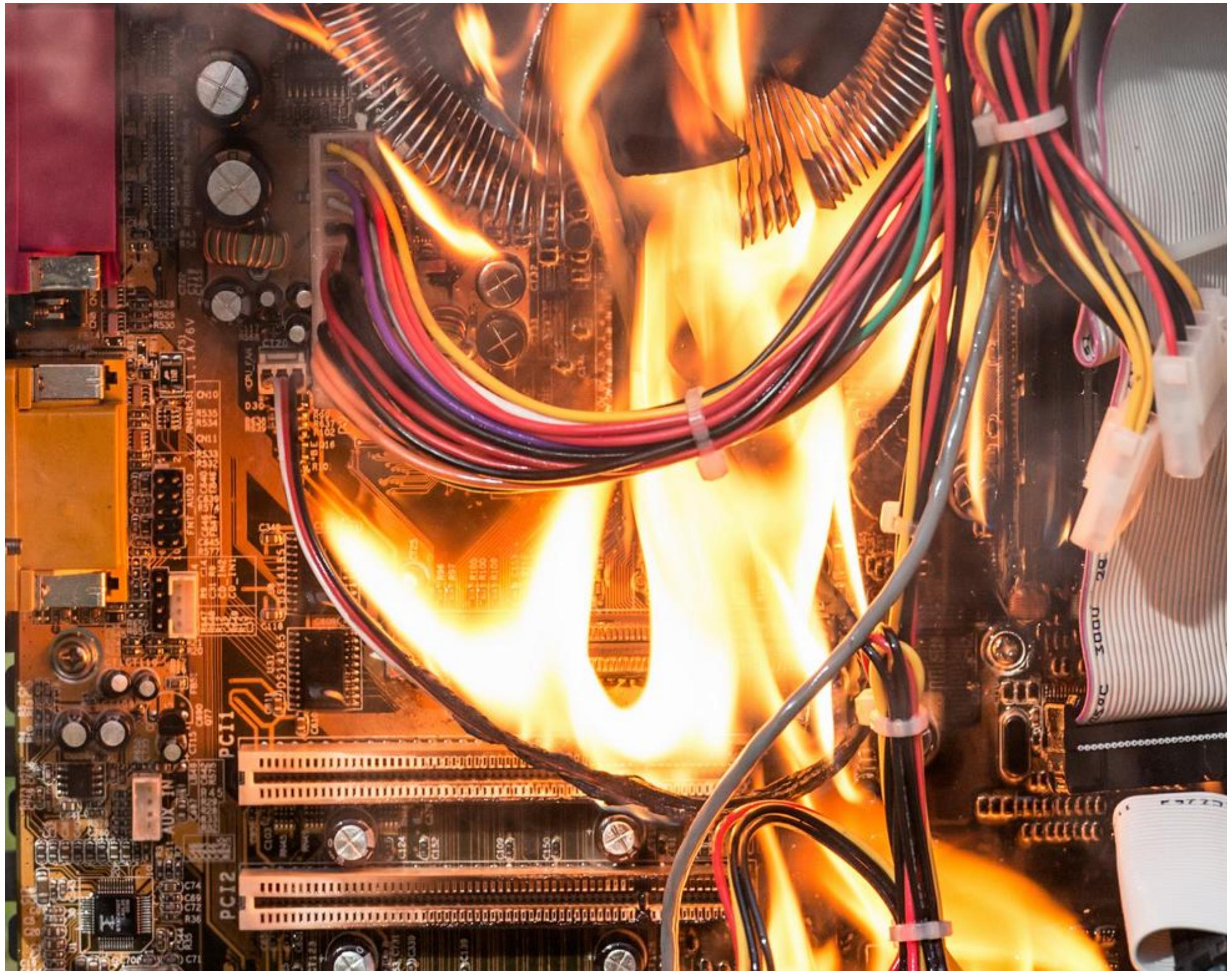
Practical Applications of Model-Based Systems Engineering

Case Study: Simulation-Driven Safety Analysis in MBSE

Valtteri Forsman
Application Engineer
MathWorks

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



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 Follow *and Soobin Kim*

Updated Aug. 7, 2024 6:54 pm ET

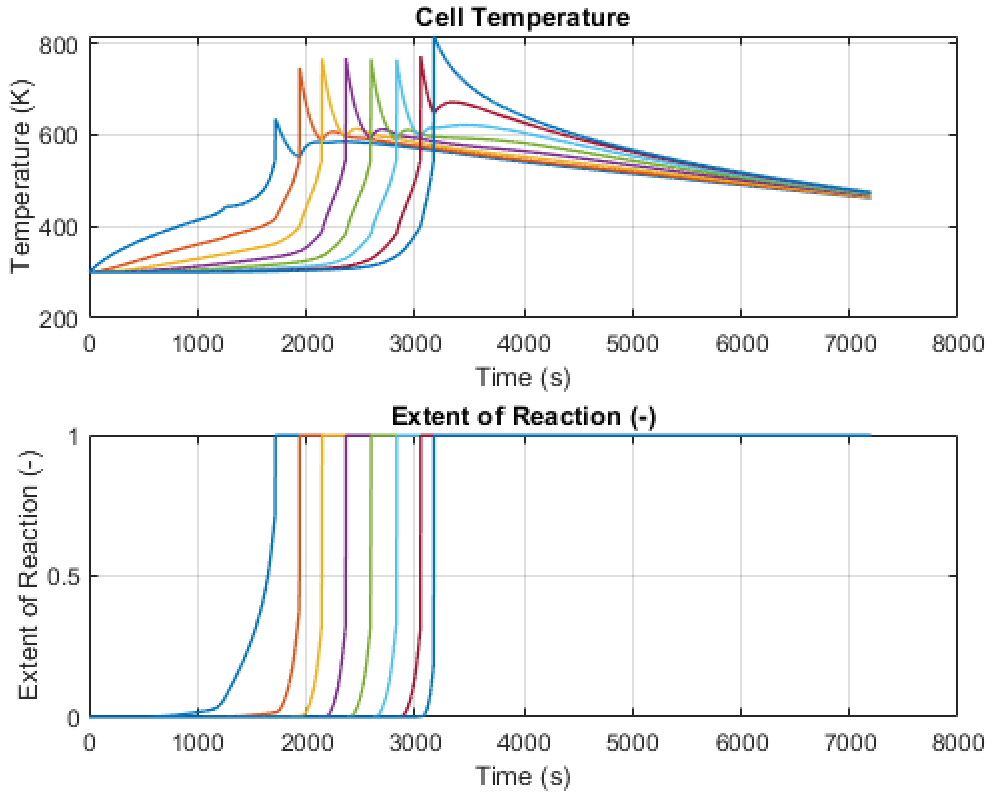
Share Resize Listen (2 min)

