

MathWorks
**AUTOMOTIVE
CONFERENCE 2024**
Europe

Fault Injection Testing and simulation-based FMEA

Dr. Marc Segelken, MathWorks



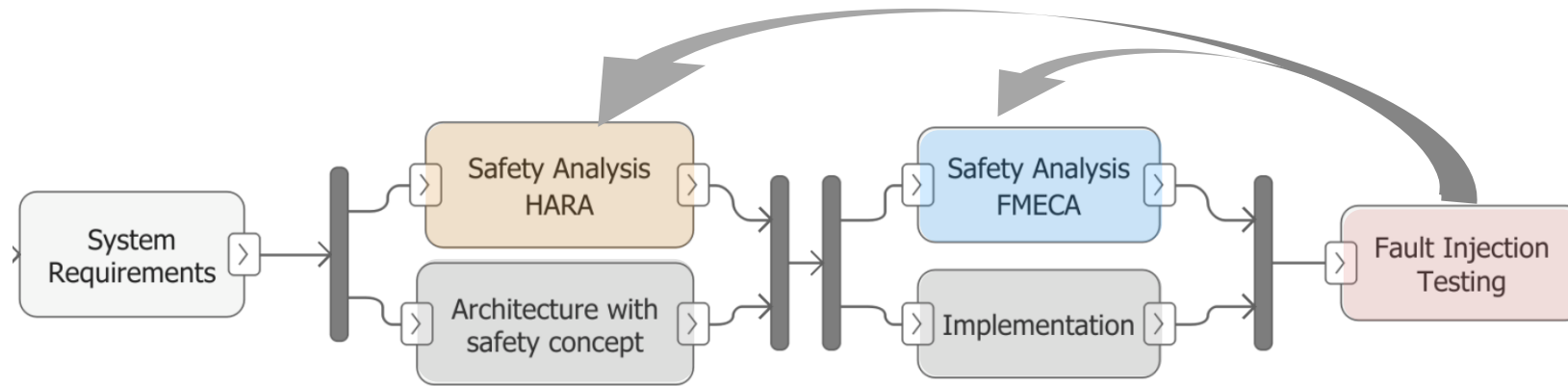
Agenda

- Safety Analysis, like Failure Mode, Effects, and Criticality Analysis (FMECA)
- Fault Injection Testing

A	B	C	D	E	F	G	H	I
ID	Function Name	Function Path	Functional Failure	Detection Method	Detection Logic Path	Local Effect	System Effect	Derived Req
1	Function 1	Model/Package1/Block1	Loss of...	Model Check	SimulinkModel/ControlLogic/Monitor	Loss of Protection	Loss of shutdown	ModuleName:#1
2	Function 2	Model/Package1/Block2	Loss of...	Model Check	SimulinkModel/ControlLogic/Monitor1	Loss of Redundancy	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



Safety Analysis, Detection and Mitigation, Verification



■ Safety Analysis

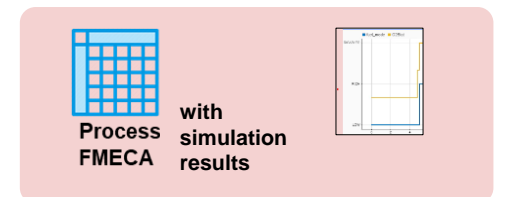
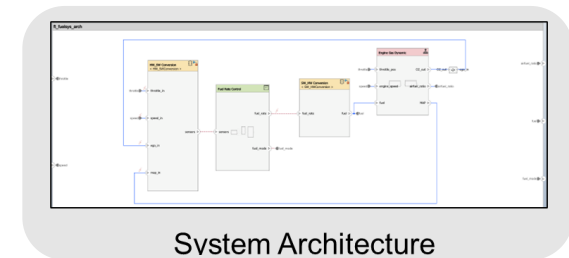
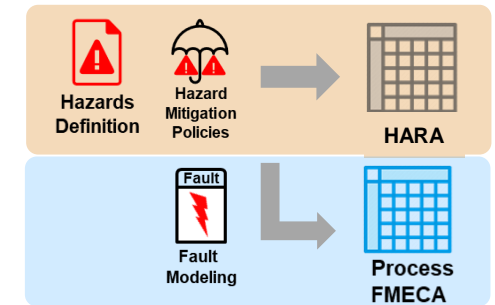
- Identify hazardous events and mitigation strategy:
HARA (Hazard Analysis & Risk Assessment)
- Failure Mode, Effects, and Criticality Analysis (**FMECA**)
for detailed list of failure modes, their causes and effects

■ Safety Concept Development

- Implementation of **mitigation strategies with detection mechanisms**

■ Verification and Validation of safety mechanisms in Implementation

- **Fault injection testing**



How Safety Analysis Is Done Today

A	B	C	D	E	F	G	H	I
ID	Function Name	Function Path	Script Type	Script Content	Local Effect	System Effect	Derived Req	
1	Function 1	Model/Package	Create Script	001 ' Oracle Create Table Script	/Monitor	Loss of Protection	Loss of shutdown	ModuleName:#1
2	Function 2	Model/Package		002 Function TableHeader(Table, Options)	/Monitor1	Loss of Redundacy	None	
3	Function 3	Model/Package		003 TableHeader = "----" & vbLf & "----"	/Monitor2	None	None	
4	Function 4	Model/Package		004 TableHeader = TableHeader & Object	/Monitor1	Loss of Control	Control	ModuleName:#4

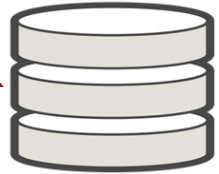
Script Type: Create Script

123

```

001 ' Oracle Create Table Script
002 Function TableHeader(Table, Options)
003   TableHeader = "----" & vbLf & "----"
004   TableHeader = TableHeader & Object
005   TableHeader = TableHeader & vbLf &
006 End Function
007
008 Function nested_table_col_properties(C
009   nested_table_col_properties = ""
010   Dim Columns
011   Dim Column
012   Dim ColType
013   Dim ColTypeType
014   Dim Clause
015   Set Columns = Table.Children("Col
016   Dim ColumnTable
017   For Each Column In Columns
018     Set ColType = Column.Property
019     ColTypeType = ColType.Property
020     If ColTypeType = "Object" Then
021       Clause = nested table col

