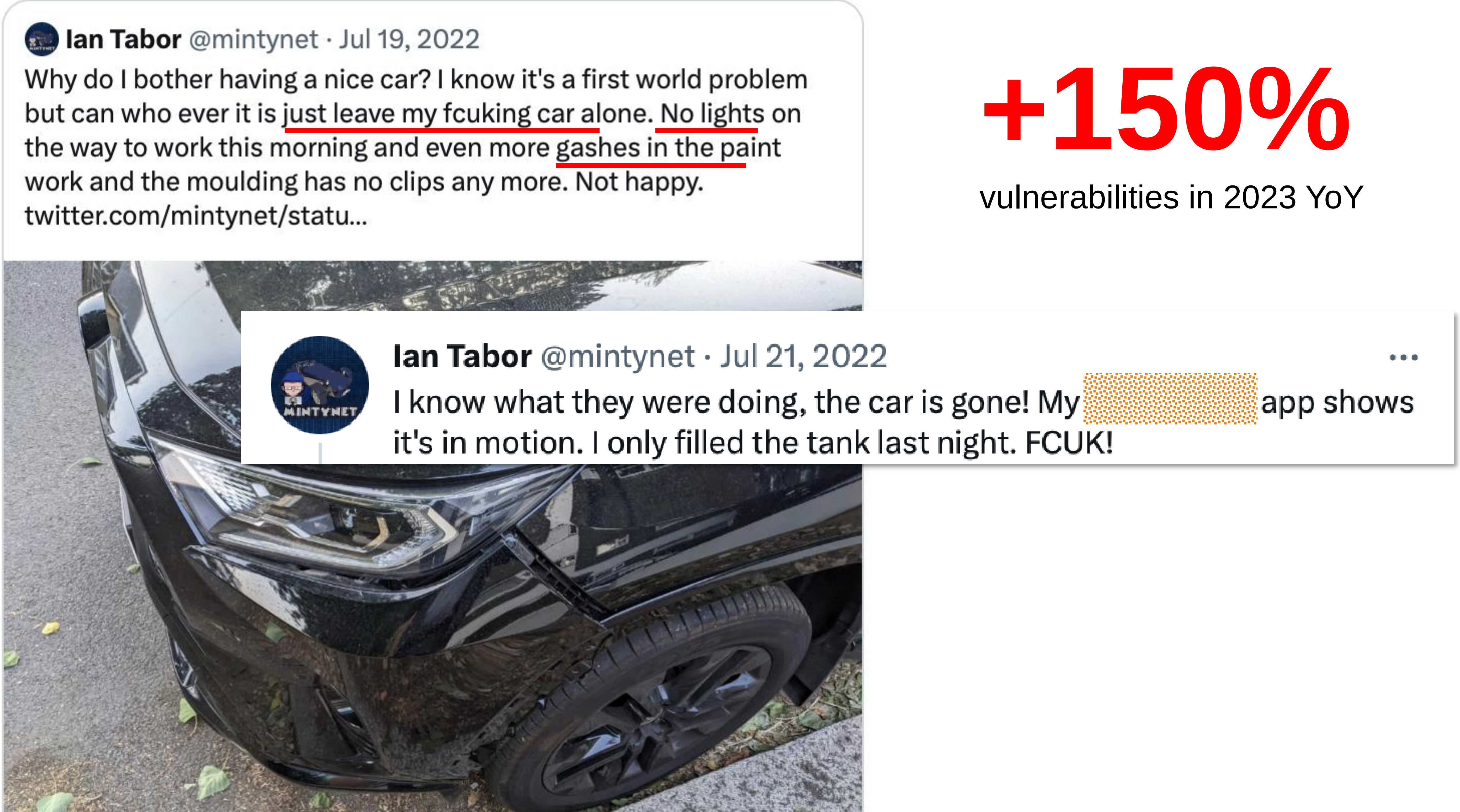
MathWorks
AUTOMOTIVE CONFERENCE 2024
Europe

Cybersecurity: ISO/SAE 21434 and UNECE with Model-Based Design

Dr. Martin Becker, The MathWorks

MathWorks



Ian Tabor @mintynet · Jul 19, 2022

Why do I bother having a nice car? I know it's a first world problem but can who ever it is just leave my fcuking car alone. No lights on the way to work this morning and even more gashes in the paint work and the moulding has no clips any more. Not happy. twitter.com/mintynet/statu...

Ian Tabor @mintynet · Jul 21, 2022

I know what they were doing, the car is gone! My [redacted] app shows it's in motion. I only filled the tank last night. FCUK!

+150%

vulnerabilities in 2023 YoY

Agenda

- Cybersecurity is now mandatory.
- Agility and consistency are key to get cybersecurity.
- Your existing MBD tools can do cybersecurity!

Agenda

- Cybersecurity is now mandatory.
- Agility and consistency are key to get cybersecurity.
- Your existing MBD tools can do cybersecurity!

55 days remaining to become secure… (today is 2024 May 7th)

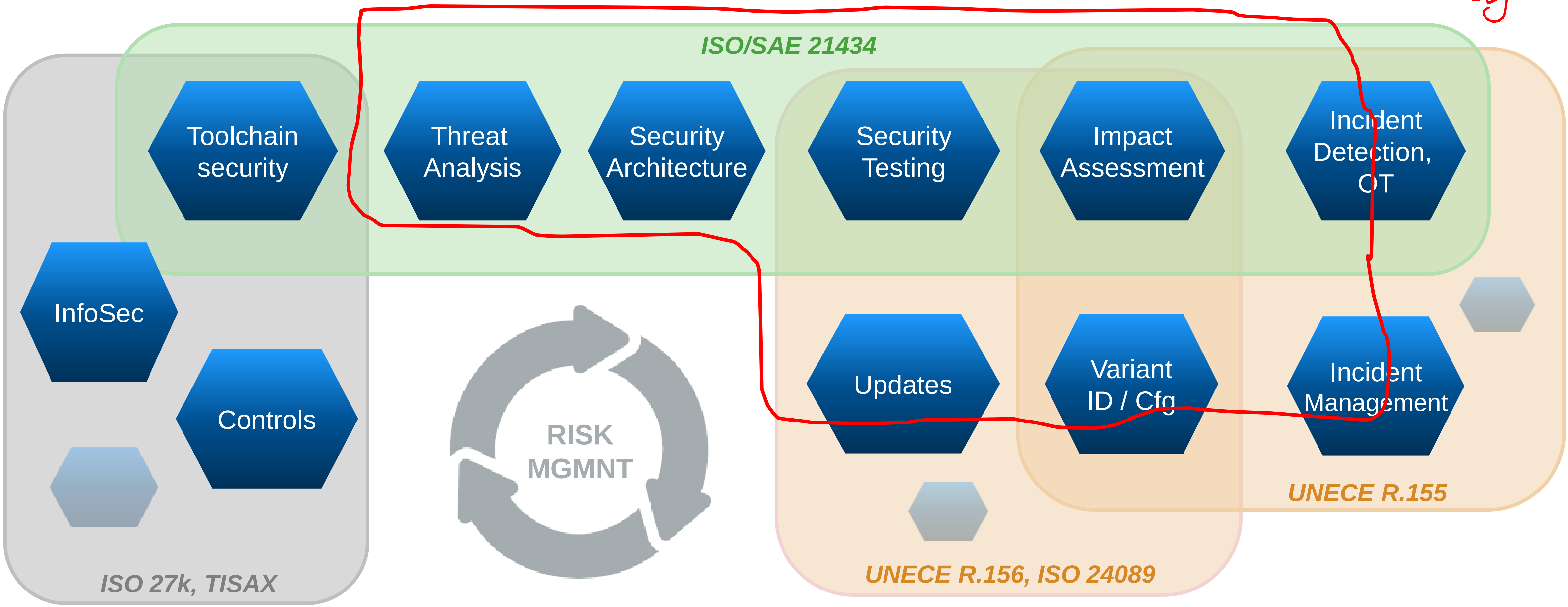
- **UN Regulations**
- Cybersecurity Management System (CSMS)
- Software Update Management System (SUMS)
- **Required for Type Approval**

