자유와 활력이 넘치는
파워풀 대구

FIX All on AI
Future Innovation tech eXpo Conference 2025

Regulatory trends related to Cybersecurity testing in Automotive: DEKRA perspective, test cases and methodologies

Antonio Vizcaíno
DEKRA

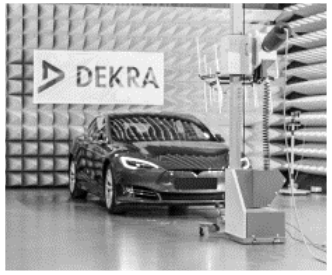
DEKRA 100 YEARS

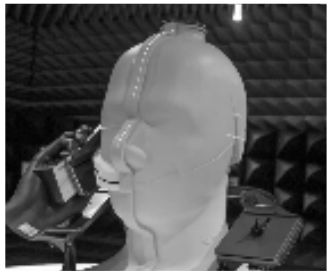
Antonio David Vizcaíno

Cybersecurity Technical Sales

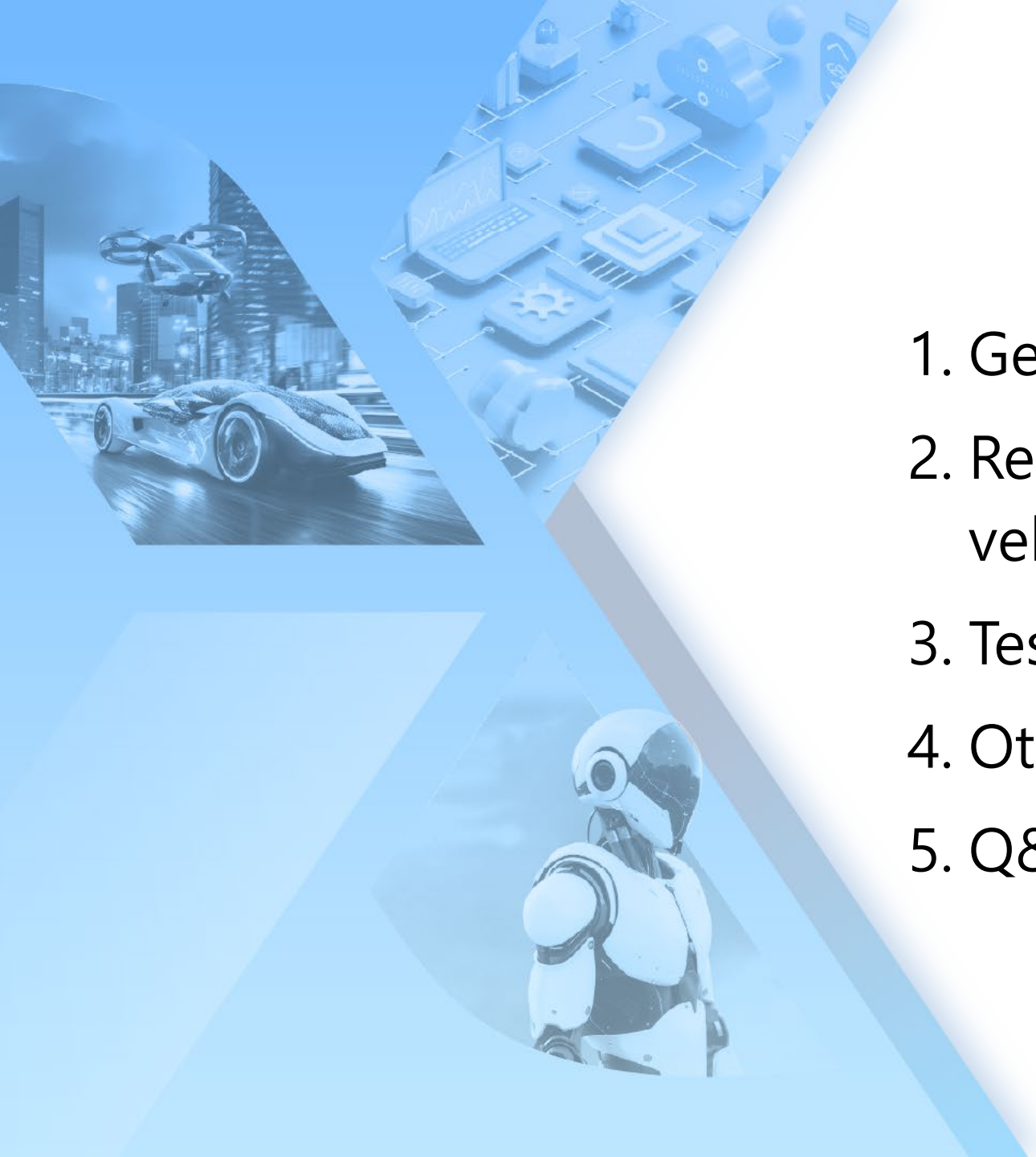
Get in Touch!

