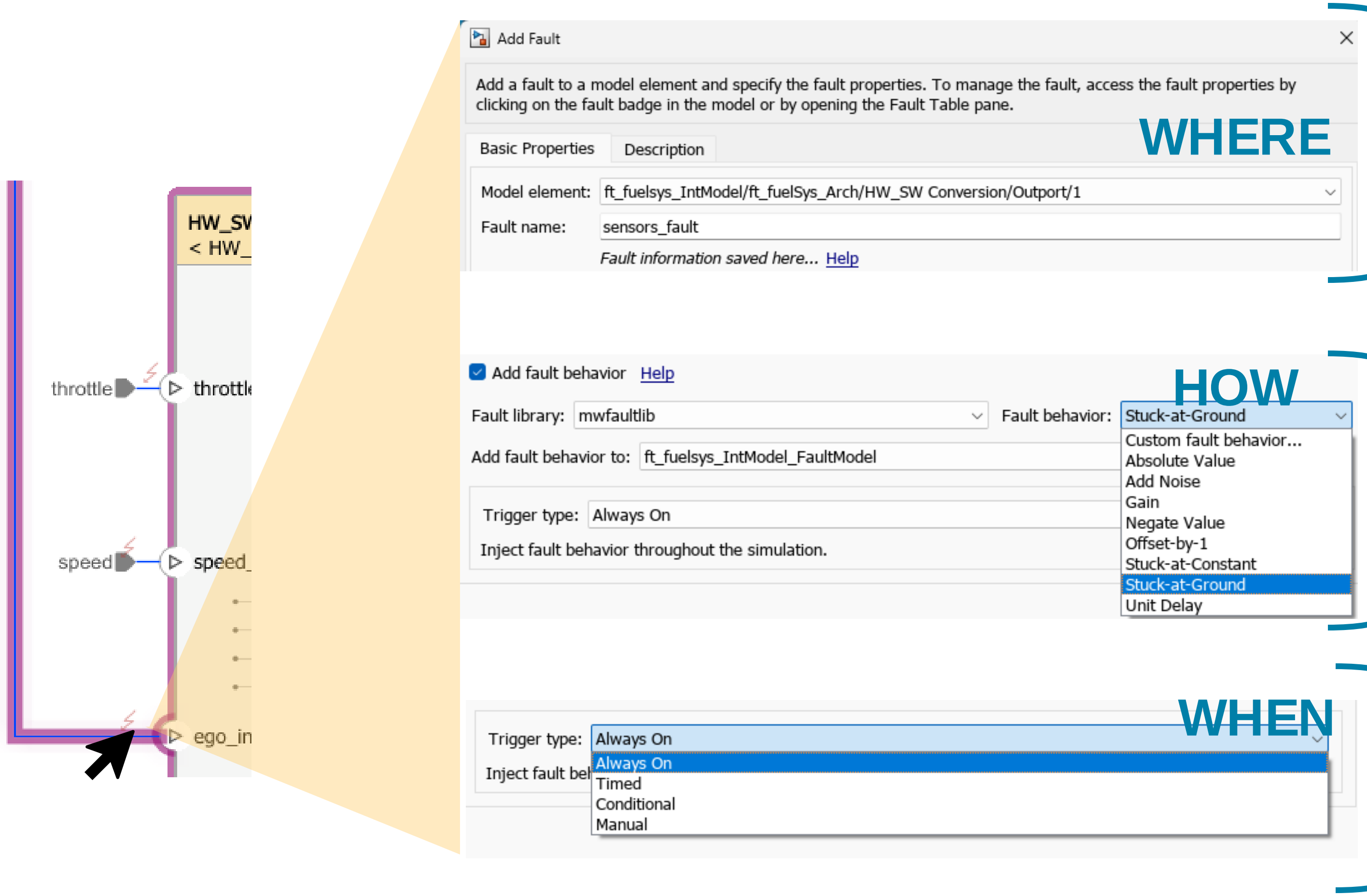
» **Characterize Faults**

Static Checks

Inject Faults & Explore Effects

Validate through Simulation

Model complex faults and easily define WHERE, HOW and WHEN to apply them in simulations



Add Fault

Add a fault to a model element and specify the fault properties. To manage the fault, access the fault properties by clicking on the fault badge in the model or by opening the Fault Table pane.

Basic Properties | Description

Model element: ft_fuelsys_IntModel/ft_fuelSys_Arch/HW_SW Conversion/Outport/1

Fault name: sensors_fault

Fault information saved here... Help

☑ Add fault behavior Help

Fault library: mwfaultlib

Fault behavior: Stuck-at-Ground

Add fault behavior to: ft_fuelsys_IntModel_FaultModel

Trigger type: Always On

Inject fault behavior throughout the simulation.