```

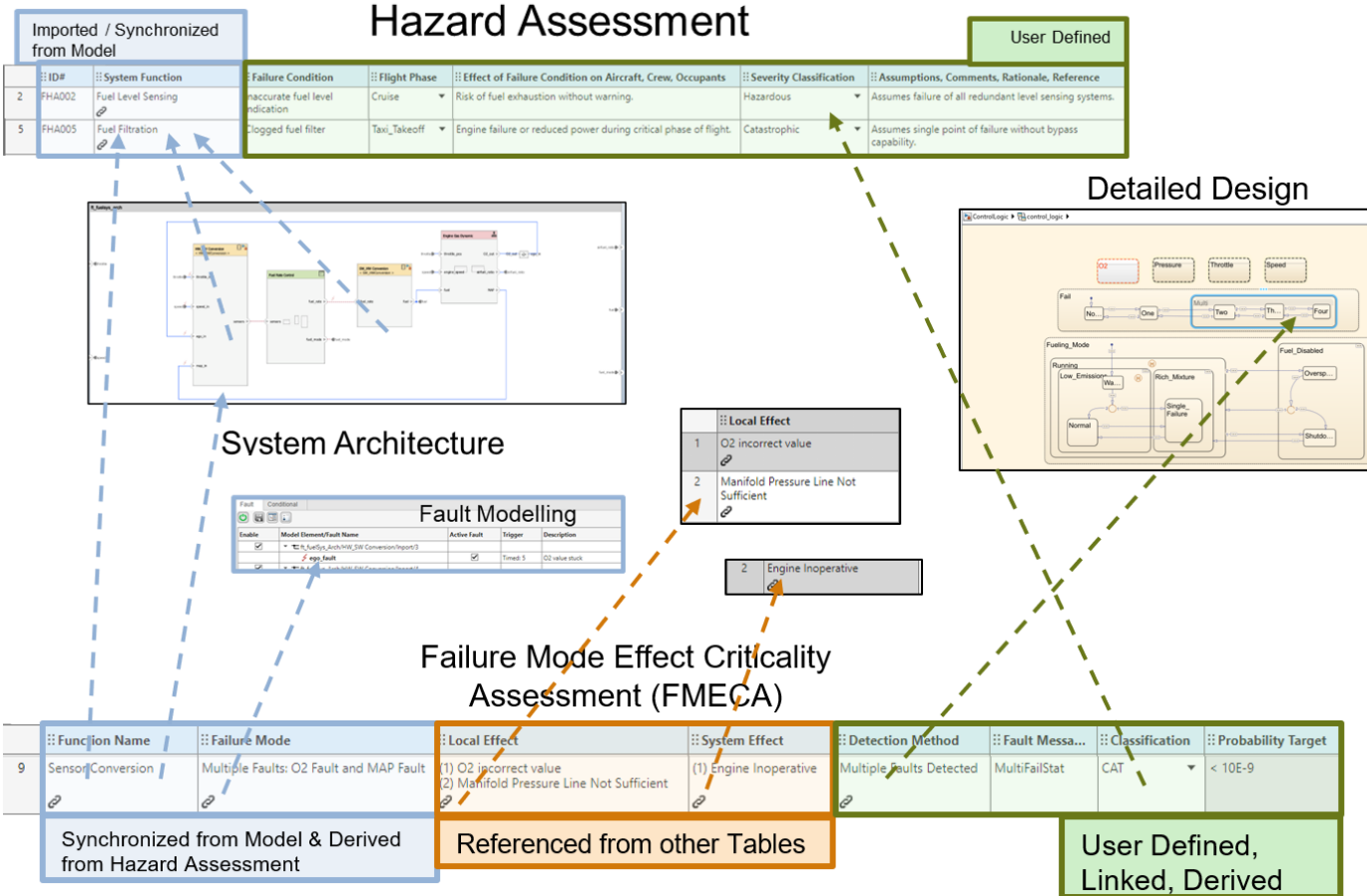


Requirements

Non Model-Based Safety Analysis is ...

- ... **decoupled** from design work
- ... **complex and complicated**
- ... **error-prone**

Why Model-Based Safety Analysis is the way to go

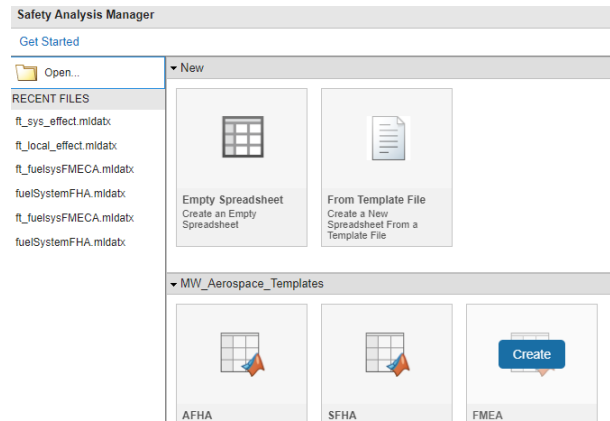


Model-Based Safety Analysis is ...

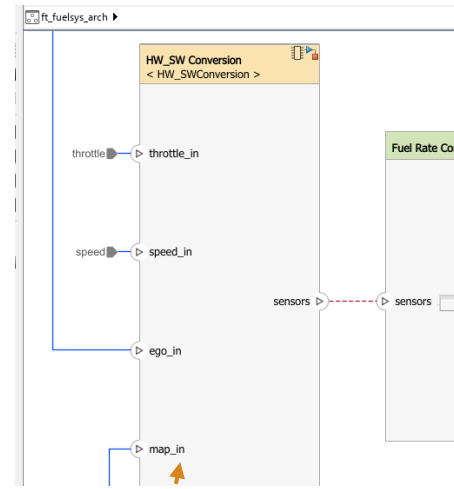
- ... **fully integrated** with design
- ... **fully traceable** (changes etc.)
- ... **consistent & validated**
- Synergy: fault modeling, FTA, tests

Capture Analysis, Link to Architecture & Perform Validation Checks

Instantiate From Template



Link To Architecture



Execute Validation Checks

	Local Effect	System Effect
	!	!
1 error	<ul style="list-style-type: none"> Local Effect should not be empty 	(1) Engine Operation Interrupted

Function Name	Failure Mode	Local Effect
1 Sensor Conversion	O2 stuck	(1) O2 incorrect value
2 Sensor Conversion	Manifold Pressure Zero	(1) Manifold Pressure Line Not Sufficient
3 Sensor Conversion	Manifold Pressure Zero	(1) Manifold Pressure Line Not Sufficient
4 Sensor Conversion	speed high	(1) Engine Speed too high

Properties

Cell Spreadsheet

Description

Cell Description

Links

Related to:

[HW_SW Conversion](#)

Example Walkthrough – instantiate analysis

The screenshot displays the MathWorks environment with a spreadsheet, a dropdown menu, a Callbacks Editor window, and a Properties panel.

Spreadsheet: A table with columns: Function Name, Failure Mode, Failure Rate (E-06), Flight Phase, Failure Effect, Detection Method, and Comments. Row 1 is currently selected.

Flight Phase Dropdown: A dropdown menu is open, showing options: Unset, Unset, Taxi_Takeoff, OnGround, Climb, Cruise, Descent, Approach, and Landing. A red arrow points from the 'Climb' option to the 'AnalyzeFcn*' function in the Callbacks Editor.