UN R155
UN R156
a
E 4
a/3
15X

Production stop: VW Up, T6.1, Porsche Boxter, Macan, Renault Zoe, Audi TT…

The Big Cybersecurity Picture

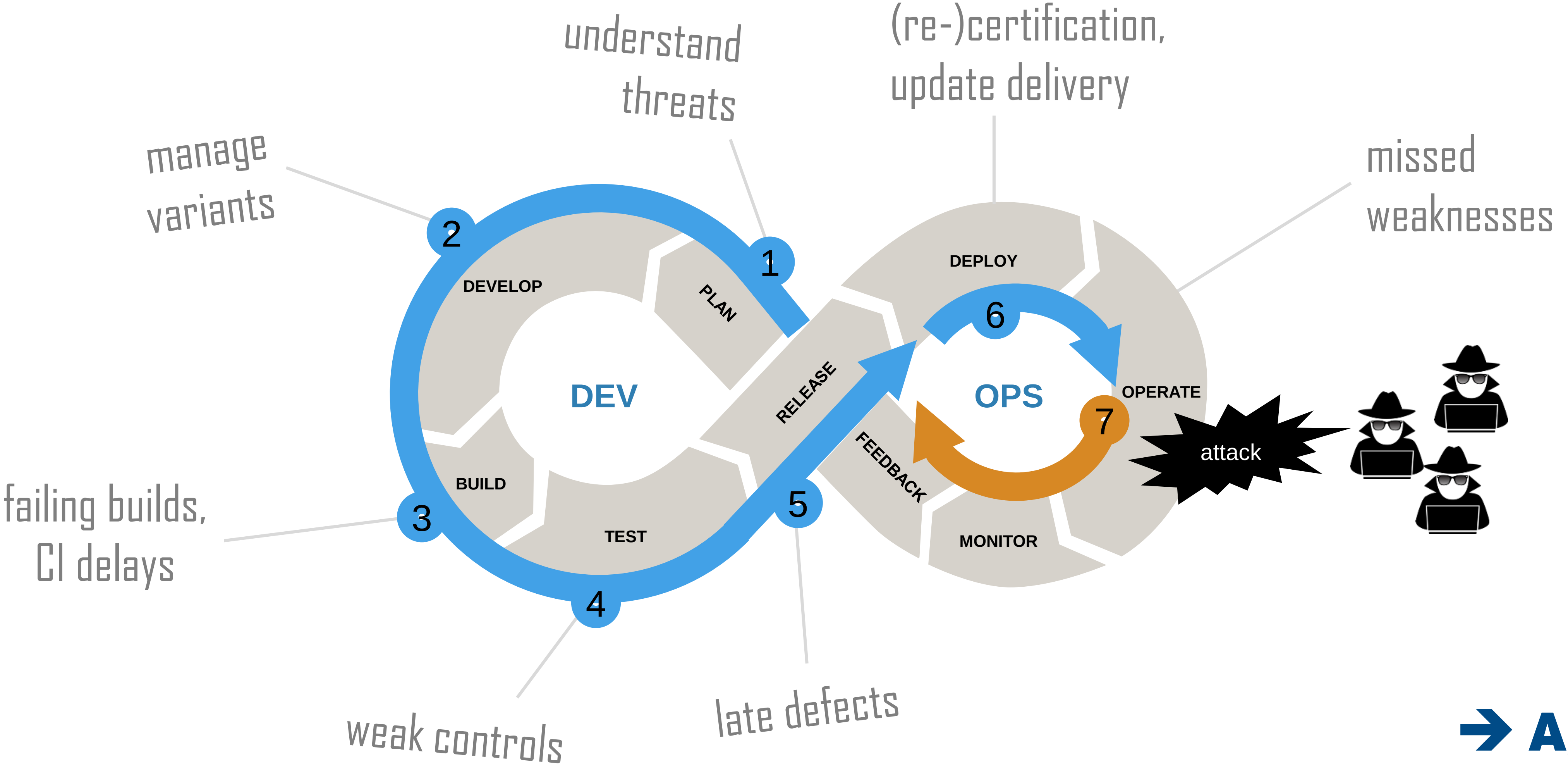
This talk:
Embedded Security



Agenda

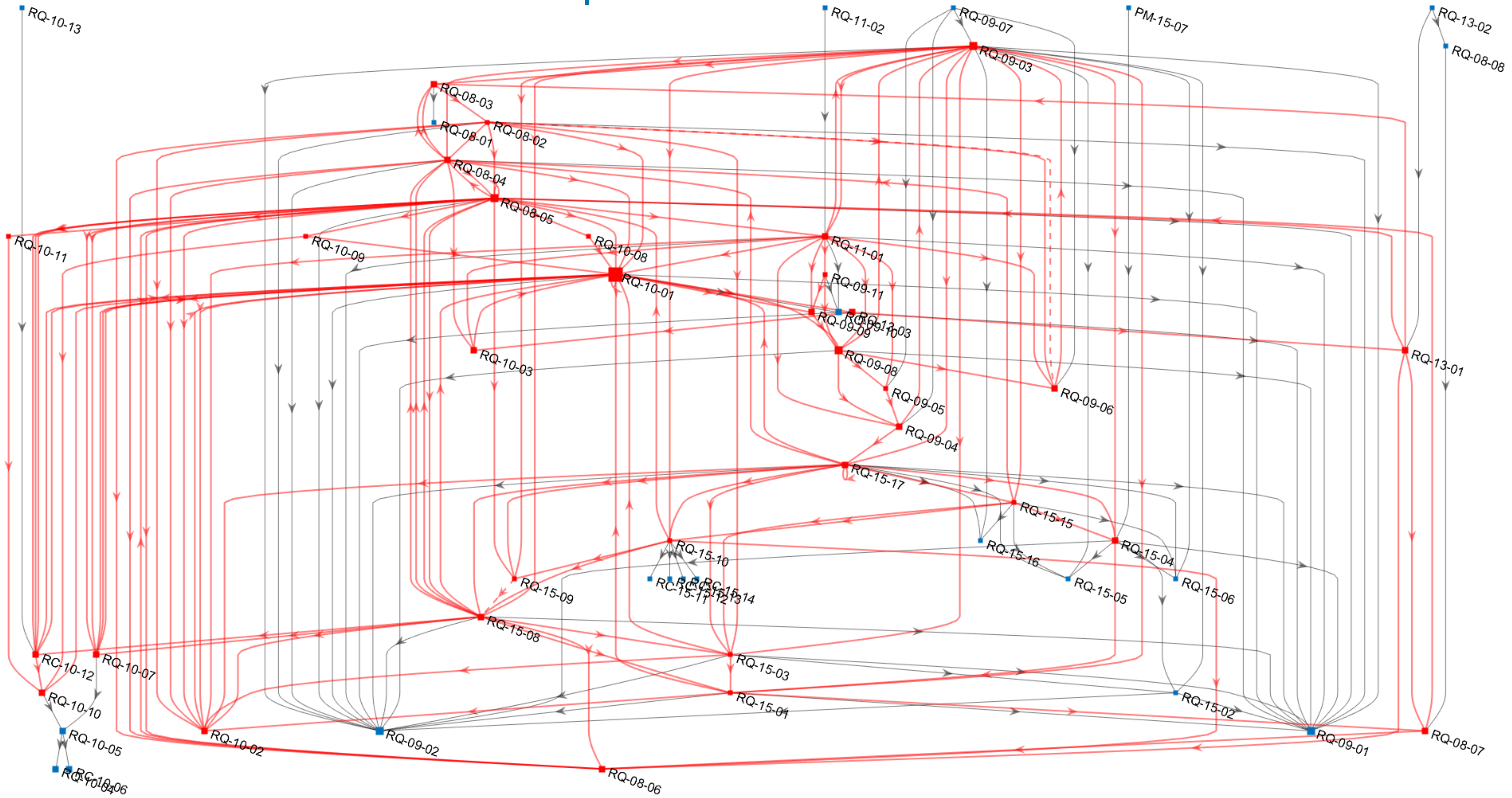
- Cybersecurity is now mandatory.
- Agility and consistency are key to get cybersecurity.
- Your existing MBD tools can do cybersecurity!

