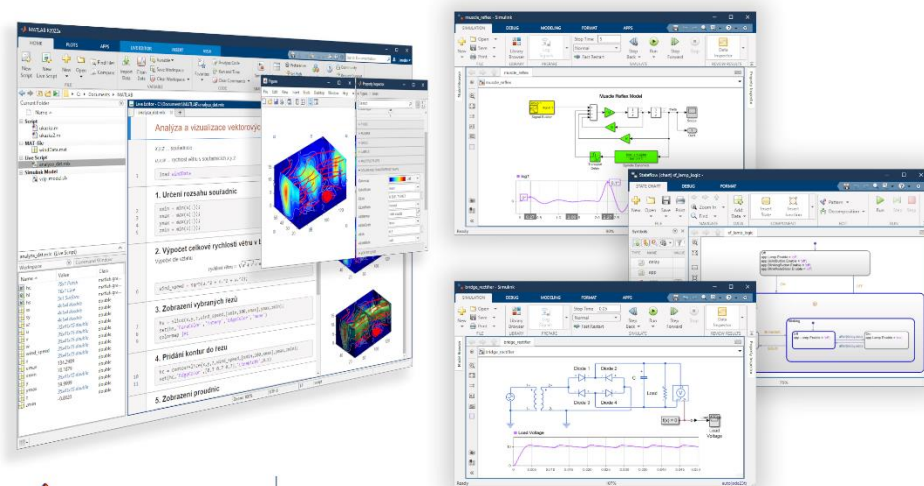


5.9.2024 Technical Computing Camp 2024

Modelování a simulace poruch v technických systémech

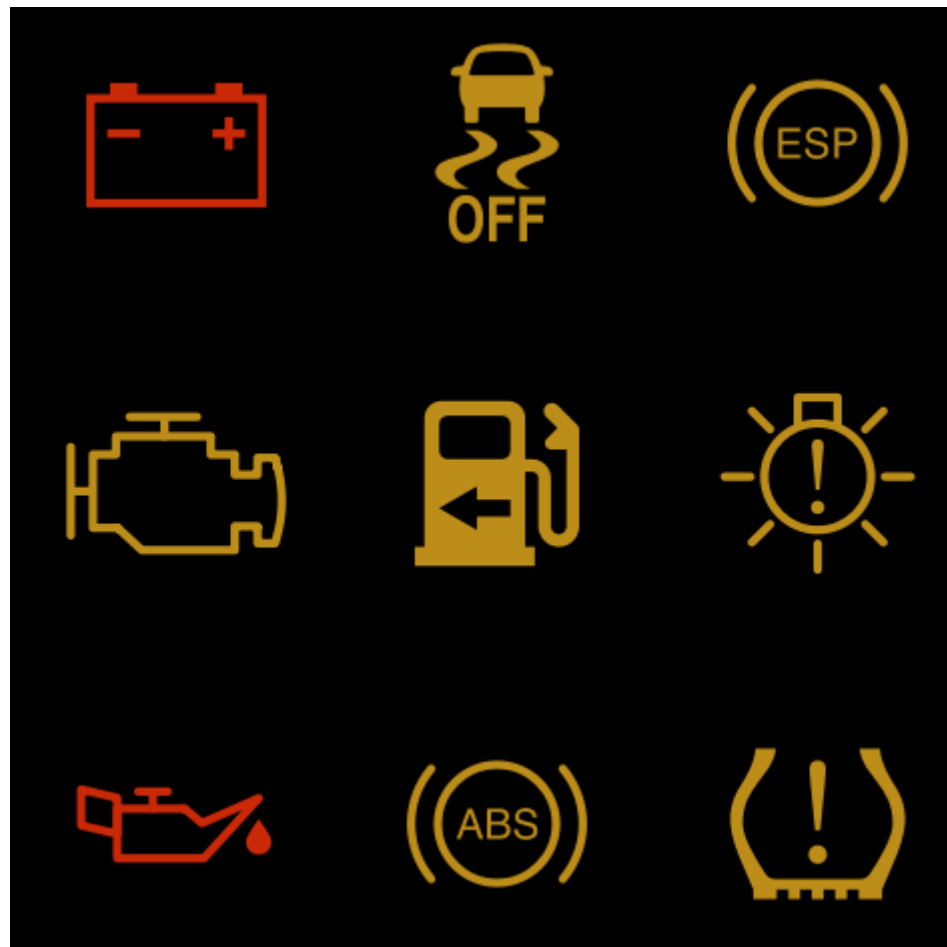


Jaroslav Jirkovský
jirkovsky@humusoft.cz

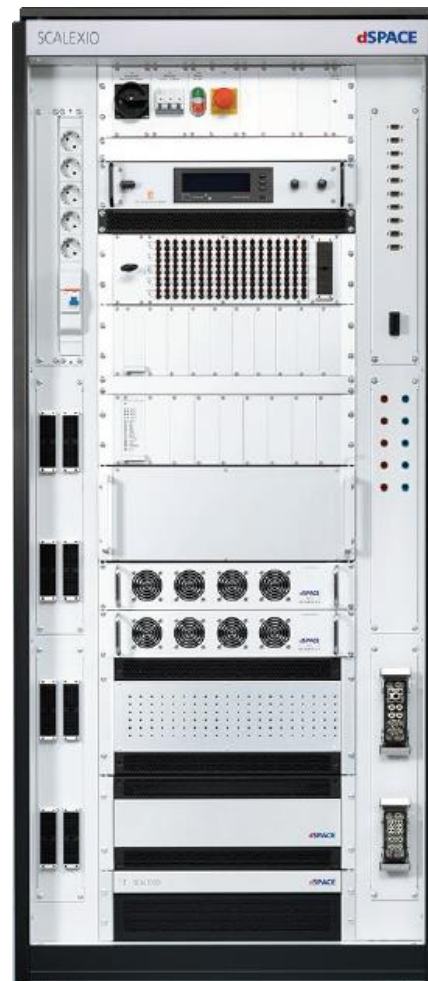
www.humusoft.cz
info@humusoft.cz

www.mathworks.com

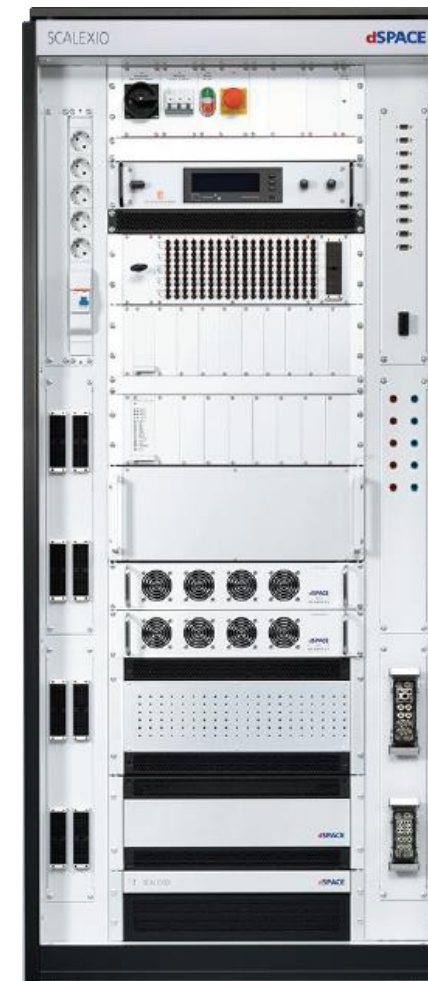
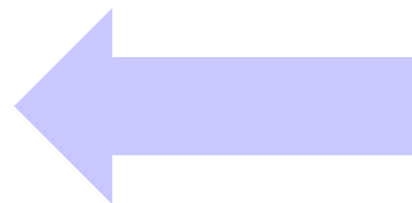
Proč ověřovat robustnost systému?



