drivesec

we secure your things

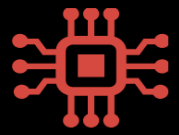
About Drivesec

Founded in 2017 by automotive leaders with robust product development background

Team of Cybersecurity Engineers with strong automotive background

Delivers Services and Products to support the design of secure Automotive systems

Specialized in Cybersecurity Regulations (eg. UN reg 155 and 156)



Wide Experience in hw and sw security design and development

Develop Tools to validate cybersecurity posture of cyber physical systems

Mission

Help Automotive and IoT industries to design, test and deliver products that are inherently resilient to cyber attacks

Drivesec products, enable security testing automation, ensure compliance with existing and upcoming regulations and increase reliability of tests

drivesec

Regulations and Scenarios

Regulation Overview

UNECE R155

Uniform provisions concerning the approval of vehicles with regards to Cybersecurity and Cybersecurity management system

Radio Equipment Directive (RED)

Directive **modification** to **extend cybersecurity requirements** to specific products

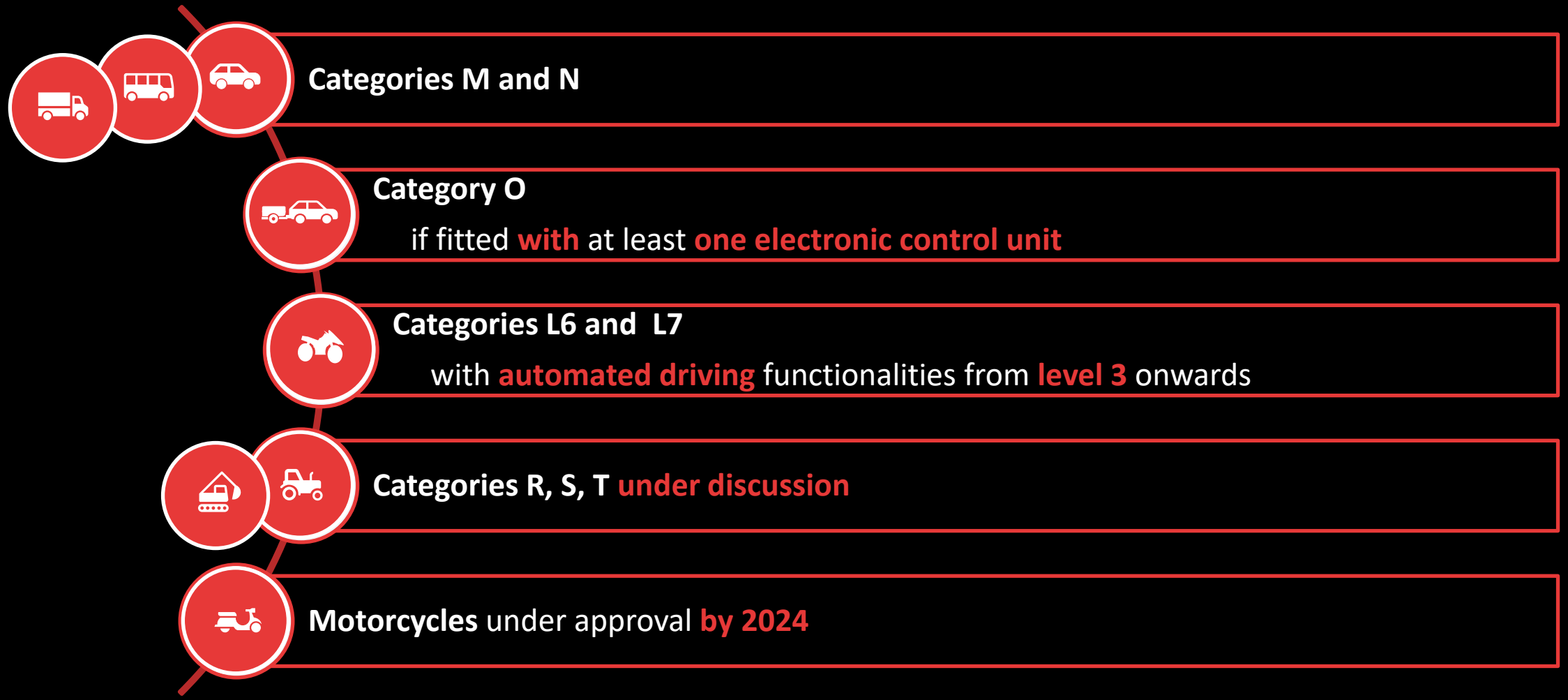
Directive EU 2023/1230 on machinery

Introduce **cybersecurity** requirements in **Annex III** Reference standards for cybersecurity: IEC 62443 – IEC TS 63074

Cyber Resilience Act

Act to **extend cybersecurity** requirements **to all products** that **have digital element** with direct/indirect, logical/physical data connection to a device or network