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

Thermal runaway can lead to catastrophic failure

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



Key Takeaways

Shift-Left – Identify issues sooner in the development process

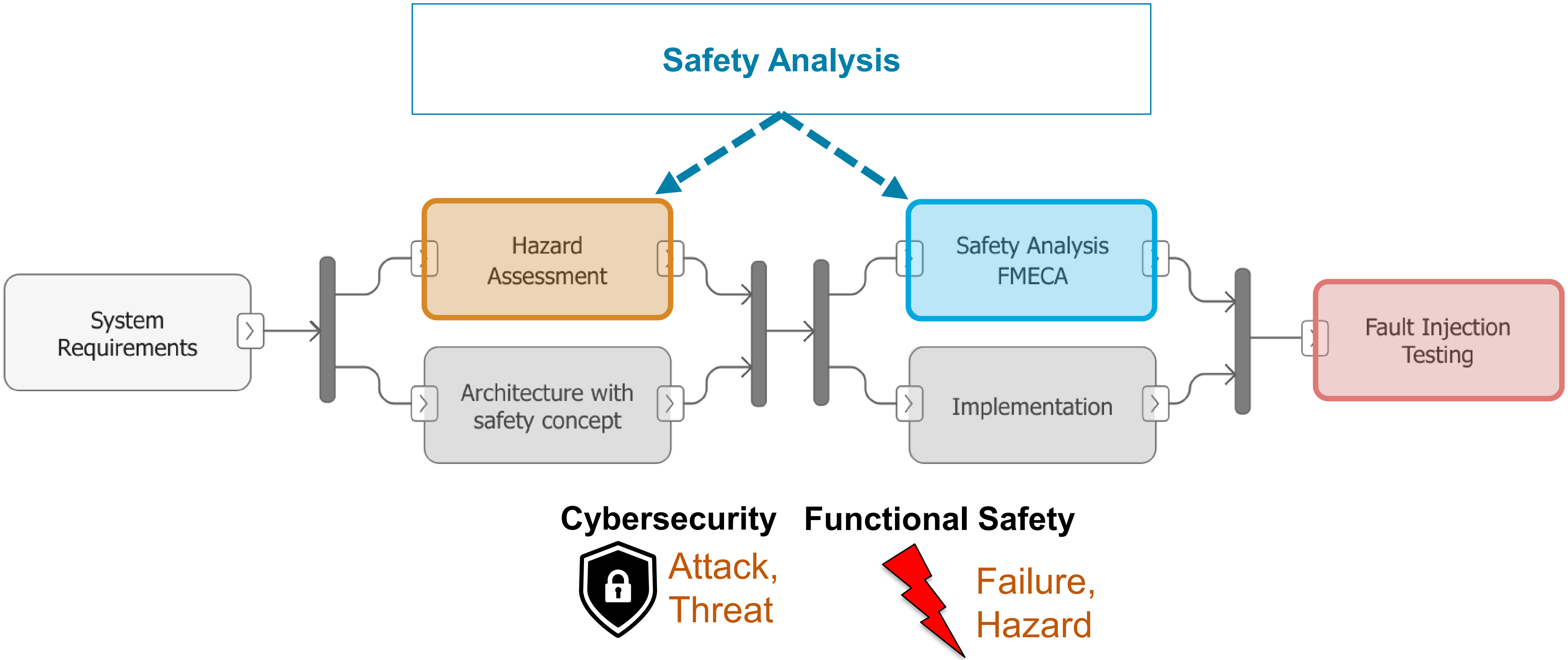
Fault Injection Modeling – essential for identifying and mitigating potential system failures proactively

Fault Injection Testing – Validate safety of systems by simulation

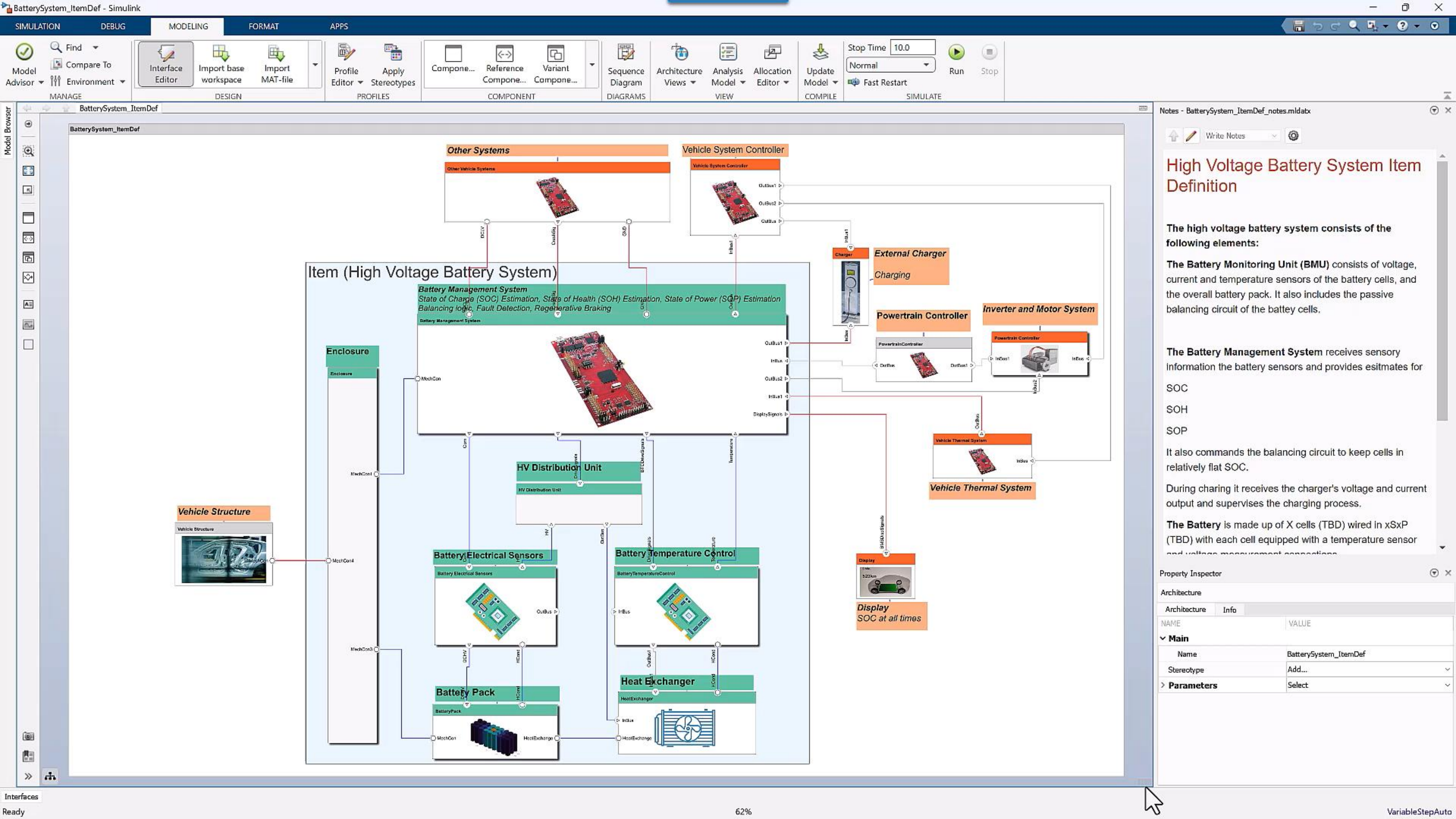
Agenda of this session

- Importance of safety in systems development
- Safety analysis workflow: BMS case study
- AI-Assisted Model-Based Systems Engineering