Trigger type: Always On

Inject fault bel

WHERE

Where the faults is applied in the model

HOW

What's the behavior when injected

WHEN

Time/condition when to be injected

Develop Architecture

Perform Hazard Analysis

Link Analysis to Design Artifacts

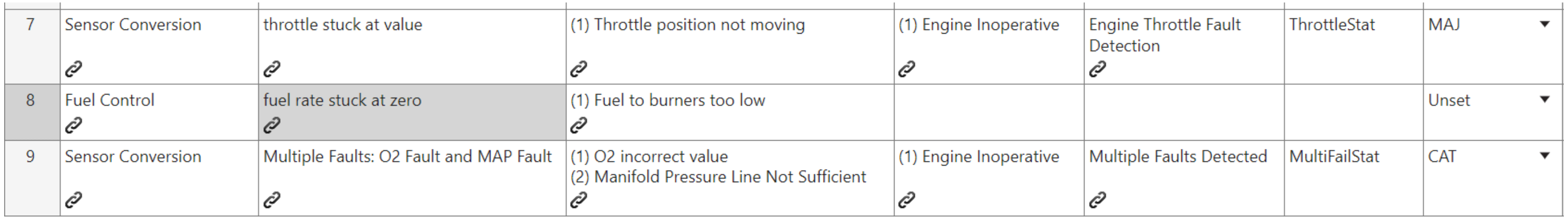
Characterize Faults

» Static Checks

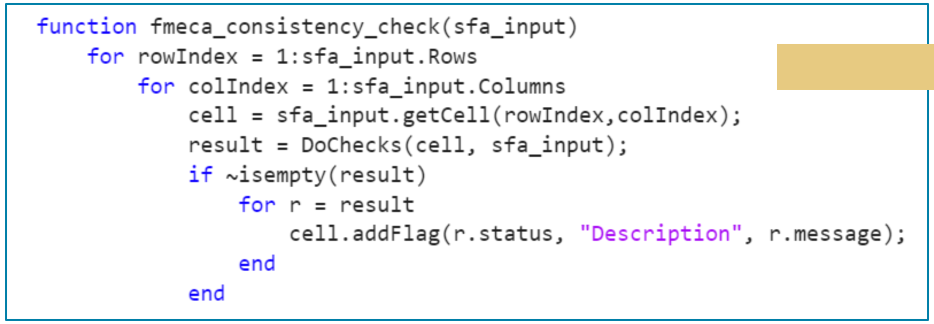
Inject Faults & Explore Effects

Validate through Simulation

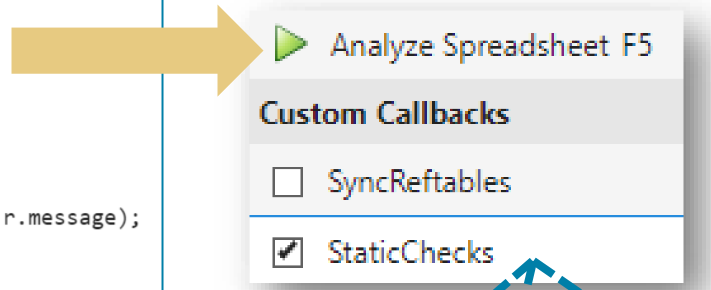
Analyze your safety analysis tables using MATLAB scripts for completeness analysis

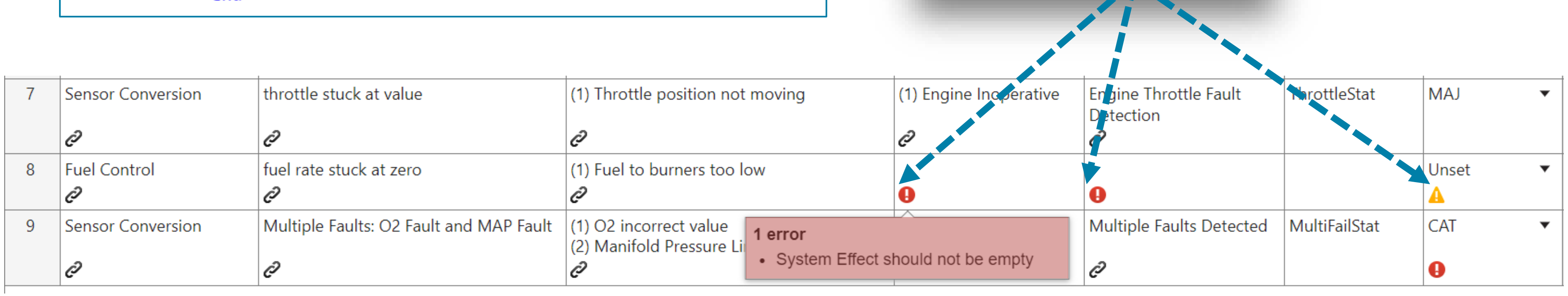


7	Sensor Conversion	throttle stuck at value	(1) Throttle position not moving	(1) Engine Inoperative	Engine Throttle Fault Detection	ThrottleStat	MAJ ▾
8	Fuel Control	fuel rate stuck at zero	(1) Fuel to burners too low				Unset ▾
9	Sensor Conversion	Multiple Faults: O2 Fault and MAP Fault	(1) O2 incorrect value (2) Manifold Pressure Line Not Sufficient	(1) Engine Inoperative	Multiple Faults Detected	MultiFailStat	CAT ▾



```
function fmeca_consistency_check(sfa_input)
    for rowIndex = 1:sfa_input.Rows
        for colIndex = 1:sfa_input.Columns
            cell = sfa_input.getCell(rowIndex,colIndex);
            result = DoChecks(cell, sfa_input);
            if ~isempty(result)
                for r = result
                    cell.addFlag(r.status, "Description", r.message);
                end
            end
```





7	Sensor Conversion	throttle stuck at value	(1) Throttle position not moving	(1) Engine Inoperative	Engine Throttle Fault Detection	ThrottleStat	MAJ ▾
8	Fuel Control	fuel rate stuck at zero	(1) Fuel to burners too low	❗	❗		Unset ▾ ⚠
9	Sensor Conversion	Multiple Faults: O2 Fault and MAP Fault	(1) O2 incorrect value (2) Manifold Pressure Li		Multiple Faults Detected	MultiFailStat	CAT ▾ ❗