UNECE R155 applies to

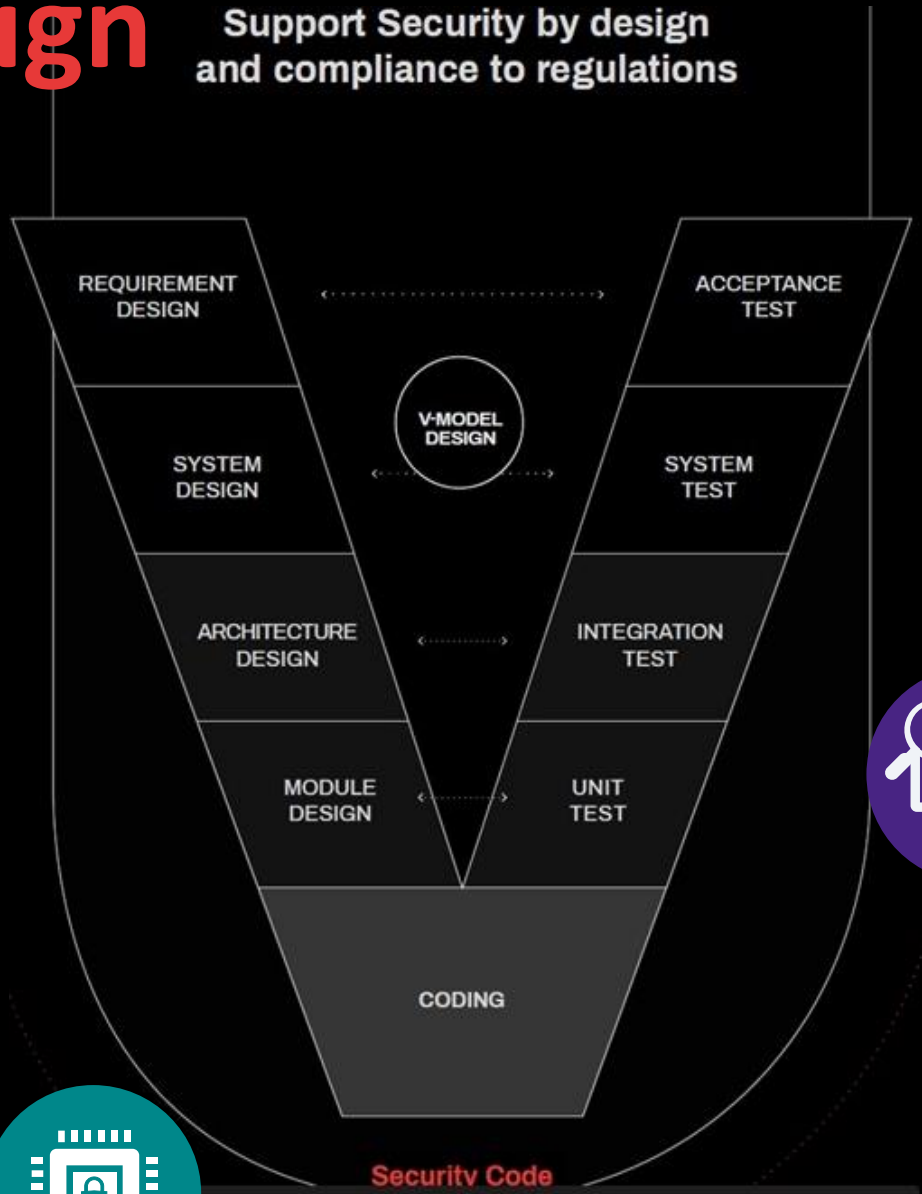


V-Model & Cybersecurity

Security by Design

drivesec

Support Security by design and compliance to regulations



Cybersecurity Processes Design and Risk Analysis

Architecture & Concept Development

Secure code design and verification

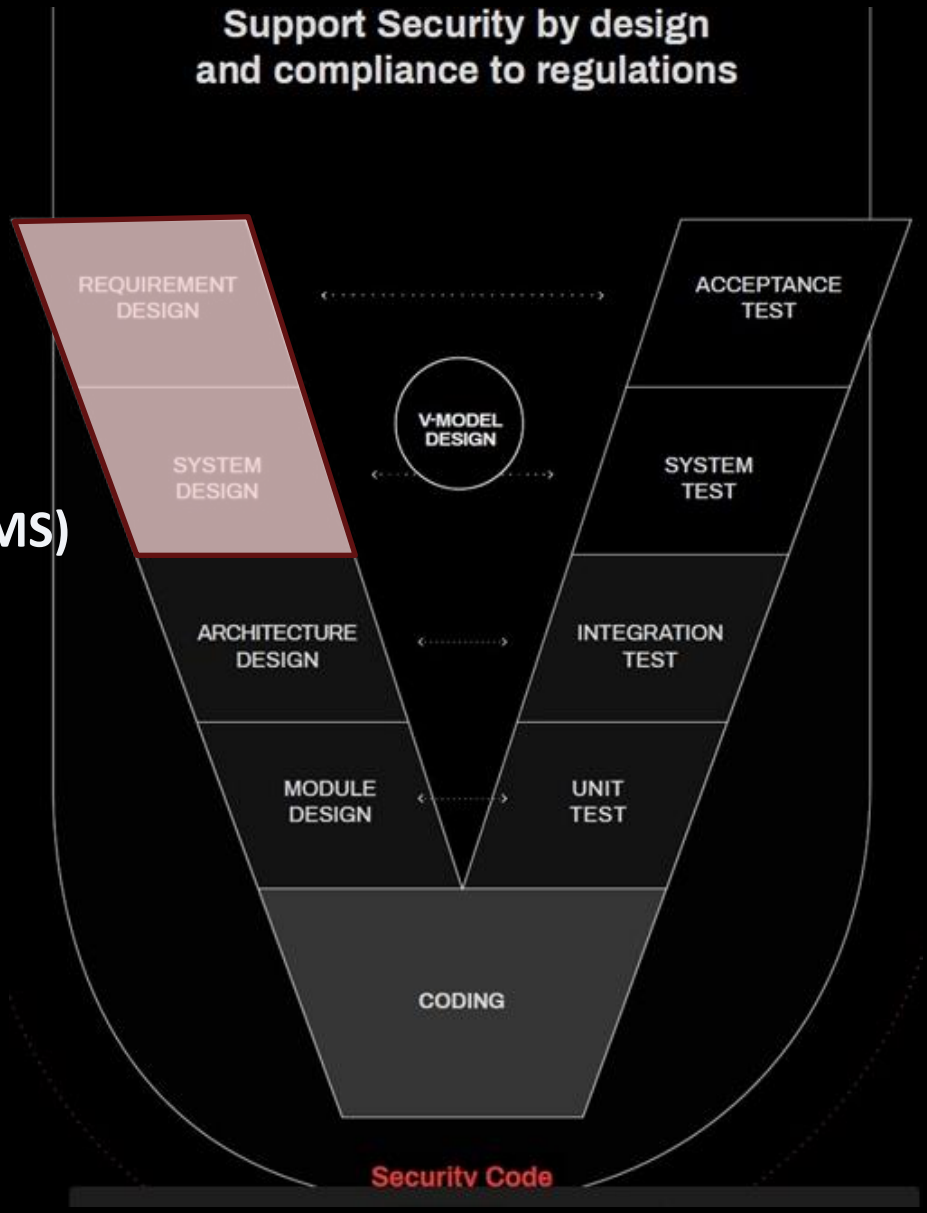
Continuous Monitoring

Penetration Tests

Vulnerability Assessment and Requirements Verification