About DEKRA



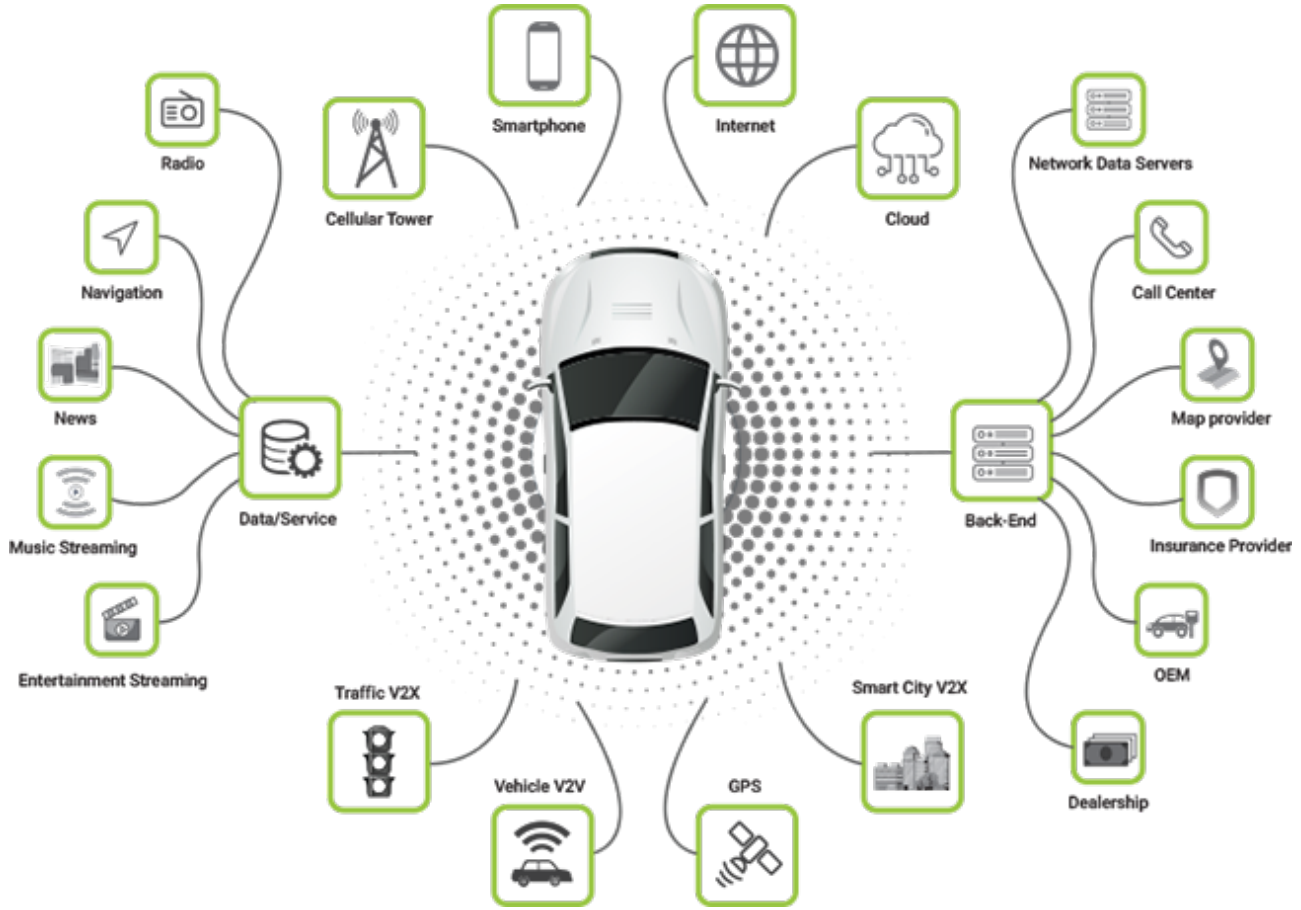


- **Established in 1925** to ensure road safety, DEKRA's mission today is to ensure safety, security and sustainability
- **DEKRA offers a broad service portfolio** as a global neutral partner for testing, inspection and certification in different technology fields and industry sectors
- **More than 48.000 employees** in 60 countries generate revenues of ~ 4.1B EUR (2023)
- **DEKRA**
  - …is experienced in product testing and is a technical service for vehicle type approval authorities



1. General concepts
2. Regulations for vehicles: EU motor vehicles & UNECE R155
3. Testing
4. Other Regulations
5. Q&A

General concepts



State-of-the-art : Cars become more and more data centers on wheels

A modern car can generate data volumes in the MB/GB range per day

The information generated in this way is mainly transmitted internally, but also externally via communication interfaces