1 error
- System Effect should not be empty

Develop Architecture

Perform Hazard Analysis

Link Analysis to Design Artifacts

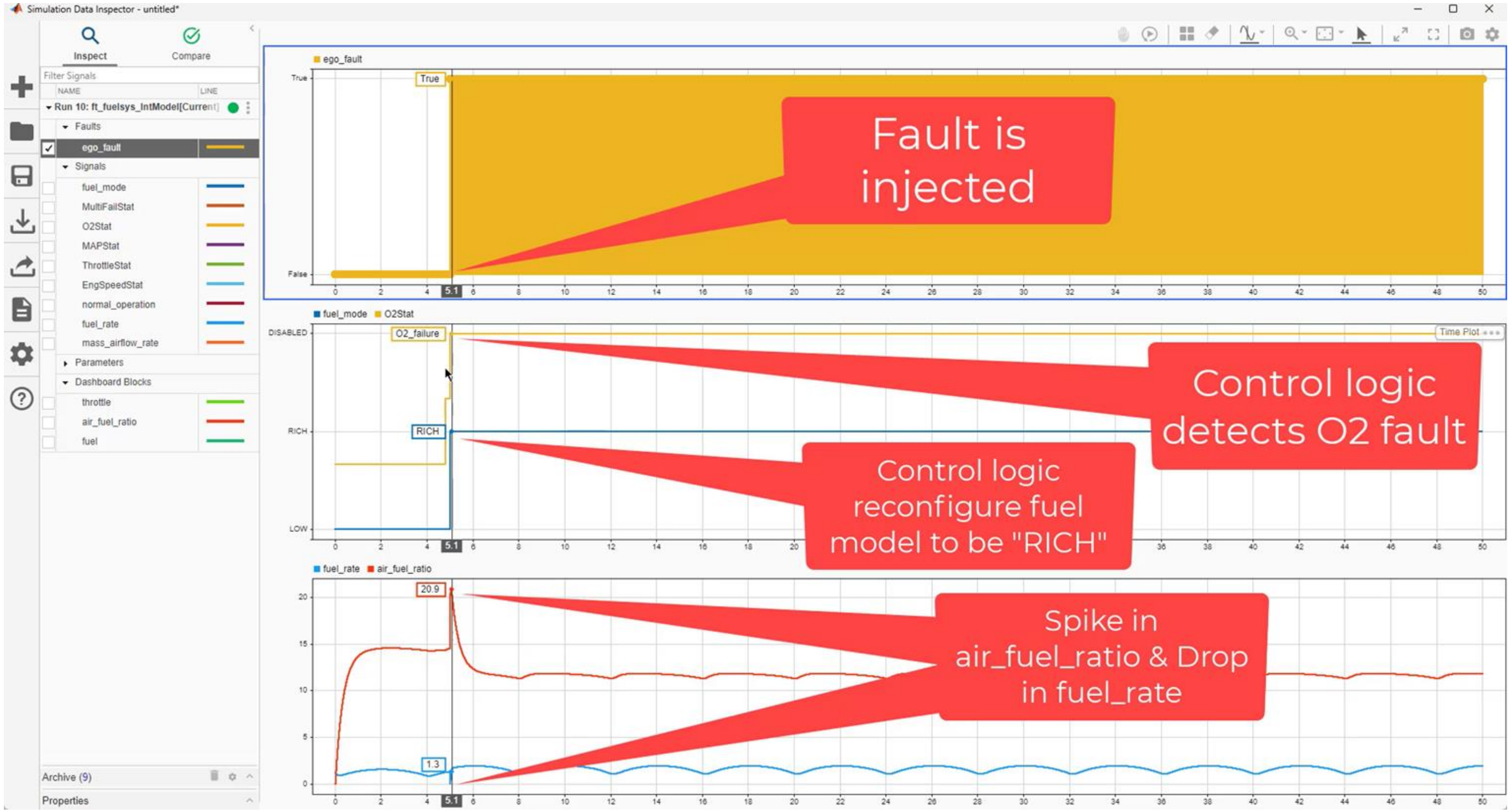
Characterize Faults

Static Checks

» Inject Faults & Explore Effects

Validate through Simulation

Inject faults in system simulations to explore effects and confirm detection mechanisms have triggered

