Model-Based Engineering for Cybersecurity: Preparing for UN ECE Regulation and ISO/SAE-21434

July 1st 2020 | EUROPE

MathWorks
AUTOMOTIVE
CONFERENCE 2020

MathWorks®

In the News 5 years ago…

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

Miller (left) and Valasek demonstrated the rest of their attacks on the Jeep while I drove it around an empty parking lot. WHITNEY CURTIS FOR WIRED

Source: https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/

In the News 5 years ago…

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

Miller (left) and Valasek demonstrated the rest of their attacks on the Jeep while I drove it around an empty parking lot. WHITNEY CURTIS FOR WIRED

Source: https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/

In the News 5 years ago…

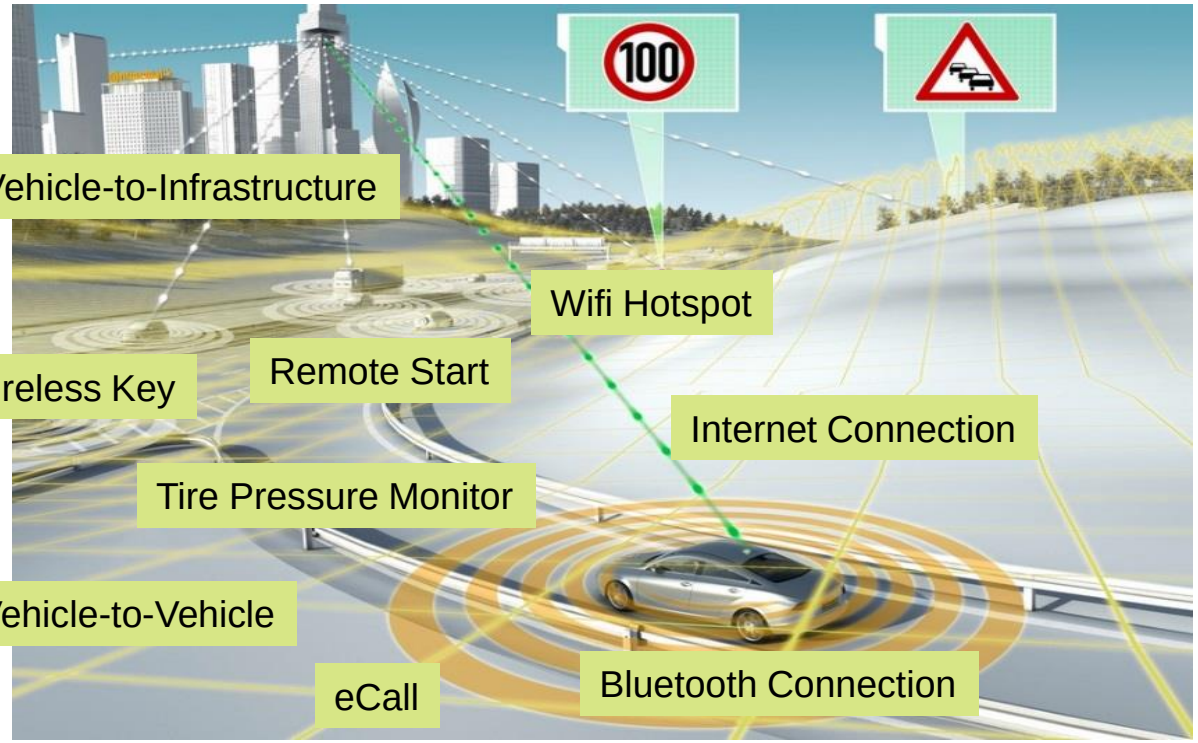
HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

Miller (left) and Valasek demonstrated the rest of their attacks on the Jeep while I drove it around an empty parking lot. WHITNEY CURTIS FOR WIRED

Source: https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/

Cybersecurity – Emerging Topic

On-Board & V2X Communication



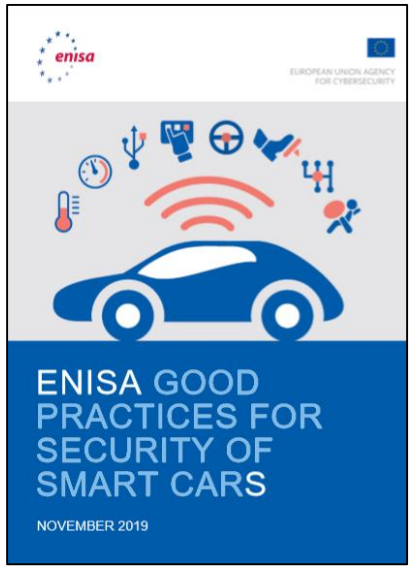
- Growing communication of on-board systems, sensors and external sites
- Car becomes another node of IoT
- Security can compromise vehicle safety

„FCA recalls 1.4 Million cars after Jeep hack“

http://www.blogcdn.com/www.autoblog.com/media/2013/02/2014-jeep-cherokee-1.jpg

Current milestones around regulations, guidelines and standards

11/2019
ENISA publishes "GOOD PRACTICES FOR SECURITY OF SMART CARS"