Larger attack surface

Understanding the new ecosystem

Automotive Ecosystem

Vehicle type | User | Gateway | Communication | Cloud Server | Management System

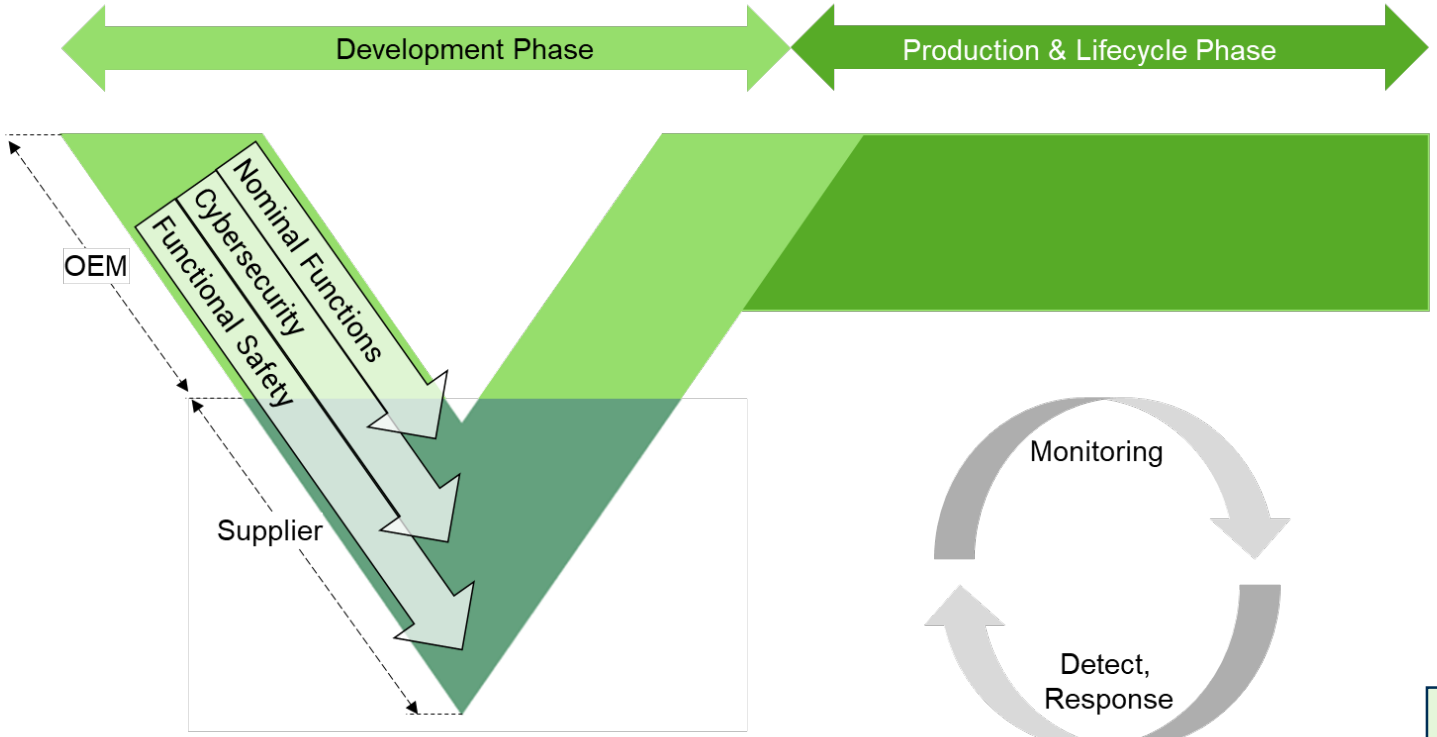
Important Security Principles

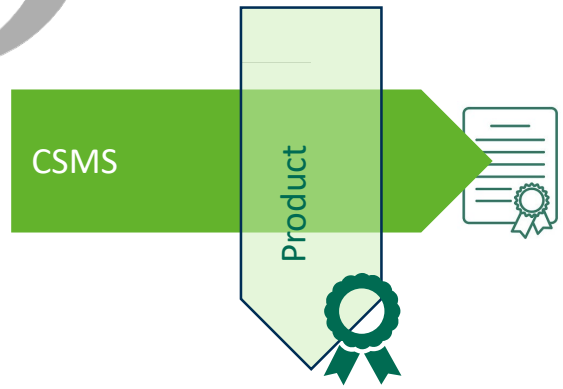
- Secure Component and vehicle type
- Secure Communications
- Certified Management System
- Secure Lifecycle Management

V-Cycle and Product dimension

Risk management applied across the entire lifecycle

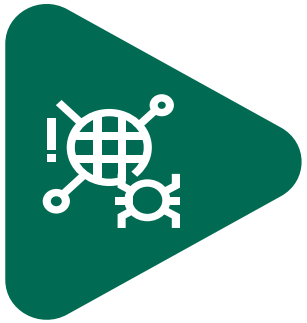
- Principle of risk minimization
- Mature organization (Process, Governance, Roles)
- Cybersecure Products
- Continuous market and product monitoring, incident detection and response





Impact on Cybersecurity test strategy

Cybersecurity Relevant Testing Methods



Vulnerability scanning

Fuzz Testing

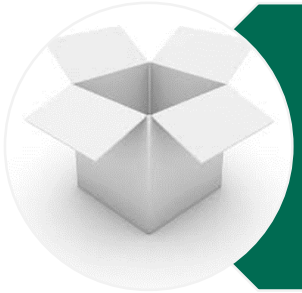
Penetration Testing

General evaluation of the level of security – performed continuously	Can be performed relatively early in the validation phase	Component and system level testing

▪ Identification of known vulnerabilities in different components
  ▪ Software components
  ▪ Hardware components
▪ Vulnerability scanning
  ▪ BOM based
  ▪ Network scanning tools
  ▪ Software Composition Analysis
	▪ Fuzz testing is an “automated” software testing technique
	▪ Massive amounts of “random” data, called fuzz, to crash or break the system
	▪ Find “software” bugs in code
	▪ Exploits systems vulnerabilities, so it can be fixed in due time
		▪ Penetration testing is a form of ethical hacking to find vulnerabilities
		▪ Pen-testing can also be referred to as a simulated cyber attack.
		▪ Find vulnerabilities
		▪ “Sometimes” Manual and creative

Framework conditions?
ISO 8477

Penetration Testing Approach



White-box

- Internals fully known
- Weak points can be identified before penetration testing starts
- Can include source code analysis
- More rigorous and comprehensive testing