Callbacks Editor: A window showing MATLAB code for the 'AnalyzeFcn*' function. The code includes comments and logic for checking data types and links in the spreadsheet.

```

1  % This script fetches the value of the cells for which a completeness fl
2  % would be calculated.
3  % The following completeness checks are provided:
4  % - flight phase should not be set to their default value (i.e. Unset
5  %   If so an error flag will be added
6  % - failure mode, failure effect and detection method should not be e
7  %   If so a warning flag will be added
8  % - failure rate should contain a number. If not a warning will be ac
9  % - Function name should have a link to a model element.
10 %   If not a warning will be added
11 %
12 % Copyright 1984-2023 The MathWorks, Inc
13
14 for rowIndex = 1:sfa_spreadsheet.Rows
15 % Get relevant cells for which completeness flag would be calculate
16 funcname      = getCell(sfa_spreadsheet,rowIndex,"Function Name");
17 failmod       = getCell(sfa_spreadsheet,rowIndex,"Failure Mode");
18 flightphase   = getCell(sfa_spreadsheet,rowIndex,"Flight Phase");
19 failurerate  = getCell(sfa_spreadsheet,rowIndex,"Failure Rate (E
20 failureeffect = getCell(sfa_spreadsheet,rowIndex,"Failure Effect'
21 detecmethod   = getCell(sfa_spreadsheet,rowIndex,"Detection Methc
22
23 % Define the list of cell for which we want to raise a warning if
24 % there is no link to a model element
25 warn_cell_nolink_list_handle = {funcname};
26

```

Properties Panel: A panel on the right side of the interface showing document attributes. It includes a table with columns 'Property' and 'Value'.

Property	Value
System	
SubSystem	
Equipment ATA	
Description	
Author	
Revision	
Status	

Flags: 0 errors; 0 warnings; 0 checks

Grouped by: Row

No flags

- Templates with predefined data type
- Templates with predefined analysis function

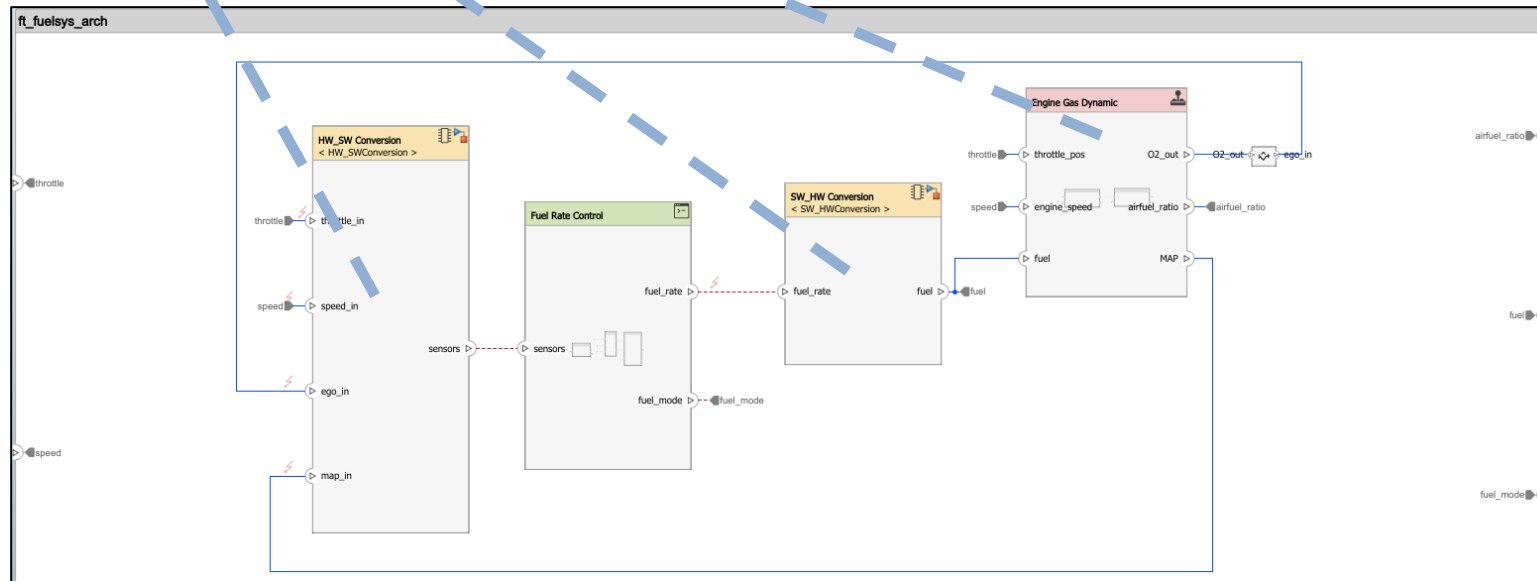
Example Walkthrough – fill the analysis and link with Architecture

Imported / Sync from Model

Hazard Assessment

User Defined

ID#	System Function	Failure Condition	Flight Phase	Effect of Failure Condition on Aircraft, Crew, Occupants	Severity Classification	Assumptions, Comments, Rationale, Reference
2	FHA002 Fuel Level Sensing	Inaccurate fuel level indication	Cruise	Risk of fuel exhaustion without warning.	Hazardous	Assumes failure of all redundant level sensing systems.
5	FHA005 Fuel Filtration	Clogged fuel filter	Taxi_Takeoff	Engine failure or reduced power during critical phase of flight.	Catastrophic	Assumes single point of failure without bypass capability.

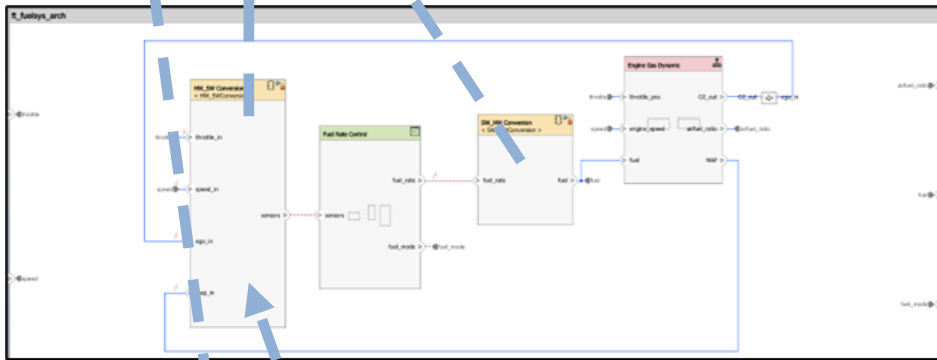


System Architecture

Example Walkthrough – fill the analysis and link with Architecture

Hazard Assessment

Imported / Synchronized from Model		User Defined				
ID#	System Function	Failure Condition	Flight Phase	Effect of Failure Condition on Aircraft, Crew, Occupants	Severity Classification	Assumptions, Comments, Rationale, Reference
2	FHA002 Fuel Level Sensing	Inaccurate fuel level indication	Cruise	Risk of fuel exhaustion without warning.	Hazardous	Assumes failure of all redundant level sensing systems.
5	FHA005 Fuel Filtration	Clogged fuel filter	Taxi_Takeoff	Engine failure or reduced power during critical phase of flight.	Catastrophic	Assumes single point of failure without bypass capability.