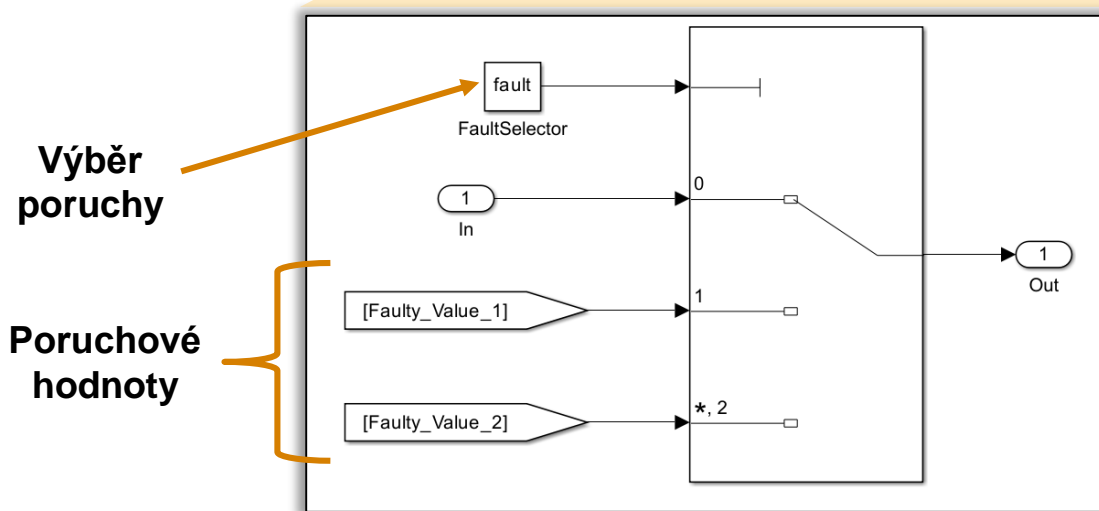
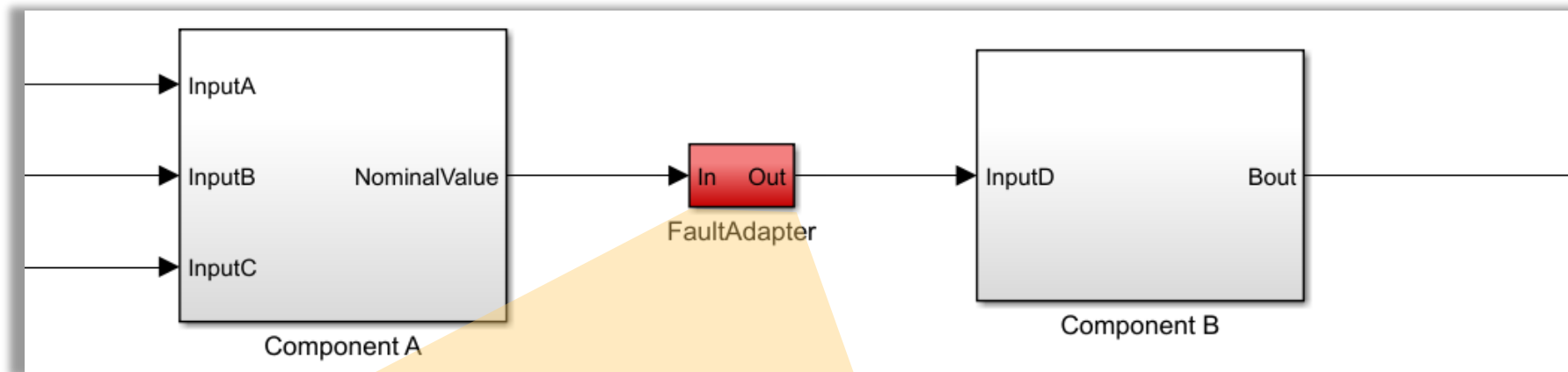
Robustnost je často testována pomocí HIL simulací



Simulujte poruchy dříve

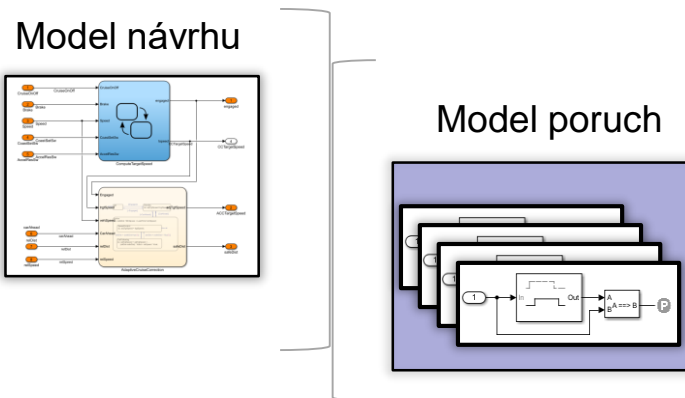


„Klasické“ modelování poruch v prostředí Simulink



- Omezení tohoto přístupu
 - modifikuje návrh
 - může neúmyslně změnit chování simulace
 - obtížné analyzovat účinky
 - jak zachytit vztah poruch a rizik?