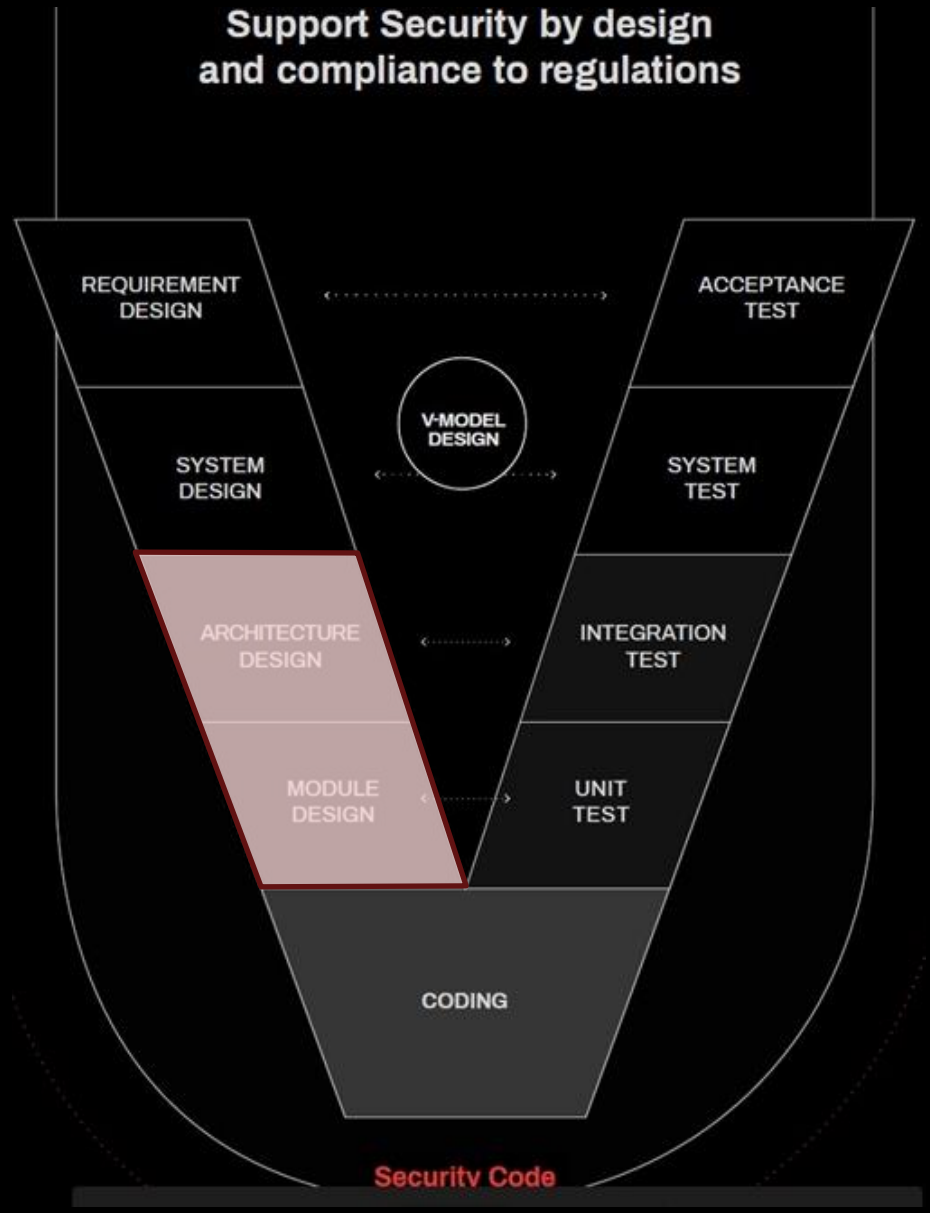
Cybersecurity Processes Design and Risk Analysis

- Compliance to Cyber Security Management System (CSMS)
- Compliance to Software Update Management System (SUMS)
- Item definition
- Threat Analysis and Risk Assessment (TARA)



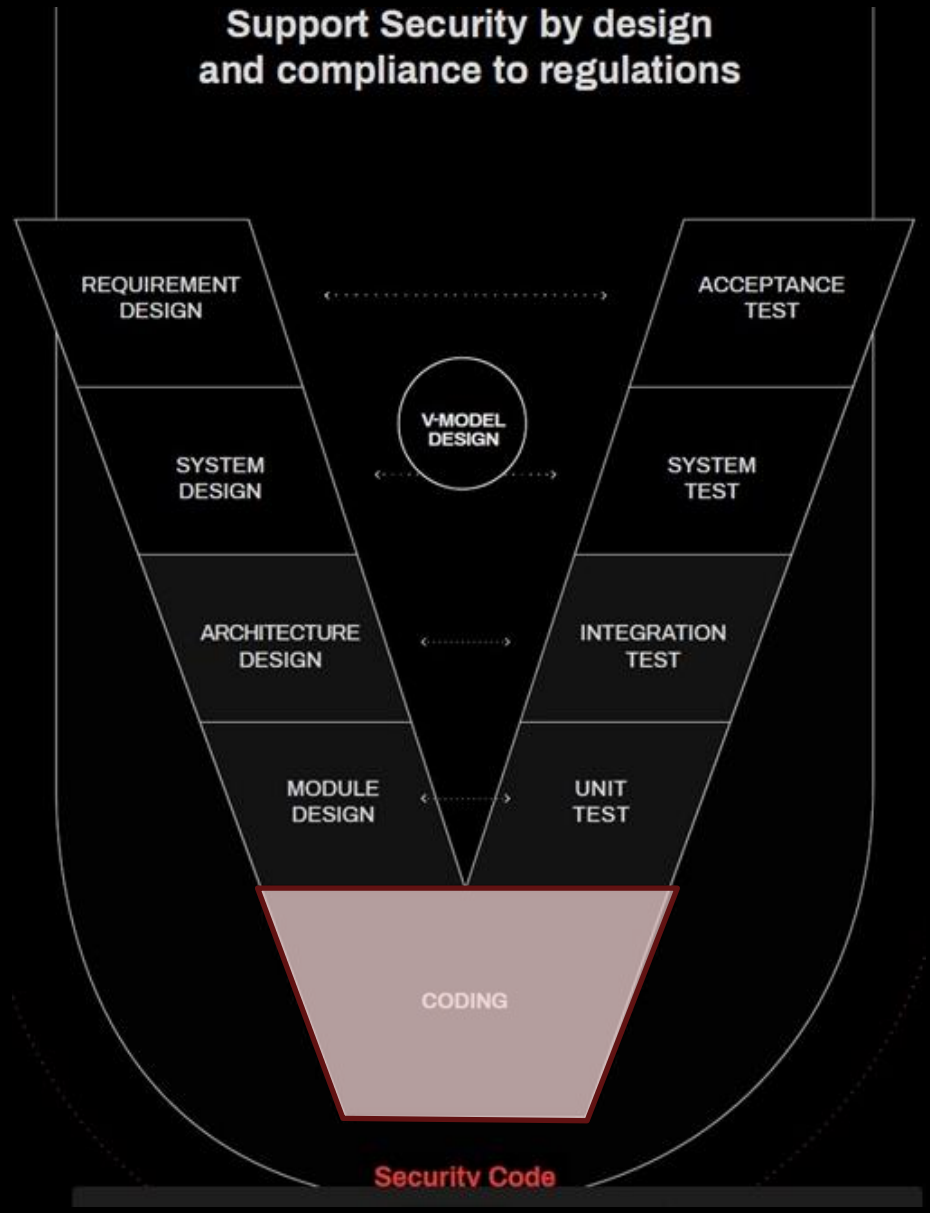
Architecture & Concept Development

- Requirements Engineering
- Cybersecurity Concept
- Cybersecurity Specification and Architectural Design