02/2020
ISO/SAE 21434 DIS is published

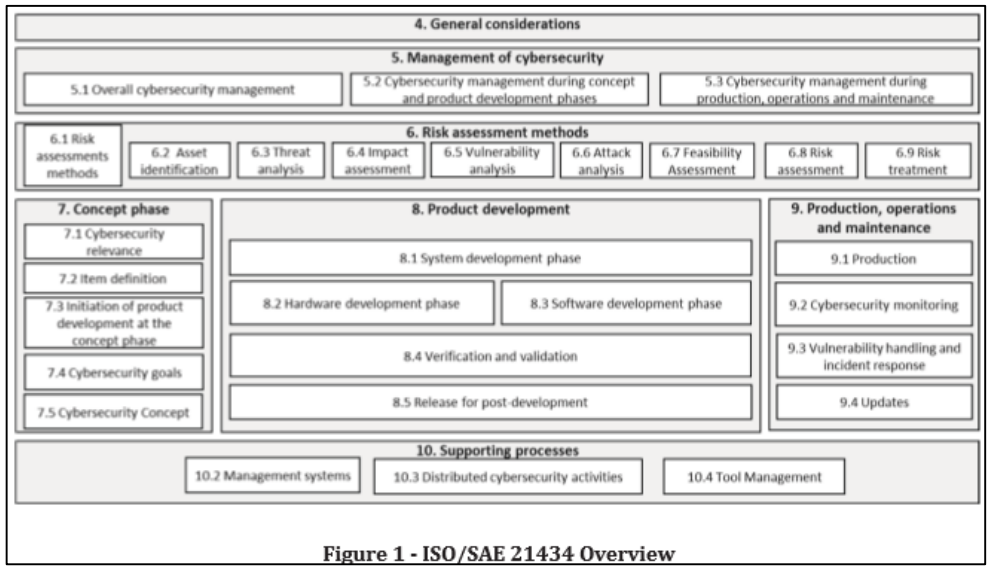


Figure 1 - ISO/SAE 21434 Overview

06/2020
UN ECE WP.29 discussing adoption


United Nations ECE/TRANS/WP.29/2020/79

Economic and Social Council

Distr.: General
2 April 2020

Original: English

Economic Commission for Europe

Inland Transport Committee

World Forum for Harmonization of Vehicle Regulations

181st session
Geneva, 23-25 June 2020
Item 4.12.4 of the provisional agenda
1958 Agreement:
Consideration of proposals for new UN Regulations submitted by the Working Parties subsidiary to the World Forum

Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system

Submitted by the Working Party on Automated/autonomous and Connected Vehicles*

The text reproduced below, proposing a new UN Regulation on on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system, was drafted by the Task Force on Cyber Security and Over-the-Air issues and reviewed by GRVA. It was produced in accordance with the Framework Document on the safety of Automated Vehicles ECE/TRANS/WP.29/2019/34 as revised. It was adopted by the Working Party on Automated/autonomous and Connected Vehicles at its fifth session, see ECE/TRANS/WP.29/GRVA/6, para. 23., based on ECE/TRANS/WP29/GRVA/2020/3 as amended by GRVA-06-19-Rev.1. It is submitted to the World Forum for Harmonization of Vehicle Regulations (WP.29) and its Administrative Committee for the 1958 Agreement (AC.1) for consideration and vote at their June 2020 sessions.

GRVA was not in the position to finalize the drafting of paragraph 5.3. due to the lack of time. The Contracting Parties having expressed a position on this paragraph volunteered to further discuss after the session and to prepare a document solving the issue on para. 5.3. and subparagraphs complementing this document. This document is bearing the official symbol ECE/TRANS/WP.29/2020/97.

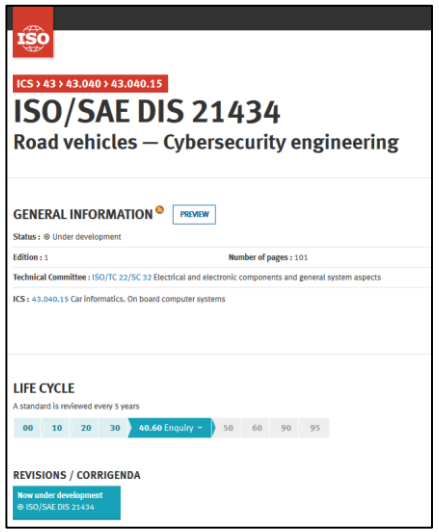
* In accordance with the programme of work of the Inland Transport Committee for 2020 as outlined in proposed programme budget for 2020 (A/74/6 (part V sect. 20) para 20.37), the World Forum will develop, harmonize and update UN Regulations in order to enhance the performance of vehicles. The present document is submitted in conformity with that mandate.

GE.20-05054(E)

Please recycle

06/2020
TODAY

12/2020
ISO/SAE 21434 FDIS to be published


ICS › 43 › 43.040 › 43.040.15

ISO/SAE DIS 21434

Road vehicles — Cybersecurity engineering

GENERAL INFORMATION PREVIEW

Status : Under development

Edition : 1 Number of pages : 101

Technical Committee : ISO/TC 22/SC 32 Electrical and electronic components and general system aspects

ICS : 43.040.15 Car Informatics. On board computer systems

LIFE CYCLE

A standard is reviewed every 5 years

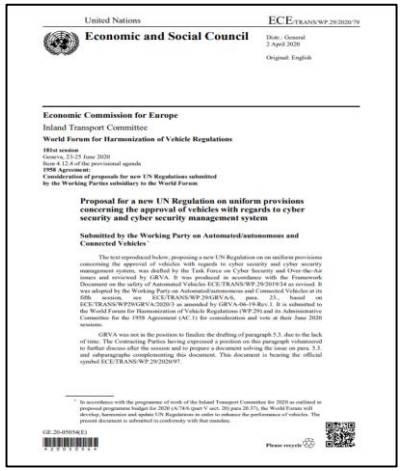
00 10 20 30 40.60 Enquiry 50 60 90 95

REVISIONS / CORRIGENDA

Now under development
ISO/SAE DIS 21434

Why is this important?

- UN ECE/TRANS/WP.29/2020/79 regulation proposal on Cybersecurity
  - Uniform provisions concerning the approval of vehicles with regard to cyber security and of their cybersecurity management systems (CSMS)
  - Relevant for homologation
  - Automotive supply-chain to implement the UN Regulation



United Nations ECE/TRANS/WP.29/2020/79

Economic and Social Council

Economic Commission for Europe

Inland Transport Committee

World Forum for Harmonization of Vehicle Regulations

Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system

Submitted by the Working Party on Automated/autonomous and Connected Vehicles

- ISO/SAE 21434 – “Road vehicles – Cybersecurity engineering”
  - Widely seen as reference implementation of a CSMS for E/E Systems
  - Development processes need to be adapted to deal with Cybersecurity Threats and Risks

ICS › 43 › 43.040 › 43.040.15

ISO/SAE DIS 21434

Road vehicles — Cybersecurity engineering

GENERAL INFORMATION

Status : Under development

Edition : 1

Number of pages : 101

Technical Committee : ISO/TC 22/SC 32 Electrical and electronic components and general system aspects