Modelování poruch nástrojem Simulink Fault Analyzer

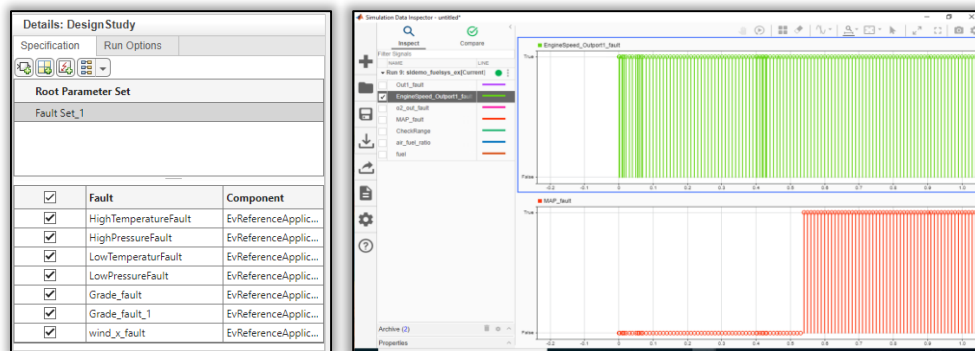


Modelování poruch bez modifikace návrhu

Enable	Model Element/Fault Name	Active Fault	Trigger
<input checked="" type="checkbox"/>	Environment/Constant6/Output/1 HighTemperatureFault	<input type="checkbox"/>	Conditional: highSpeedCondition
<input checked="" type="checkbox"/>	Environment/Constant7/Output/1 LowTemperatureFault	<input checked="" type="checkbox"/>	Conditional: SampleConditional
<input checked="" type="checkbox"/>	Environment/Constant7/Output/1 HighPressureFault	<input checked="" type="checkbox"/>	Timed: 20
<input checked="" type="checkbox"/>	Environment/Constant7/Output/1 LowPressureFault	<input type="checkbox"/>	Always On
<input checked="" type="checkbox"/>	Environment/Constant2/Output/1 Grade_fault	<input checked="" type="checkbox"/>	Always On
<input checked="" type="checkbox"/>	Environment/Constant3/Output/1 Grade_fault_1	<input type="checkbox"/>	Always On
<input checked="" type="checkbox"/>	wind_x_fault	<input checked="" type="checkbox"/>	Always On
<input checked="" type="checkbox"/>	Passenger Car/Electric Plant/Simscape/Inductor1/Inductor Inductor1_fault	<input checked="" type="checkbox"/>	Behavioral

Jednotná správa poruch v různých doménách

Simulink Fault Analyzer™



Simulace, zkoumání a analýza vlivu poruch

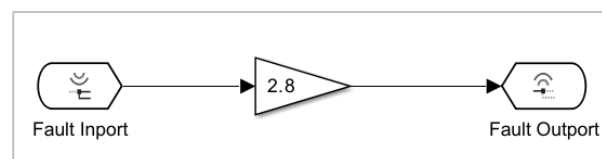
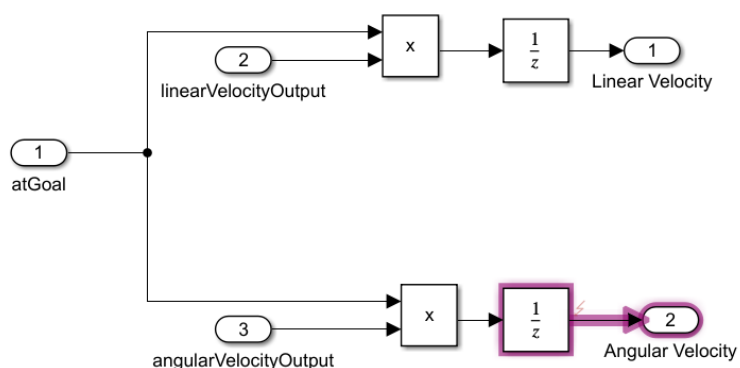
Failure Mode	Failure Rate (E-06)	Failure Effect	Detection Method
1 Angular Velocity Invalid After 50 seconds	1	Robot spins	Safety Lock
2 Angular Velocity Invalid at Maximum Pose	1	Robot spins	Safety Lock

1 warning
• Simulation errored out without Detection Method working.

Systematická bezpečnostní analýza s využitím simulací

Co je porucha?

- Porucha = jakékoliv abnormální chování, které chceme simulovat
- Parametry poruchy
 - **KDE** : umístění signálu, jehož hodnotu chceme ovlivnit
 - **CO** : abnormální chování, které chceme aplikovat
 - **KDY** : nastavení spouštěcího mechanismu poruchy



▼ Fault

Name:

Fault behavior: [warehouseFaultedRobot_FaultModel/angularVelocity_MaxPos](#)

Trigger

Trigger type:

Inject fault behavior when a logical co

Select conditional from model:

[View conditional](#)

Trigger stays on once activated

Conditional

Always On

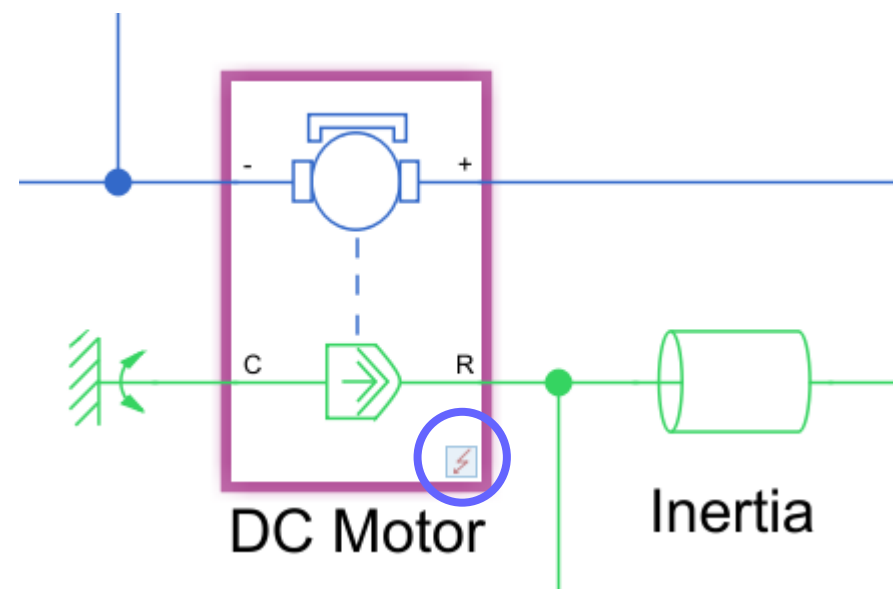
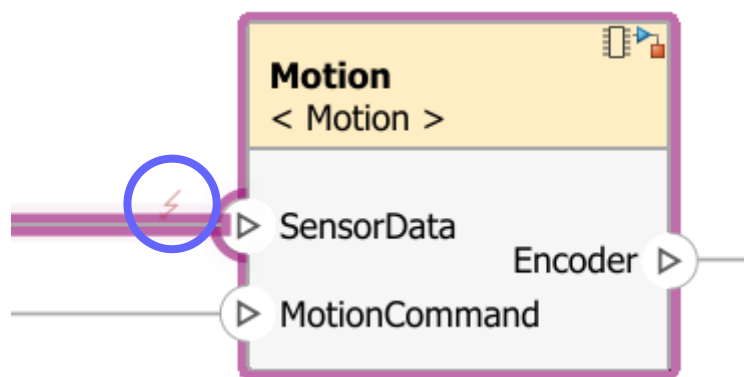
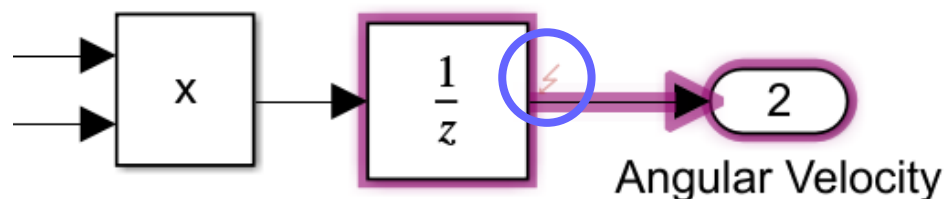
Timed

