2025 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION EUROPE

MUNICH, GERMANY
OCTOBER 14-15, 2025

Cybersecurity: A Model-Based Systems Engineering Approach to Risk Analysis and Mitigation

Marco Bimbi

Principal Application Engineer – MBSE

MathWorks®

accellera SYSTEMS INITIATIVE

While We Give an Introduction…

Open the tutorial in MATLAB Online (trial license included)

1) Go to tinyurl.com/dvcon25-cybersec

2) Click on 

3) Double-click on **Robot.prj**

Or use your own MATLAB Online account (license required)

1) Go to https://github.com/mathworks/example-security-risk-analysis

2) Click on 

Today’s Agenda

- Trends in Modern Product Development
- Why Safe does not exists without Secure
- Model-based security workflow Case Study
- Conclusion & Take Away
- What about SysML v2?

Today’s Agenda

- Trends in Modern Product Development
- Why Safe does not exists without Secure
- Model-based security workflow Case Study
- Conclusion & Take Away
- What about SysML v2?

Trends in Modern Product Development

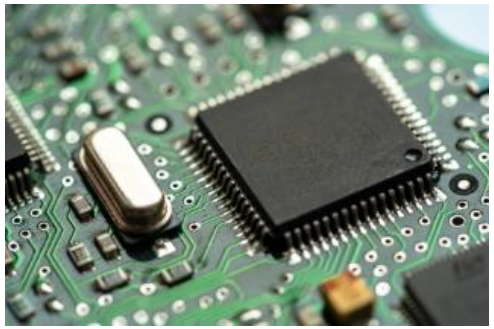
More Connectivity

Increased amount of access points to critical components

More Autonomy

Decision making is no longer only human

More COTS Tech.



Generic platforms, easy access, suited for critical systems?

More Standardization

IEC 62443

ISO/SAE 21434

DO-326A set

Why is security relevant for embedded systems now?

More Targets
More Devices

More Connectivity
More Damage

Cheaper Technology
More Adversaries

§ISO21434, UNECE

§DO-326A set

§CRA, IEC 62443

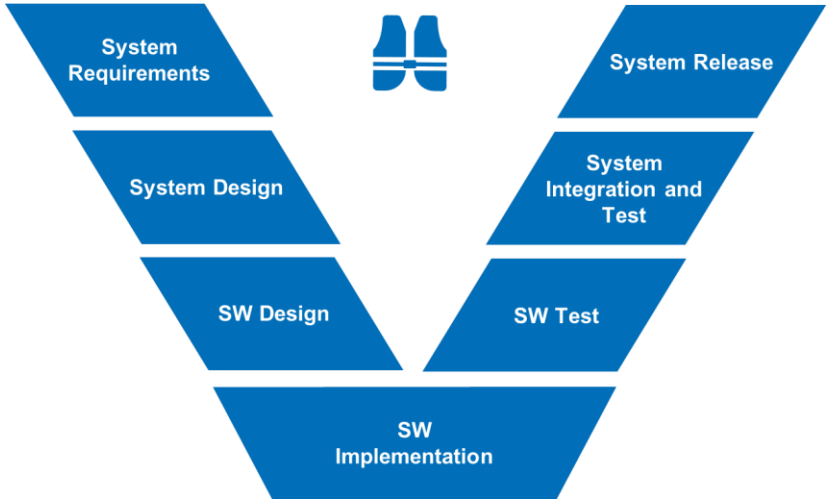
CE

Type approval / trade permission

Today’s Agenda

- Trends in Modern Product Development
- **Why Safe does not exists without Secure**
- Model-based security workflow Case Study
- Conclusion & Take Away
- What about SysML v2?