ICS : 43.040.15 Car informatics. On board computer systems

LIFE CYCLE

A standard is reviewed every 5 years

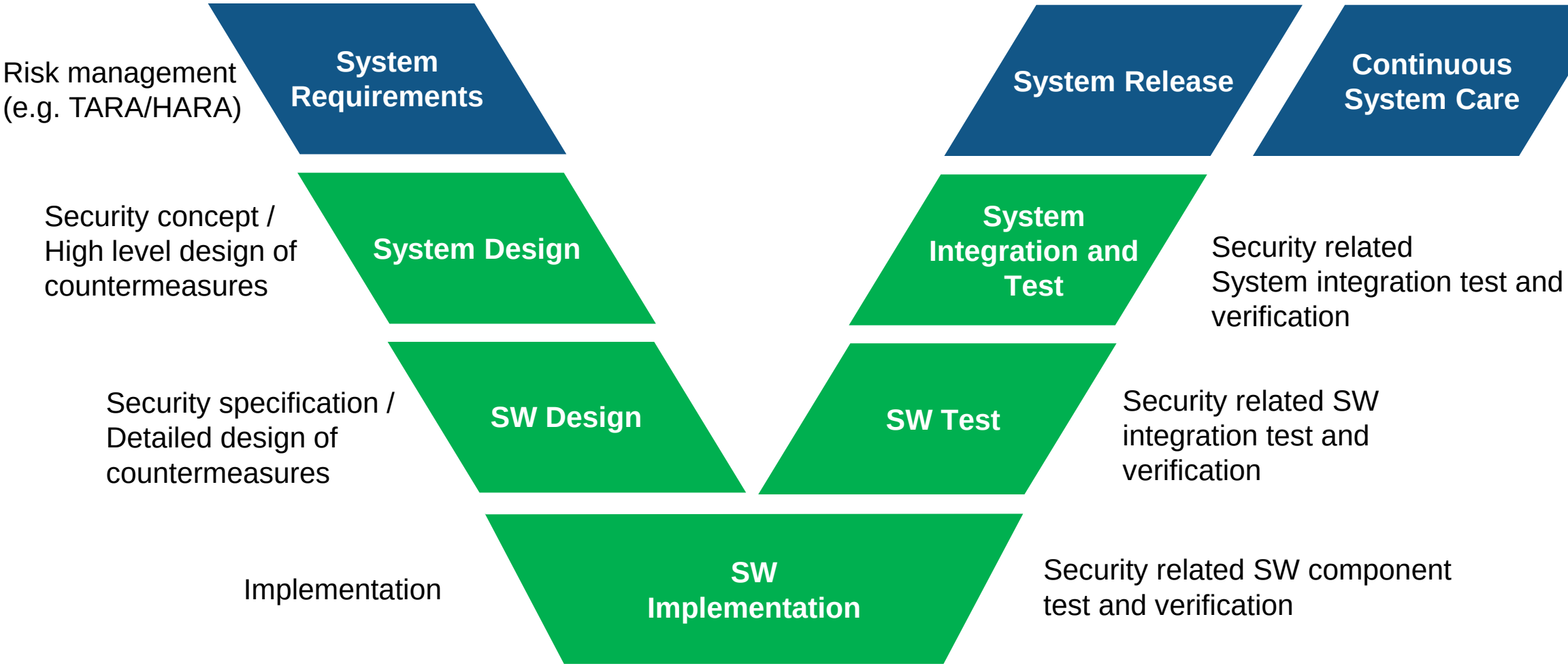
00 10 20 30 40.60 Enquiry 50 60 90 95

REVISIONS / CORRIGENDA

Now under development

ISO/SAE DIS 21434

ISO/SAE 21434 is aligned with the V model and ISO 26262



Embedded Systems Threats and Vulnerabilities

Network

- Incorrect order of network connection operations
- Tainted data

File System

- TOCTOU (race condition)
- Vulnerable path manipulation
- Use of non-secure temporary file

HSM

- Deterministic random output from constant seed
- Vulnerable pseudo-random number generator
- Sensitive heap memory not cleared before release

3rd party software

- Execution of a binary/Load of library from a relative path can be controlled by an external actor
- Tainted Data

User Input

- Tainted Data

Sensors

- Tainted Data

HSM: Hardware Security Module

Databases collecting security vulnerabilities and exploits

- CVE – Common Vulnerabilities & Exposures (cve.mitre.org)
- OSVDB – Open Source Vulnerability Database (osvdb.org)
- SANS Institute - SysAdmin, Audit, Network, Security (www.sans.org)
- OWASP - Open Web Application Security Project (www.owasp.org)

Rank	Score	ID	Name
[1]	93.8	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
[2]	83.3	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
[3]	79.0	CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
[4]	77.7	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
[5]	76.9	CWE-306	Missing Authentication for Critical Function
[6]	76.8	CWE-862	Missing Authorization
[7]	75.0	CWE-798	Use of Hard-coded Credentials
[8]	75.0	CWE-311	Missing Encryption of Sensitive Data
[9]	74.0	CWE-434	Unrestricted Upload of File with Dangerous Type
[10]	73.8	CWE-807	Reliance on Untrusted Inputs in a Security Decision
[11]	73.1	CWE-250	Execution with Unnecessary Privileges

CERT and other organizations share secure coding practices

source: https://www.securecoding.cert.org

Secure Coding

Seiten

BEREICHSVERKNÜPFUNGEN

- Dashboard
- Home
- Android
- C
- C++
- Java
- Perl

Top 10 Secure Coding Practices

Erstellt von Robert Seacord, zuletzt geändert von Robert Seacord (Manager) am Mär 01, 2011

Top 10 Secure Coding Practices

Validate inputs

Validate input from all untrusted data sources. Proper input validation can eliminate the vast majority of software vulnerabilities. Be suspicious of most external data sources, including command line arguments, network interfaces, environmental variables, and user controlled

Heed compiler warnings and use static and dynamic analysis tools

available for your compiler and eliminate warnings by modifying the code [C MSC00-A, C++ MSC00-A]. Use static and dynamic analysis tools to detect