Conditional

Manual

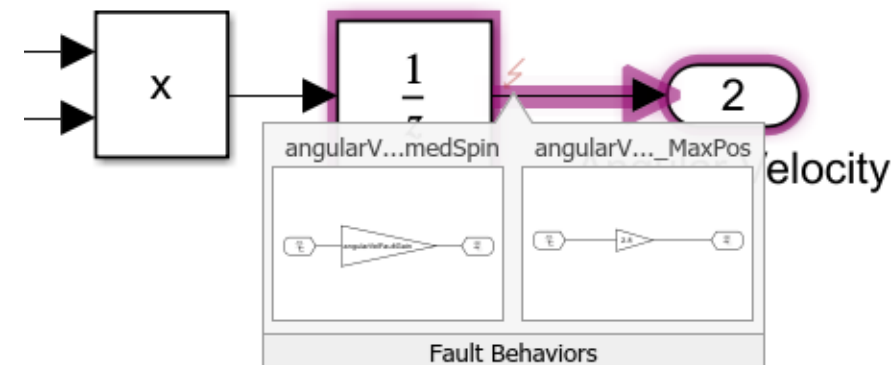
Modelování poruch

- Společný přístup k modelování poruch napříč různými doménami
- Simulink / Simscape / System Composer



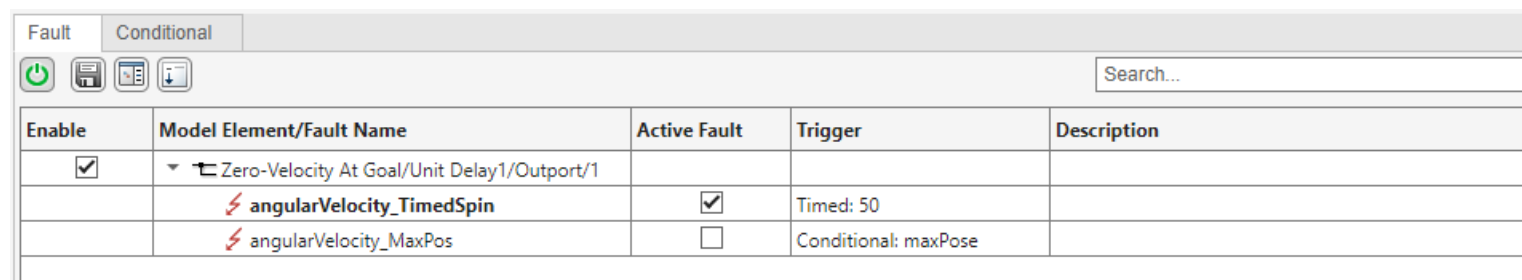
Modelování poruch bez modifikace návrhového modelu



- Model poruch – samostatný model s definicí poruch
 - využití knihovny připravených poruch *mwfaultlib*
 - vytvoření vlastního modelu poruchy (Custom fault behavior ...)
- Soubor s popisem poruch
 - XML soubor popisující vztah poruch s návrhovým modelem
- Přiřazení poruchy k signálu
 - ke všem větvím nebo pouze k vybraným koncům
 - k jednomu prvku může být přiřazeno více poruch



Zavedení poruch do simulace

- Správa poruch v panelu Fault Table
 - povolení / zakázání poruchy u daného prvku
 - výběr poruchy u daného prvku



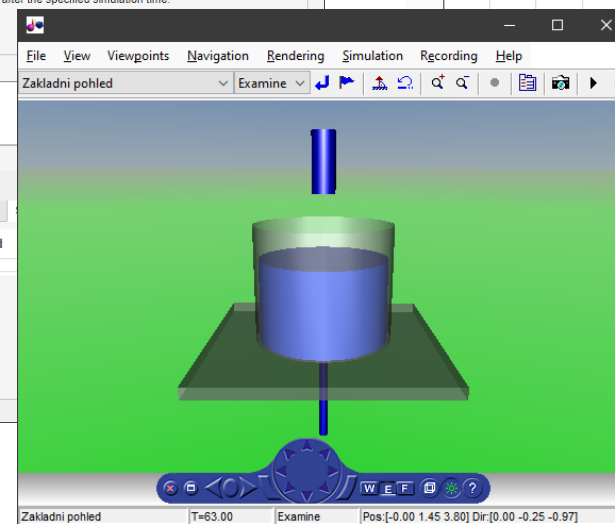
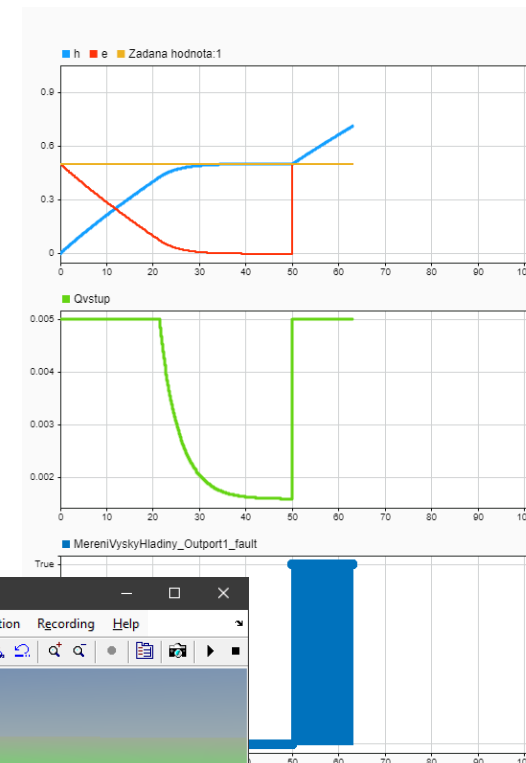
Enable	Model Element/Fault Name	Active Fault	Trigger	Description
<input checked="" type="checkbox"/>	Zero-Velocity At Goal/Unit Delay1/Outport/1			
	 angularVelocity_TimedSpin	<input checked="" type="checkbox"/>	Timed: 50	
	 angularVelocity_MaxPos	<input type="checkbox"/>	Conditional: maxPose	