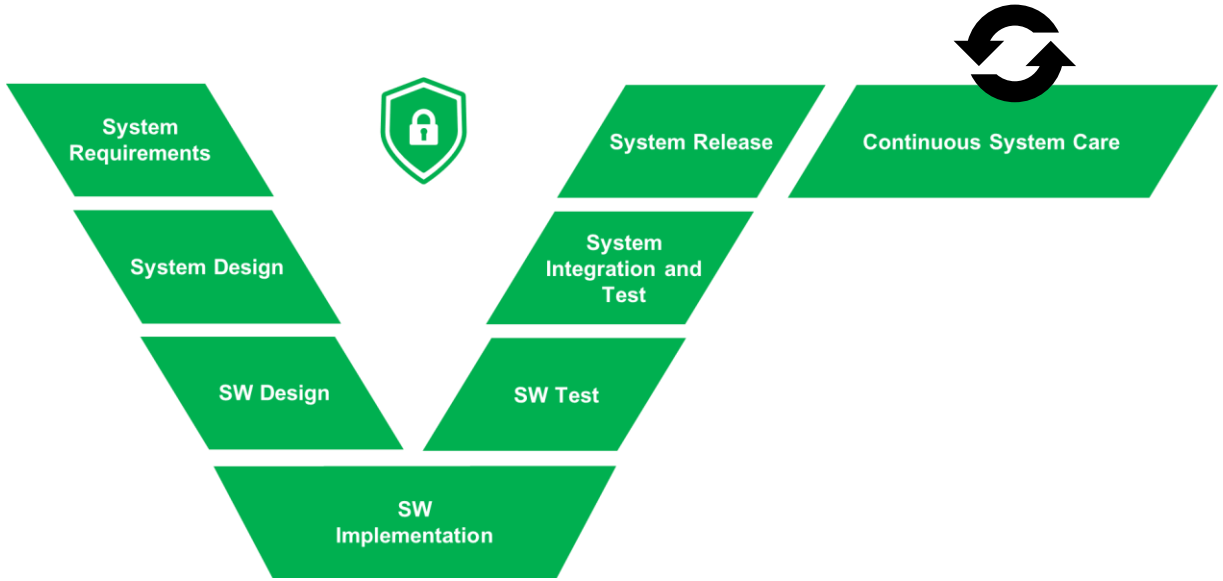
Safety



Old aspects:

- Design for reliability/failure
- Focus on what is known
- Rigorous testing
- …

Security

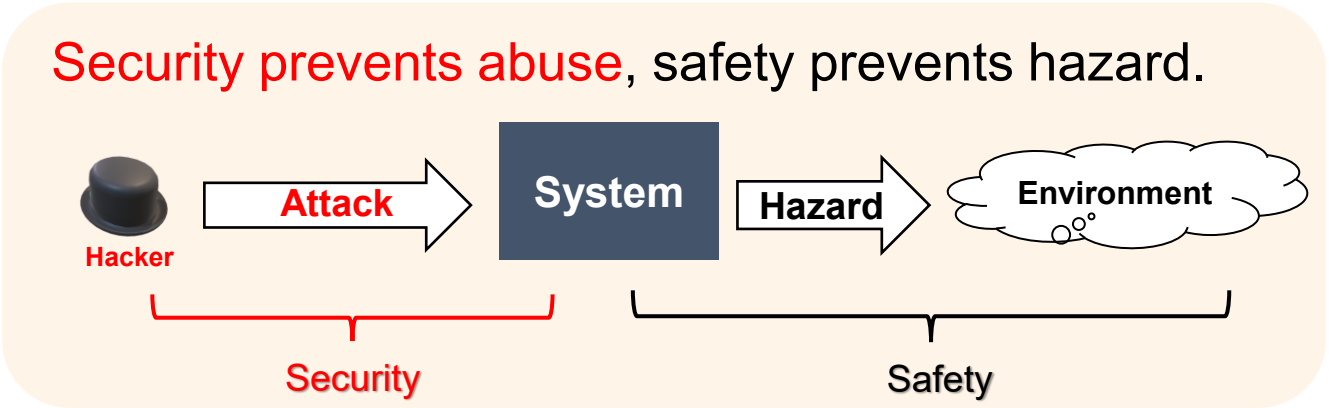


New aspects:

- Design for malicious attacks
- Focus on what is unknown (“more paranoia”)
- Incident monitoring & updates (repeated V-cycle)
- …

Systems cannot be safe without being secure

- Safety: "**Absence of hazard**"
  - Negative consequences on user(s) and environment, e.g., injury, loss of lives, catastrophic environmental impact
- Security: "**Safe and proper system operation** in presence of Adversaries"
  - Absence of hazard in presence of adversaries



Takeaway

Systems cannot be safe without being secure.