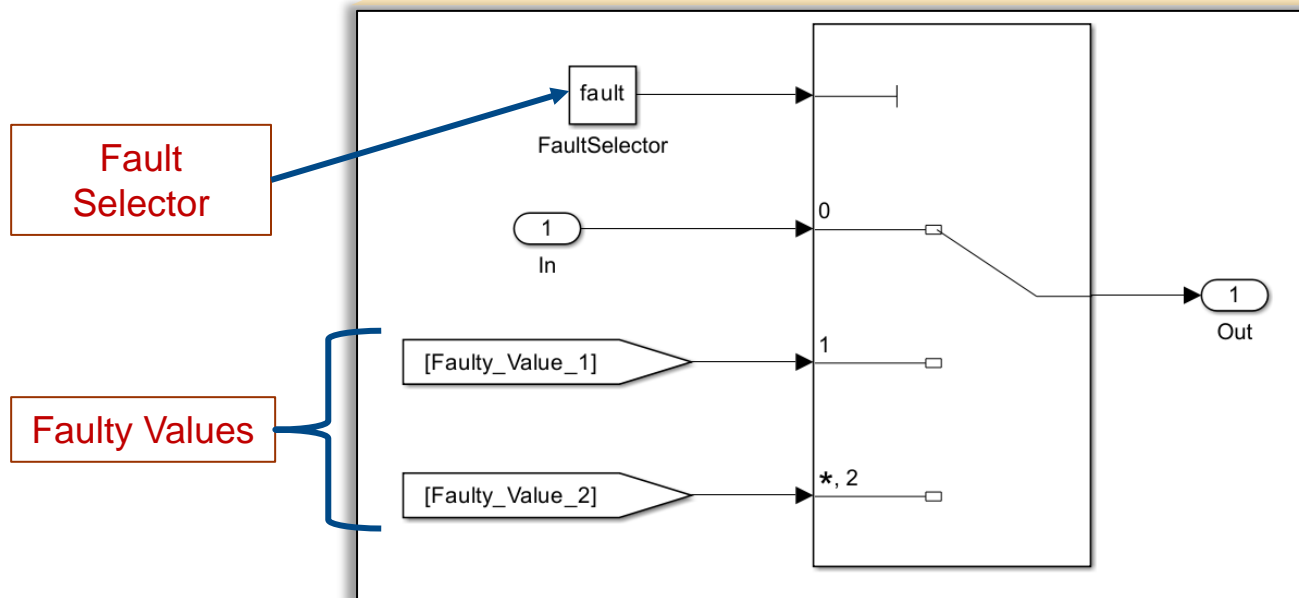
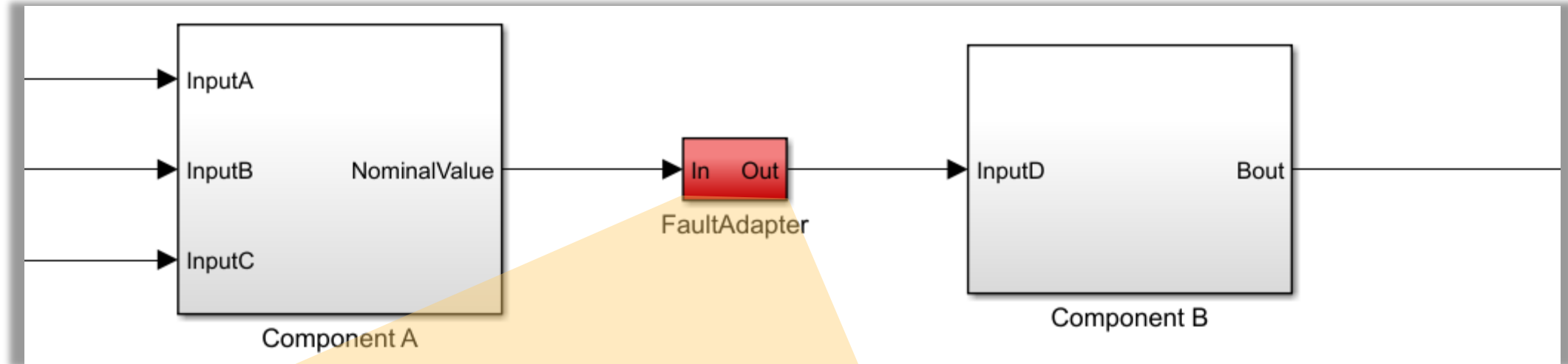
System Architecture

Failure Mode Effect Criticality Assessment (FMECA)

ID#	Function Name	Failure Mode	Local Effect	System Effect	Detection Method	Fault Message	Classification	Probability Target
9	Sensor Conversion							

Synchronized from Model & Derived from Hazard Assessment

Fault Modeling Before Simulink Fault Analyzer



- **Modifies the design**
- **Can inadvertently change simulation behavior**
- **Difficult to analyze effects**
- **How do faults relate to hazards?**

Model faults without modifying Design

Design Model

Fault Model

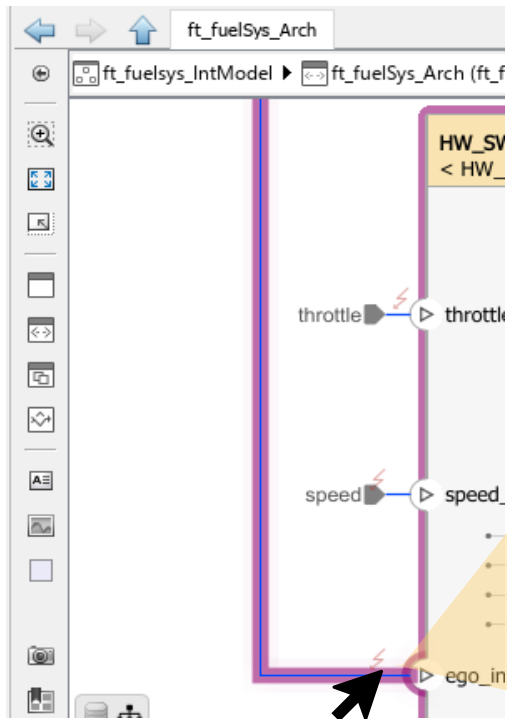
Fault Table - ft_fuelsys_IntModel_faultInfo.xml

Enable	Model Element/Fault Name	Active Fa
<input type="checkbox"/>	ft_fuelSys_Arch/HW_SW Conversion/l...	

Fault Input

Fault Output

Model faults without modifying Design



The 'Add Fault' dialog box is shown, detailing the configuration of a fault. The dialog is divided into sections for 'Basic Properties', 'Fault behavior', and 'Trigger type'. The 'WHERE' section (Basic Properties) shows the model element 'ft_fuelSys_IntModel/ft_fuelSys_Arch/HW_SW Conversion/Output/1' and the fault name 'sensors_fault'. The 'HOW' section (Fault behavior) shows the 'Fault library' set to 'mwfaultlib' and the 'Fault behavior' set to 'Stuck-at-Ground'. The 'WHEN' section (Trigger type) shows the 'Trigger type' set to 'Always On'. The dialog also includes a checkbox for 'Add fault behavior' and a section for 'Inject fault behavior throughout the simulation'.