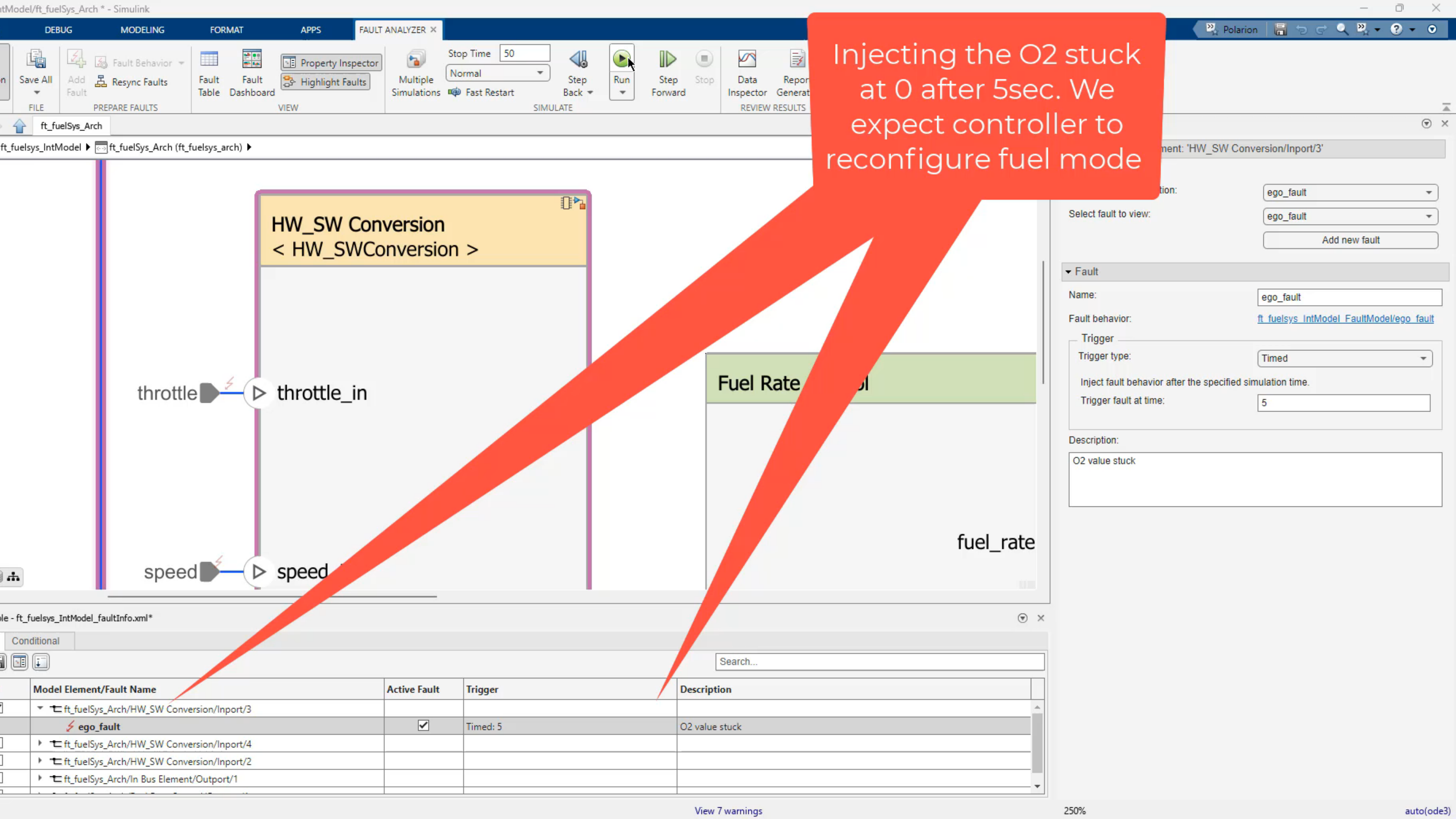


Fault is injected

Control logic detects O2 fault

Control logic reconfigure fuel model to be "RICH"

Spike in air_fuel_ratio & Drop in fuel_rate



Injecting the O2 stuck at 0 after 5sec. We expect controller to reconfigure fuel mode

Stop Time: 50

Normal

ment: 'HW_SW Conversion/Inport/3'

tion: ego_fault

Select fault to view: ego_fault

Add new fault

Fault

Name: ego_fault

Fault behavior: ft_fuelsys_IntModel_FaultModel/ego_fault

Trigger

Trigger type: Timed

Inject fault behavior after the specified simulation time.

Trigger fault at time: 5

Description: O2 value stuck

le - ft_fuelsys_IntModel_faultInfo.xml*

Search...

Model Element/Fault Name	Active Fault	Trigger	Description
ft_fuelSys_Arch/HW_SW Conversion/Inport/3			
ego_fault	☑	Timed: 5	O2 value stuck
ft_fuelSys_Arch/HW_SW Conversion/Inport/4			
ft_fuelSys_Arch/HW_SW Conversion/Inport/2			
ft_fuelSys_Arch/In Bus Element/Outport/1			

Develop Architecture

Perform Hazard Analysis

Link Analysis to Design Artifacts

Characterize Faults

Static Checks

Inject Faults & Explore Effects

» **Validate through Simulation**

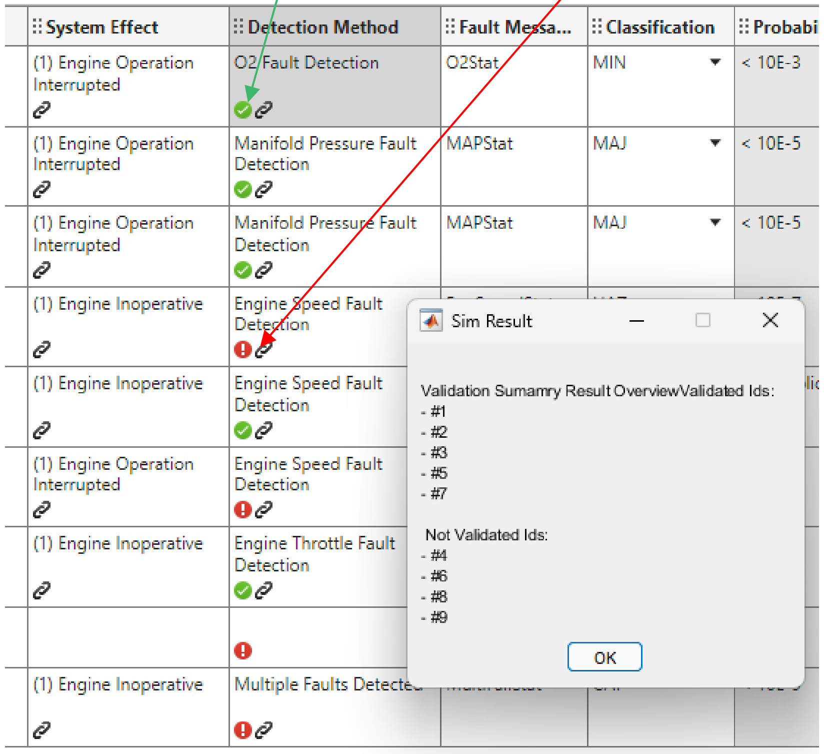
Perform simulations to validate your FMECA and correct design logic in case of fault not detected