- Spouštěcí mechanismus poruchy
 - vždy zapnuto
 - porucha v zadaném čase
 - podmíněná porucha – porucha ze zavede při splnění zadané podmínky
 - manuální spuštění

Ukázka: Model PID regulace hladiny v nádrži

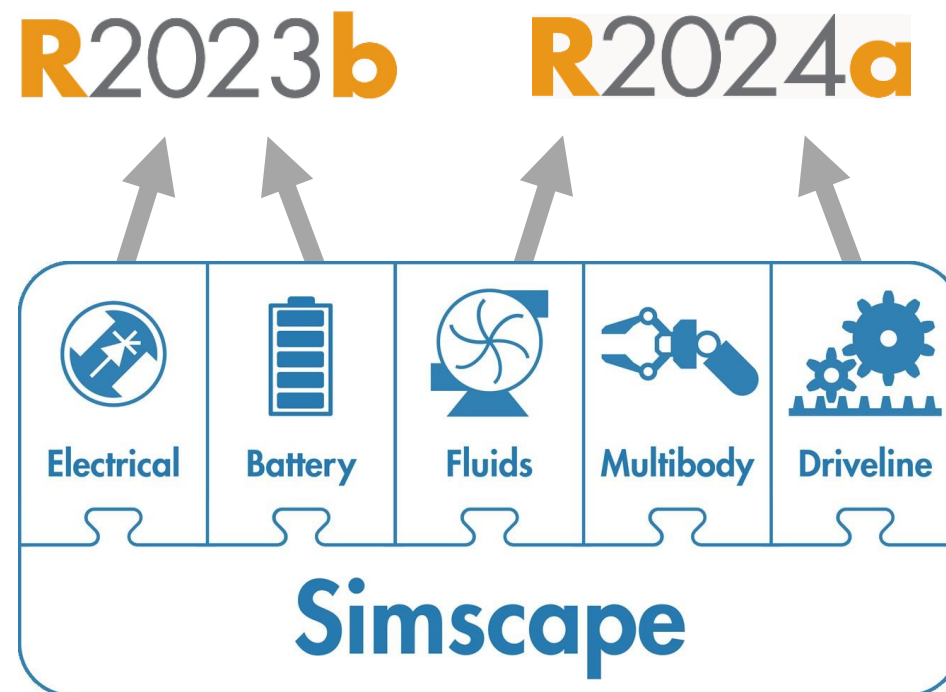
FAULT TABLE - Nadoba_rizeni_PID_faultInfo.xml*

Enable	Model Element/Fault Name	Active Fault	Trigger	Description
<input checked="" type="checkbox"/>	Mereni vysky hladiny/Output/1			
<input checked="" type="checkbox"/>	MereniVyskyHladiny_Output1_fault	<input checked="" type="checkbox"/>	Timed: 50	
<input checked="" type="checkbox"/>	MereniVyskyHladiny_Output1_noise	<input type="checkbox"/>	Manual	

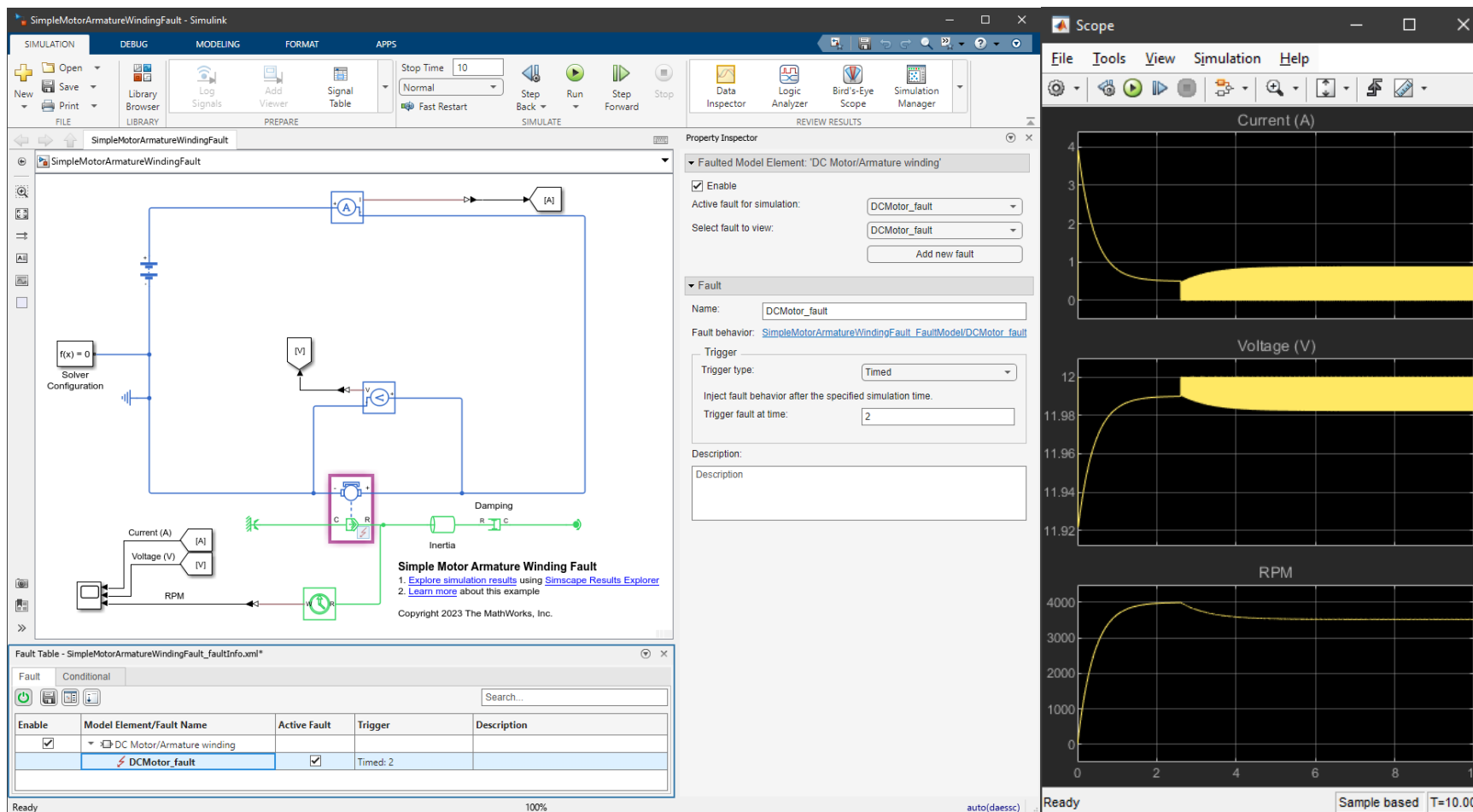


Modelování poruch v modelech Simscape

- R2023b
 - Simscape Electrical
 - Simscape Battery
- R2024a
 - Simscape Fluids
 - Simscape Driveline



Ukázka: DC motor Simscape



Simple Motor Armature Winding Fault

1. Explore simulation results using Simscape Results Explorer
 2. Learn more about this example
 Copyright 2023 The MathWorks, Inc.