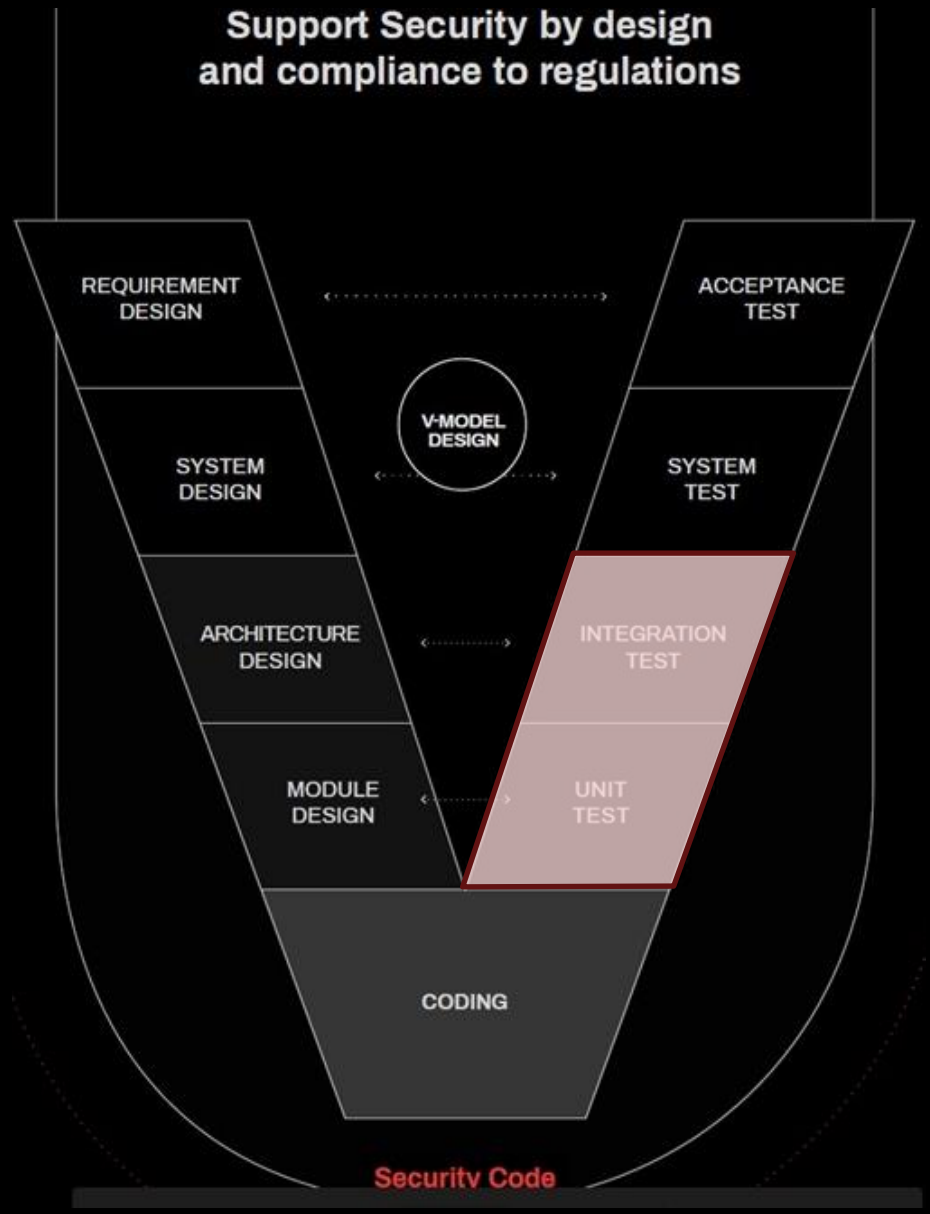
Cybersecurity Design

- Security SW & HW design
- Secure Coding and Design
- Secure Operating Systems and Configurations
- Code Verification



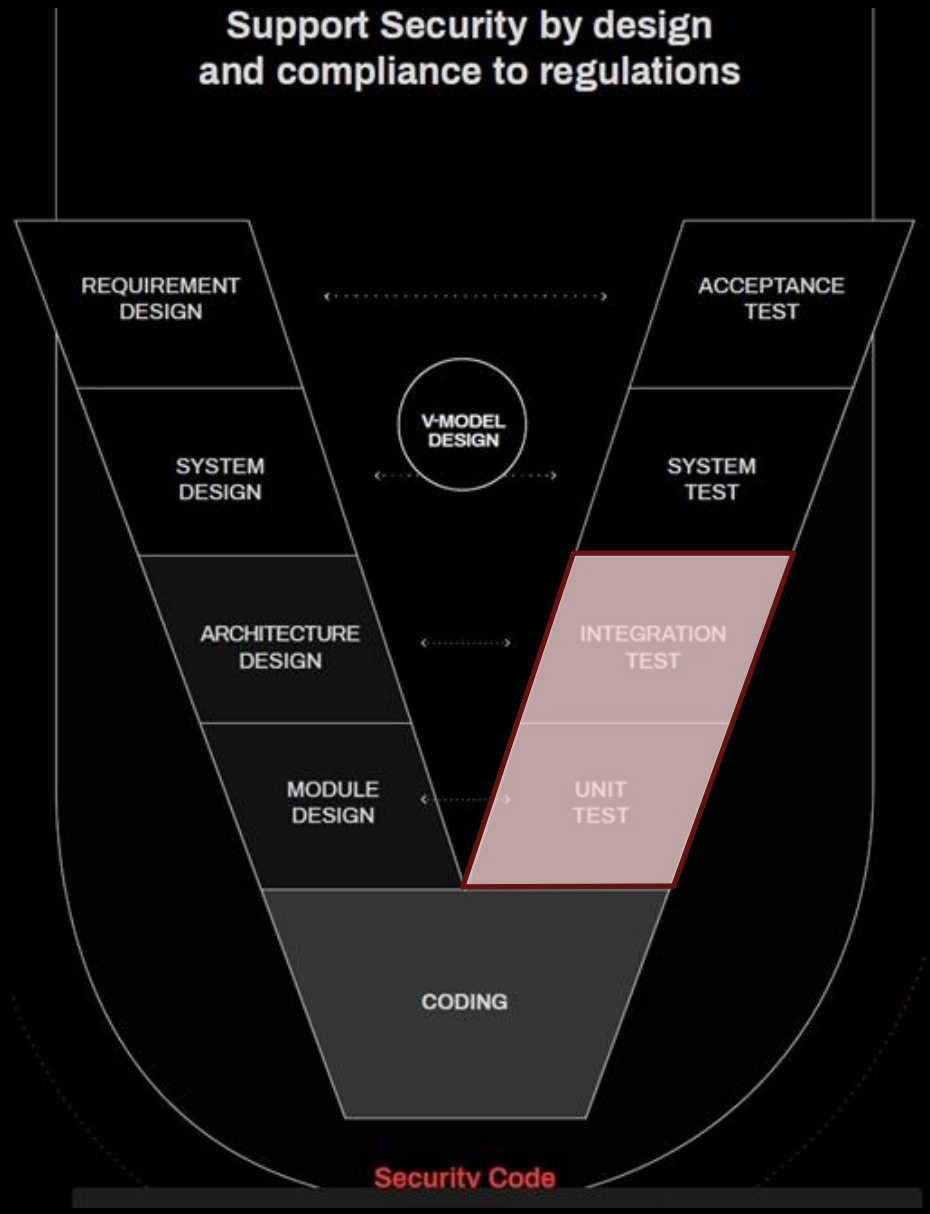
Vulnerability Assessment and Penetration Tests