Model-based safety analysis is a highly iterative workflow involving detection, mitigation, and verification

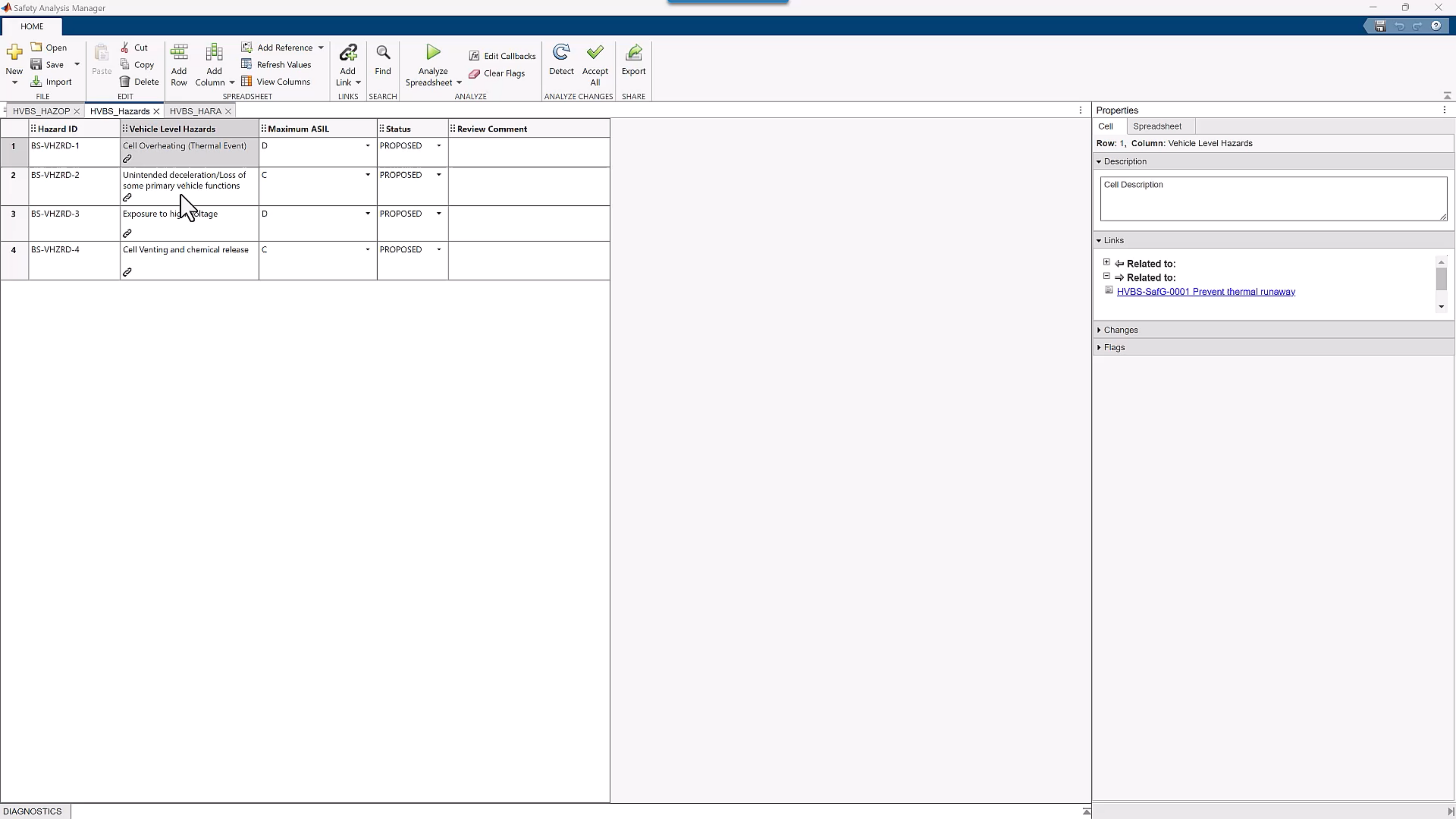


Defining system requirements and architecture



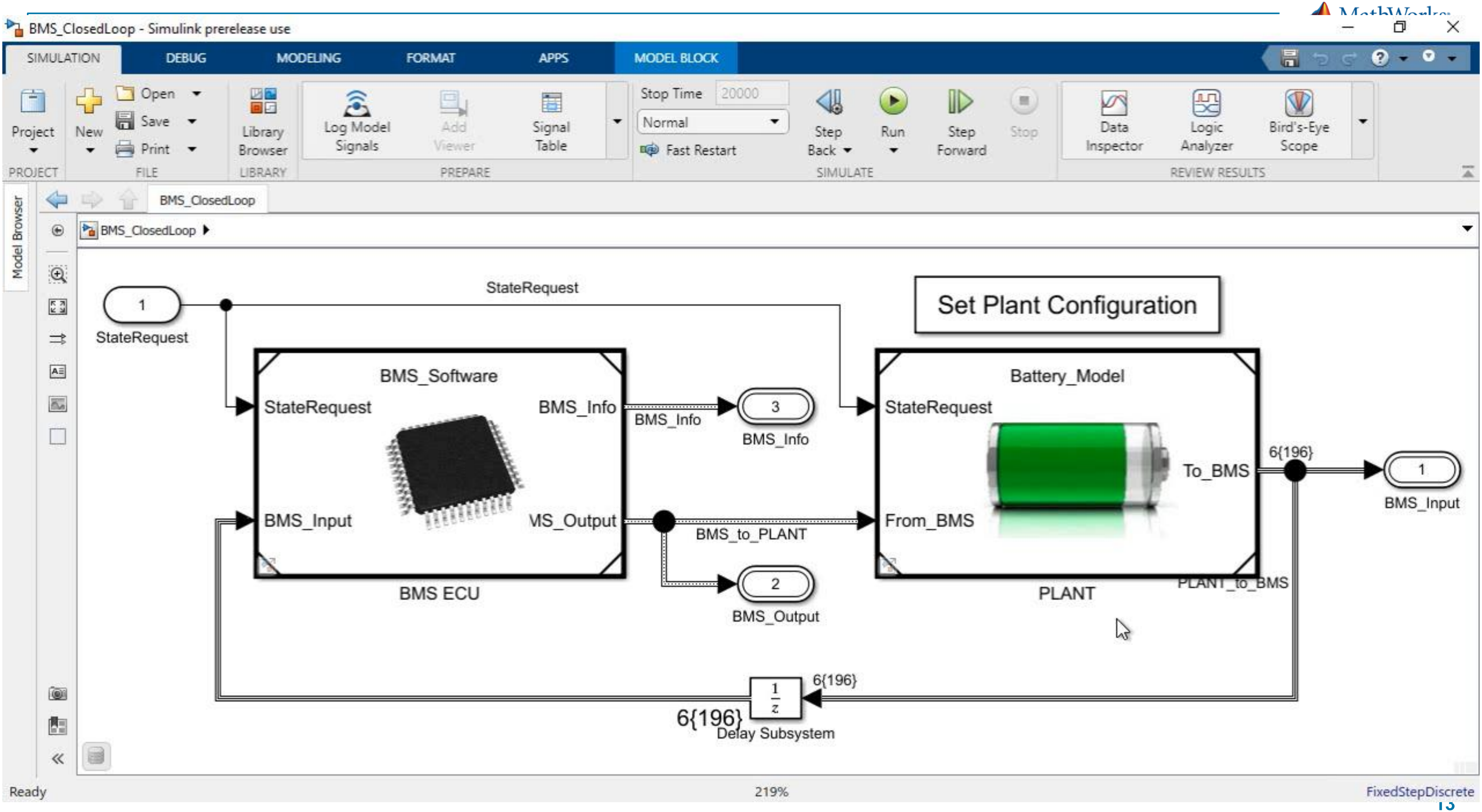
BatterySystem_ItemDef - Simulink
SIMULATION
DEBUG
MODELING
FORMAT
APPS
Model Advisor
Find
Compare To
Environment
MANAGE
Interface Editor
Import base workspace
Import MAT-file
DESIGN
Profile Editor
Apply Stereotypes
PROFILES
Compone...
Reference Compone...
Variant Compone...
COMPONENT
Sequence Diagram
DIAGRAMS
Architecture Views
Analysis Model
Allocation Editor
VIEW
Update Model
COMPILE
Stop Time 10.0
Normal
Fast Restart
Run
Stop
SIMULATE
BatterySystem_ItemDef
Other Systems
Vehicle System Controller
External Charger
Charging
Item (High Voltage Battery System)
Battery Management System
State of Charge (SOC) Estimation, State of Health (SOH) Estimation, State of Power (SOP) Estimation
Balancing logic, Fault Detection, Regenerative Braking
Powertrain Controller
Inverter and Motor System
Enclosure
HV Distribution Unit
Vehicle Thermal System
Vehicle Structure
Battery Electrical Sensors
Battery Temperature Control
Display
SOC at all times
Battery Pack
Heat Exchanger
Notes - BatterySystem_ItemDef_notes.mldatx
Write Notes
High Voltage Battery System Item Definition
The high voltage battery system consists of the following elements:
The Battery Monitoring Unit (BMU) consists of voltage, current and temperature sensors of the battery cells, and the overall battery pack. It also includes the passive balancing circuit of the battey cells.
The Battery Management System receives sensory information the battery sensors and provides esitmates for
SOC
SOH
SOP
It also commands the balancing circuit to keep cells in relatively flat SOC.
During charing it receives the charger's voltage and current output and supervises the charging process.
The Battery is made up of X cells (TBD) wired in xSxP (TBD) with each cell equipped with a temperature sensor
Property Inspector
Architecture
Architecture
Info
NAME
VALUE
Main
Name
BatterySystem_ItemDef
Stereotype
Add...
Parameters
Select
Interfaces
Ready
62%
VariableStepAuto