Run

Run For All Faults

Fault detected

Fault Not Detected



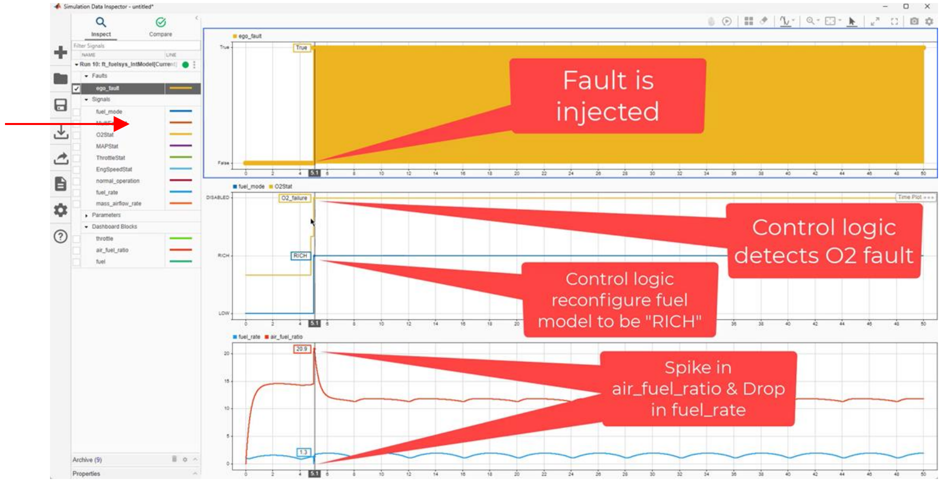
System Effect	Detection Method	Fault Messa...	Classification	Probabi
(1) Engine Operation Interrupted	O2 Fault Detection ✓	O2Stat	MIN	< 10E-3
(1) Engine Operation Interrupted	Manifold Pressure Fault Detection ✓	MAPStat	MAJ	< 10E-5
(1) Engine Operation Interrupted	Manifold Pressure Fault Detection ✓	MAPStat	MAJ	< 10E-5
(1) Engine Inoperative	Engine Speed Fault Detection ❗			
(1) Engine Inoperative	Engine Speed Fault Detection ✓			
(1) Engine Operation Interrupted	Engine Speed Fault Detection ❗			
(1) Engine Inoperative	Engine Throttle Fault Detection ✓			
	❗			
(1) Engine Inoperative	Multiple Faults Detected ❗			

Sim Result

Validation Sumamry Result OverviewValidated Ids:
- #1
- #2
- #3
- #5
- #7

Not Validated Ids:
- #4
- #6
- #8
- #9

OK



Fault is injected

Control logic detects O2 fault

Control logic reconfigure fuel model to be "RICH"

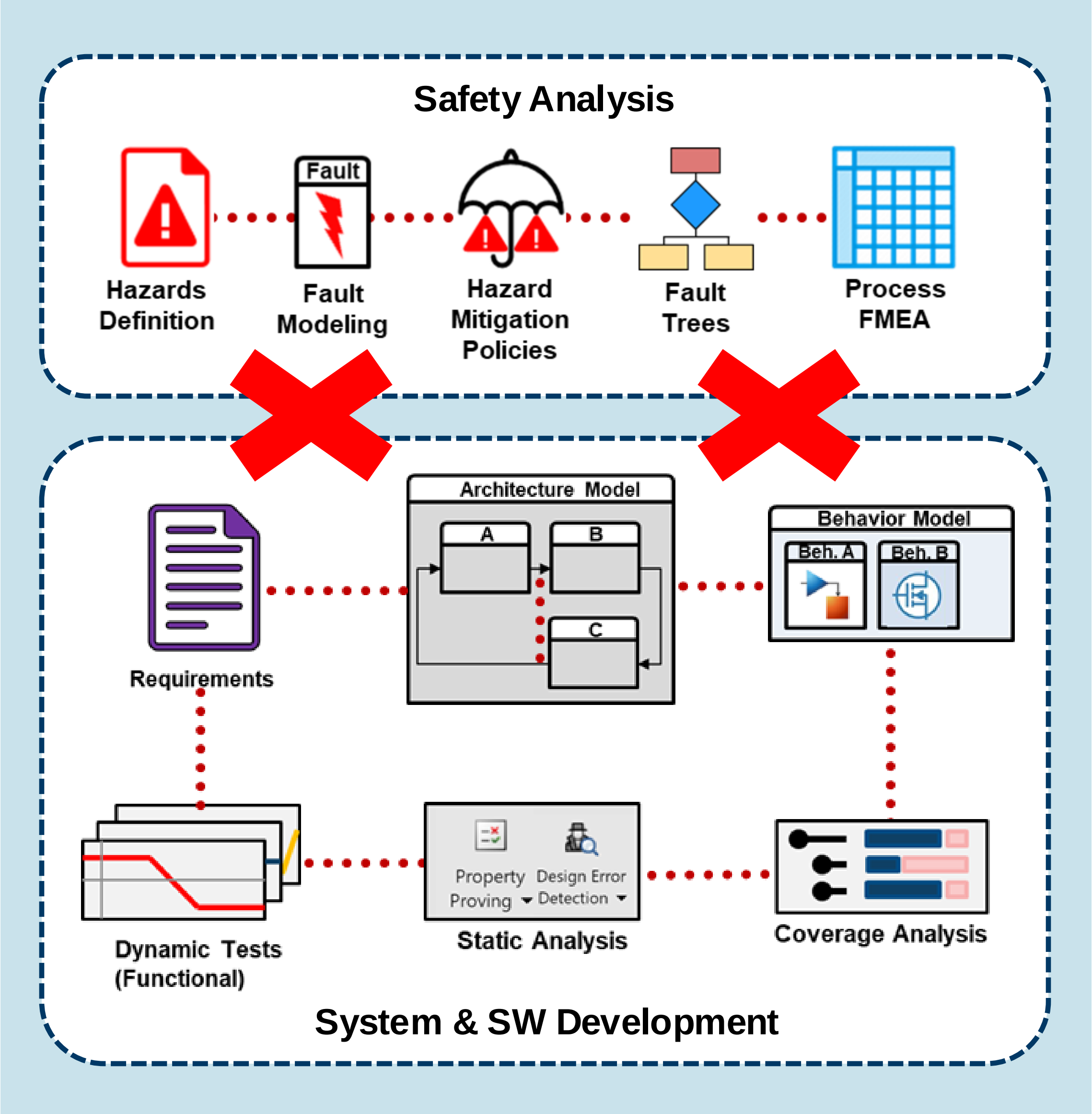
Spike in air_fuel_ratio & Drop in fuel_rate