Property Inspector

Faulted Model Element: 'DC Motor/Armature winding'

Enable
 Active fault for simulation: DCMotor_fault
 Select fault to view: DCMotor_fault
 Add new fault

Fault

Name: DCMotor_fault
 Fault behavior: SimpleMotorArmatureWindingFault_FaultModel/DCMotor_fault

Trigger
 Trigger type: Timed
 Inject fault behavior after the specified simulation time.
 Trigger fault at time: 2

Description:
 Description

Fault Table - SimpleMotorArmatureWindingFault_faultInfo.xml*

Enable	Model Element/Fault Name	Active Fault	Trigger	Description
<input checked="" type="checkbox"/>	DC Motor/Armature winding			
<input checked="" type="checkbox"/>	DCMotor_fault	<input checked="" type="checkbox"/>	Timed: 2	

Scope

Current (A)

Voltage (V)

RPM

Ready auto(daessc) Sample based T=10.000

Definice a správa poruch pomocí příkazů

- Poruchy lze definovat a ovládat pomocí příkazů
- Umožní automatizaci managementu poruch pomocí skriptů

▼ Model Functions
<code>Simulink.fault.addConditional</code>
<code>Simulink.fault.addFault</code>
<code>Simulink.fault.deleteConditional</code>
<code>Simulink.fault.deleteFault</code>
<code>Simulink.fault.findConditionals</code>
<code>Simulink.fault.findFaultedElements</code>
<code>Simulink.fault.findFaults</code>
<code>Simulink.fault.getFaultModels</code>
<code>Simulink.fault.libraries</code>
<code>Simulink.fault.libraryBlocks</code>
<code>Simulink.fault.save</code>
<code>Simulink.fault.unregisterLibrary</code>
<code>Simulink.fault.updateReferences</code>

▼ Fault and Conditional Functions
<code>addBehavior</code>
<code>deleteBehavior</code>
<code>getAssociatedModel</code>
<code>getBehavior</code>
<code>getFaultModel</code>
<code>getFaultInfoFile</code>
<code>getSymbols</code>
<code>getTriggeredFaults</code>
<code>openBehavior</code>

Objects

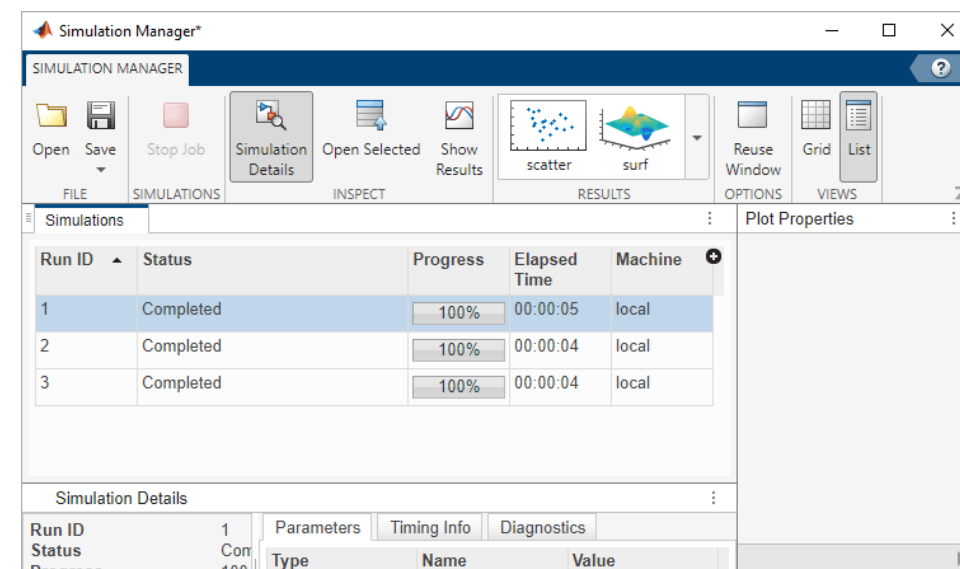
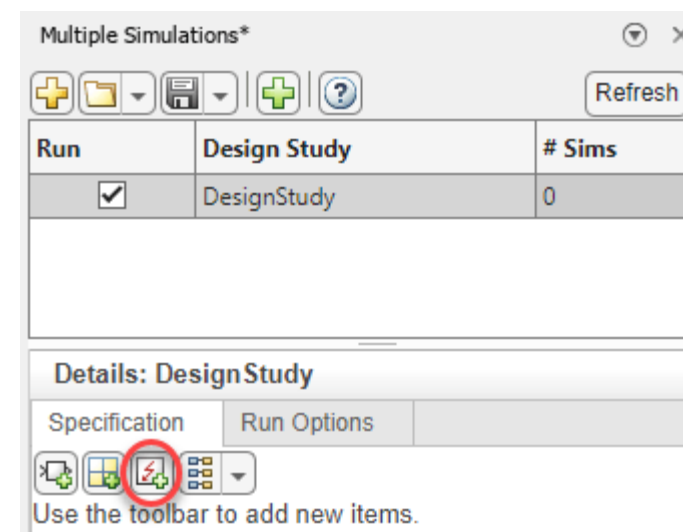
<code>Fault</code>
<code>Conditional</code>
<code>Symbol</code>

Functions

<code>activate</code>
<code>Simulink.fault.enable</code>
<code>Simulink.fault.injection</code>
<code>Simulink.fault.isEnabled</code>