WHERE

Model element: ft_fuelSys_IntModel/ft_fuelSys_Arch/HW_SW Conversion/Output/1
Fault name: sensors_fault
Fault information saved here... [Help](#)

Add fault behavior [Help](#)

Fault library: mwfaultlib Fault behavior: Stuck-at-Ground
Custom fault behavior...
Absolute Value
Add Noise
Gain
Negate Value
Offset-by-1
Stuck-at-Constant
Stuck-at-Ground
Unit Delay

Inject fault behavior throughout the simulation.

Trigger type: Always On

Inject fault behavior throughout the simulation.

Trigger type: Always On
Always On
Timed
Conditional
Manual

Where the faults is applied in the model

What's the behavior when injected

Time/condition when to be injected

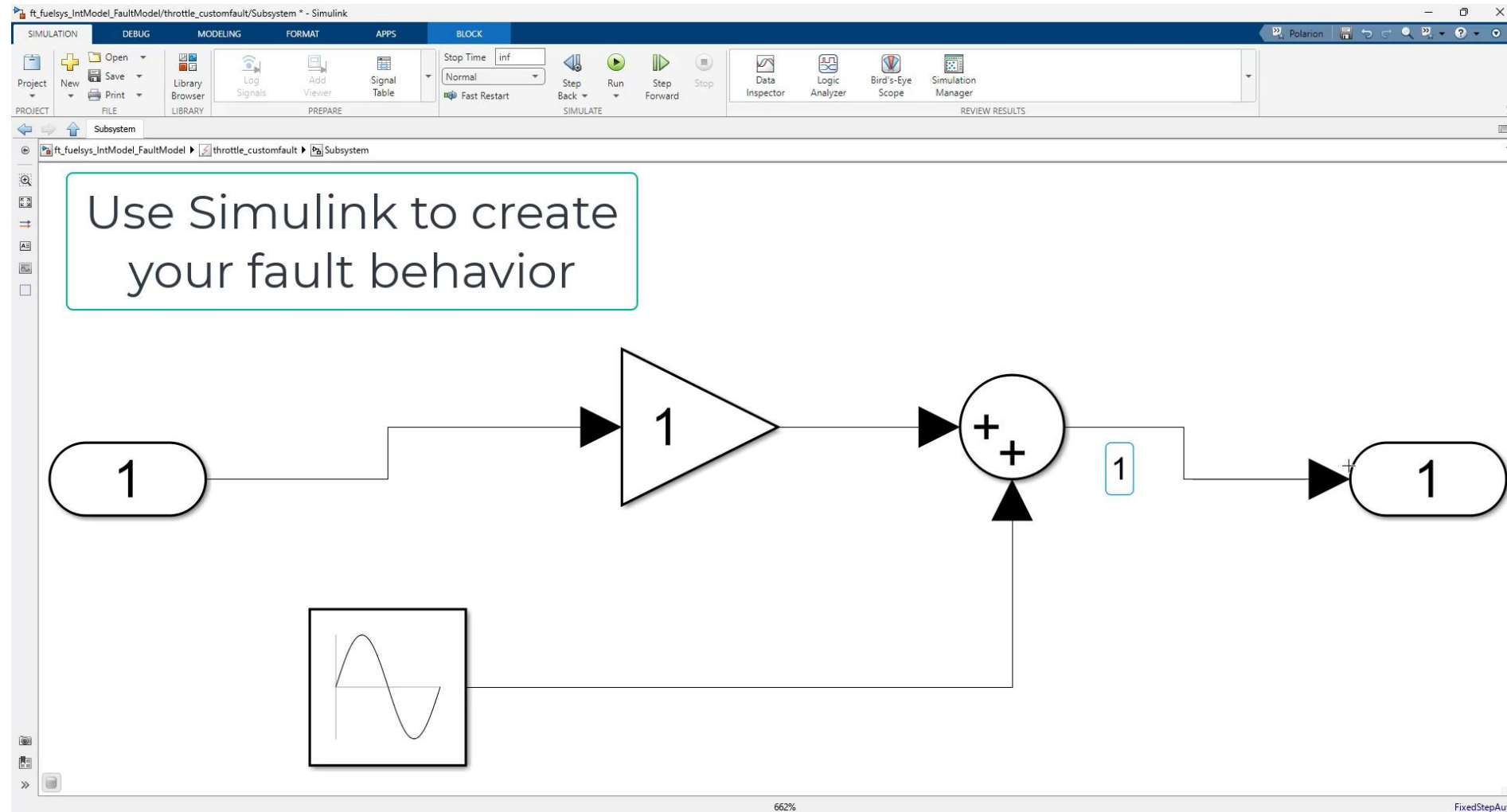
Example Walkthrough – model faults – define the “were”

The screenshot shows the Simulink software interface with the 'Add Fault' dialog box open. The dialog box is titled 'Add Fault' and contains the following fields and options:

- Model element:** ft_fuelsys_IntModel/ft_fuelSys_Arch/In Bus Element/Output/1
- Fault name:** throttle_customfault
- Fault information directory:** C:\Users\marcob\Demos\ft_fuelcontrolsystem_sa\04_fault_modelling
- 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.**

Buttons at the bottom of the dialog are 'OK', 'Cancel', and 'Help'. A red callout bubble points to the 'Fault name' field with the text 'Give it a Name'. A green callout bubble points to the 'Fault behavior' dropdown with the text 'Control'. The background shows a Simulink diagram with a 'throttle' block and a 'HW_SW < HW_S' block.

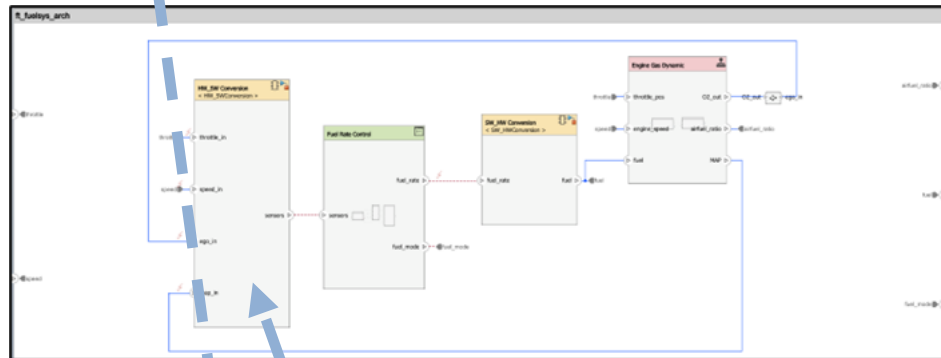
Example Walkthrough – model faults – define the “How”



Example Walkthrough – model faults

Hazard Assessment

Imported / Synchronized from Model		Hazard Assessment					User Defined
ID#	System Function	Failure Condition	Flight Phase	Effect of Failure Condition on Aircraft, Crew, Occupants	Severity Classification	Assumptions, Comments, Rationale, Reference	
2	FHA002 Fuel Level Sensing	Inaccurate fuel level indication	Cruise	Risk of fuel exhaustion without warning.	Hazardous	Assumes failure of all redundant level sensing systems.	
5	FHA005 Fuel Filtration	Clogged fuel filter	Taxi_Takeoff	Engine failure or reduced power during critical phase of flight.	Catastrophic	Assumes single point of failure without bypass capability.	