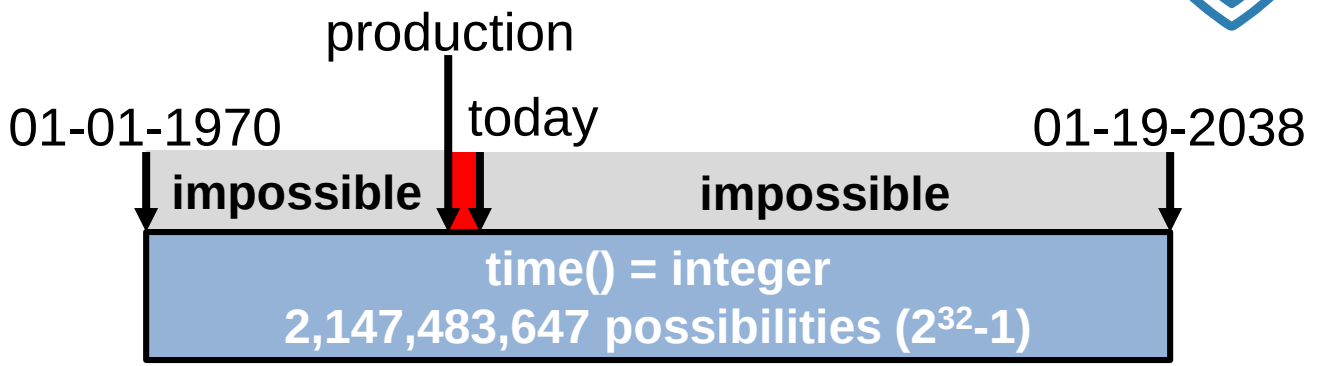
Architect/Design Software for security policies

software architecture and design your software to implement and enforce security policies. For

Jeep Hack: Deterministic Random Number Generator

Vulnerability of the in-car Wi-Fi

Polyspace Code Verifier



Source

wifi.c

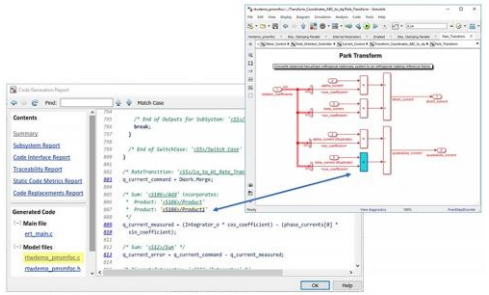
```
18          }
19          return v3;
20  }
21
22  char *get_password()
23  {
24          int c_max = 12;
25          int c_min = 8;
26          unsigned int t = time(((void *)0));
27          srand (t);
28          unsigned int len = (rand() % (c_max - c_min + 1)) + c_min;
32                  unsigned int v10 = rand();
33                  int v11 = convert_byte_to_ascii_letter(v10 % 62);
34                  password[v9] = v11;
35                  v9++;
```

Defect: ID 2: 'rand' is a cryptographically weak PRNG.
To make your program more secure, use 'CryptGenRandom' (Windows) or 'RAND_bytes' (OpenSSL) instead.

Miller (left) and Valasek demonstrated the rest of their attacks on the Jeep while I drove it around an empty parking lot. WHITNEY CURTIS FOR WIRED

Source: http://illmatics.com/Remote%20Car%20Hacking.pdf

Model-Based Design - examples of potential Cert C issues *

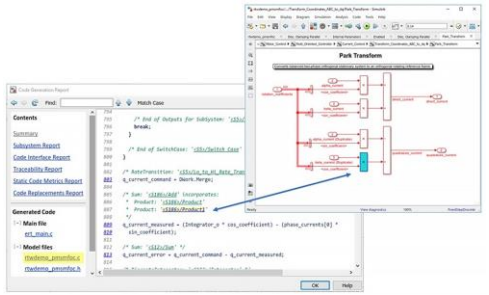


- **FLP30-C** — **2**
  - Do not use floating-point variables as loop counters
- **FLP34-C** — **41**
  - Ensure that floating-point conversions are within range of the new type
- **INT30-C** — **72**
  - Ensure that unsigned integer operations do not wrap
- **INT31-C** — **343**
  - Ensure that integer conversions do not result in lost or misinterpreted data

*) all user made; found in C code generated from 50 industry models

Model-Based Design - examples of potential Cert C issues *

The models have not been designed to comply with Cert C
(violations are specifically relevant if taint data is involved)