The repeating challenges of Cybersecurity



→ Agility & Consistency

ISO/SAE 21434: It’s complicated…

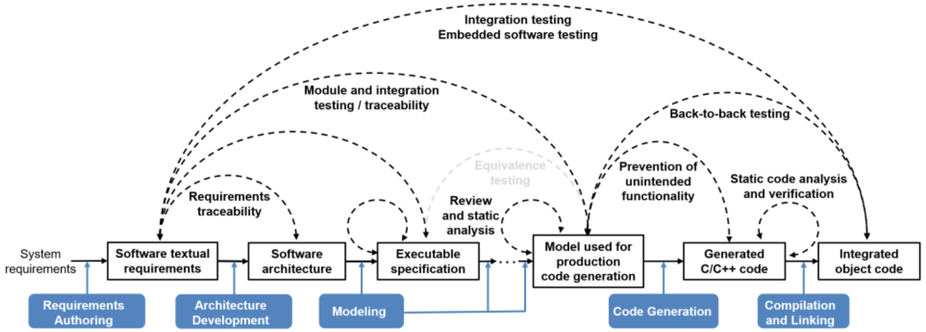


Good News: Compliance with ISO/SAE 21434, R.15x and ASPICE

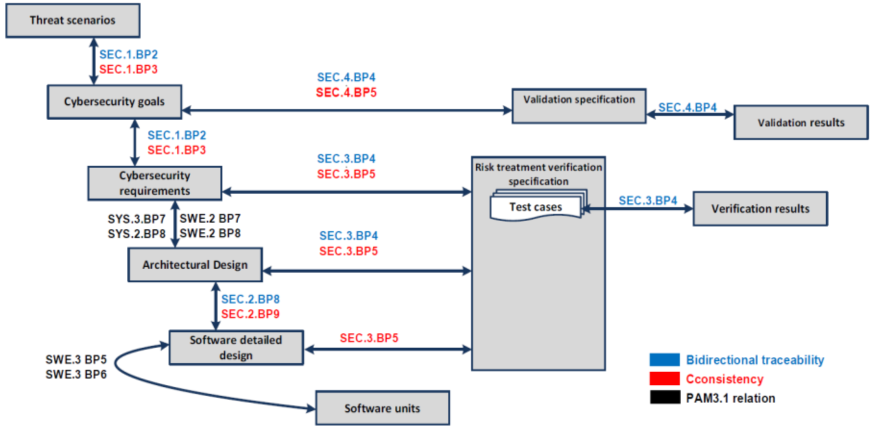
IEC Certification Kit

Model-Based Design for ISO/SAE 21434:2021 Road vehicles — Cybersecurity engineering

R2022a


Integration testing
Embedded software testing
Module and integration testing / traceability
Back-to-back testing
Equivalence testing
Prevention of unintended functionality
Static code analysis and verification
Requirements traceability
Review and static analysis
System requirements
Software textual requirements
Software architecture
Executable specification
Model used for production code generation
Generated C/C++ code
Integrated object code
Requirements Authoring
Architecture Development
Modeling
Code Generation
Compilation and Linking

- Same tools & models as for ISO 26262
- Reference workflow unchanged
- Covers essential topics



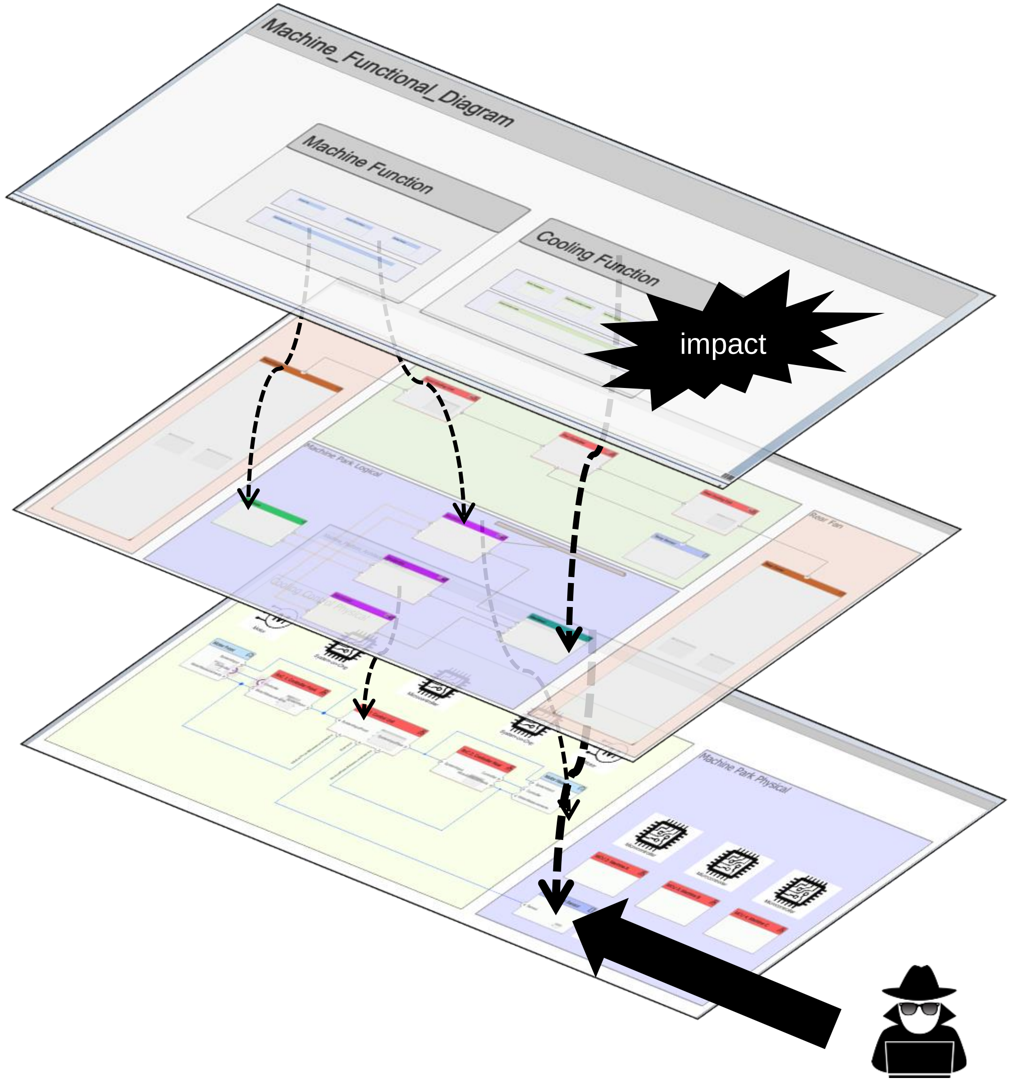
https://www.mathworks.com/solutions/automotive/standards/iso-21434.html

Agenda

- Cybersecurity is now mandatory.
- Agility and consistency are key to get cybersecurity.
- Your existing MBD tools can do cybersecurity!