Establishing digital traceability between safety artifacts



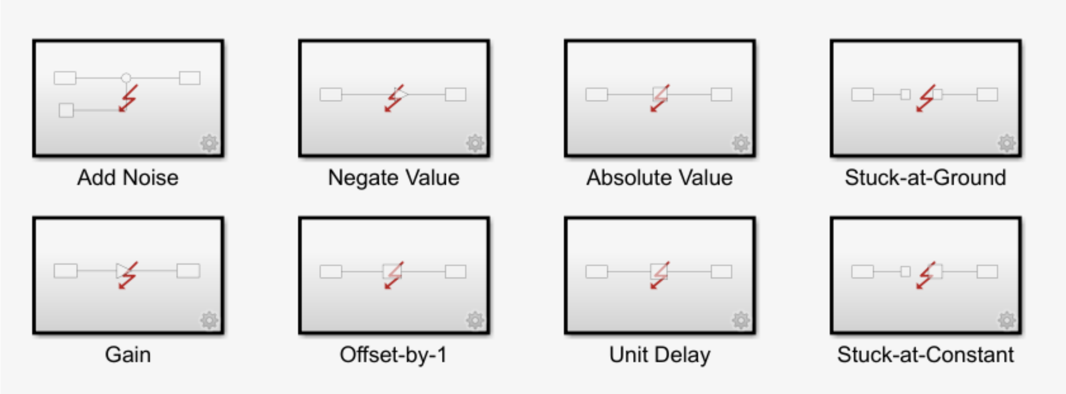
Safety Analysis Manager
HOME
New
Open
Save
Import
FILE
Paste
Cut
Copy
Delete
EDIT
Add Row
Add Column
Add Reference
Refresh Values
View Columns
SPREADSHEET
Add Link
LINKS
Find
SEARCH
Analyze Spreadsheet
Edit Callbacks
Clear Flags
ANALYZE
Detect
Accept All
ANALYZE CHANGES
Export
SHARE
HVBS_HAZOP
HVBS_Hazards
HVBS_HARA
Hazard ID
Vehicle Level Hazards
Maximum ASIL
Status
Review Comment
1
BS-VHZRD-1
Cell Overheating (Thermal Event)
D
PROPOSED
2
BS-VHZRD-2
Unintended deceleration/Loss of some primary vehicle functions
C
PROPOSED
3
BS-VHZRD-3
Exposure to high voltage
D
PROPOSED
4
BS-VHZRD-4
Cell Venting and chemical release
C
PROPOSED
Properties
Cell
Spreadsheet
Row: 1, Column: Vehicle Level Hazards
Description
Cell Description
Links
Related to:
Related to:
HVBS-SafG-0001 Prevent thermal runaway
Changes
Flags
DIAGNOSTICS

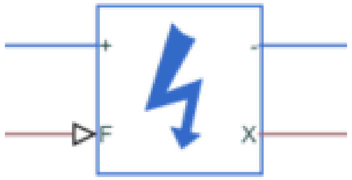
Modelling faults without modifying the design

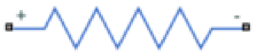

BMS_ClosedLoop - Simulink prerelease use
SIMULATION
DEBUG
MODELING
FORMAT
APPS
MODEL BLOCK
Project
New
Open
Save
Print
Library Browser
Log Model Signals
Add Viewer
Signal Table
Stop Time
20000
Normal
Fast Restart
Step Back
Run
Step Forward
Stop
Data Inspector
Logic Analyzer
Bird's-Eye Scope
PROJECT
FILE
LIBRARY
PREPARE
SIMULATE
REVIEW RESULTS
Model Browser
BMS_ClosedLoop
StateRequest
1
StateRequest
Set Plant Configuration
BMS_Software
StateRequest
BMS_Info
BMS_Input
MS_Output
BMS ECU
BMS_Info
3
BMS_Info
BMS_to_PLANT
2
BMS_Output
Battery_Model
StateRequest
To_BMS
From_BMS
PLANT
PLANT_to_BMS
6{196}
1
BMS_Input
1
z
6{196}
6{196}
Delay Subsystem
Ready
219%
FixedStepDiscrete