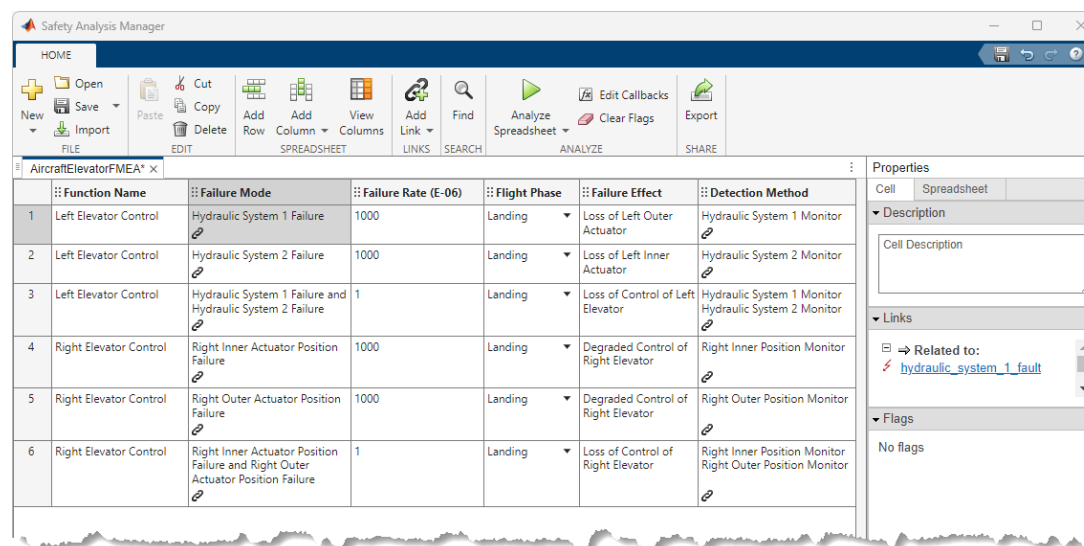
Analýza vlivu poruch na systém

- Studie citlivosti na poruchy
 - cílem je určit účinnost systému detekce a potlačení poruch při výskytu daného abnormálního chování
- Multiple Simulations panel a Simulation Manager
 - automatická změna parametrů poruch a jejich kombinací
 - opakovaná simulace
 - agregace výsledků



Systematická bezpečnostní analýza

- Failure Mode and Effects Analysis (FMEA)
- Functional Hazard Assessment (FHA)
- Safety Analysis Manager
 - vytváření a úprava dokumentů pro bezpečnostní analýzy v prostředí MATLAB a Simulink



Function Name	Failure Mode	Failure Rate (E-06)	Flight Phase	Failure Effect	Detection Method
1 Left Elevator Control	Hydraulic System 1 Failure	1000	Landing	Loss of Left Outer Actuator	Hydraulic System 1 Monitor
2 Left Elevator Control	Hydraulic System 2 Failure	1000	Landing	Loss of Left Inner Actuator	Hydraulic System 2 Monitor
3 Left Elevator Control	Hydraulic System 1 Failure and Hydraulic System 2 Failure	1	Landing	Loss of Control of Left Elevator	Hydraulic System 1 Monitor Hydraulic System 2 Monitor
4 Right Elevator Control	Right Inner Actuator Position Failure	1000	Landing	Degraded Control of Right Elevator	Right Inner Position Monitor
5 Right Elevator Control	Right Outer Actuator Position Failure	1000	Landing	Degraded Control of Right Elevator	Right Outer Position Monitor
6 Right Elevator Control	Right Inner Actuator Position Failure and Right Outer Actuator Position Failure	1	Landing	Loss of Control of Right Elevator	Right Inner Position Monitor Right Outer Position Monitor

Co je FMEA

- Failure Mode and Effects Analysis
 - Failure Mode = konkrétní způsob, jakým může proces nebo produkt fungovat nesprávně
- Strukturovaná metodika
 - navržena pro identifikaci a řešení potenciálních chyb a poruch v systému
- Základní myšlenka FMEA
 - předvídat a snižovat možnost selhání systému
- FMEA je založena na podrobném prozkoumání systému k přesnému určení:
 - kde a jak může dojít k selhání
 - jaké by mohly být příčiny selhání
 - jaké jsou potenciální dopady na celý systém

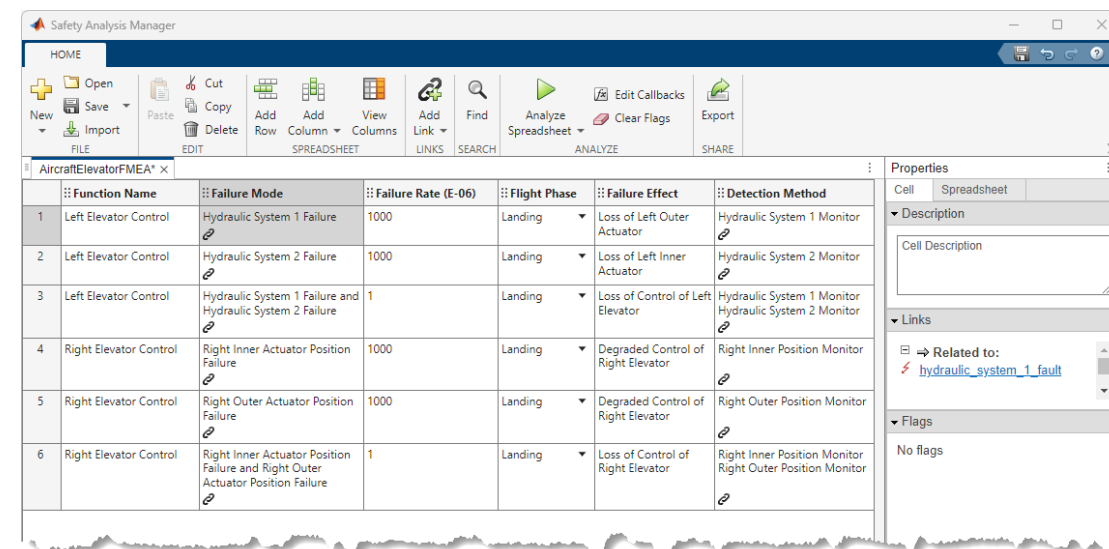
Proč a Jak je FMEA prováděna

- Proaktivní přístup s cílem **posílení integrity a robustnosti** návrhu
 - systematická analýza možných selhání a jejich potenciálních dopadů
- Základní kroky
 1. Sestavení týmu odborníků
 2. Provedení analýzy
 3. Stanovení akčních plánů
- Analýza zahrnuje
 - a. Určení systému nebo jeho součásti, které chceme analyzovat
 - b. Identifikace potenciálních způsobů selhání – všechny možnosti nesprávného chování prvku
 - c. Určení všech možných příčin pro každé uvažované selhání
 - d. Vyhodnocení dopadu selhání – posouzení možných důsledků každého uvažovaného selhání
 - e. Posouzení účinnosti opatření pro detekci nesprávného chování systému

FMEA je iterativní proces, který je třeba provádět po celou dobu životnosti produktu. Je to živý dokument, který je třeba pravidelně revidovat a aktualizovat.