Model-Based Design: Digital Threa*d* instead of Digital Threa*t*

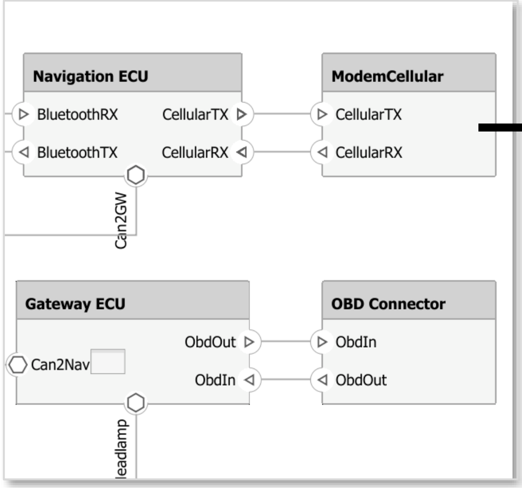
- From security goals to code
- Understand attack impact and change through traceability
- Security through analysis & sim.
- Quick updates with codegen
- **Examples …**



Model-Based Threat Analysis & Risk Assessment (TARA)

System Composer

1 Architecture Models



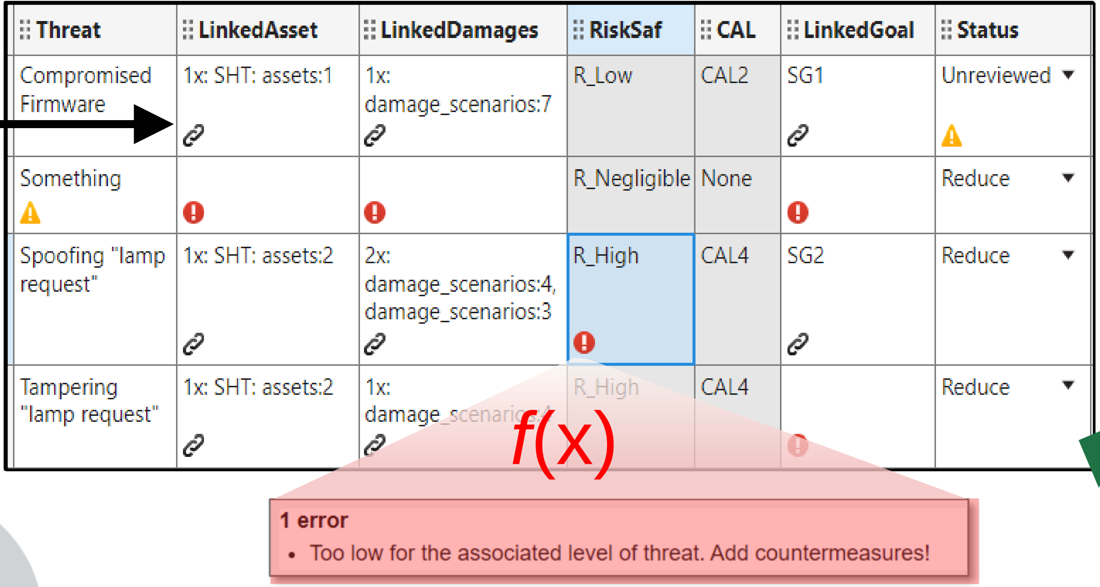
2 asset scan

NEW

Safety Analysis Manager

3 Static analysis

Auto-calculated risk



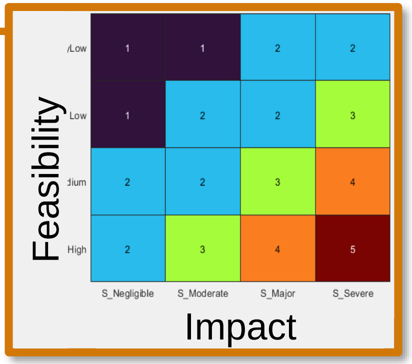
Threat	LinkedAsset	LinkedDamages	RiskSaf	CAL	LinkedGoal	Status
Compromised Firmware	1x: SHT: assets:1	1x: damage_scenarios:7	R_Low	CAL2	SG1	Unreviewed ▾ ⚠
Something ⚠	❗	❗	R_Negligible	None	❗	Reduce ▾
Spoofing "lamp request"	1x: SHT: assets:2	2x: damage_scenarios:4, damage_scenarios:3	R_High ❗	CAL4	SG2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

f(x)

1 error

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

Enforced Threat & Risk Model



Feasibility	S_Negligible	S_Moderate	S_Major	S_Severe
/Low	1	1	2	2
Low	1	2	2	3
dium	2	2	3	4
High	2	3	4	5