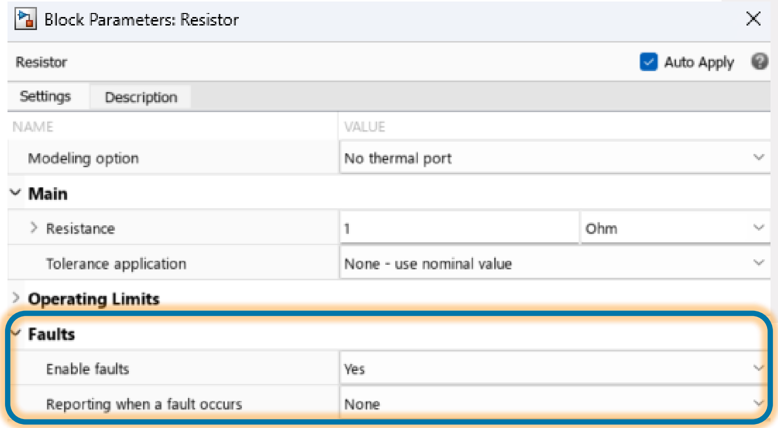
Faults and system protection – modelling thermal runaway

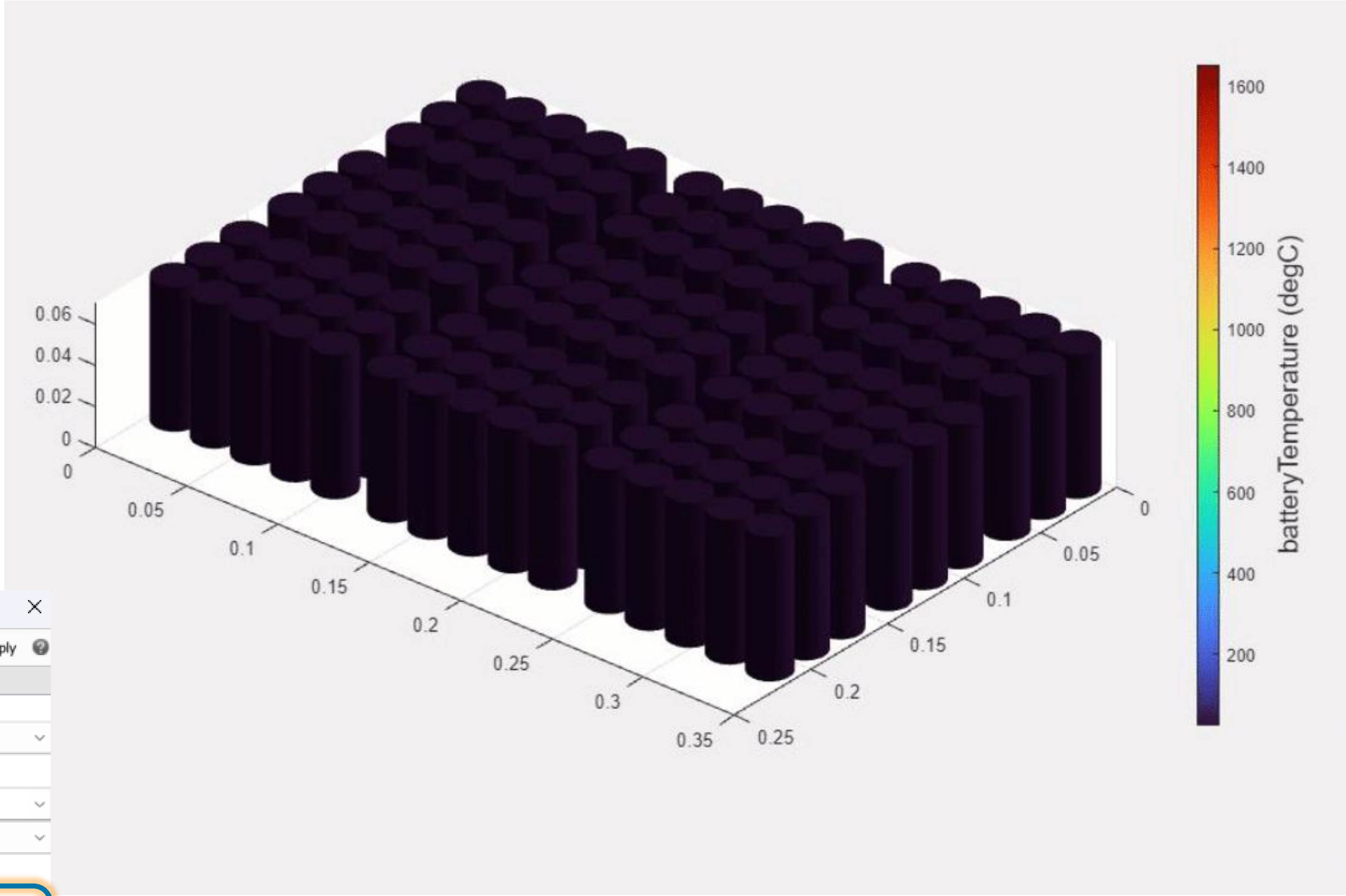
- Simscape
  - Foundation Library
  - Utilities
  - Battery