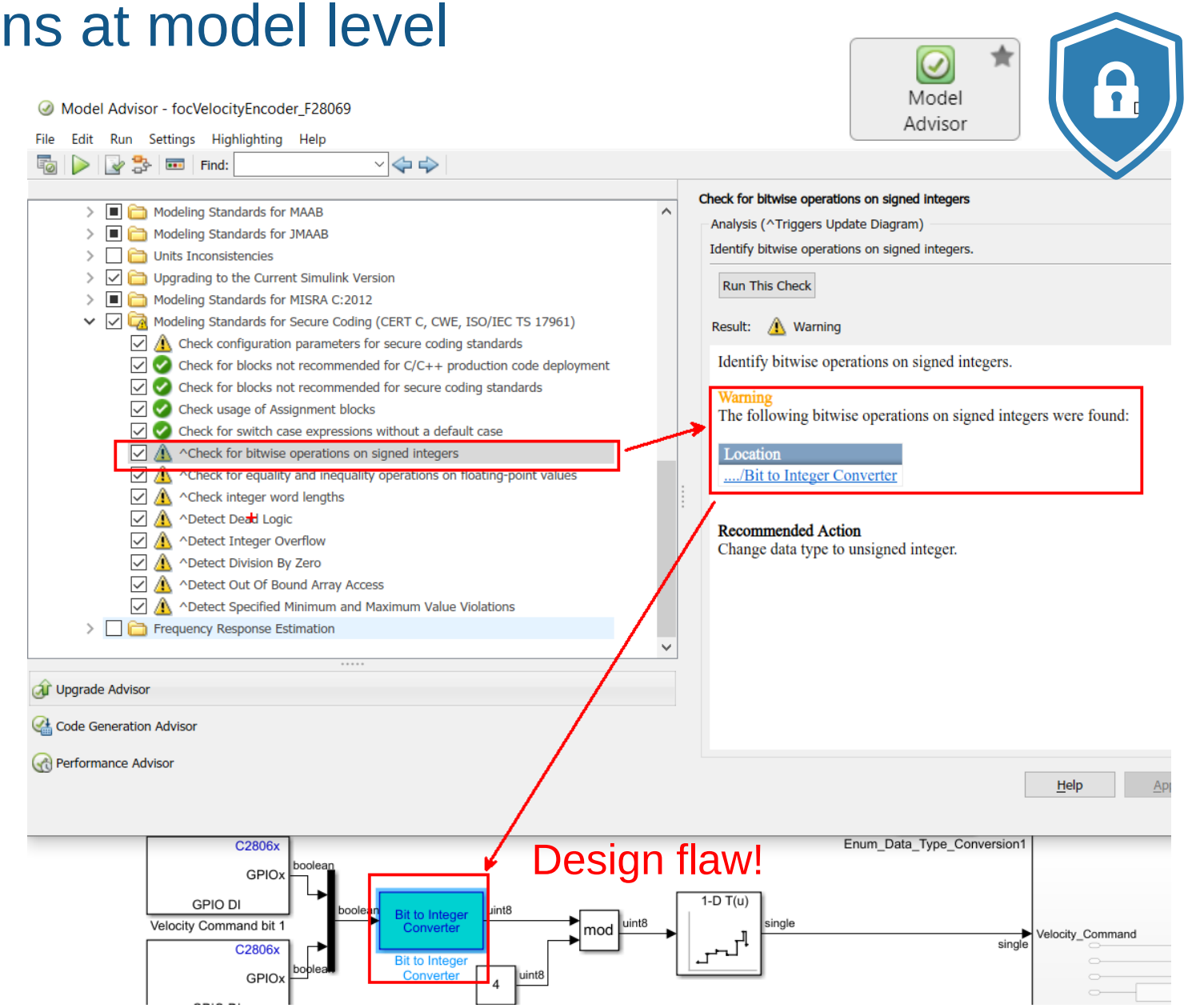


- **FLP30-C** **2**
  - Do not use floating-point variables as loop counters
- **FLP34-C** **41**
  - Ensure that floating-point conversions are within range of the new type
- **INT30-C** **72**
  - Ensure that unsigned integer operations do not wrap
- **INT31-C** **343**
  - Ensure that integer conversions do not result in lost or misinterpreted data

*) all user made; found in C code generated from 50 industry models

Early security considerations at model level

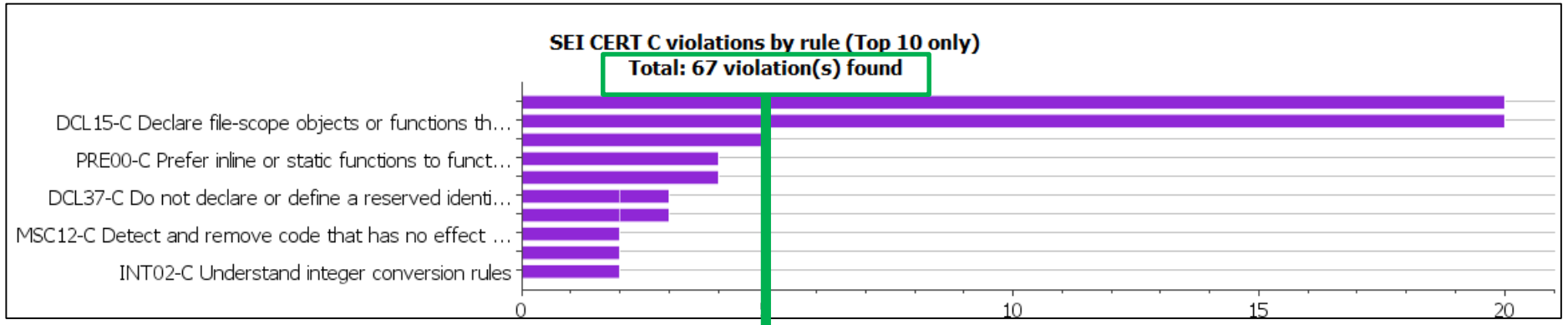
- Identify ...
  - Discouraged blocks
  - Non-determinism
  - Basic design flaws
- Covers:
  - Most frequent issues (according the inhouse study)
  - CERT C, CWE and other checks
- Result:
  - Analyzable model
  - Removed basic flaws



Quantifying Security Compliance at Code Level

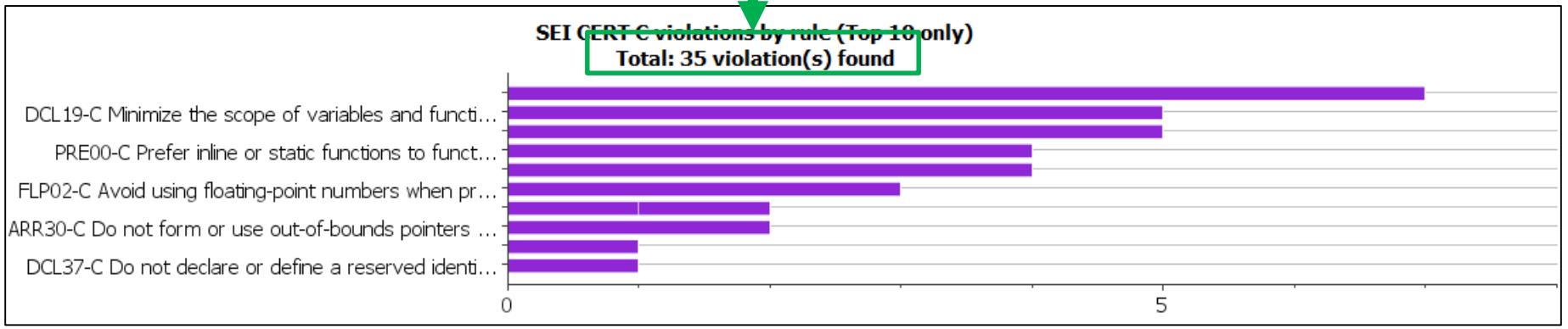
Polyspace Code Verifier

Code from original example model:



~50% fewer Cert-C violations!