Impact

Risk matrix

import/export

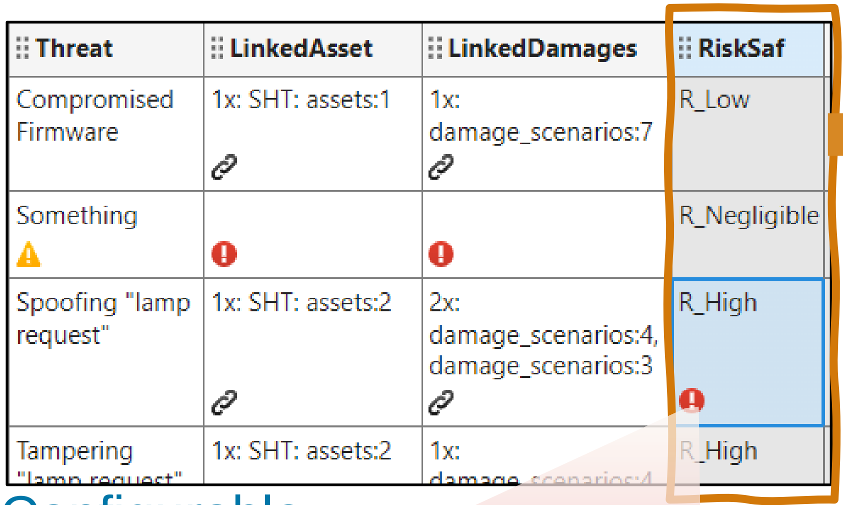
PDF

4 Security Goals

✔ **Fully consistent**

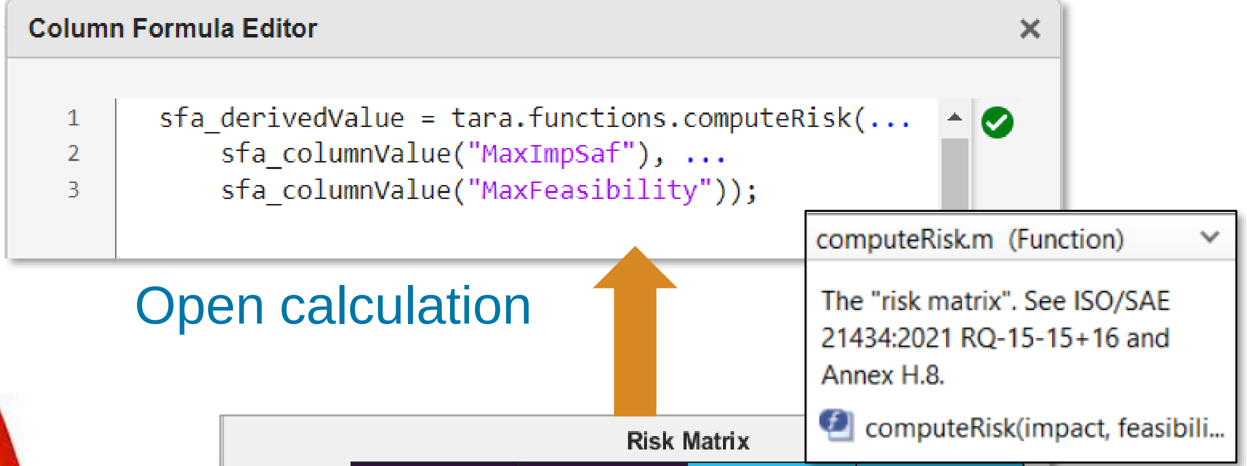
Fully traceable

Model-based TARA - Fully Customizable Templates



Threat	LinkedAsset	LinkedDamages	RiskSaf
Compromised Firmware	1x: SHT: assets:1 🔗	1x: damage_scenarios:7 🔗	R_Low
Something ⚠	❗	❗	R_Negligible
Spoofing "lamp request"	1x: SHT: assets:2 🔗	2x: damage_scenarios:4, damage_scenarios:3 🔗	R_High ❗
Tampering "lamp request"	1x: SHT: assets:2	1x: damage_scenarios:4	R_High

Configurable tables



Column Formula Editor

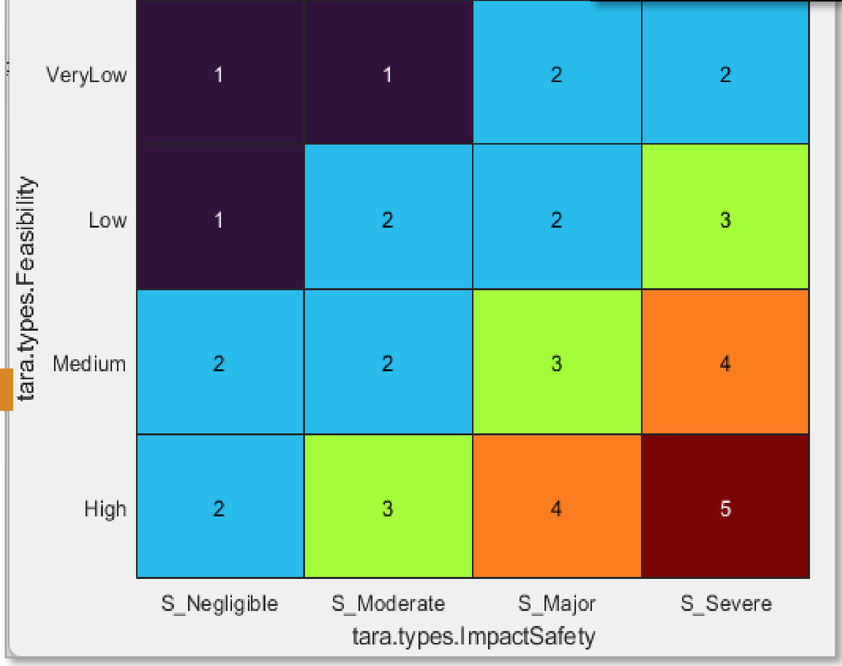
```
sfa_derivedValue = tara.functions.computeRisk(...
    sfa_columnValue("MaxImpSaf"), ...
    sfa_columnValue("MaxFeasibility"));
```

computeRisk.m (Function)

The "risk matrix". See ISO/SAE 21434:2021 RQ-15-15+16 and Annex H.8.

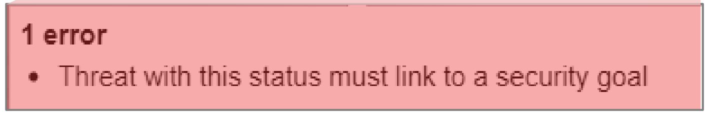
computeRisk(impact, feasibili...

Open calculation



Risk Matrix

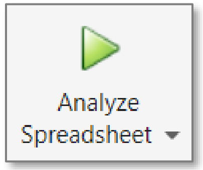
tara.types.Feasibility	S_Negligible	S_Moderate	S_Major	S_Severe
VeryLow	1	1	2	2
Low	1	2	2	3
Medium	2	2	3	4
High	2	3	4	5

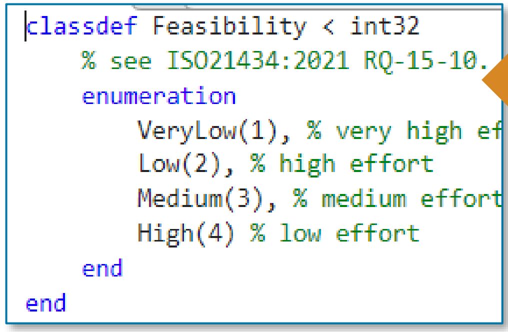


1 error

- Threat with this status must link to a security goal

Your own validation checks



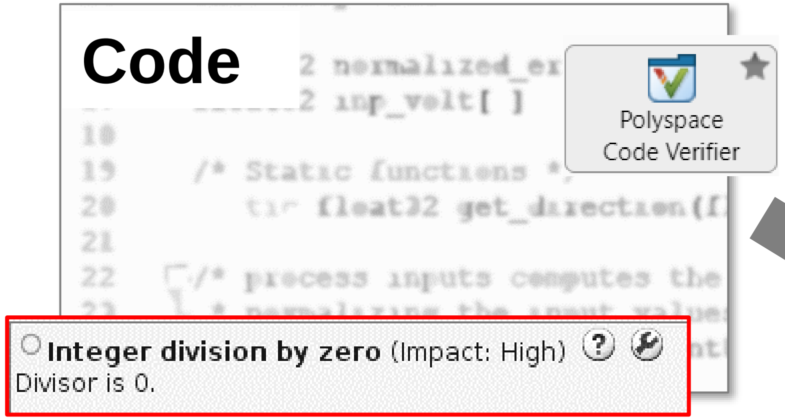


```
classdef Feasibility < int32
    % see ISO21434:2021 RQ-15-10.
    enumeration
        VeryLow(1), % very high ef
        Low(2), % high effort
        Medium(3), % medium effort
        High(4) % low effort
    end
end
```