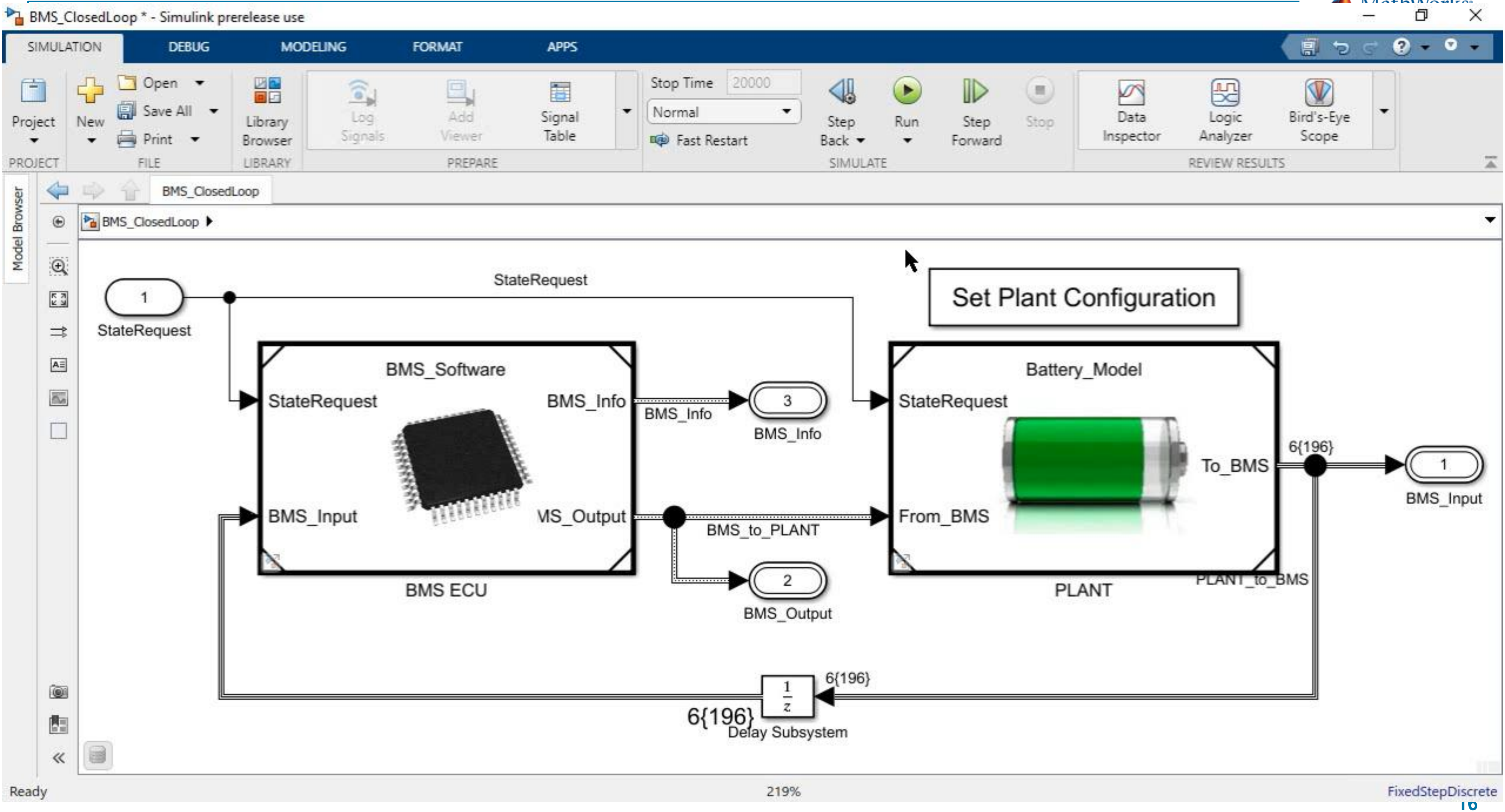








Validating Safety Analysis through Fault Injection Testing


BMS_ClosedLoop * - Simulink prerelease use
SIMULATION
DEBUG
MODELING
FORMAT
APPS
Project
New
Open
Save All
Print
Library Browser
Log Signals
Add Viewer
Signal Table
Stop Time
20000
Normal
Fast Restart
Step Back
Run
Step Forward
Stop
Data Inspector
Logic Analyzer
Bird's-Eye Scope
PROJECT
FILE
LIBRARY
PREPARE
SIMULATE
REVIEW RESULTS
Model Browser
BMS_ClosedLoop
StateRequest
Set Plant Configuration
1
StateRequest
BMS_Software
StateRequest
BMS_Info
BMS_Input
MS_Output
BMS ECU
BMS_Info
3
BMS_Info
BMS_to_PLANT
2
BMS_Output
Battery_Model
StateRequest
To_BMS
From_BMS
PLANT
PLANT_to_BMS
6{196}
1
BMS_Input
1/z
6{196}
6{196}
Delay Subsystem
Ready
219%
FixedStepDiscrete

Model-based safety analysis is fully integrated and traceable

Hazard Assessment

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

Basic Properties | Description

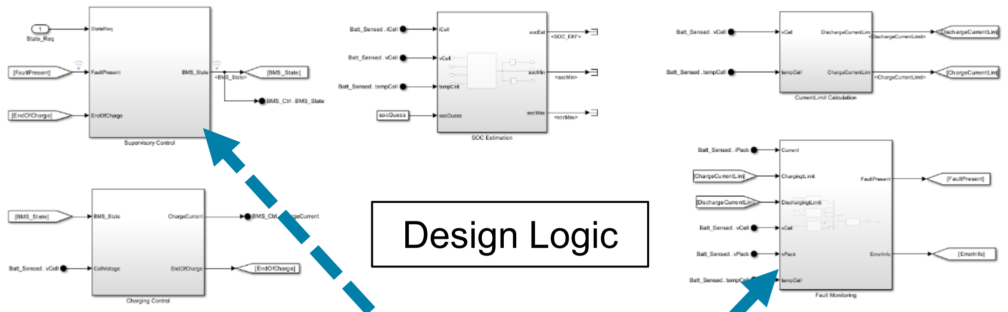
Model element: BMS07_fault_1/Battery Plant/EV_BatteryPack1/ModuleAssembly1/Module1/

Fault name: Cell1/Additional resistance

- Cell1/Additional resistance
- Cell1/Exothermic reactions
- Cell1/Internal short

Fault information directory: Fault_Analyze...

Fault Modeling



Design Logic

Run

Run For All Faults

Safety Analysis (e.g. FMEA)

	Assembly	Module	Fault Behavior	Condition	Assembly_Module_Fault_Condition	Detection	Mitigation	Validated
5	2	4	Internal Short	Driving	2_4_Internal Short_Driving	UndervoltageError	BMS_State	☐

Key Takeaways

Shift-Left – Identify issues sooner in the development process

Fault Injection Modeling – essential for identifying and mitigating potential system failures proactively

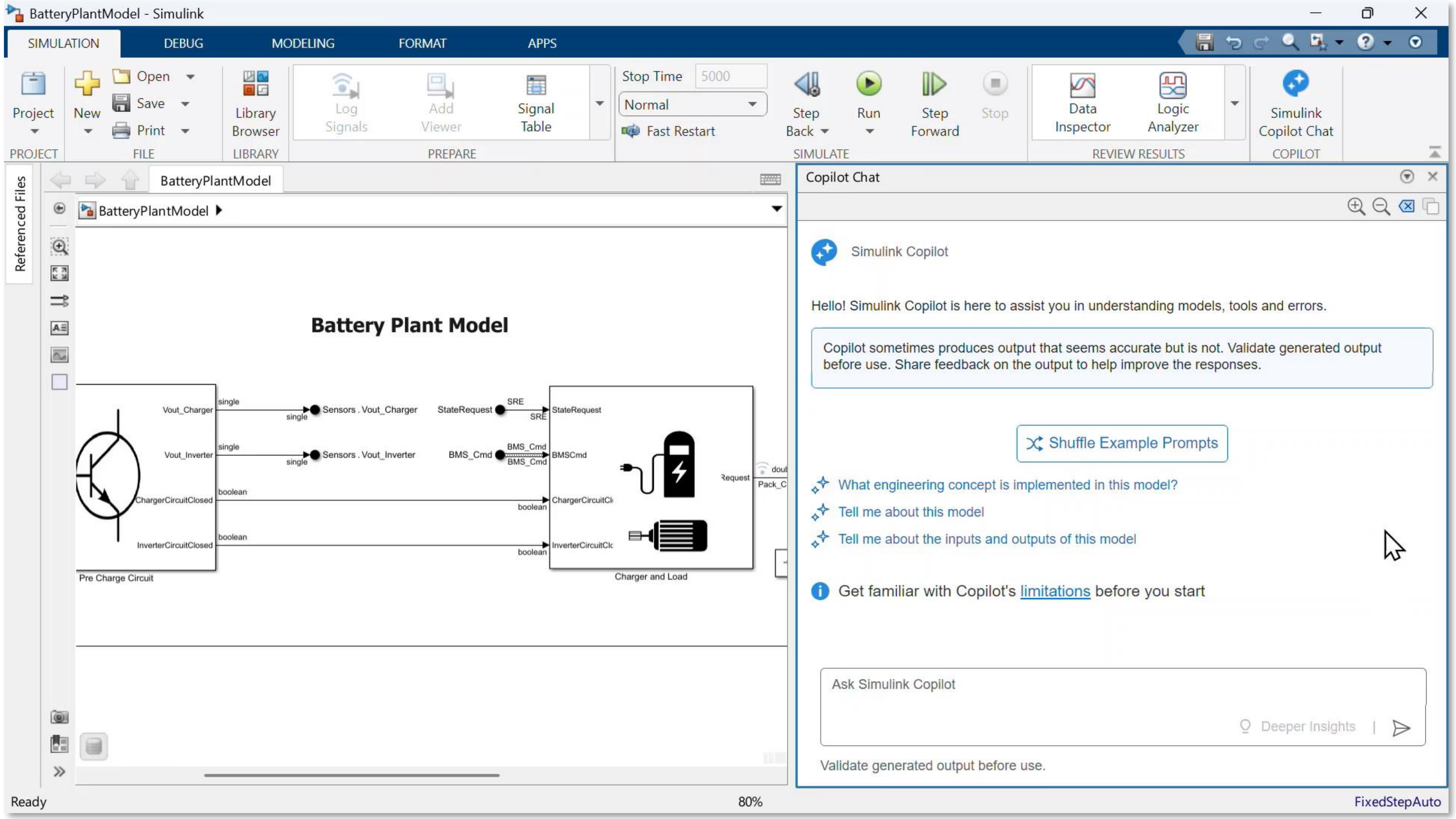
Fault Injection Testing – Validate safety of systems by simulation