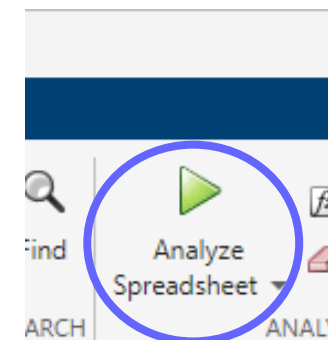
Safety Analysis Manager

- Připravené šablony
 - s typickým uspořádáním pro FMEA a FHA
 - možnost vytvořit vlastní šablonu
- Hodnoty v tabulce lze
 - zadávat ručně
 - vypočítat je na základě ostatních položek
- Přiřazení metainformací k položkám
- Provázání položek v tabulce s dalšími prvky
 - bloky v modelu, poruchy, testy nebo požadavky
- Tvorba funkcí pro analýzu dokumentu s využitím výsledků simulací
- API pro práci pomocí příkazů a funkcí

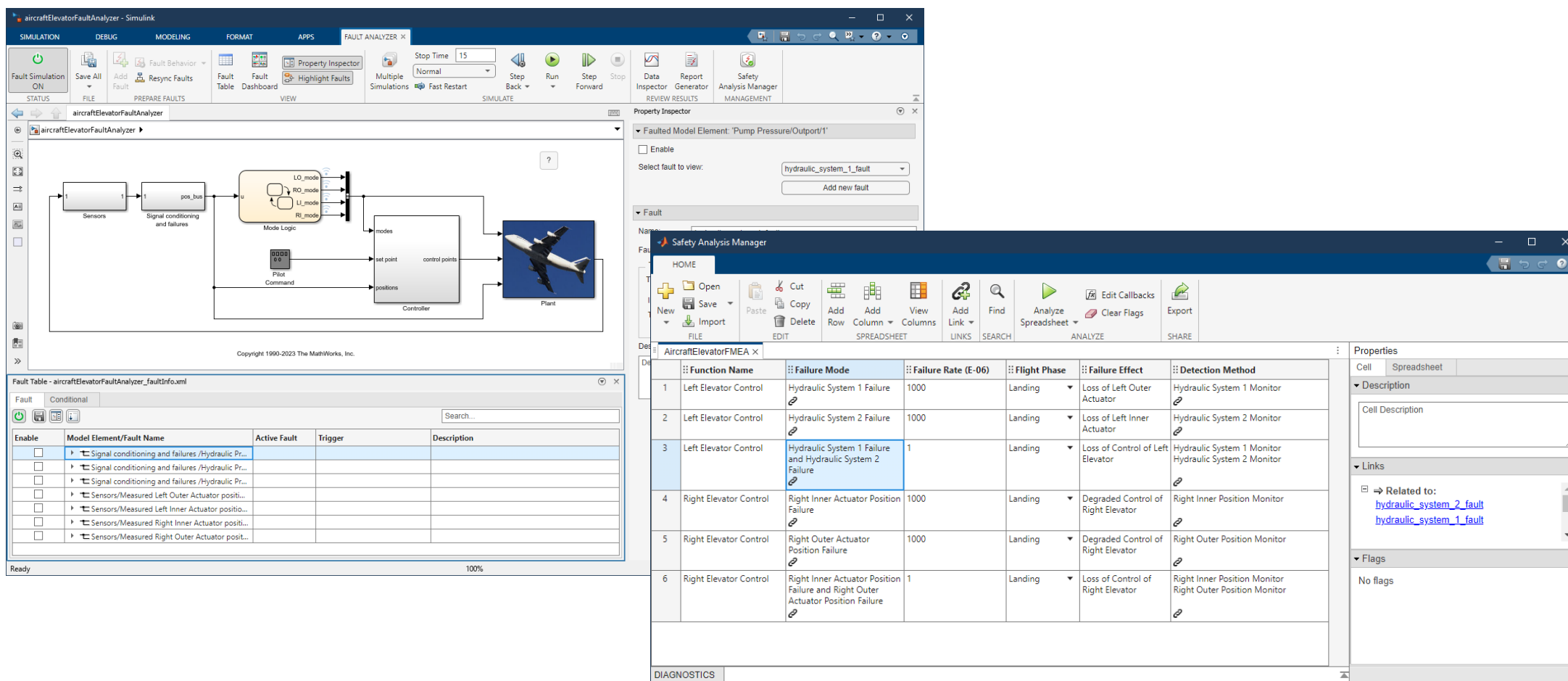


	Function Name	Failure Mode	Failure Rate (E-06)	Flight Phase	Failure Effect	Detection Method
1	Left Elevator Control	Hydraulic System 1 Failure	1000	Landing	Loss of Left Outer Actuator	Hydraulic System 1 Monitor
2	Left Elevator Control	Hydraulic System 2 Failure	1000	Landing	Loss of Left Inner Actuator	Hydraulic System 2 Monitor
3	Left Elevator Control	Hydraulic System 1 Failure and Hydraulic System 2 Failure	1	Landing	Loss of Control of Left Elevator	Hydraulic System 1 Monitor Hydraulic System 2 Monitor
4	Right Elevator Control	Right Inner Actuator Position Failure	1000	Landing	Degraded Control of Right Elevator	Right Inner Position Monitor
5	Right Elevator Control	Right Outer Actuator Position Failure	1000	Landing	Degraded Control of Right Elevator	Right Outer Position Monitor
6	Right Elevator Control	Right Inner Actuator Position Failure and Right Outer Actuator Position Failure	1	Landing	Loss of Control of Right Elevator	Right Inner Position Monitor Right Outer Position Monitor

Metrika : Risk Priority Number
 $RPN = \text{závažnost} \times \text{pravděpodobnost} \times \text{detekovatelnost}$



Ukázka: FMEA



The screenshot displays the Simulink Fault Analyzer environment for an aircraft elevator control system. The main workspace shows a block diagram with components like Sensors, Signal conditioning and failures, Mode Logic, Controller, and Plant. A Property Inspector window is open, showing details for a faulted model element: 'Pump Pressure/Output/1'. A Safety Analysis Manager window is also open, displaying a table of failure modes.

Function Name	Failure Mode	Failure Rate (E-06)	Flight Phase	Failure Effect	Detection Method
1 Left Elevator Control	Hydraulic System 1 Failure	1000	Landing	Loss of Left Outer Actuator	Hydraulic System 1 Monitor
2 Left Elevator Control	Hydraulic System 2 Failure	1000	Landing	Loss of Left Inner Actuator	Hydraulic System 2 Monitor
3 Left Elevator Control	Hydraulic System 1 Failure and Hydraulic System 2 Failure	1	Landing	Loss of Control of Left Elevator	Hydraulic System 1 Monitor Hydraulic System 2 Monitor
4 Right Elevator Control	Right Inner Actuator Position Failure	1000	Landing	Degraded Control of Right Elevator	Right Inner Position Monitor
5 Right Elevator Control	Right Outer Actuator Position Failure	1000	Landing	Degraded Control of Right Elevator	Right Outer Position Monitor
6 Right Elevator Control	Right Inner Actuator Position Failure and Right Outer Actuator Position Failure	1	Landing	Loss of Control of Right Elevator	Right Inner Position Monitor Right Outer Position Monitor

Below the table, the Properties panel shows a description field and a 'Related to' section with links to 'hydraulic_system_2_fault' and 'hydraulic_system_1_fault'.

Děkuji za pozornost