Extensible types

Vulnerability Analysis (& less iterations) at Multiple Levels

Code

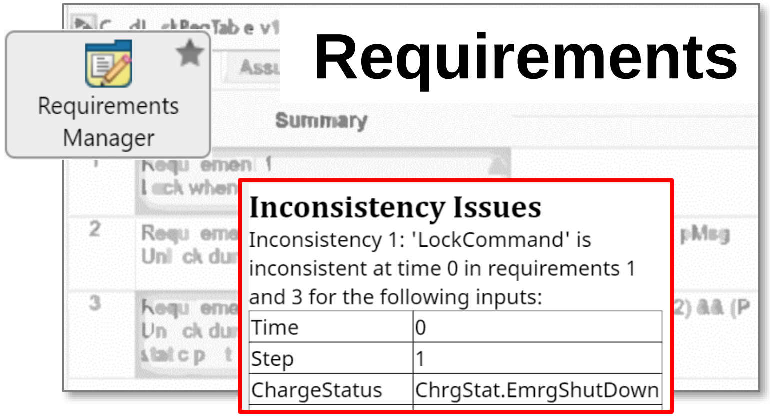


```
2 normalized_er
2 inp_volt[ ]
/* Static functions *
float32 get_direction(f
/* process inputs computes the
* normalizing the input values
```

○ **Integer division by zero** (Impact: High)
Divisor is 0.

Memory errors, overflows, race conditions, crashes, CWE, …

Requirements



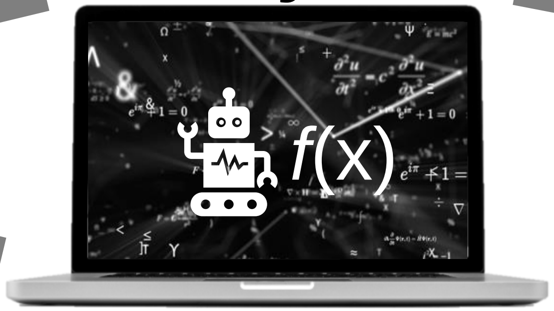
Inconsistency Issues

Inconsistency 1: 'LockCommand' is inconsistent at time 0 in requirements 1 and 3 for the following inputs:

Time	0
Step	1
ChargeStatus	ChrgStat.EmrgShutDown

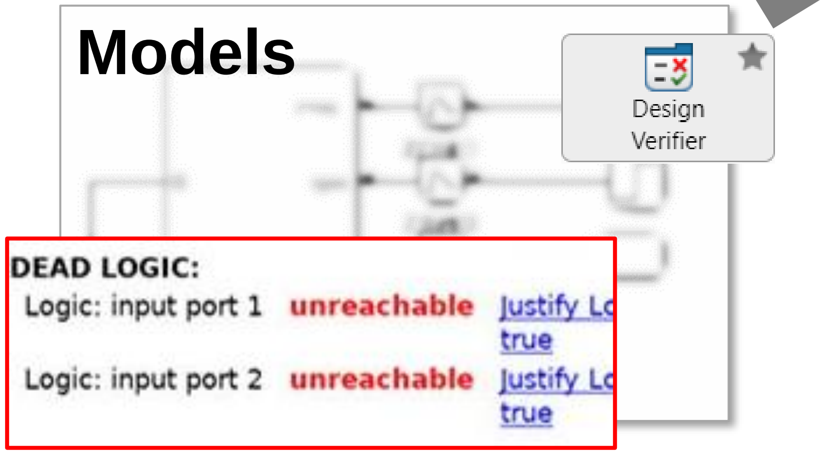
Contradictions, incompleteness

Static Analysis



Mathematical analysis. Provides counter-examples.

Models

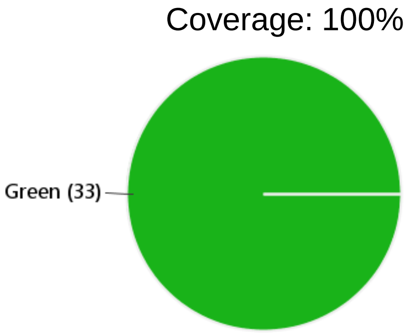


DEAD LOGIC:

Logic: input port 1	**unreachable**	Justify Lo true
Logic: input port 2	**unreachable**	Justify Lo true

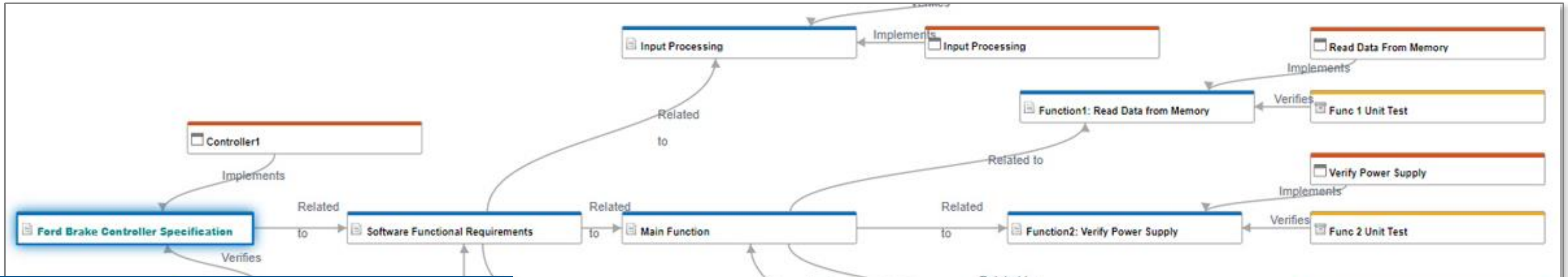
Exceeding ranges, **specification mismatch**, dead logic, …

Less vulnerabilities!

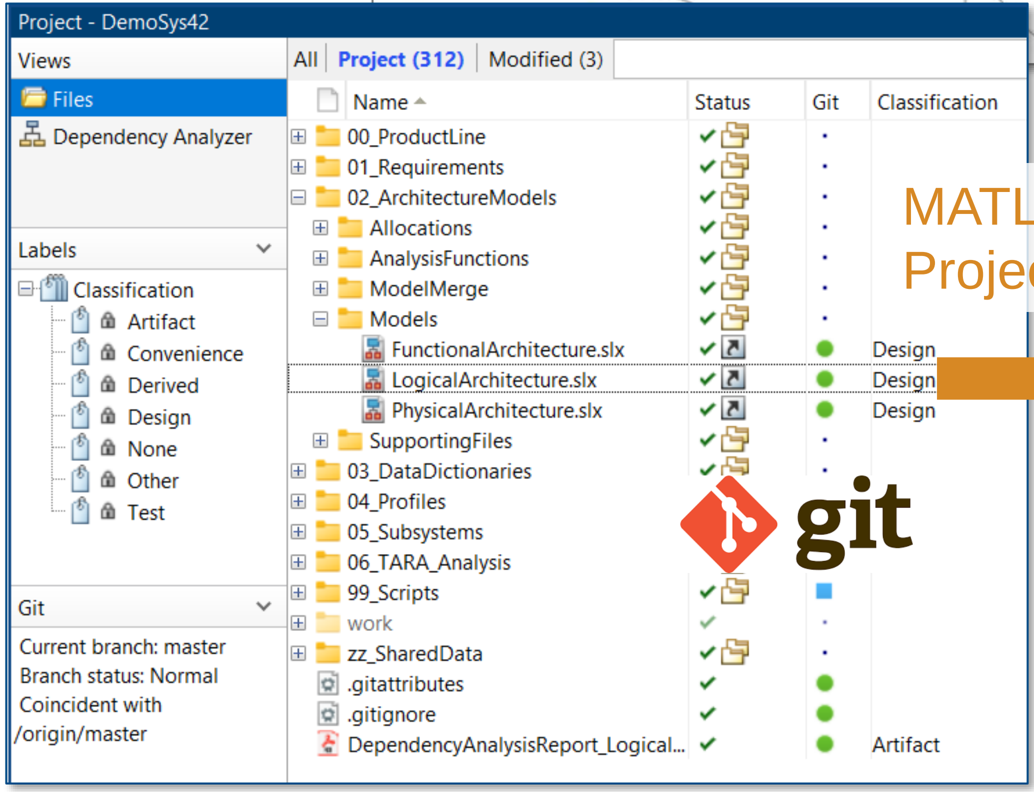


Memory-safety.
Robustness.
Consistency.