Agenda of this session

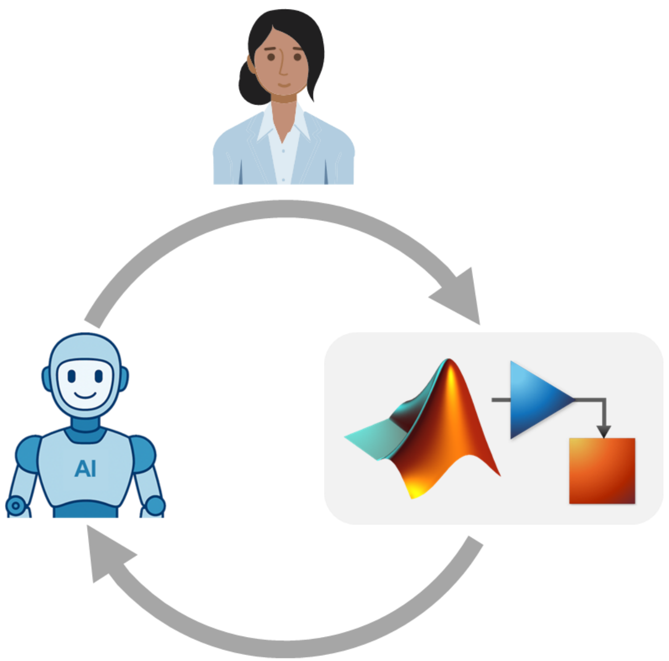
- Importance of safety in systems development
- Safety analysis workflow: BMS case study
- AI-Assisted Model-Based Systems Engineering

Simulink Copilot is built to help with our everyday work

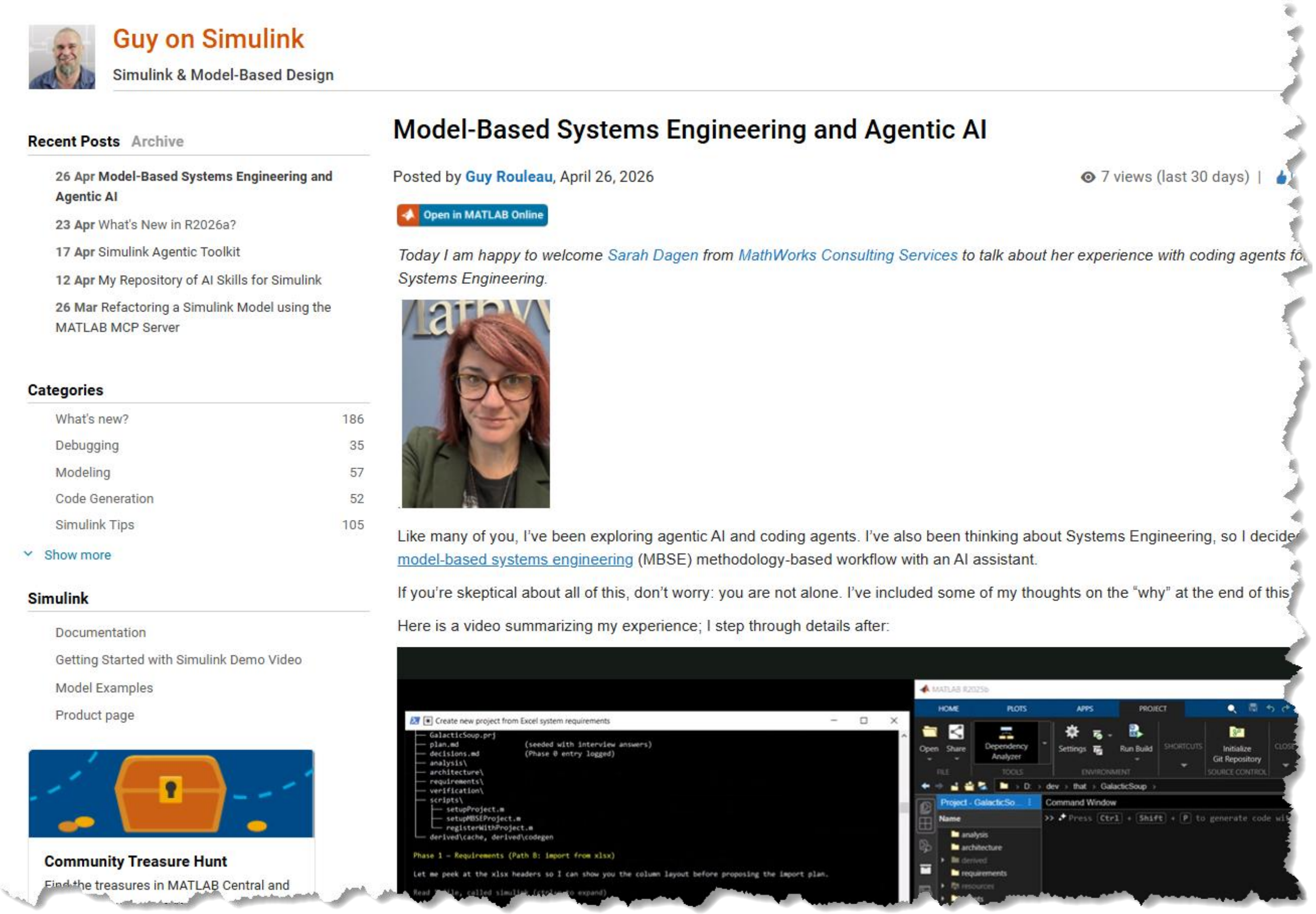
- ✓ Chat & Learn
- ✓ Understand
- ✓ Search
- ✓ Analyze & Implement



MBSE and Agentic AI: What might this actually look like…



…with **Simulink Agentic Toolkit**?