System Architecture

Fault Modelling				
Enable	Model Element/Fault Name	Active Fault	Trigger	Description
<input checked="" type="checkbox"/>	ft_fuelSys_Arch/HW_SW Conversion/Input/3			
<input checked="" type="checkbox"/>	ego_fault	<input checked="" type="checkbox"/>	Timed: 5	O2 value stuck

Failure Mode Effect Criticality Assessment (FMECA)

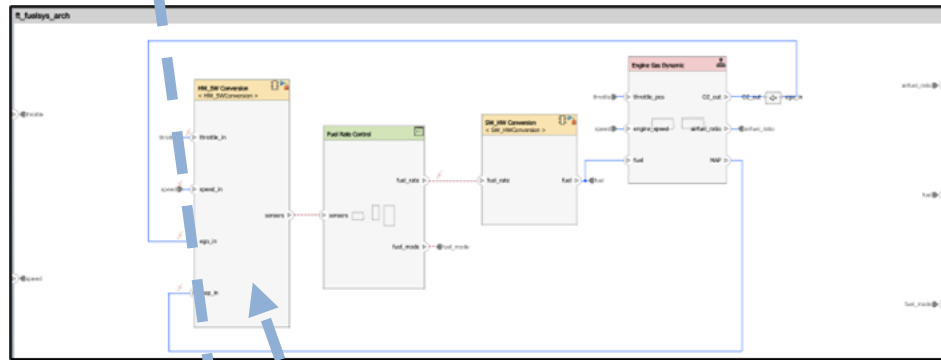
Function Name	Failure Mode	Local Effect	System Effect	Detection Method	Fault Messa...	Classification	Probability Target
9 Sensor Conversion	Multiple Faults: O2 Fault and MAP Fault						

Synchronized from Model & Derived from Hazard Assessment

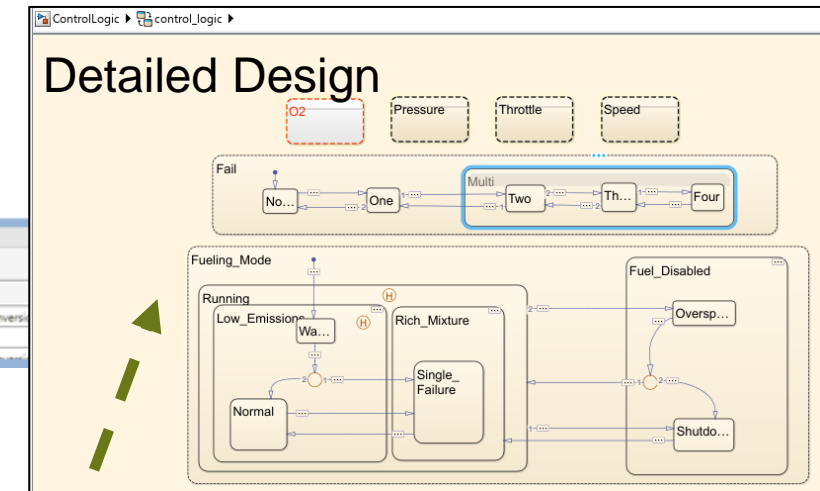
Example Walkthrough – link detection method

Hazard Assessment

Imported / Synchronized from Model		User Defined				
ID#	System Function	Failure Condition	Flight Phase	Effect of Failure Condition on Aircraft, Crew, Occupants	Severity Classification	Assumptions, Comments, Rationale, Reference
2	FHA002 Fuel Level Sensing	Inaccurate fuel level indication	Cruise	Risk of fuel exhaustion without warning.	Hazardous	Assumes failure of all redundant level sensing systems.
5	FHA005 Fuel Filtration	Clogged fuel filter	Taxi_Takeoff	Engine failure or reduced power during critical phase of flight.	Catastrophic	Assumes single point of failure without bypass capability.



System Architecture



Failure Mode Effect Criticality Assessment (FMECA)

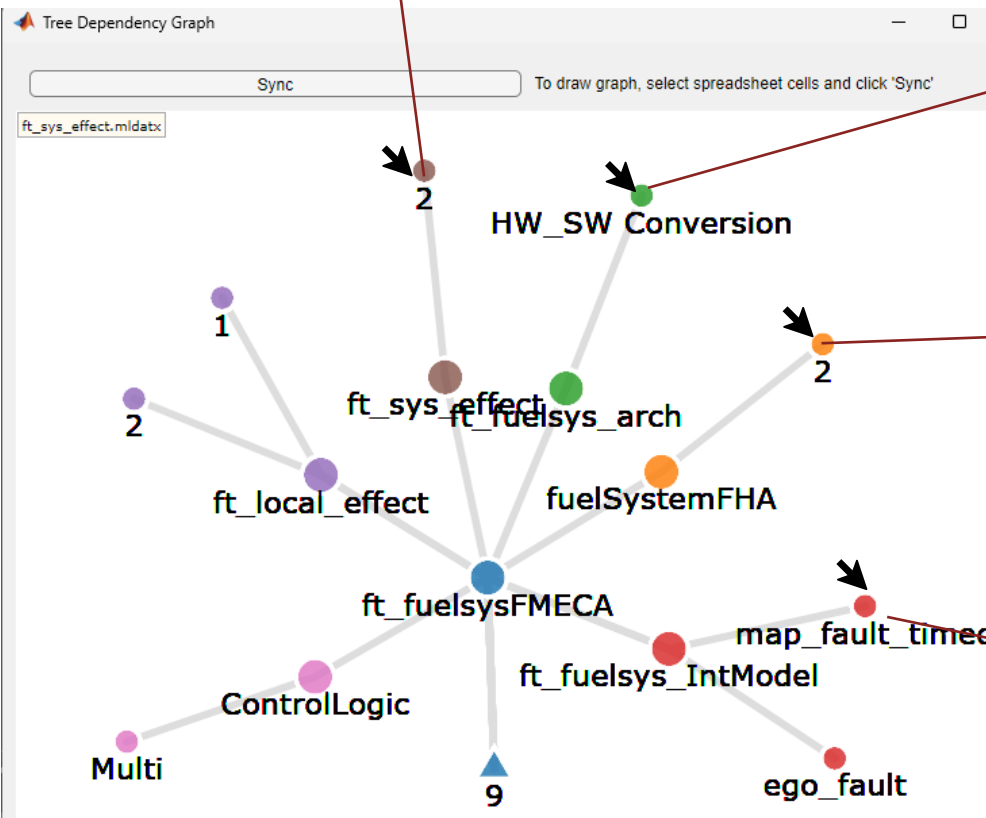
Function Name	Failure Mode	Local Effect	System Effect	Detection Method	Fault Messa...	Classification	Probability Target
Sensor Conversion	Multiple Faults: O2 Fault and MAP Fault	(1) O2 incorrect value (2) Manifold Pressure Line Not Sufficient	(1) Engine Inoperative	Multiple Faults Detected	MultiFailStat	CAT	< 10E-9