- Vulnerability Scan & Assessment
- Functional Security Testing
- Penetration Testing
- Secure Operating Systems and Configurations



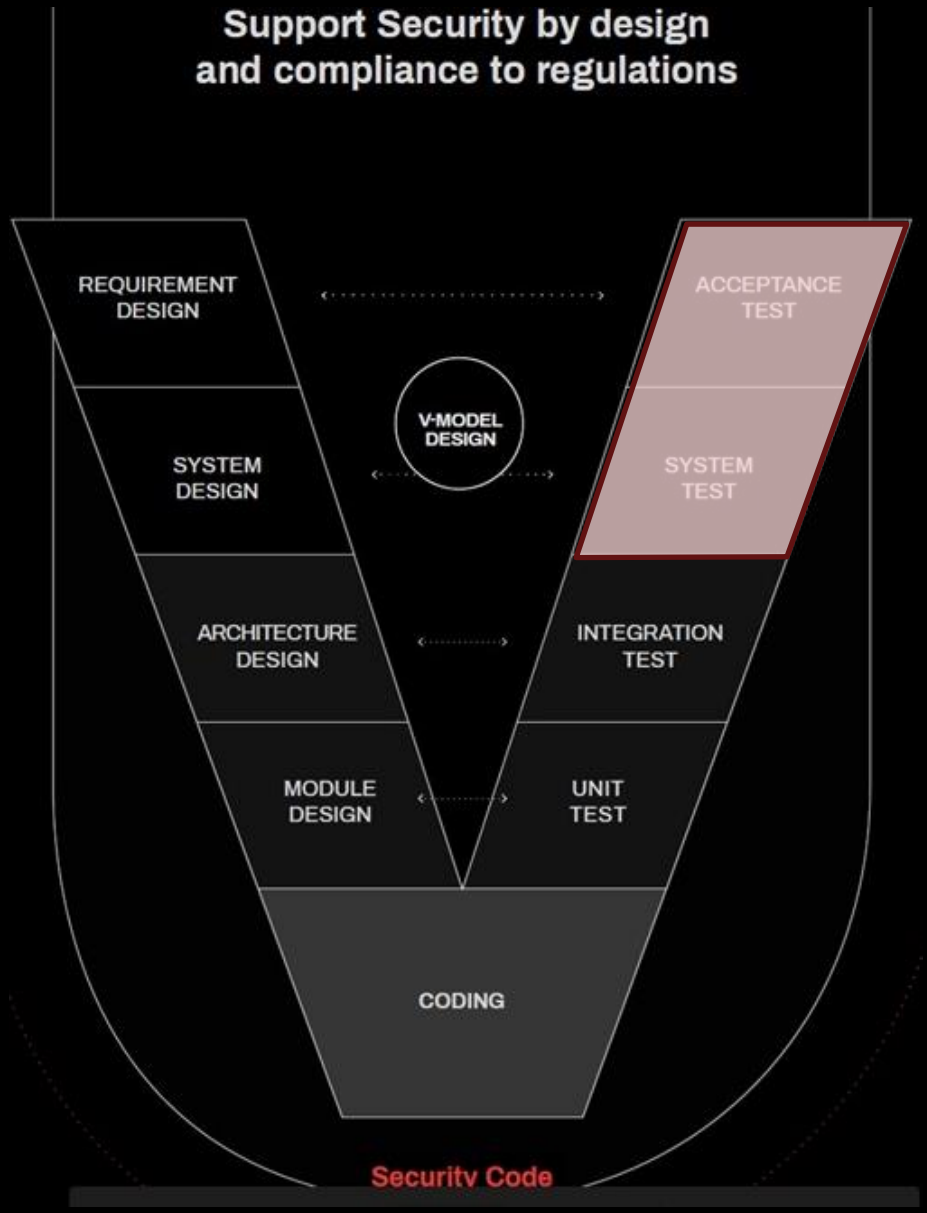
Vulnerability Assessment and Penetration Tests

- Vulnerability Scan & Assessment
- Functional Security Testing
- Penetration Testing
- Secure Operating Systems and Configurations