Code from improved example model:

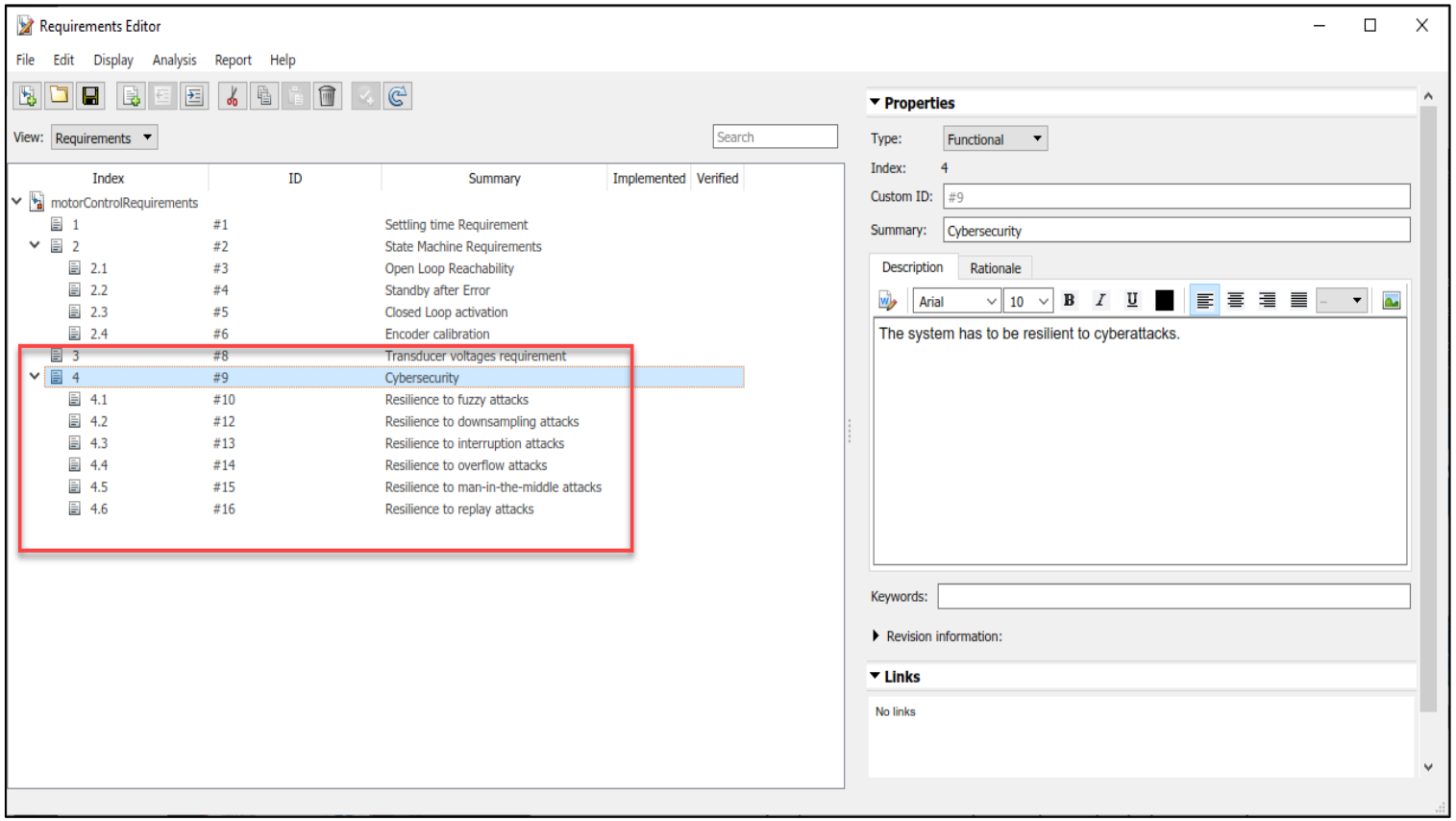


Design improvements reduce late findings in C code and design iterations!

Documenting formal cybersecurity requirements

- Outcome of Threat Analysis and Risk Assessment (TARA) needs to be documented and linked to a system or a component

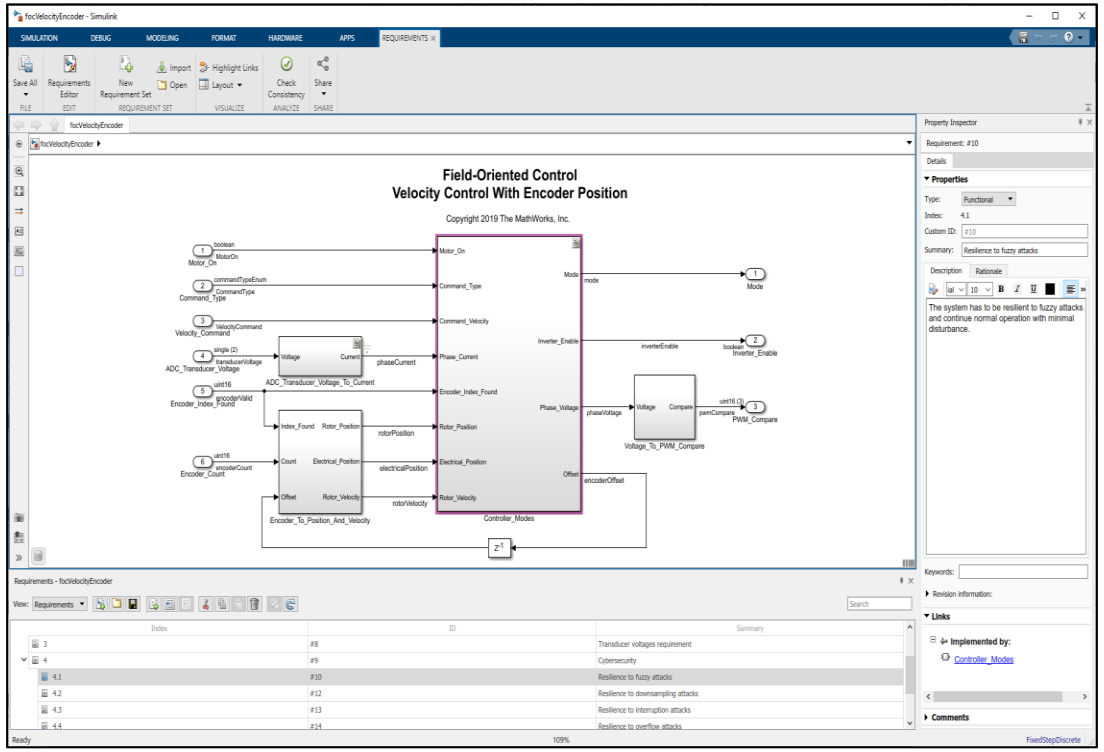
- Each threat can be mitigated by one or more requirements