Synchronized from Model & Derived from Hazard Assessment

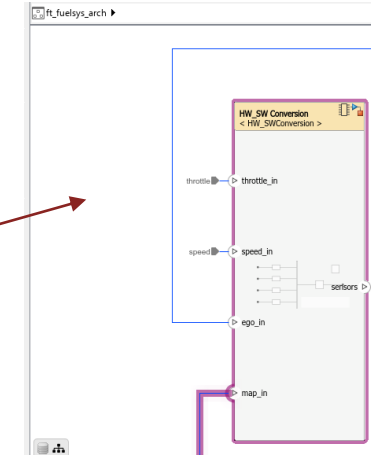
User Defined, Linked, Derived

Example Walkthrough – navigate between artifacts

ft_sys_effect x	
System Effect	
1	Engine Operation Interrupted
2	Engine Inoperative



fuelSystemFHA x					
ID#	System Function	Failure Condition	Flight Phase	Effect of Failure Co	
1	FHA001	Fuel Pump Operation	Fuel pump failure	Taxi_Takeoff	Reduced engine perfc
2	FHA002	Fuel Level Sensing	Inaccurate fuel level indication	Cruise	Risk of fuel exhaustio



Enable	Model Element/Fault Name	Active Fault	Trigger
<input type="checkbox"/>	ft_fuelSys_Arch/HW_SW Conversion/Inport/3		
	ego_fault		Timed: 5
<input type="checkbox"/>	ft_fuelSys_Arch/HW_SW Conversion/Inport/4		
	map_fault_timed		Timed: 10
	map_fault_conditional		Conditional: SampleConditional

Example Walkthrough – perform semantics checks

```

1 % This script performs a set of sanit and consistency check on the FMEA
2 % table
3 %
4 % Copyright 2023, The MathWorks, Inc
5
6 %% MAIN
7 function fmeca_consistency_check(sfa_input)
8     for rowIndex = 1:sfa_input.Rows
9         for colIndex = 1:sfa_input.Columns
10            cell = sfa_input.getCell(rowIndex,colIndex);
11            result = DoChecks(cell, sfa_input);
12            if ~isempty(result)
13                for r = result
14                    cell.addFlag(r.status, "Description", r.message);
15                end
16            end
17        end
18    end
19 end
20
21 %% Sub-function functions
22 % main helper function to switch to sub-checks based on coloumn name
23 function out = DoChecks(cell, sfa_input)
24     switch cell.ColumnLabel

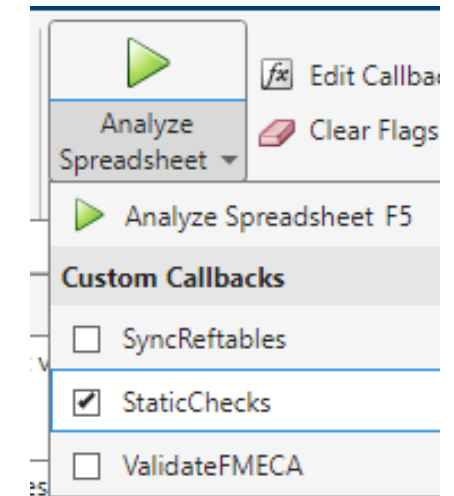
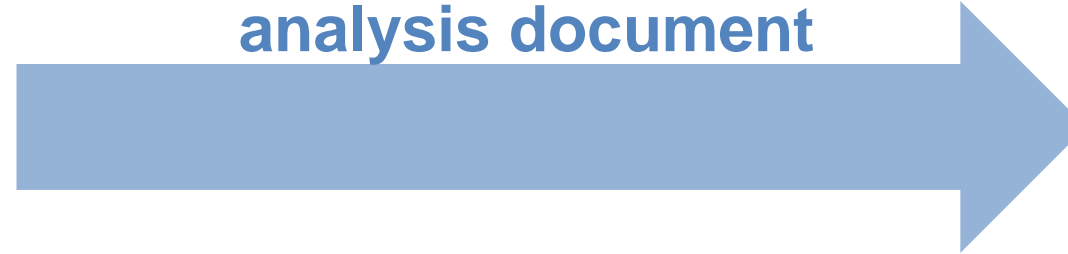
```

Define your custom checks via Matlab Script

Explore the results and check for:

- missing links to models
- missing information/empty cell
- unset values

Execute on your analysis document



	System Effect	Detection Method	Fault Messa...	Classification
8				Unset
9	(1)		MultiFailStat	CAT

1 error

- Detection Method should not be empty

Example Walkthrough – model faults – define the “when”

W_SW C
HW_SW

hrottle_i

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/In Bus Element/Outport/1

Fault name: throttle_customfault

Fault information saved here... [Help](#)

Fault information directory: C:\Users\marcob\Demos\ft_fuelcontrolsystem_sa\04_fault_modelling

Add fault behavior [Help](#)

Fault library: mwfaultlib | Fault behavior: Custom fault behavior

Add fault behavior to: ft_fuelsys_IntModel_FaultModel

Trigger type: Timed

Inject fault behavior after the specified simulation time.

Trigger fault at time: 20

OK | Cancel | Help

Injected after time X from simulation start

Active Fault	Trigger	Description
--------------	---------	-------------

Example Walkthrough – model faults – define the “when”

Map X to the model element speed

fuel_rate

fuel_mode

Property Inspector

Conditional

Conditionals are named boolean expressions composed of scalar values, operations, and scalar values. These expressions evaluate during each major timestep.