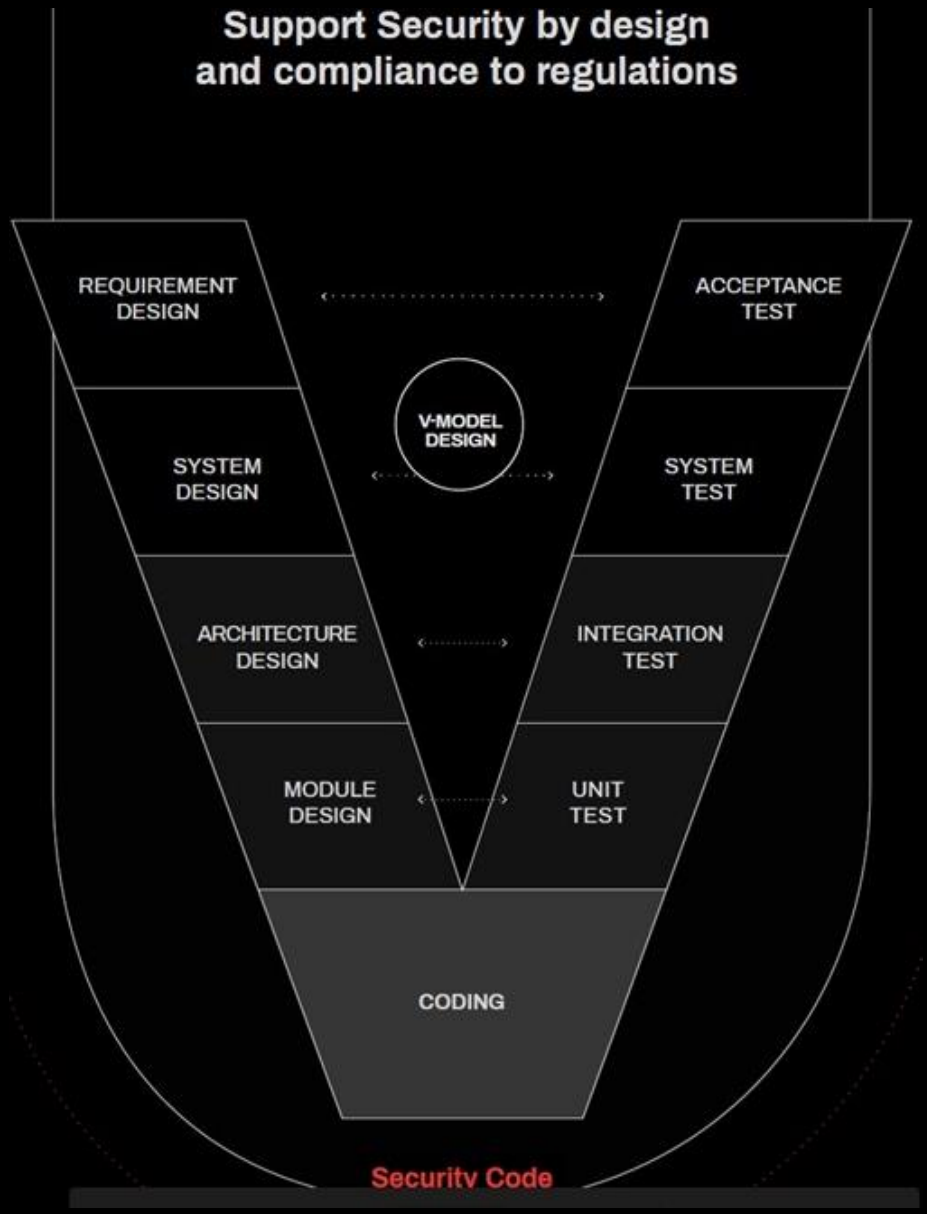
Penetration Tests

- Vulnerability Scan & Assessment at System Level
- Functional Security Testing at System Level
- Penetration Testing at System Level

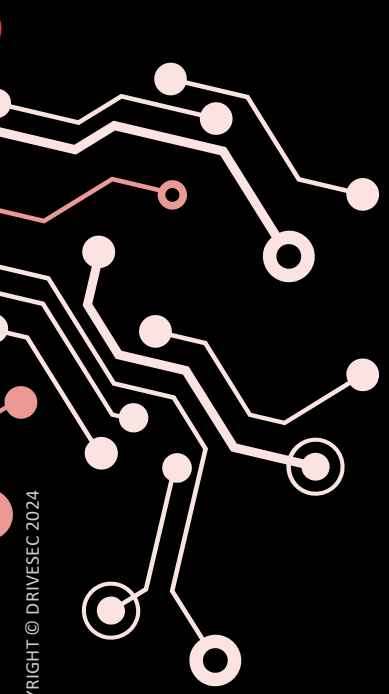


Continuous Monitoring

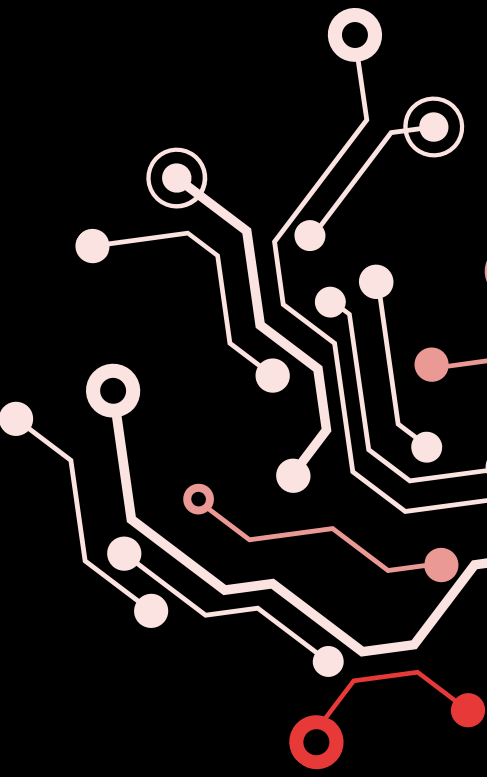
- Product management and Threat Intelligence
- Virtual Security Operations Center (VSOC)
- Incident Response Management



Test Verification Approach



Based on UNECE R155 **define a list** of cybersecurity test cases that can be performed **to demonstrate compliance** with the regulation



UNECE R155
Annex 5

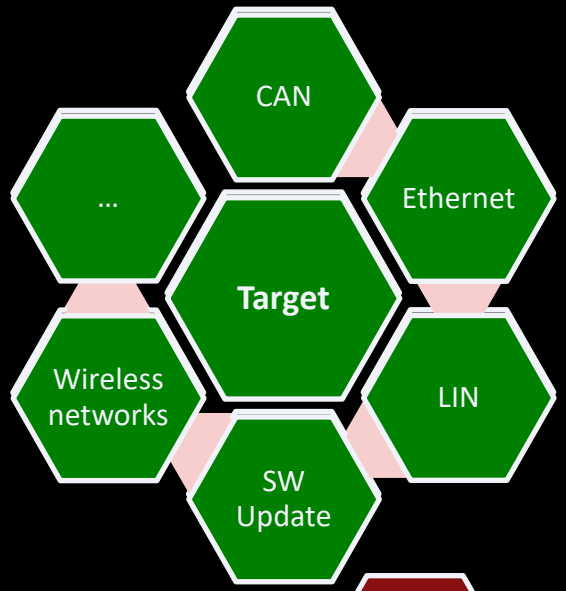
Annex 5 is a **list** of **threats** and corresponding **mitigations**