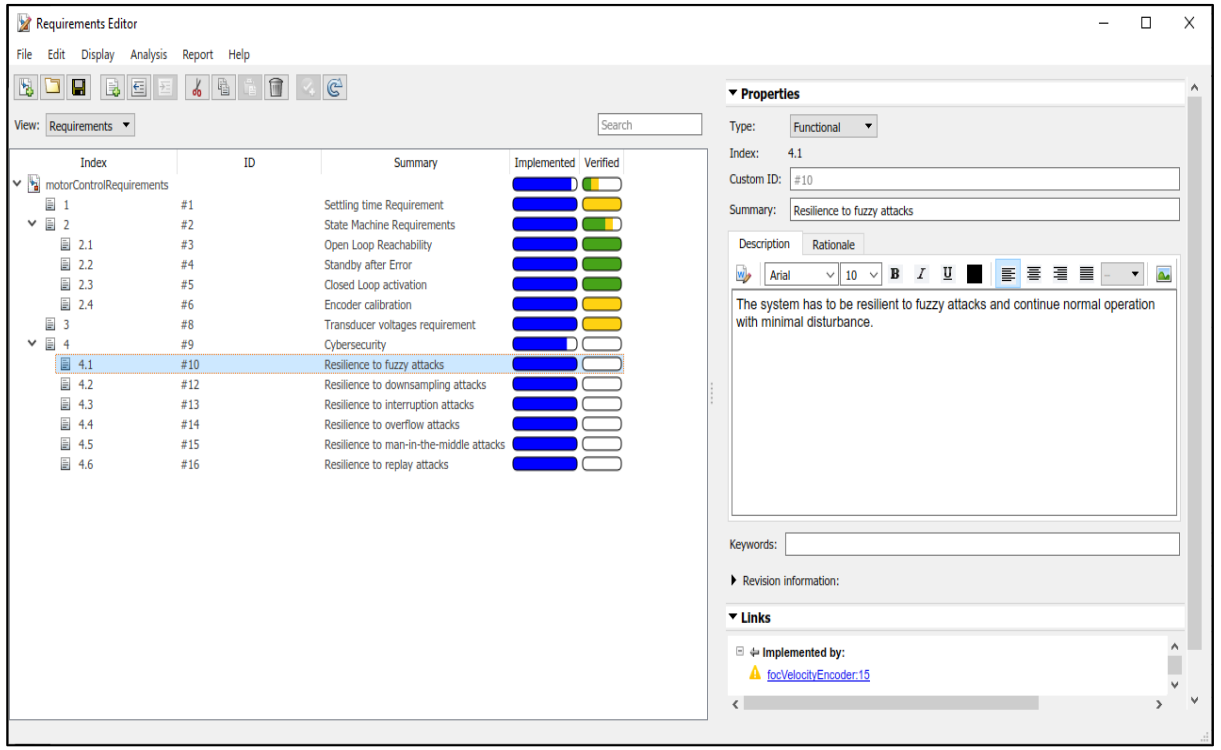
Author and manage functional/cybersecurity requirements