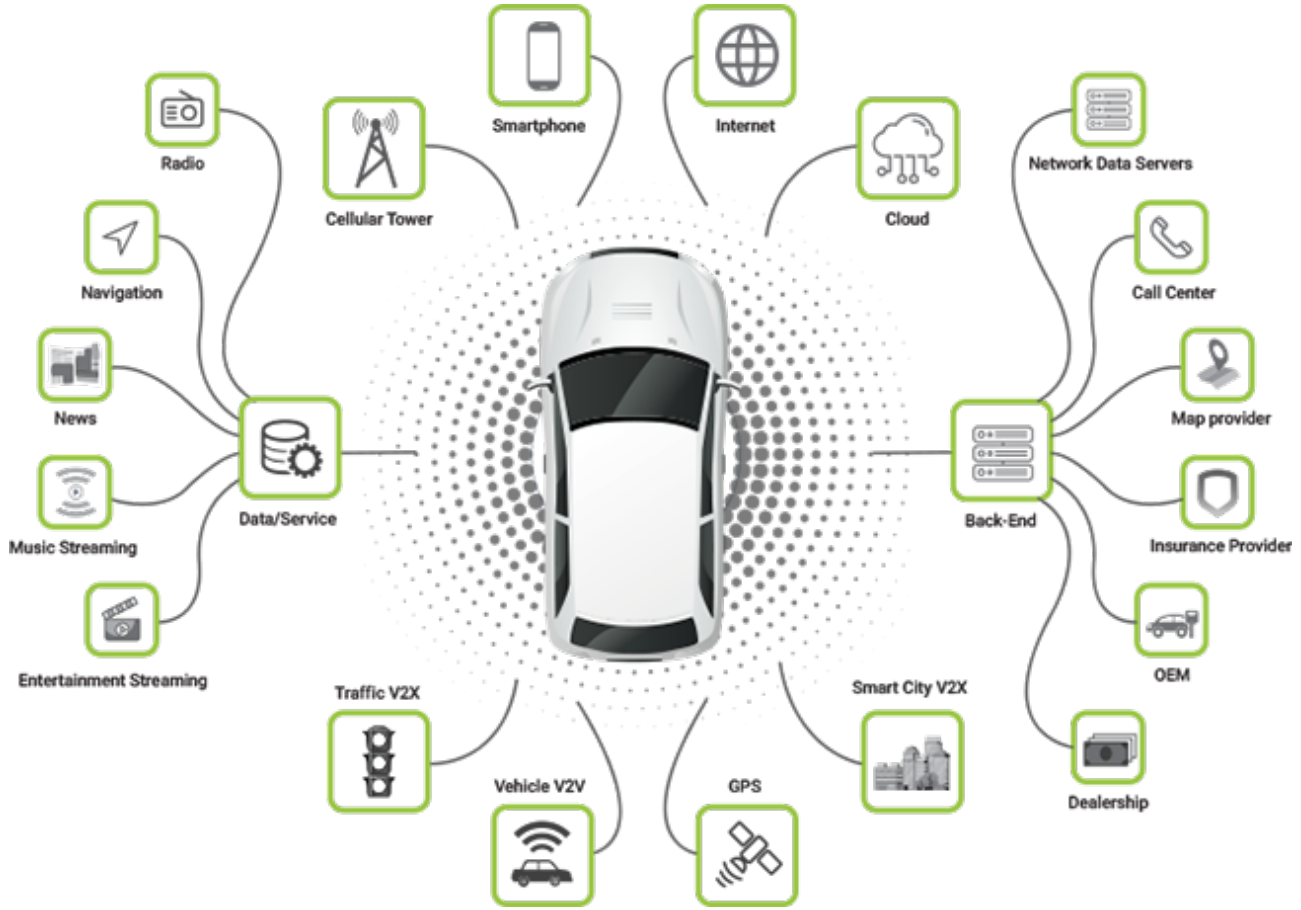
Grey-box

In between white-box and black-box, in terms of knowledge of the product under evaluation and time/cost of the evaluation
Only internals relevant to the evaluation known
Cuts down on testing time and budget, compared to black-box approach

Black-box

- No internals known
- Test the product from the perspective of an external attacker
- Does not test how secure the system is, but how well hidden the vulnerabilities are
- Time consuming – higher cost

Regulations for vehicles: EU motor vehicles & UNECE R155



Regulation (EU) 2019/2144

REGULATION (EU) 2019/2144 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 27 November 2019

on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users

(26) The connectivity and automation of vehicles increase the possibility for unauthorised remote access to in-vehicle data and the illegal modification of software over the air. In order to take into account such risks, UN Regulations or other regulatory acts on cyber security should be applied on a mandatory basis as soon as possible after their entry into force.

(27) Software modifications can significantly change vehicle functionalities. Harmonised rules and technical requirements for software modifications should be established in line with the type-approval procedures. Therefore, UN Regulations or other regulatory acts regarding software update processes should be applied on a mandatory basis as soon as possible after their entry into force. However, those security measures should not compromise the obligations of the vehicle manufacturer to provide access to comprehensive diagnostic information and in-vehicle data relevant to vehicle repair and maintenance.