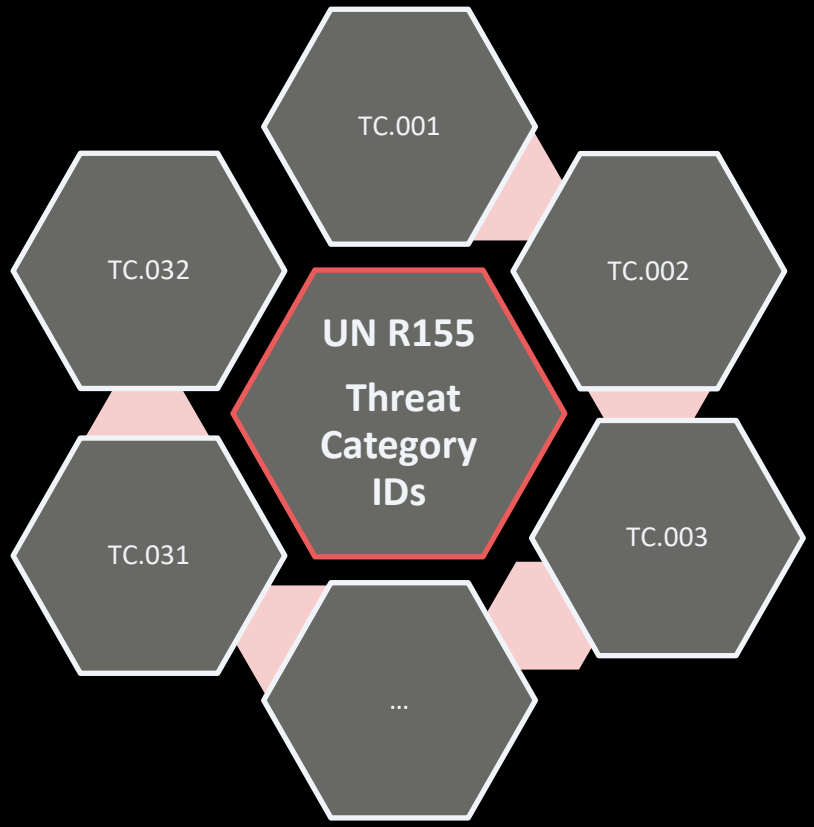
Annex 5 shall be considered for risk assessment and mitigations to be implemented by vehicle manufacturers.

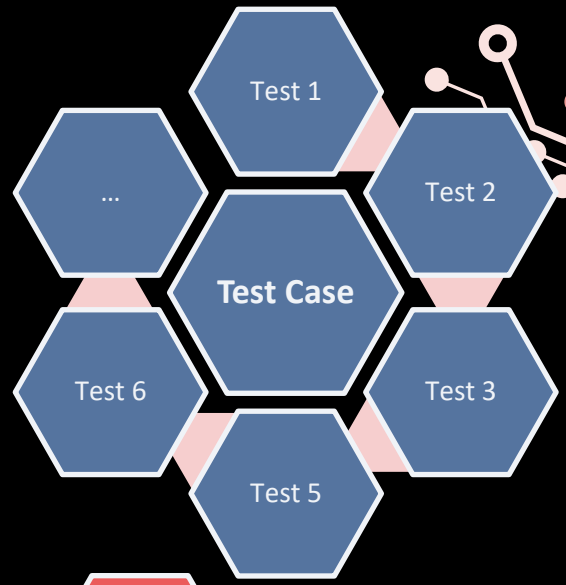
It consists of three parts:

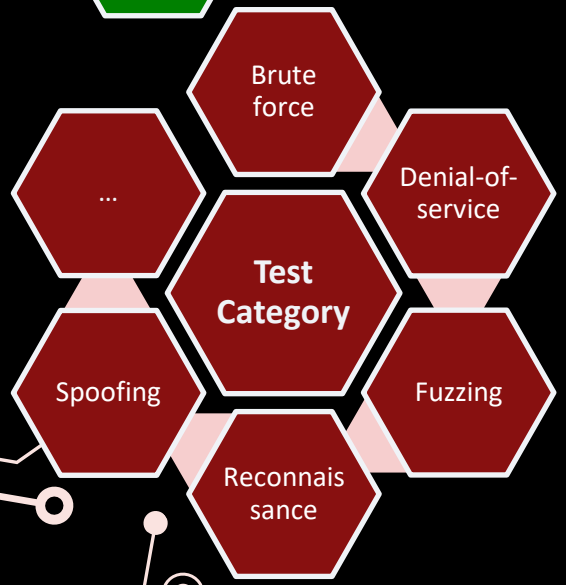
- **Part A** of the annex describes the baseline for **threats, vulnerabilities and attack methods**
- **Part B** of the annex describes **mitigations** to the threats which are intended **for vehicles**
- **Part C** describes **mitigations** to the threats **outside of vehicles**, e.g. on IT backends

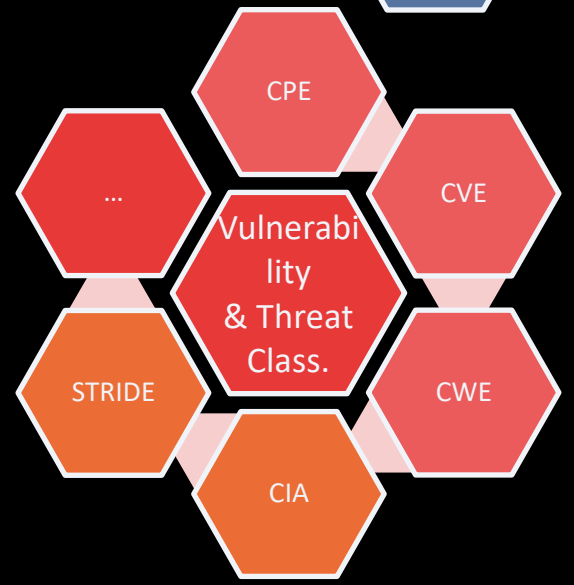
UNECE R155 mapping



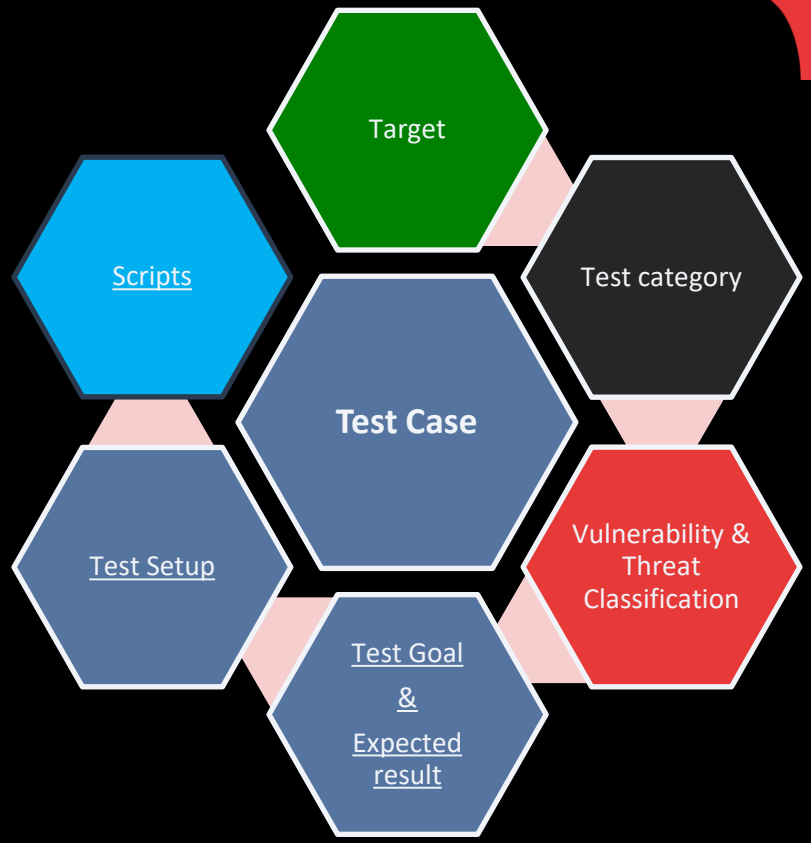








Test Case Design



Test Case Example

UNECE R155 Threats - Annex 5

- “An unprivileged user is able to gain privileged access to vehicle systems”(TC.009)
- “Cryptographic technologies can be compromised or are insufficiently applied” (TC.026)

Vulnerability

- CVE-2017-14937

Target

- Attack vector: ECU diagnostic stack

Test category

- Spoofing
- Brute force

Test Case

- **Test summary**: Verify if the ECU makes use of the best practices to reduce the effectiveness of brute force attacks against diagnostic access authentication.