Software Bill of Materials (SBOM) made easy with Model-Based Design



Digital Thread



Labels

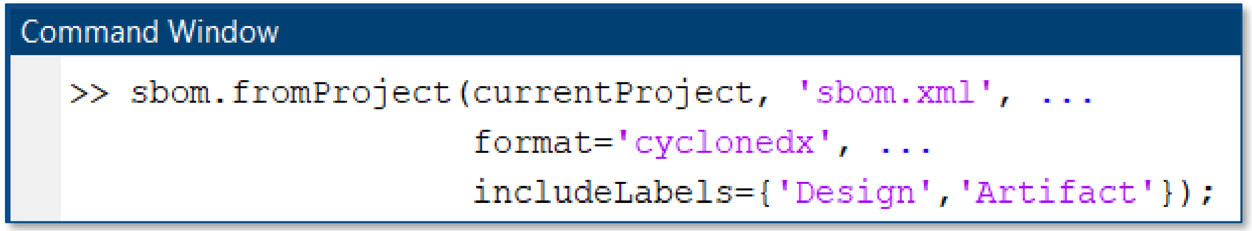
- Classification
  - Artifact
  - Convenience
  - Derived
  - Design
  - None
  - Other
  - Test

Name	Status	Git	Classification
00_ProductLine	✓	·	
01_Requirements	✓	·	
02_ArchitectureModels	✓	·	
Allocations	✓	·	
AnalysisFunctions	✓	·	
ModelMerge	✓	·	
Models	✓	·	
FunctionalArchitecture.slx	✓	●	Design
LogicalArchitecture.slx	✓	●	Design
PhysicalArchitecture.slx	✓	●	Design
SupportingFiles	✓	·	
03_DataDictionaries	✓	·	
04_Profiles			
05_Subsystems			
06_TARA_Analysis			
99_Scripts	✓	■	
work	✓	·	
zz_SharedData	✓	·	
.gitattributes	✓	●	
.gitignore	✓	●	
DependencyAnalysisReport_Logical...	✓	●	Artifact

Git

Current branch: master
Branch status: Normal
Coincident with
/origin/master

MATLAB Projects

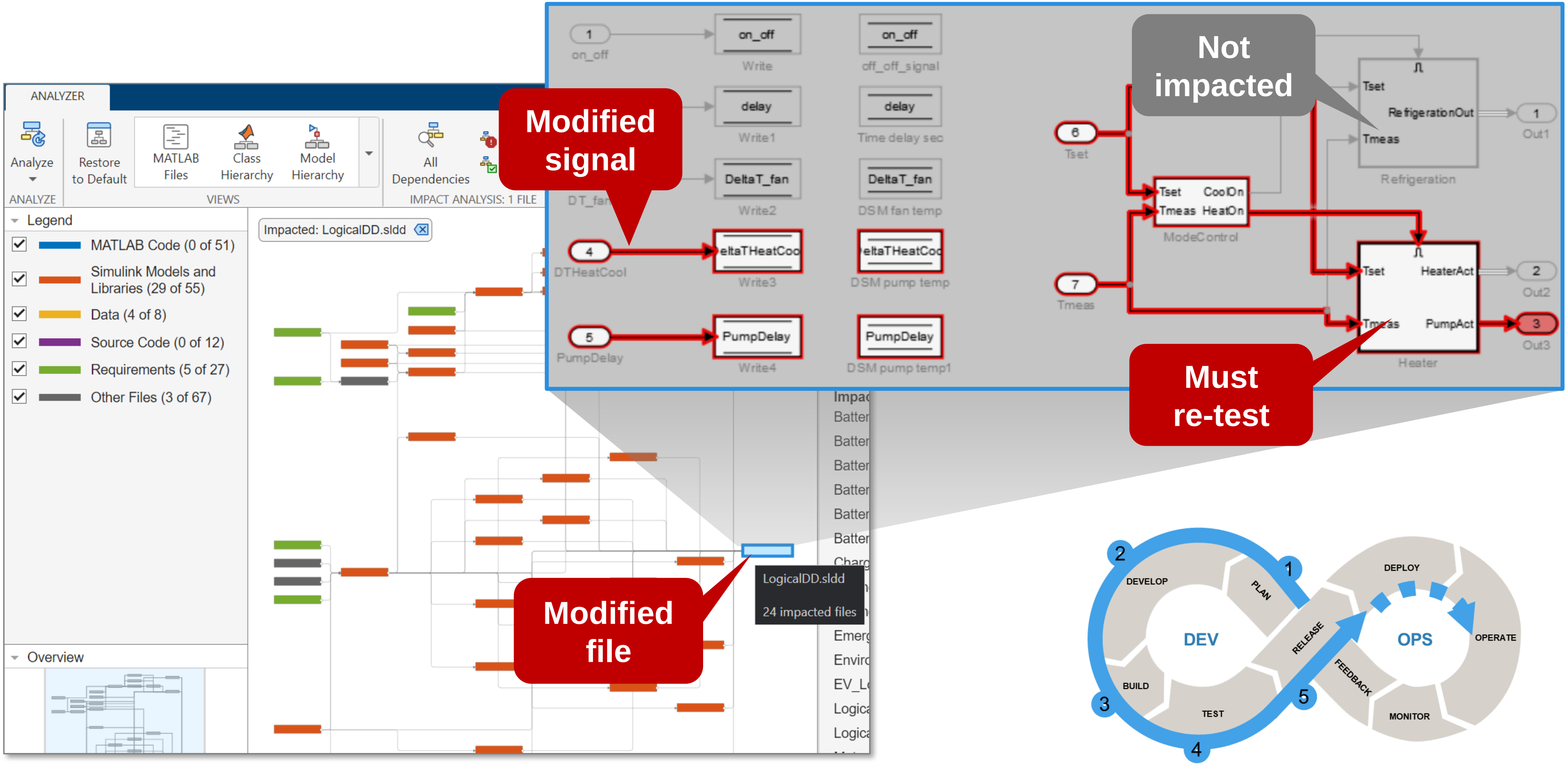


```
>> sbom.fromProject(currentProject, 'sbom.xml', ...
                    format='cyclonedx', ...
                    includeLabels={'Design','Artifact'});
```

SBOM

Components, versions, dependencies, assemblies, hashes, …

More Agility: Tracking changes and minimizing re-certification (R.156)