Guy on Simulink

Simulink & Model-Based Design

Recent Posts Archive

26 Apr Model-Based Systems Engineering and Agentic AI

23 Apr What's New in R2026a?

17 Apr Simulink Agentic Toolkit

12 Apr My Repository of AI Skills for Simulink

26 Mar Refactoring a Simulink Model using the MATLAB MCP Server

Categories

What's new?	186
Debugging	35
Modeling	57
Code Generation	52
Simulink Tips	105

Show more

Simulink

Documentation

Getting Started with Simulink Demo Video

Model Examples

Product page

Community Treasure Hunt

Find the treasures in MATLAB Central and

Model-Based Systems Engineering and Agentic AI

Posted by Guy Rouleau, April 26, 2026 — 7 views (last 30 days) |

Open in MATLAB Online

Today I am happy to welcome Sarah Dagen from MathWorks Consulting Services to talk about her experience with coding agents fo Systems Engineering.

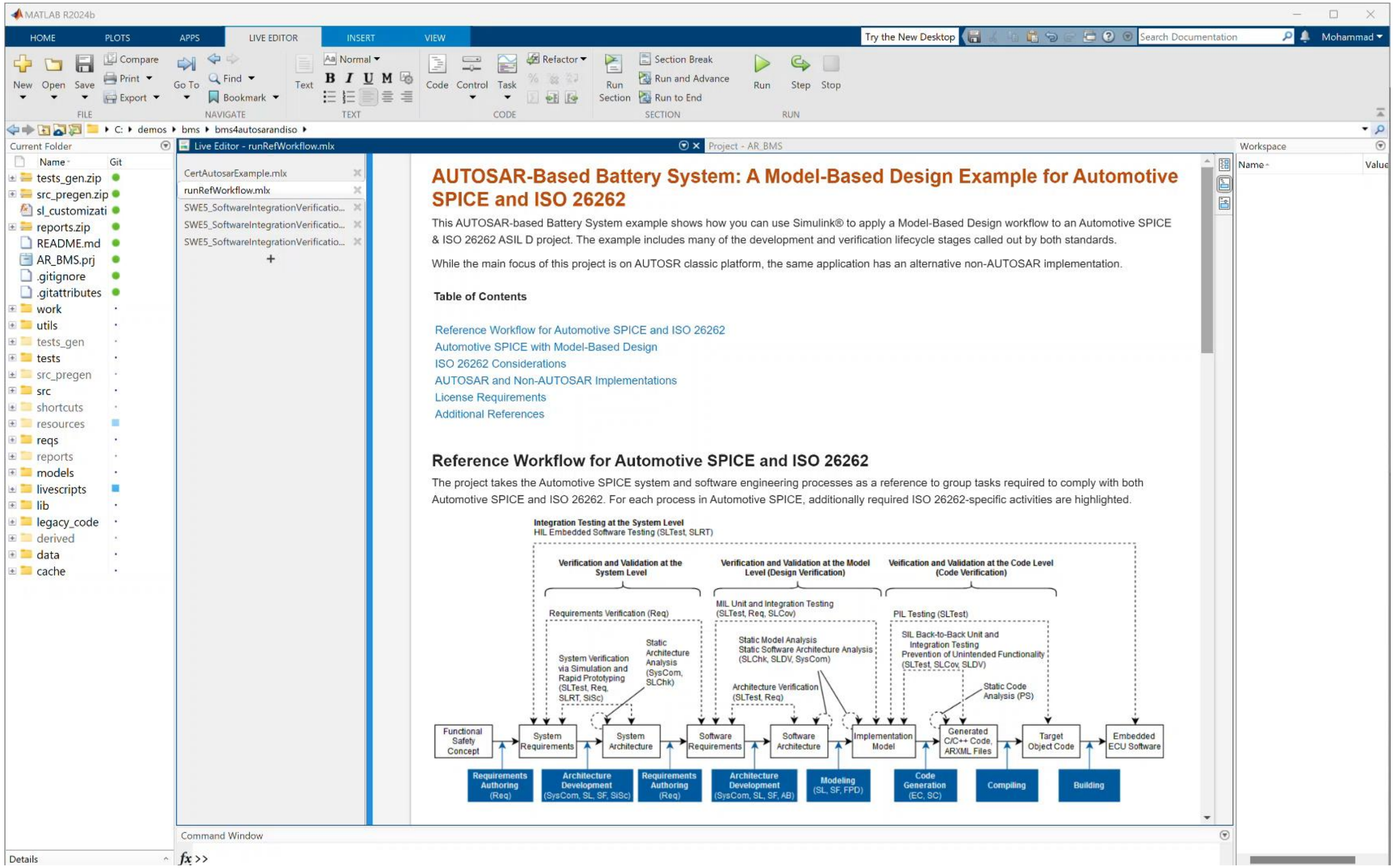
Like many of you, I've been exploring agentic AI and coding agents. I've also been thinking about Systems Engineering, so I decide model-based systems engineering (MBSE) methodology-based workflow with an AI assistant.

If you're skeptical about all of this, don't worry: you are not alone. I've included some of my thoughts on the "why" at the end of this

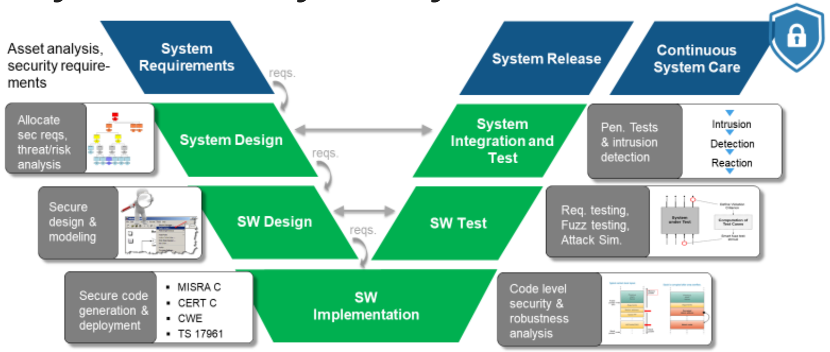
Here is a video summarizing my experience; I step through details after:

https://blogs.mathworks.com/simulink/2026/04/26/model-based-systems-engineering-and-agentic-ai/

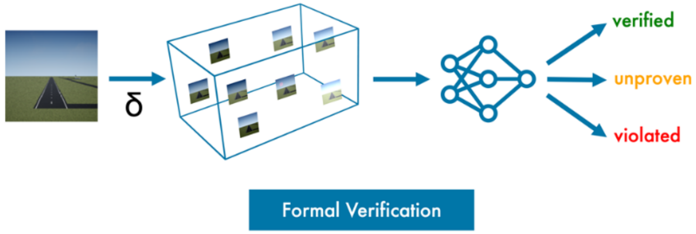
Leverage Model-Based Systems Engineering to build safer, more secure and smarter systems



Reference Example: Model-Based Cybersecurity Analysis



Reference example: Verifying Safety-Critical Deep Learning System



Feel free to ask!

Valtteri Forsman
Application Engineer
MathWorks
vforsman@mathworks.com