Today’s Agenda

- Trends in Modern Product Development
- Why Safe does not exists without Secure
- **Model-based security workflow Case Study**
- Conclusion & Take Away
- What about SysML v2?

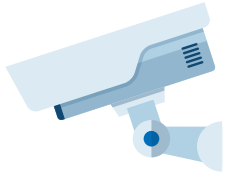
This Workshop: Security Risk Analysis (a.k.a. TARA, SRA)

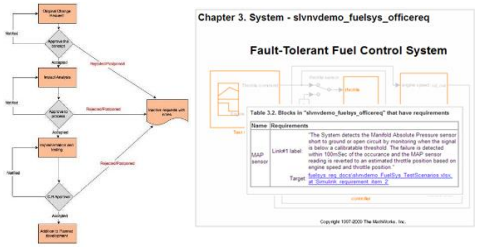
Identify assets & threats

Calculate security risk

Define & verify countermeasures

Update Risk Model & **Reporting**





Where are the weaknesses?
What applies to my architecture?
Am I missing something?

How realistic is the attack?
What would be the damage?
What is the weakest link?

Which threat is worth addressing?
How to protect?
Protection sufficient?

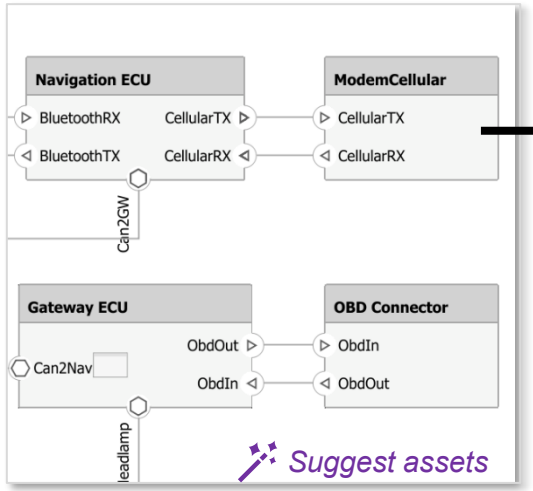
How to update the risk?
How to generate documentation and report?

Model-Based Approach to Threat and Risk Analysis

System Composer

Safety Analysis Manager

1 Architecture Models



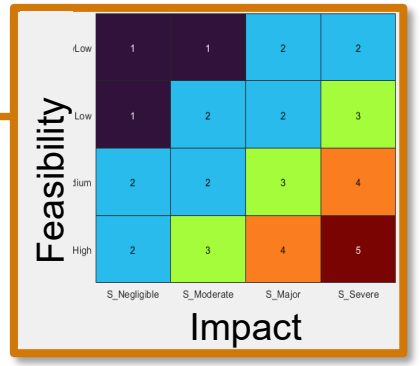
2 Asset Scan

3 Static Analysis

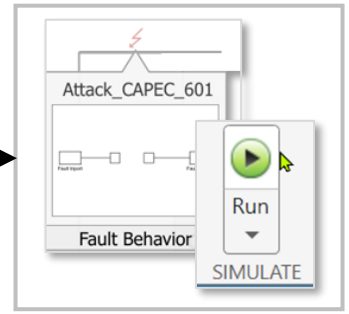
Threat	LinkedAsset	LinkedDamages	RiskSaf	CAL	LinkedGoal	Status
Compromised Firmware	1x: SHT: assets:1	1x: damage_scenarios:7	R_Low	CAL2	SG1	Unreviewed
Something			R_Negligible	None		Reduce
Spoofing "lamp request"	1x: SHT: assets:2	2x: damage_scenarios:4, damage_scenarios:3	R_High	CAL4	SG2	Reduce
Tampering "lamp request"	1x: SHT: assets:2	1x: damage_scenario	R_High	CAL4		Reduce

Suggest threats

Auto-Calculated Risk



Simulate Attack



$f(x)$

1 error
- Too low for the associated level of threat. Add countermeasures!