Regulation (EU) 2019/2144
Consolidated version 07-07-2024

Amended by:

		Official Journal No	page	date
►M1	COMMISSION DELEGATED REGULATION (EU) 2021/1243 of 19 April 2021	L 272	11	30.7.2021
►M2	COMMISSION DELEGATED REGULATION (EU) 2021/1341 of 23 April 2021	L 292	4	16.8.2021
►M3	COMMISSION DELEGATED REGULATION (EU) 2021/1958 of 23 June 2021	L 409	1	17.11.2021
►M4	COMMISSION DELEGATED REGULATION (EU) 2022/545 of 26 January 2022	L 107	18	6.4.2022
►M5	COMMISSION DELEGATED REGULATION (EU) 2022/1398 of 8 June 2022	L 213	1	16.8.2022
►M6	COMMISSION DELEGATED REGULATION (EU) 2023/2590 of 13 July 2023	L 2590	1	22.11.2023

Corrected by:

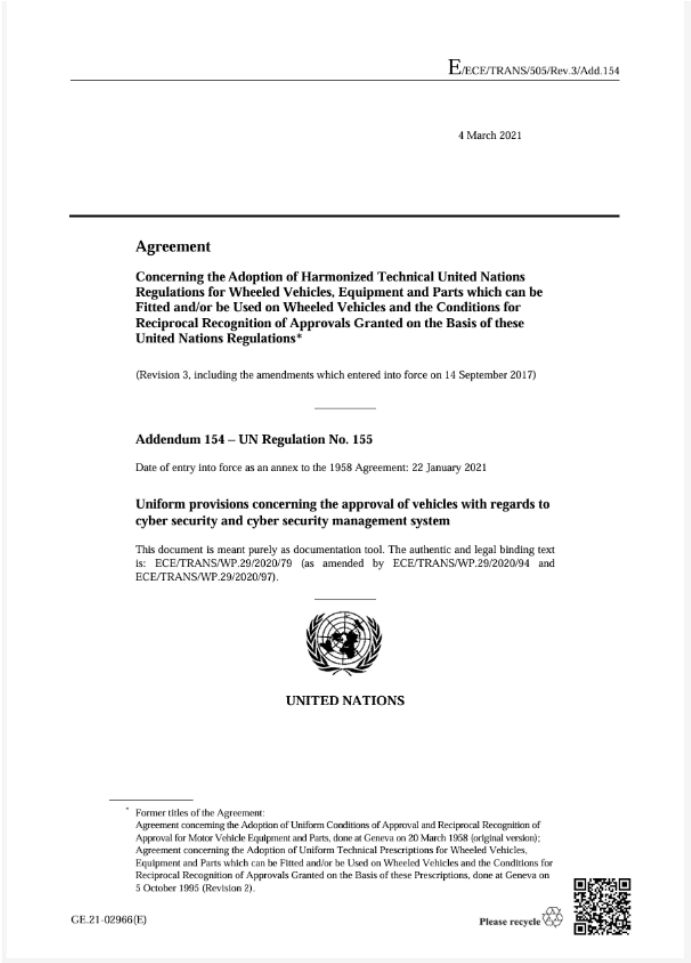
►C1	Corrigendum, OJ L 398, 11.11.2021, p. 29 (2019/2144)

ANNEX I

List of UN Regulations referred to in Article 4(2)

155	Cybersecurity and cybersecurity management system	Original version of the Regulation	OJ L 82, 9.3.2021, p. 30	M, N, O

D4 Protection of vehicle against cyberattacks	UN Regulation No 155		B	B	B	B	B	B					B	B



E/ECE/TRANS/505/Rev.3/Add.154

4 March 2021

Agreement

Concerning the Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these United Nations Regulations*

(Revision 3, including the amendments which entered into force on 14 September 2017)

Addendum 154 – UN Regulation No. 155

Date of entry into force as an annex to the 1958 Agreement: 22 January 2021

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

This document is meant purely as documentation tool. The authentic and legal binding text is: ECE/TRANS/WP.29/2020/79 (as amended by ECE/TRANS/WP.29/2020/94 and ECE/TRANS/WP.29/2020/97).

UNITED NATIONS

* Former titles of the Agreement:
Agreement concerning the Adoption of Uniform Conditions of Approval and Reciprocal Recognition of Approval for Motor Vehicle Equipment and Parts, done at Geneva on 20 March 1958 (original version);
Agreement concerning the Adoption of Uniform Technical Prescriptions for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these Prescriptions, done at Geneva on 5 October 1995 (Revision 2).

GE.21-02966(E)

Please recycle

innovating safety & security

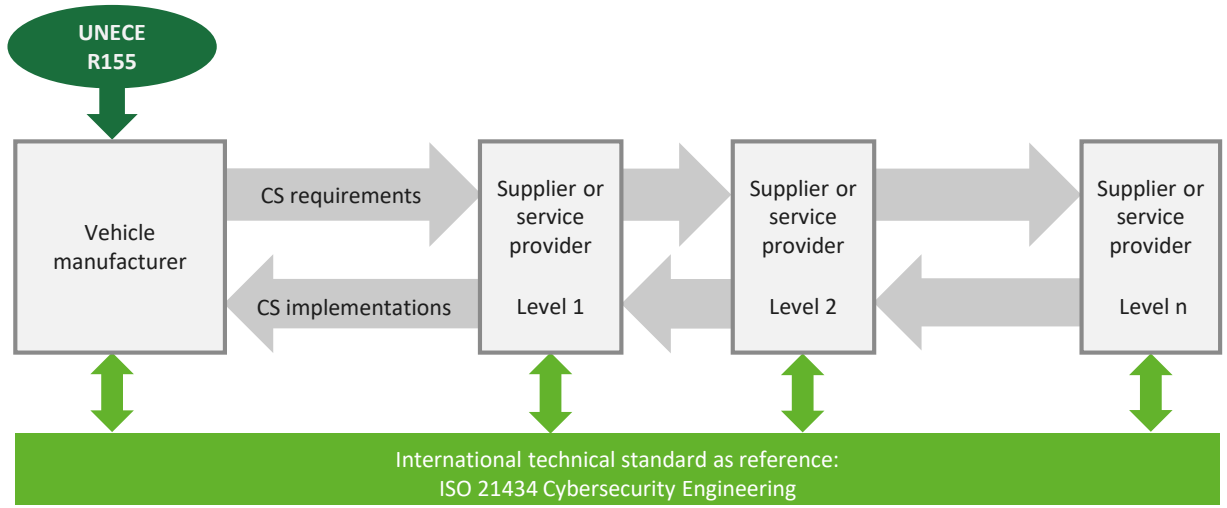
What will OEMs/supplier need to fulfill?