Today’s Agenda

- Importance of safety in product development
- System: Model-based safety analysis workflow
- Component: Fault injection modeling
- Case Study: Aircraft fuel system
- **Conclusion**

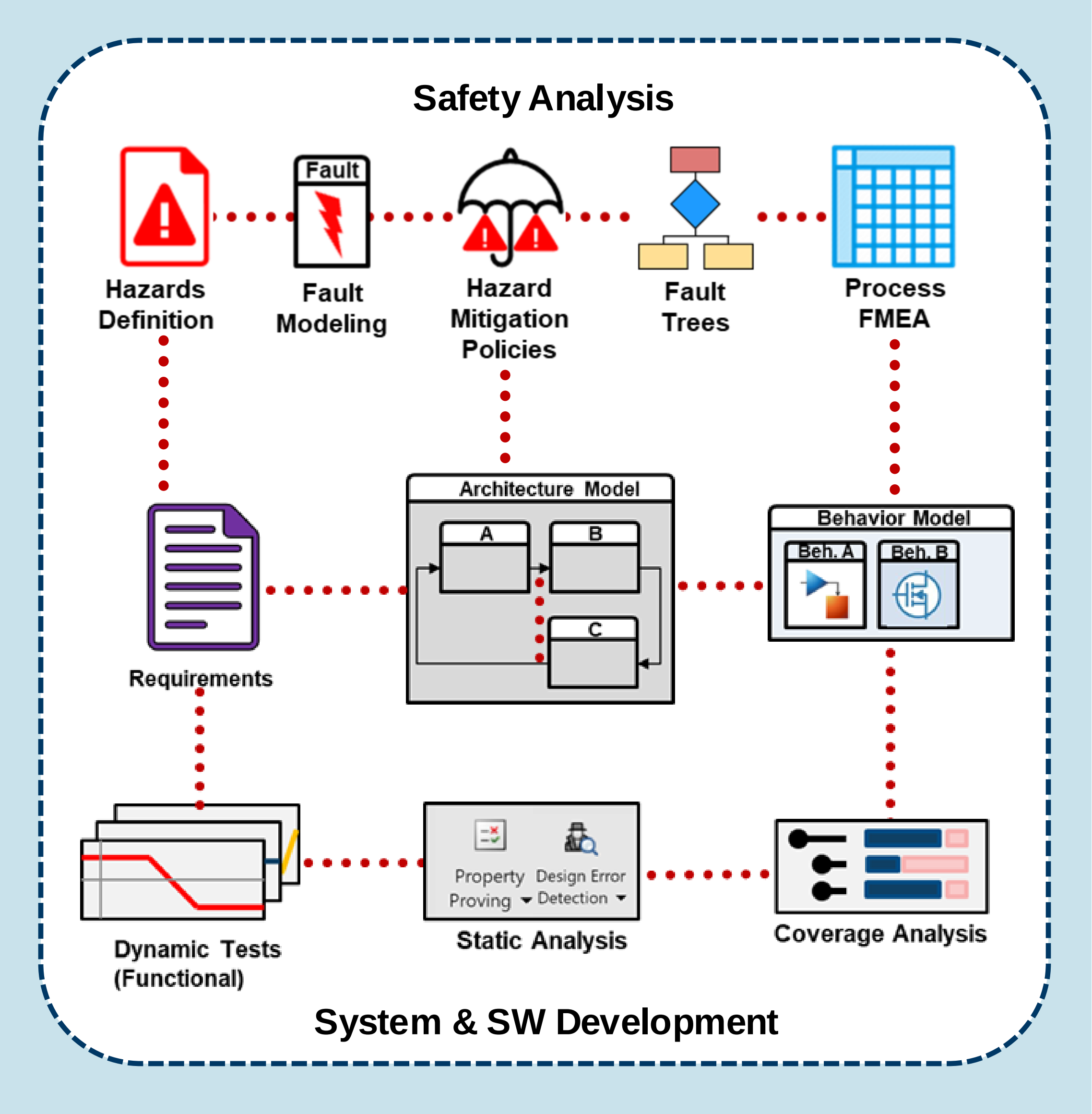
Key Takeaways

- **Traditional Safety Analysis is**
  - Decoupled from design work
  - Complex and complicated
  - Error-prone