Enforced Threat and Risk Model

Reporting

PDF

Security Goals

Suggest countermeasures

Fully customizable

Fully consistent

Fully traceable

Takeaways – Security Risk Analysis with Model-Based Design

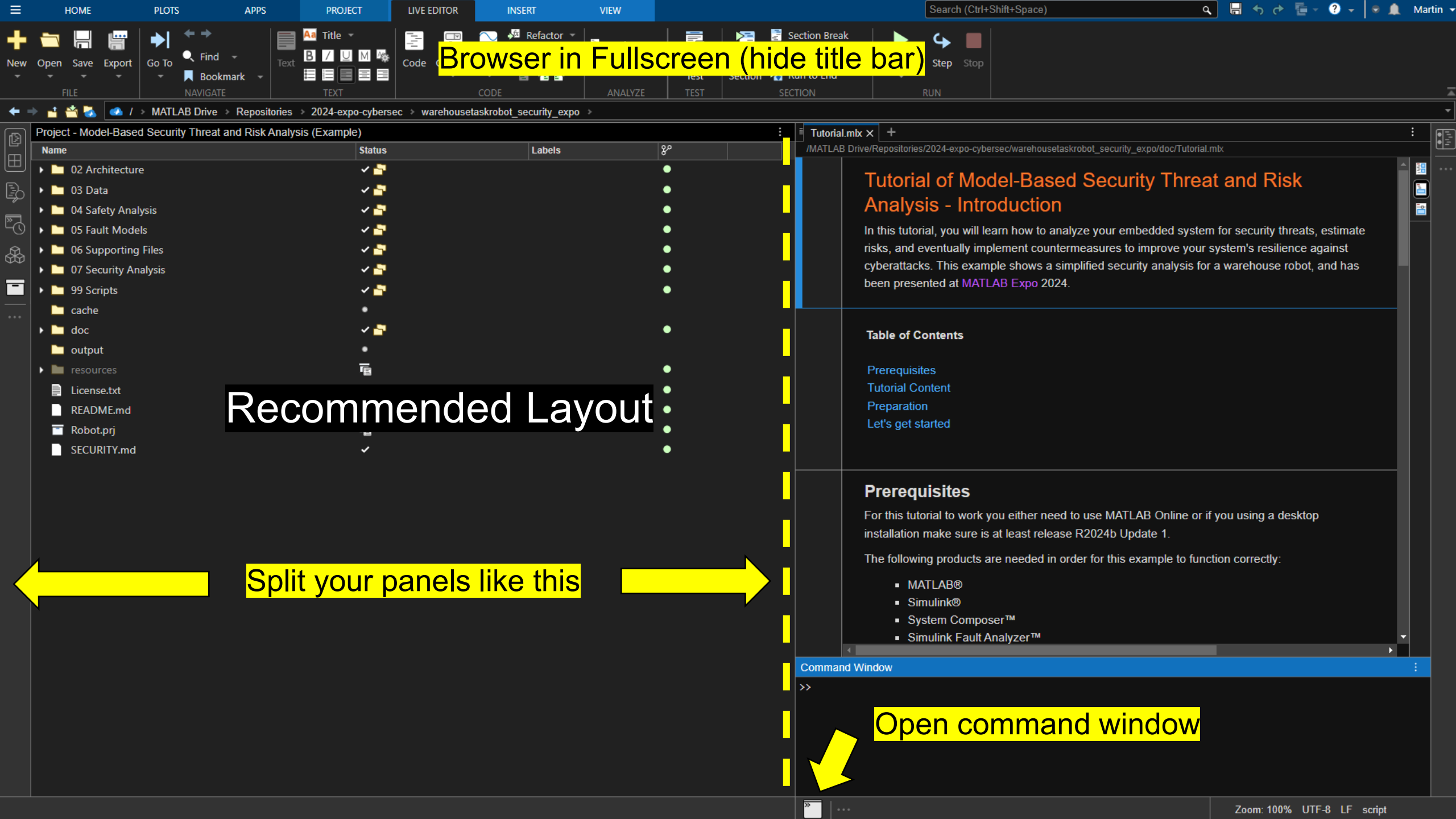
Provides tight coupling/augmentation between design, safety and security