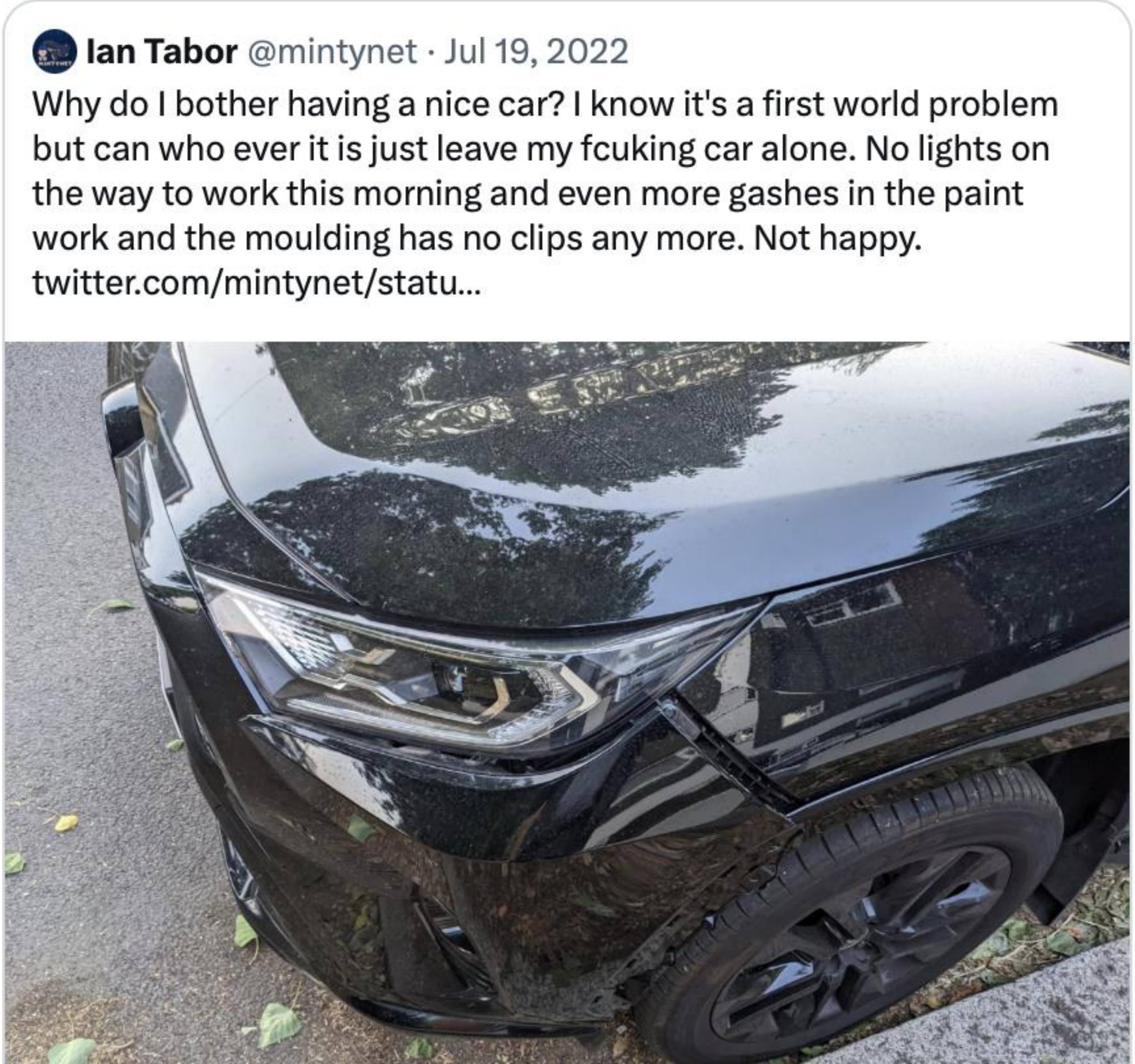


Modified signal

Not impacted

Must re-test

Modified file



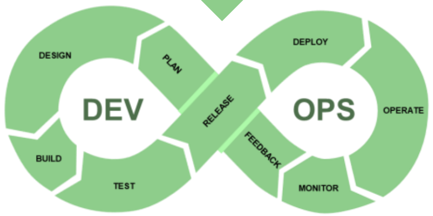
Ian Tabor @mintynet · Jul 19, 2022

Why do I bother having a nice car? I know it's a first world problem but can who ever it is just leave my fcuking car alone. No lights on the way to work this morning and even more gashes in the paint work and the moulding has no clips any more. Not happy. twitter.com/mintynet/statu...

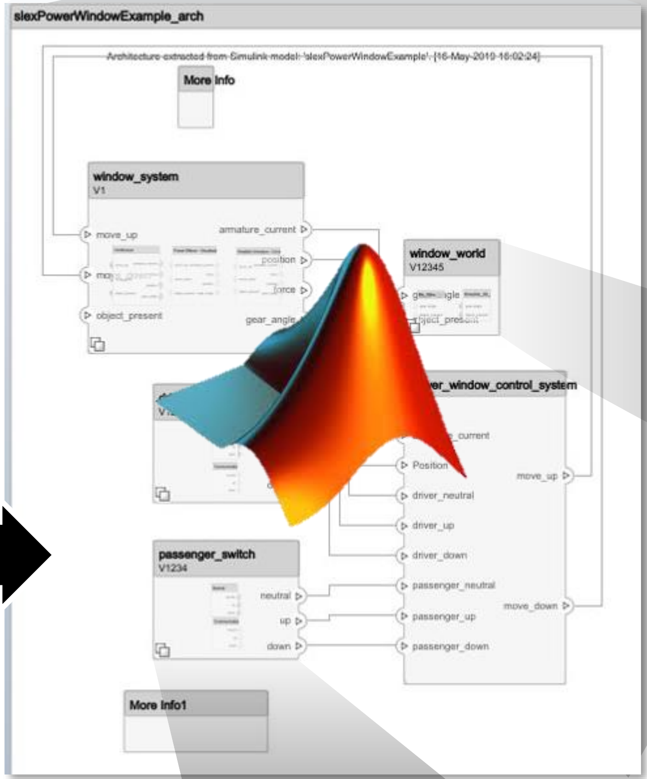
Back to the start…

Conclusion & Outlook

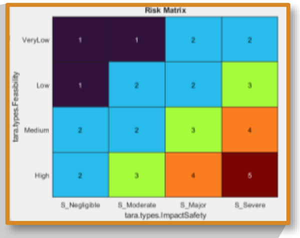
- Cybersecurity is here.
- **Use your existing MBD tools.**
- Full traceability & high agility.

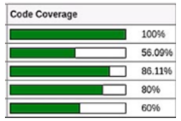


SBOM

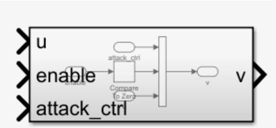


Model-based TARA/HARA





Fuzzing



Attack Simulation

CERT

CWE

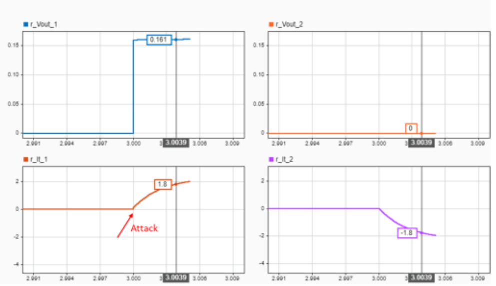
Vulnerability Analysis

Signal propagation: upstream

Starting Points [clear all]

Out Bus Element

Change Impact Analysis



Intrusion Detection & Prevention