Requirements Manager

Create, organize and view requirements directly in your models

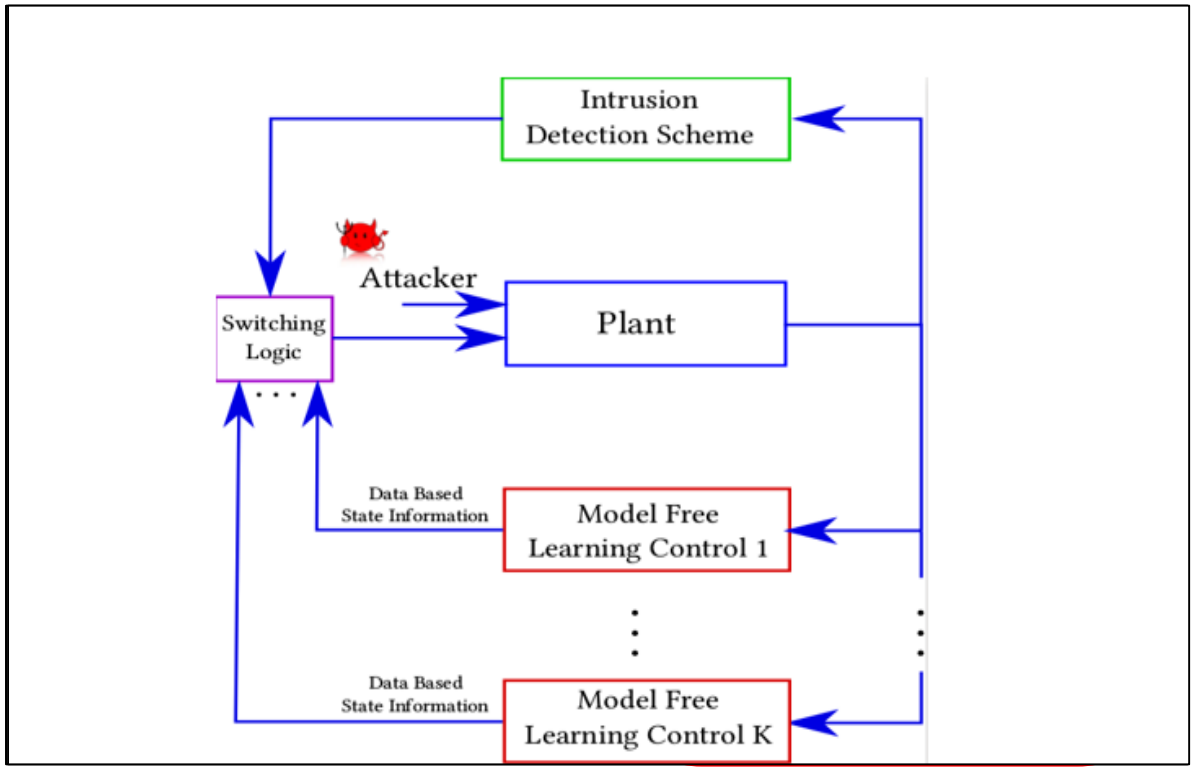


Track implementation and verification status



Cybersecurity testing in simulation using attack libraries

- Run attacks in simulation
  - Attacks can be implemented in Simulink
  - Usable for every system model and to attack almost every signal
  - Helps improve effectiveness of intrusion detection systems (IDS)
- Adaptable
  - Increase variety of cyberattacks and use masked parameters for flexibility
  - MATLAB Function blocks for more complex logic
  - Testing in SIL, PIL, HIL



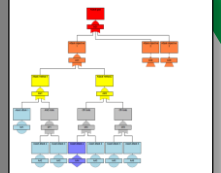
Source: https://www.mathworks.com/videos/a-reinforcement-learning-framework-for-smart-secure-and-efficient-cyber-physical-autonomy-1550746639241.html

Model-Based Engineering use cases for ISO/SAE 21434

Risk management
(e.g. TARA/HARA)

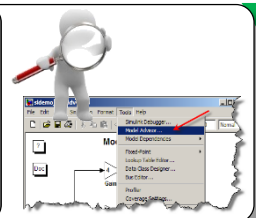
System Requirements

Threat modeling & analysis



System Design

Secure modeling & design



SW Design

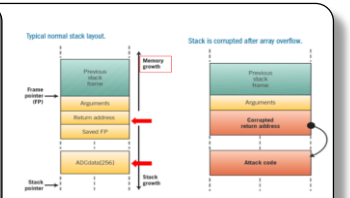
Secure code generation

- MISRA C
- CERT C
- CWE

SW Implementation

SW Test

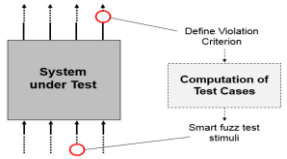
Code level security verification



System Integration and Test

System Release

Smart fuzz testing



Continuous System Care

Intrusion detection & prevention

Intrusion
Detection
Reaction

Filter by Source

- Community 80

Filter by Category

- ‹ Clear Categories
- ‹ Data Import and Analysis
  - Data Import and Export 1,101
  - Large Files and Big Data 76
  - Preprocessing Data 33
  - Descriptive Statistics 63
  - Visual Exploration 173
  - Encryption / Cryptography 80

Filter by Type

- Toolboxes 3
- Apps 1
- Functions 75

Filter by Product Family

- MATLAB 73

80 RESULTS

Encryption / Cryptography (80)

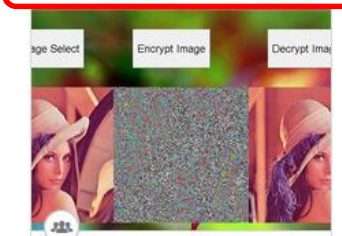


Image Encryption

This GUI does the Image Encryption of any RGB, Gray image of different formats.

65 Downloads ★★★★★

Advanced Encryption Standard (AES)-256

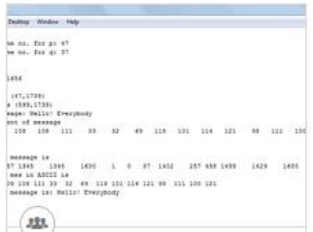
Advance Encryption Standard-256 encryption and decryption using 256-bit hexadecimal key and 128-bit

64 Downloads ★★★★★

Matlab AES Encryption Decryption Example

Advanced Encryption Standard helper class.

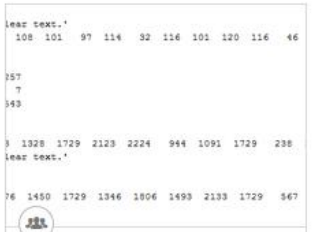
48 Downloads ★★★★★



RSA algorithm

RSA algorithm for encrypting and decrypting a message

48 Downloads ★★★★☆



RSA Public Key Encryption and Signing (32bit)

Basic RSA Public Key encryption and signing to demonstrate the principle.

45 Downloads ★★★★★

Implementation of RSA Algorithm

RSA is an algorithm for public-key cryptography.

42 Downloads ★★★★☆

Data Encryption Standard (DES)

The last generation of encryption standard, good for cryptography study and cipher design.

36 Downloads ★★★★★

Steganography using LSB substitution

The term steganography means "cover writing"

30 Downloads ★★★☆☆

Picture Encryption and Decryption

This algorithm decrypts and encrypts images based on keys

30 Downloads ★★★★☆

Caesar Cipher Encryption and Decryption with MATLAB gui guide

Using MATLAB guide this program will encrypt and decrypt letters using caesar cipher

24 Downloads ★★★★½

Fingerprint Color Image Database .v1

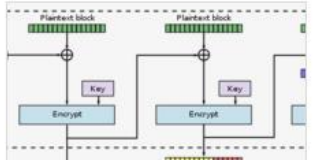
Authors: Dr. Ujwalla Gawande, Kamal Hajari and Yogesh Golhar

22 Downloads ★★☆☆☆

Caesar Cipher

This is Program for Caesar Cipher encryption Technique.

19 Downloads ★★★★★



In 2018 41% of the automotive suppliers did not have an established cybersecurity program or team

Source: Ponemon Study of Automotive Industry Cybersecurity Practices (2018)

Q&A

Are you planning to implement Cybersecurity requirements in the near future?

- YES, we're already working on it
- YES, this will be relevant for us in the next 1-2 years
- NO, this is not relevant for us

Please contact us with questions

sdavid@MathWorks.com

MathWorks®