Guides you through the steps of risk analysis and mitigation

Helps to “shift left” to validate and verify your security measures early

Let’s build a safe and secure …

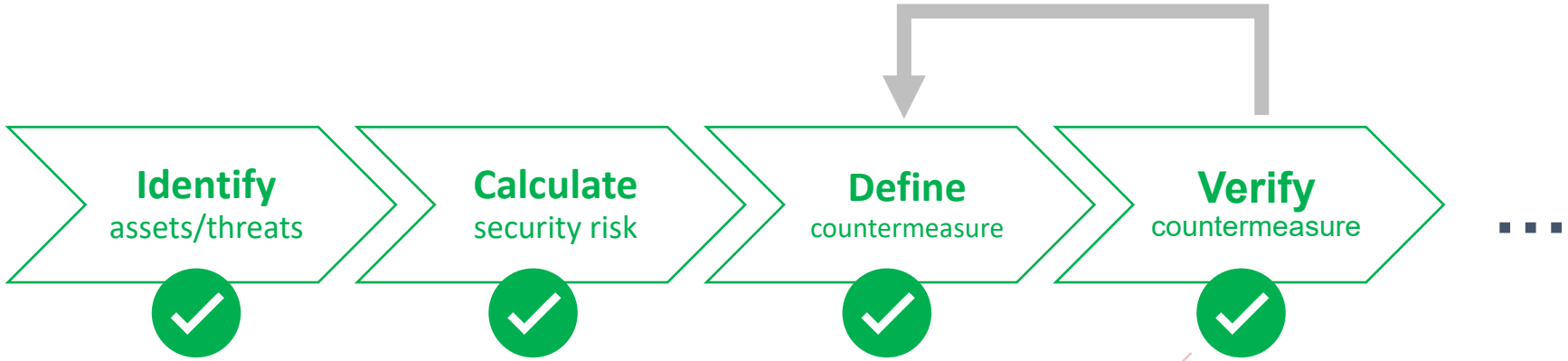
… warehouse robot


HOME
PLOTS
APPS
PROJECT
LIVE EDITOR
INSERT
VIEW
Search (Ctrl+Shift+Space)
Martin
New
Open
Save
Export
Go To
Find
Bookmark
Text
Title
Code
Refactor
Section Break
Step
Stop
FILE
NAVIGATE
TEXT
CODE
ANALYZE
TEST
SECTION
RUN
Browser in Fullscreen (hide title bar)
/ MATLAB Drive Repositories 2024-expo-cybersec warehousetaskrobot_security_expo
Project - Model-Based Security Threat and Risk Analysis (Example)
Name
Status
Labels
02 Architecture
03 Data
04 Safety Analysis
05 Fault Models
06 Supporting Files
07 Security Analysis
99 Scripts
cache
doc
output
resources
License.txt
README.md
Robot.prj
SECURITY.md
Recommended Layout
Split your panels like this
Tutorial.mlx
/MATLAB Drive/Repositories/2024-expo-cybersec/warehousetaskrobot_security_expo/doc/Tutorial.mlx
Tutorial of Model-Based Security Threat and Risk Analysis - Introduction
In this tutorial, you will learn how to analyze your embedded system for security threats, estimate risks, and eventually implement countermeasures to improve your system's resilience against cyberattacks. This example shows a simplified security analysis for a warehouse robot, and has been presented at MATLAB Expo 2024.
Table of Contents
Prerequisites
Tutorial Content
Preparation
Let's get started
Prerequisites
For this tutorial to work you either need to use MATLAB Online or if you using a desktop installation make sure is at least release R2024b Update 1.
The following products are needed in order for this example to function correctly:
MATLAB®
Simulink®
System Composer™
Simulink Fault Analyzer™
Command Window
>>
Open command window
Zoom: 100%
UTF-8
LF
script

Today’s Agenda

- Trends in Modern Product Development
- Why Safe does not exists without Secure
- Model-based security workflow Case Study
- **Conclusion & Take Away**
- What about SysML v2?