OEMs:

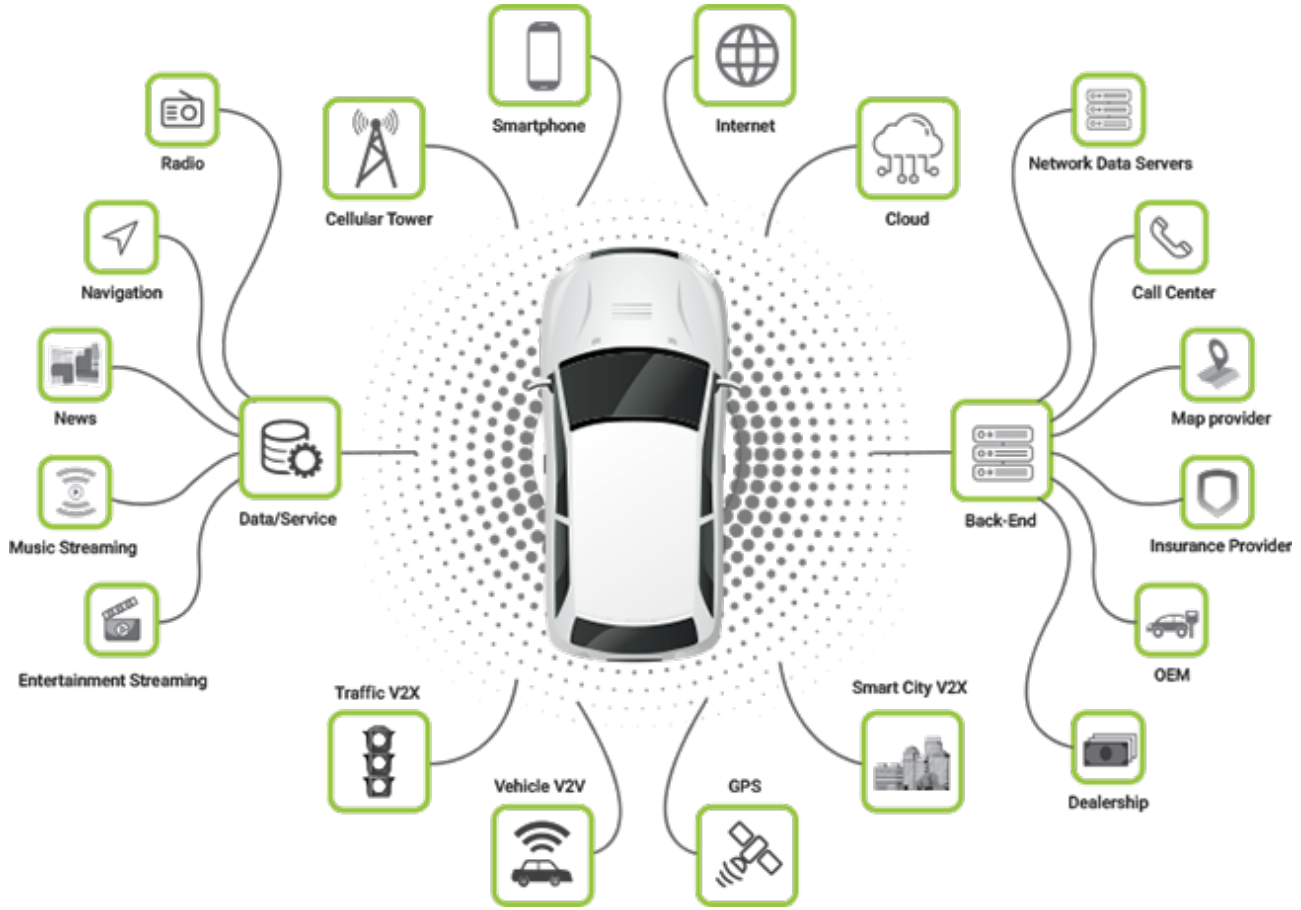
- UNECE R155 (and R156)
  - Part 1: Company-oriented - CSMS (certified)
  - Part 2: Vehicle Oriented - Type approval
- Relatively free **how** the requirements are met (R155 is defined at a very high level)
  However, they will use ISO 21434 (and ISO 24089) to control his supply chain.

Suppliers:

- Will likely be forced by OEMs to fulfill ISO 21434 (and ISO 24089)
- Will use ISO 21434 (and ISO 24089) to control his suppliers



Testing


Radio
Navigation
News
Music Streaming
Entertainment Streaming
Data/Service
Cellular Tower
Smartphone
Internet
Cloud
Network Data Servers
Call Center
Map provider
Insurance Provider
OEM
Dealership
Back-End
Traffic V2X
Vehicle V2V
GPS
Smart City V2X

Penetration Testing, ISO 21434 and UN R155

Penetration testing is a group of **testing methods used to find vulnerabilities** present in a system that can be exploited by an adversary to take control, gain privileged access, expose privileged data, or simply cause system malfunction.