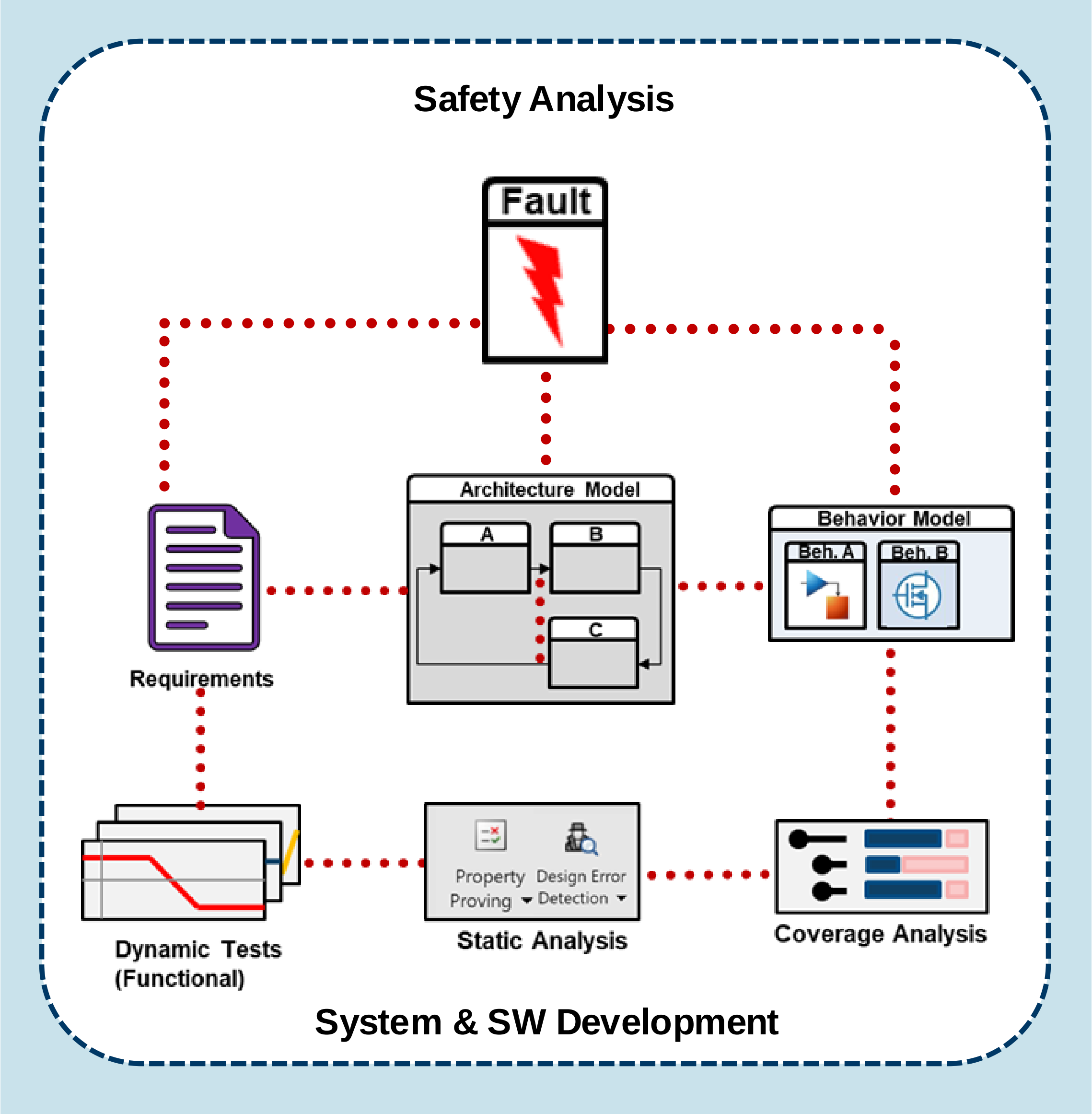
Key Takeaways

- **<u>Model-Based</u> Safety Analysis is**
  - **Fully integrated** with design
  - **Fully traceable** w.r.t. changes
  - **Consistent**
  - **Validated** by simulation



Key Takeaways

- **Enhanced Fault Modeling**
  - **Separated** from design
  - Supports **complex** faults
  - **Analyze** fault effects
  - **Connected** to hazards



Simulink Fault Analyzer

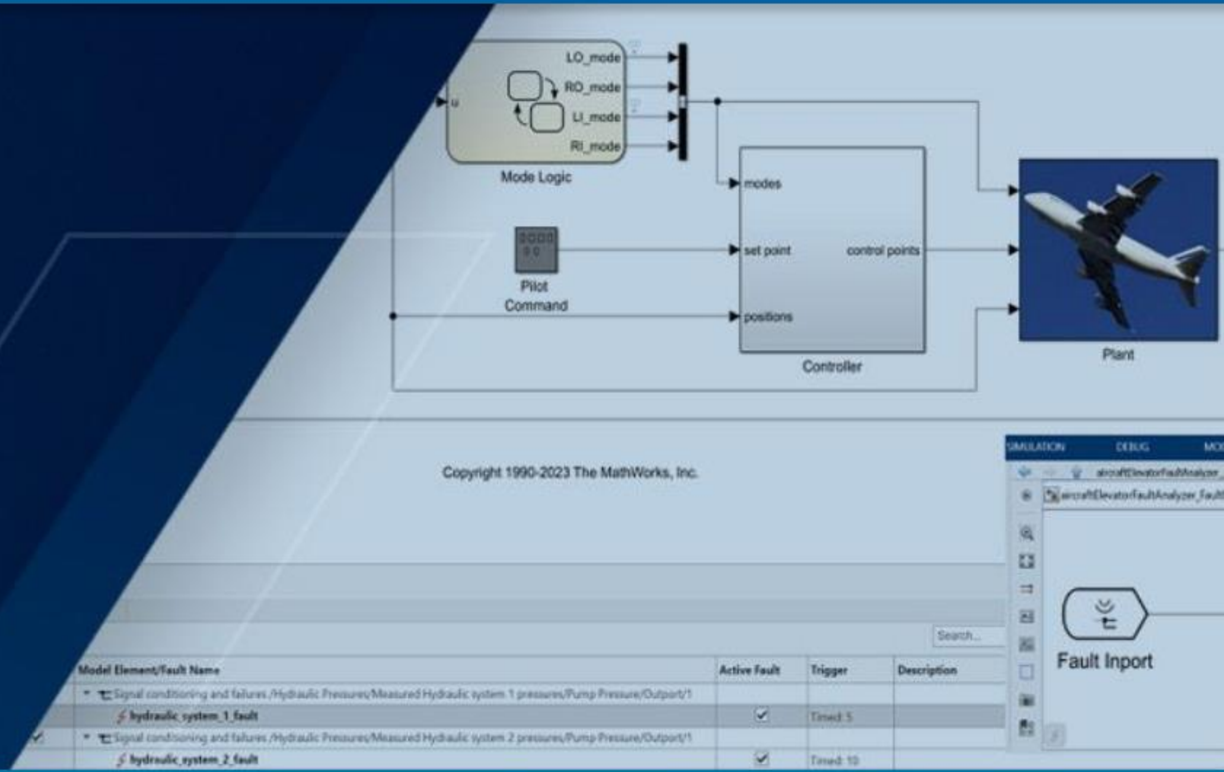
Simulink Fault Analyzer

Model faults and analyze effects

Get a free trial

View pricing

Have questions? Contact sales.