Name: speed_high

Condition Expression: $x > 10$

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

Symbols

Name	Mapped To	Value
x	Model Element	ft_fuelsys IntM

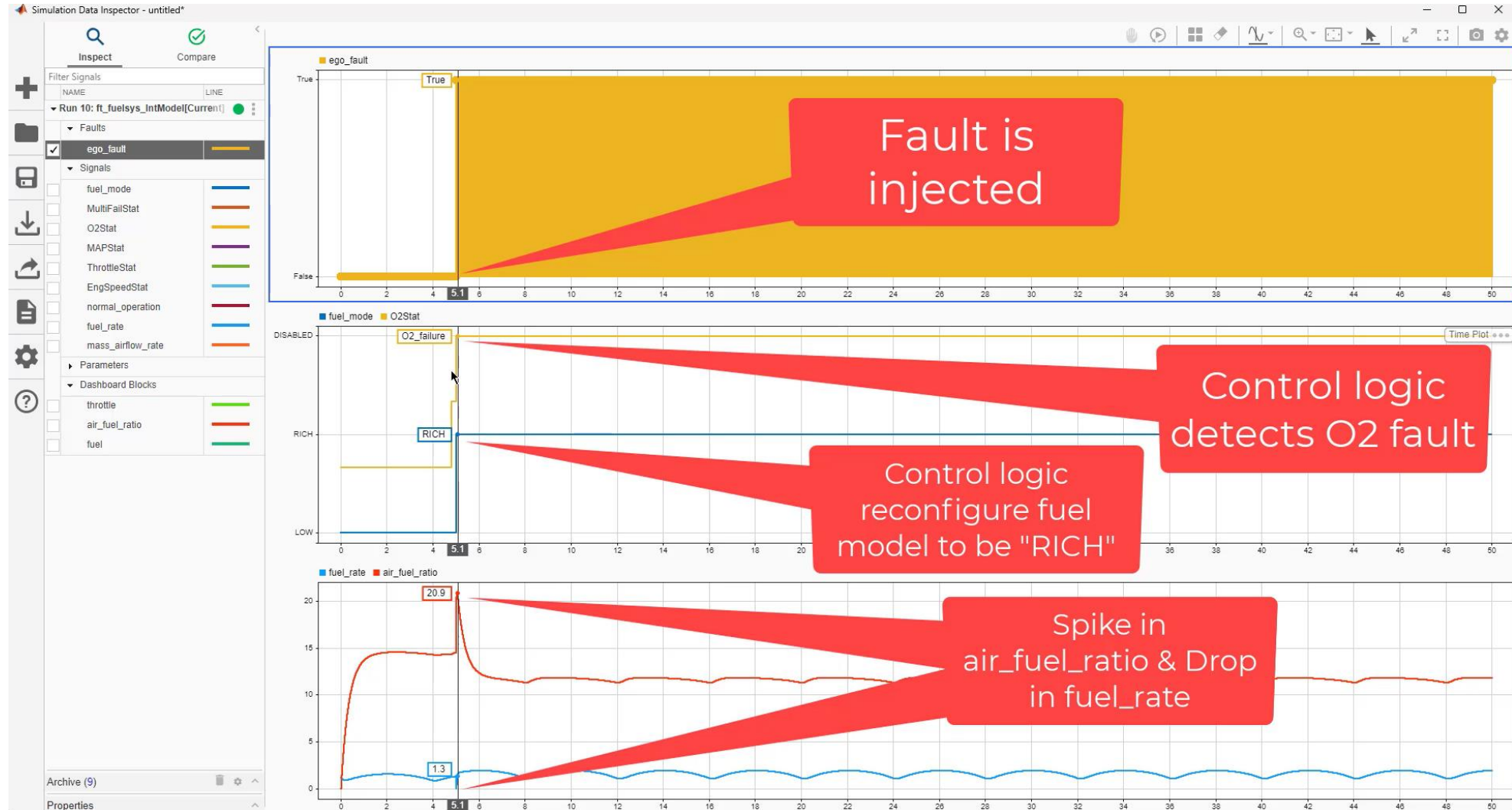
Use symbols in conditional expressions to retrieve and use the value of an expression or a model element. Expressions evaluate once at the start of simulation. Model elements evaluate during each timestep.

Associated Faults

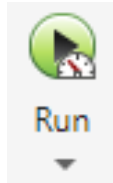
Log Activity

Condition	Log Activity
$x == true$	<input type="checkbox"/>

Example Walkthrough – use simulation for validation



Example Walkthrough – use simulation for validation



Run For All Faults

Fault detected

Fault Not Detected

System Effect	Detection Method	Fault Message	Classification	Probability
(1) Engine Operation Interrupted	O2 Fault Detection	O2Stat	MIN	< 10E-5
(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 Summary Result Overview

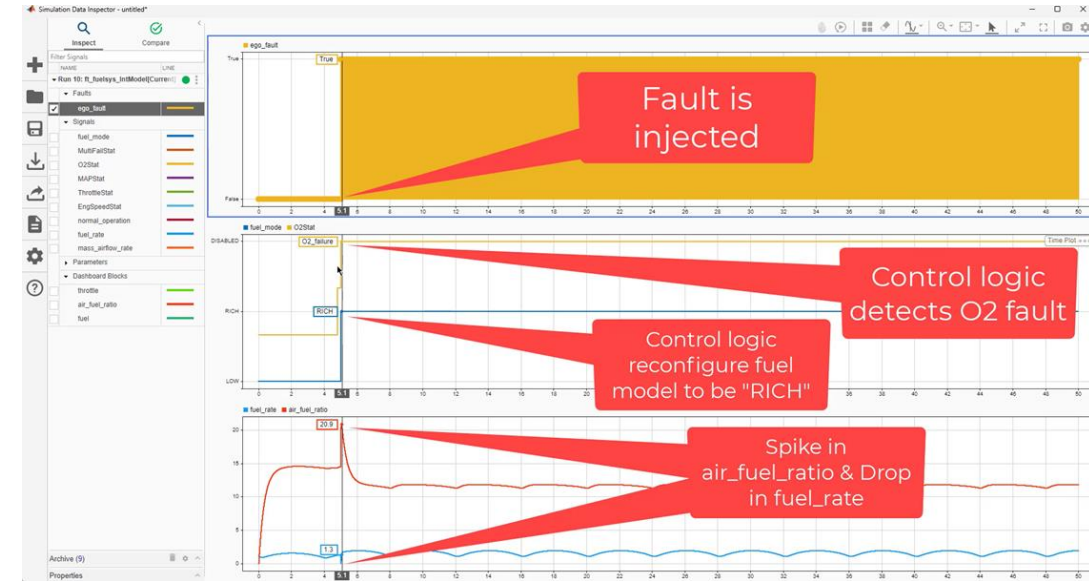
Validated Ids:

- #1
- #2
- #3
- #5
- #7

Not Validated Ids:

- #4
- #6
- #8
- #9

OK



For the cases of fault not detected:

- re-run the simulation
- use data inspector to understand what is going on
- correct your design logic

Recap – Fault Analyzer Capabilities

Instantiate From Template

Link To Architecture

Execute Validation Checks

Failure Name	Failure Mode	Local Effect	System Effect
1. Torque Conversion	O2 stuck	(1) O2 incorrect value	
2. Sensor Conversion	Manifold Pressure Zero	(1) Manifold Pressure Line Not Sufficient	
3. Sensor Conversion	Manifold Pressure Zero	(1) Manifold Pressure Line Not Sufficient	
4. Sensor Conversion	speed high	(1) Engine Speed too high	

Design Model

Fault Model

Capture Analysis, Link to Architecture & Perform Validation Checks

Simulink Fault Analyzer™

Model Faults Without Modifying Design

WHERE

Where the faults is applied in the model

HOW

What's the behavior when injected

WHEN

Time/condition when to be injected

Characterize Faults Behavior

Fault Injected

Fuel Mode Reconfigure for faulty behavior

Run For All Faults

Fault detected

Fault Not Detected

System Effect	Detection Method	Fault Mode	Classification	Prebail
(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	EngineSpeedStat	MAJ	< 10E-5
(1) Engine Inoperative	Engine Speed Fault Detection	EngineSpeedStat	MAJ	< 10E-5
(1) Engine Inoperative	Engine Throttle Fault Detection	ThrottleStat	MAJ	< 10E-5
(1) Engine Inoperative	Multiple Faults Detection	MultipleFaultsStat	MAJ	< 10E-5

Use Simulation to Validate Safety Analysis

MathWorks
**AUTOMOTIVE
CONFERENCE 2024**
Europe

Thank you