- Penetration testing can be performed with different levels of knowledge about the system (i.e., black, grey, and white box testing).
- The output of the penetration testing helps to identify cybersecurity requirements and controls to harden items or components against potential threats.

ISO/SAE 21434 (ECUs)

Penetration Testing is a recommendation included in ISO 21434:

- **Product Development**

Component testing methods

[RC-10-03] Recommendation Component testing should be performed to search for unidentified vulnerabilities.

- **Cybersecurity Validation**

[RC-11-01] Recommendation Penetration testing should be performed to validate the cybersecurity goals as part of the validation activities of [RQ-11-01].

UN R155 (Vehicles)

Automotive Testing Methodology based on Annex V

Although it is mentioned in the standard as a recommendation, penetration testing is the most effective way to discover vulnerabilities in systems.

ISO 21434 Cybersecurity Testing Methods

- Product Development
  - Component testing methods

- [RC-10-03] Recommendation Component testing should be performed to search for unidentified vulnerabilities.

- Testing Methods can include
  - Functional testing
  - Vulnerability scanning
  - Fuzz testing
  - Penetration testing

Penetration Testing
cybersecurity testing in which real-world attacks are mimicked to identify ways to compromise cybersecurity goals

Automotive Penetration Testing Key Aspects

Challenges

- Complexity
- Safety
- Proprietary protocols and systems
- Evolving threat landscape
- Expanded attack surface

Components

- Telematics Control Units (TCUs)
- In-Vehicle Infotainment (IVI) Systems
- Vehicle-to-Everything (V2X) components
- Security Gateway
- Advanced Driver Assistance Systems (ADAS)
- Tire Pressure Monitoring System (TPMS)

Attack Vectors

- Wireless Interfaces
- Physical Access
- Supply Chain
- Associated Services

Component Penetration Testing – CS Goals

DEKRA performs Penetration Testing to identify risks, vulnerabilities and security flaws.

Goal of the penetration testing is to validate whether it is possible to gain access to the ECU via the existing interfaces. (*)

Penetration testing is complex as it requires a thorough understanding of the complete ecosystem and how its parts work together. The Penetration testing can include, among others, the following goals:

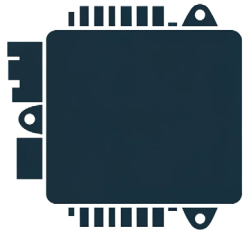
- ECU code dump and reverse engineering
- Upload and run to ECU of non-authentic code
- Extraction of security Keys
- Resilience of access regulation functionalities
- Diagnostic stack
- Resilience to brute force and swamping attacks through the interfaces (CAN, LIN, etc.)
- Resilience to attacks through CAN aimed to tamper key functionalities (Fuzz testing)
- Connection to ECUs resources by means of protocols and interfaces like:
  - Serial, USB and Ethernet interfaces
- Fuzz Testing and vulnerability scanning
- Data dump and tampering of external memories

(*) In case that the component has a mobile app or cloud service, they should be included in the penetration testing scope
(**) Fault injections and side-channel attacks are usually considered out of scope.

ECU Types

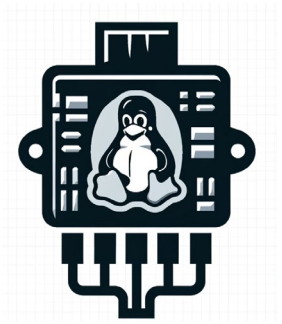
Limited Surface

- **ECU with SoC** (RTOS)
- **Wired Interfaces** (CAN, LIN, Ethernet)
- **Example:** Rear Lamp system integrating one NXP S32118K SoC using AUTOSAR OS with 2 x CAN and a LIN interface



Regular Surface

- **ECU with one VµC** (RTOS) **and another SoC** (e.g. Linux)
- **Wired Interfaces** and internal communications through **UART, SPI**, …
- **Example:** Instrument Cluster Panel with an RH850 vehicle microcontroller running AUTOSAR OS and another ARM Cortex M3 running Linux OS. Available interfaces 2 CAN, 1 LIN and 1 DoIP.