Model Element/Fault Name	Active Fault	Trigger	Description
Signal conditioning and failures /Hydraulic Pressures/Measured Hydraulic system 1 pressures/Pump Pressure/Outport/1			
hydraulic_system_1_fault	✓	Timed: 5	
Signal conditioning and failures /Hydraulic Pressures/Measured Hydraulic system 2 pressures/Pump Pressure/Outport/1			
hydraulic_system_2_fault	✓	Timed: 10	

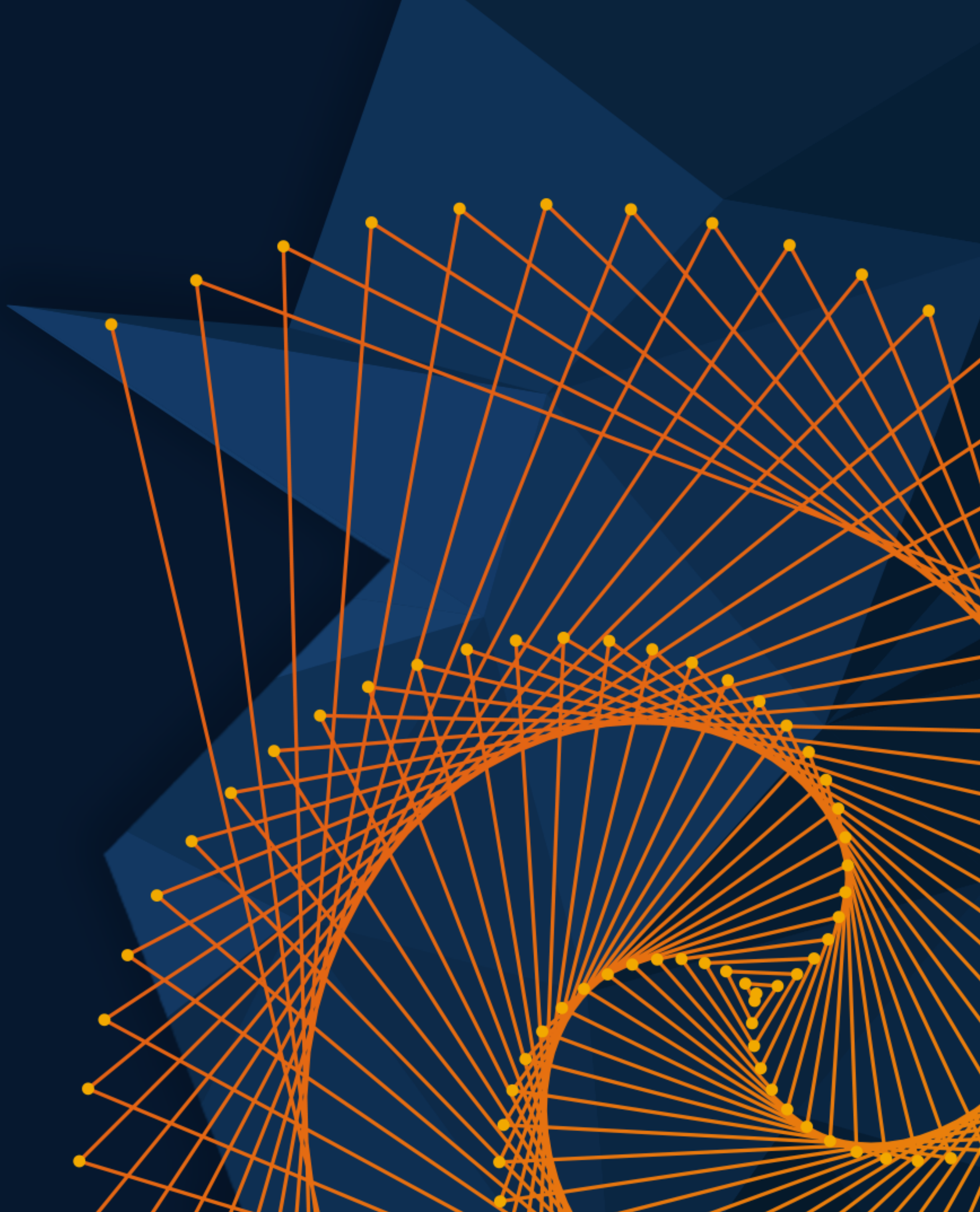
Simulink Fault Analyzer enables systematic fault effect and safety analysis using simulation.

Simulink Fault Analyzer performs fault injection simulations without modifying your design. Faults can be timed or triggered by system conditions. You can manage faults that are modeled in Simulink, Simscape, and System Composer. Fault effects can be analyzed with Simulation Data Inspector. You can conduct fault sensitivity

MATLAB EXPO

UNITED KINGDOM

Thank you!



MATLAB EXPO

Continue your experience: Register for MATLAB EXPO 2024

November 13–14, 2024 | Online

Further your connections, deepen your knowledge, and enhance your skills.

- **Hands-On Workshops**
- **Technology Showcase**
- **What’s New**

Register at **matlabexpo.com/online**

MathWorks®