- **Expected result**: Target ECU enforces a time delay when one or more authentication attempts have been failed.

- **CIA**: Integrity
- **STRIDE**: Spoofing & Escalation of Privilege

- **Test setup**

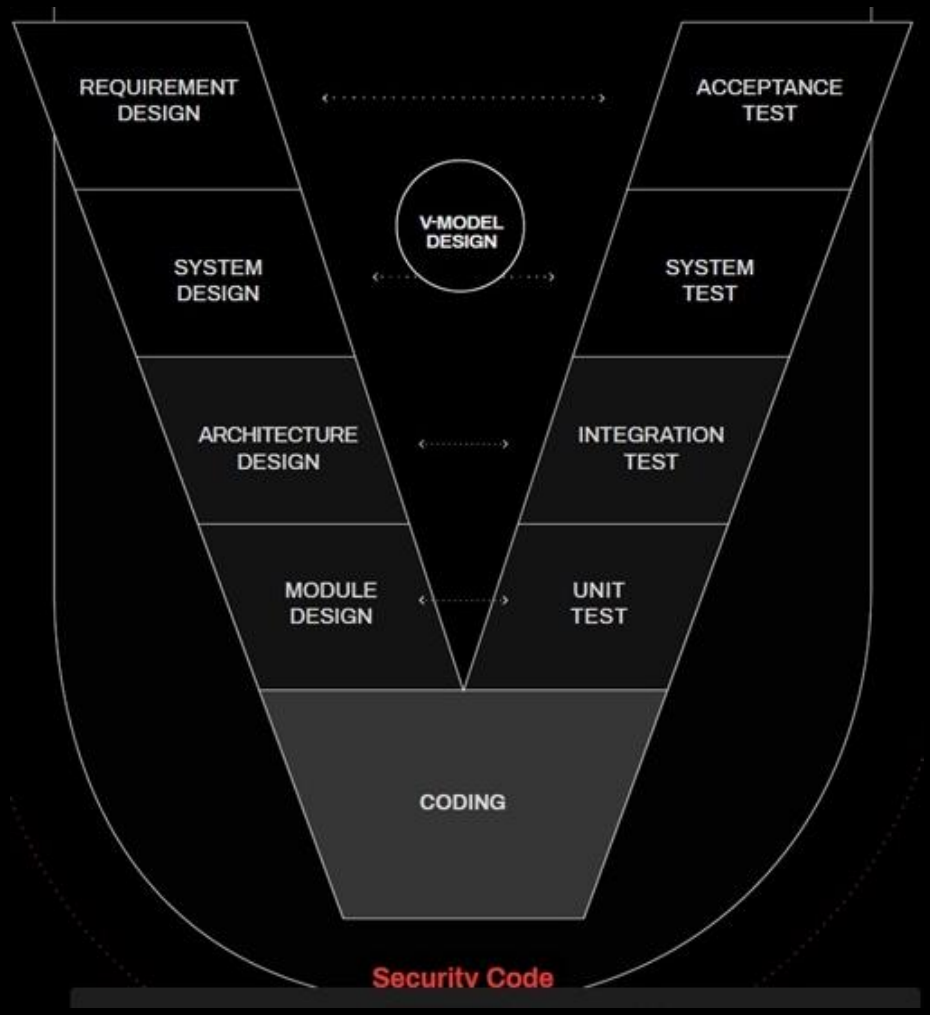
1. Identify the pinouts related to the target
2. Connect the target to HW adapter/converter

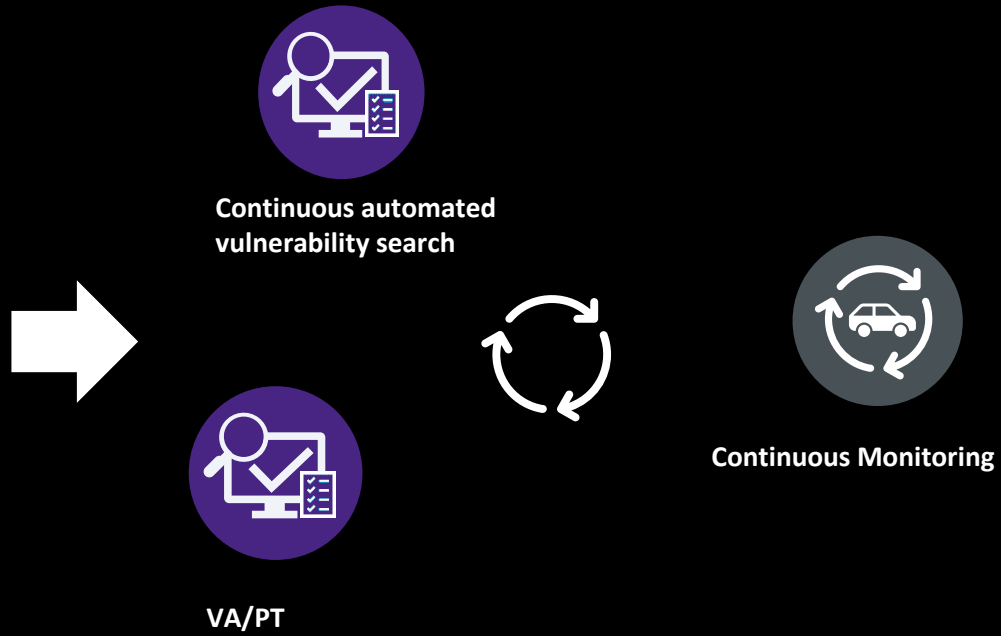
- **Test output:**
  - Vulnerability found, if any
  - Warnings

Test Reporting

- Collect information to demonstrate that risk are identified and managed
- Document Risk Assessment reports
- Show evidence of Requirements and Risks coverage
- Submit to Approval Authority all evidence of test execution
- Install a continuos monitoring process
- Write and share lesson learnt and improve organization

Build a continuous monitoring process





Build internal Knowledge base