Recap: What We Have Learned So Far



Outlook: Residual Risk Analysis

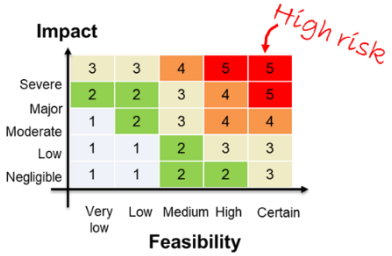
Identify assets/threats

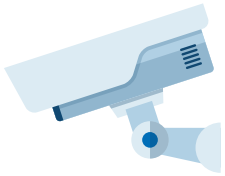
Calculate security risk

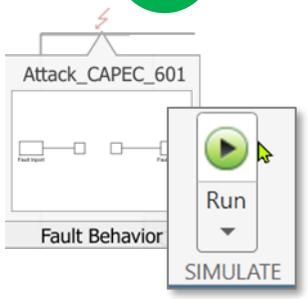
Define countermeasure

Verify countermeasure

Update feasibility and impact



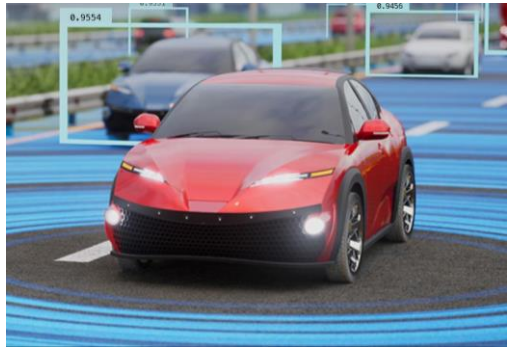




Difficulty of attack increased?
Severity of damage reduced?
Is the remaining risk acceptable?

Details depend on regulation and standards!

Industry-Specific Risk Analysis Templates Available



§ ISO21434, UNECE

§ IEC 62443,
EU Cyber Resilience Act

§ DO-326A set

Outlook: Automated Threat Modeling and Analysis

Takeaways

Provides tight coupling/augmentation between design, safety and security

Guides you through the steps of risk analysis and mitigation

Helps to “shift left” to validate and verify your security measures early

➔ Try at your own pace – Your trial license is valid for several days.

Today’s Agenda

- Trends in Modern Product Development
- Why Safe does not exists without Secure
- Model-based security workflow Case Study
- Conclusion & Take Away
- What about SysML v2?

SysML v2 Background – why a new language?

v1	✗ Based on UML	✗ Diagram-oriented communication	✗ Weak file-based interoperability
v2	✓ Language specialized for systems	✓ Conducive to formal analysis & flexible visualizations	✓ Standard service-based API to access the model

"Interoperability Live – SysML v2 API in Action" Blog Article

- Creation of requirements, functional & physical architecture SysML v2
- Visualization of model
- Usage of the system model data for mass calculation in the CAD tool
- Update of parameters in system model from CAD tool
- Usage of system model data for preparation of life cycle assessment (LCA)
- Usage of system model data for solving a constraint optimization problem

2023 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION EUROPE 10 YEAR ANNIVERSARY

Questions?

Marco Bimbi - marcob@mathworks.com

accellera SYSTEMS INITIATIVE

2023 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION EUROPE 10 YEAR ANNIVERSARY

Thank You!!

Marco Bimbi - marcob@mathworks.com

accellera SYSTEMS INITIATIVE