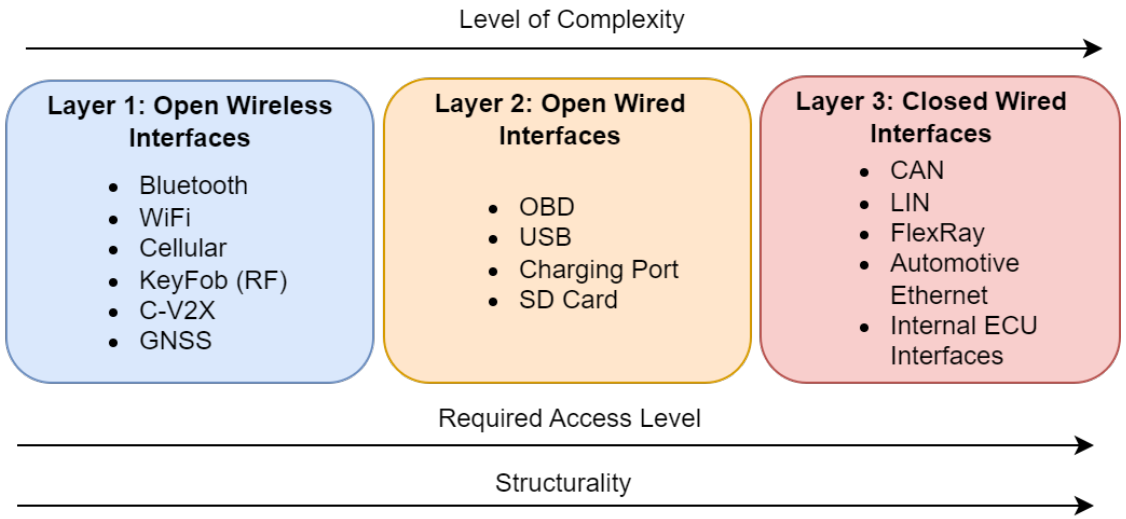


Extended Surface

- **ECU with one VµC** (RTOS) **and another SoC** (e.g. Android)
- **Wired and Wireless interfaces** (Wi-Fi, 4G/5G, Bluetooth)
- **Example:** Infotainment system using NXP RH850 Vehicle micro controller running AUTOSAR OS and ARM Cortex M3 running Android 12 including wired interfaces (2xCAN, 1 LIN, 1 DoIP) and wireless interfaces Wi-Fi (hotspot), 4G LTE and Bluetooth LE.

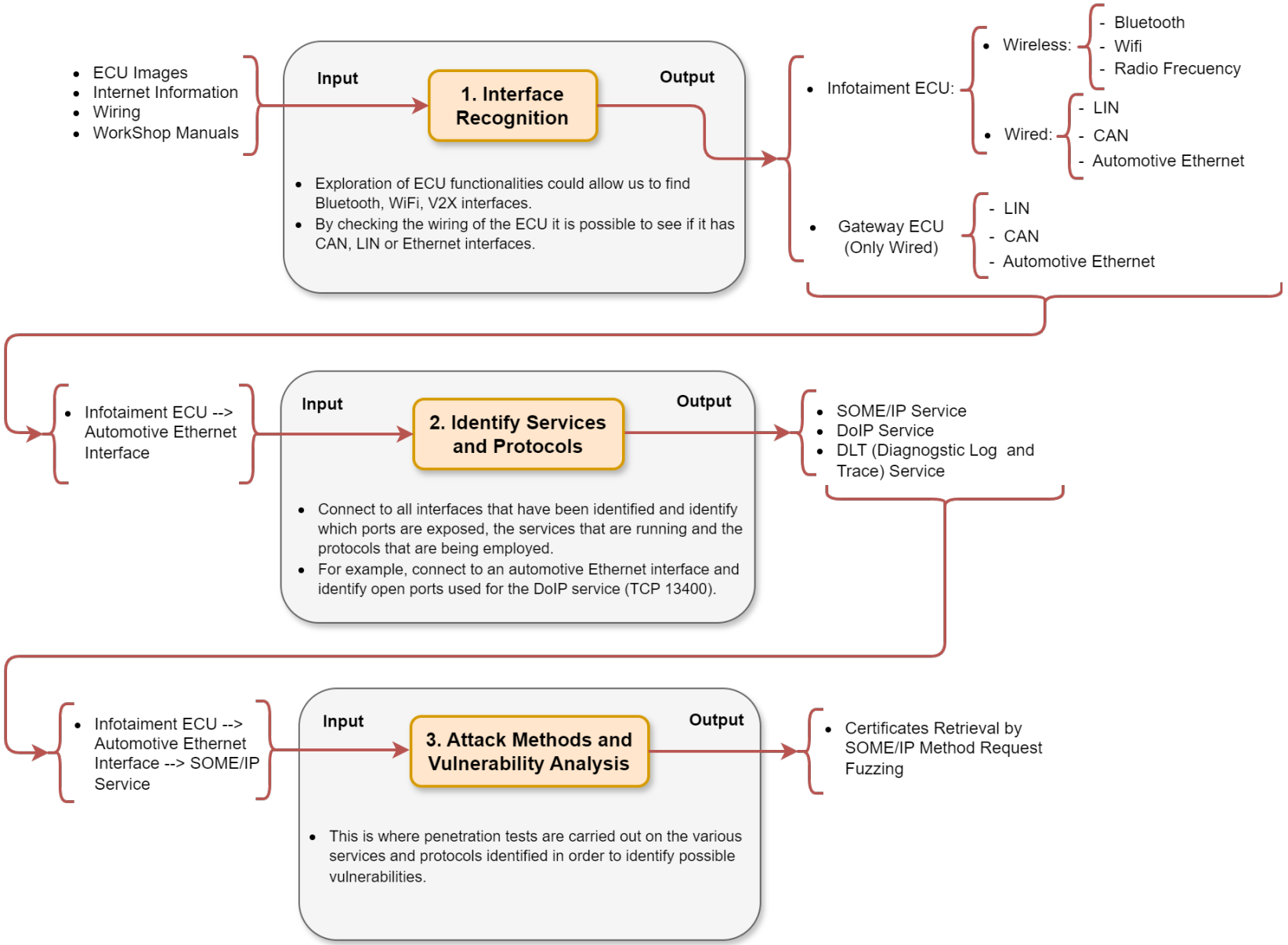
Vehicle Penetration Testing Overview

We can consider 3 layers when dealing with vehicle penetration testing:



- Layer 1: Target wireless interfaces (e.g., Bluetooth, Wi-Fi, NFC, Cellular) without physically accessing or disassembling the vehicle.
- Layer 2: Assess the security of wired interfaces that can be accessed without any disassembly.
- Layer 3: Conduct in-depth testing of wired interfaces that require partial disassembly of the vehicle, such as accessing internal ECUs or hidden connectors.

Methodology Overview



Vehicle Penetration Testing – General Approach

Phase 1 - Lab Premises

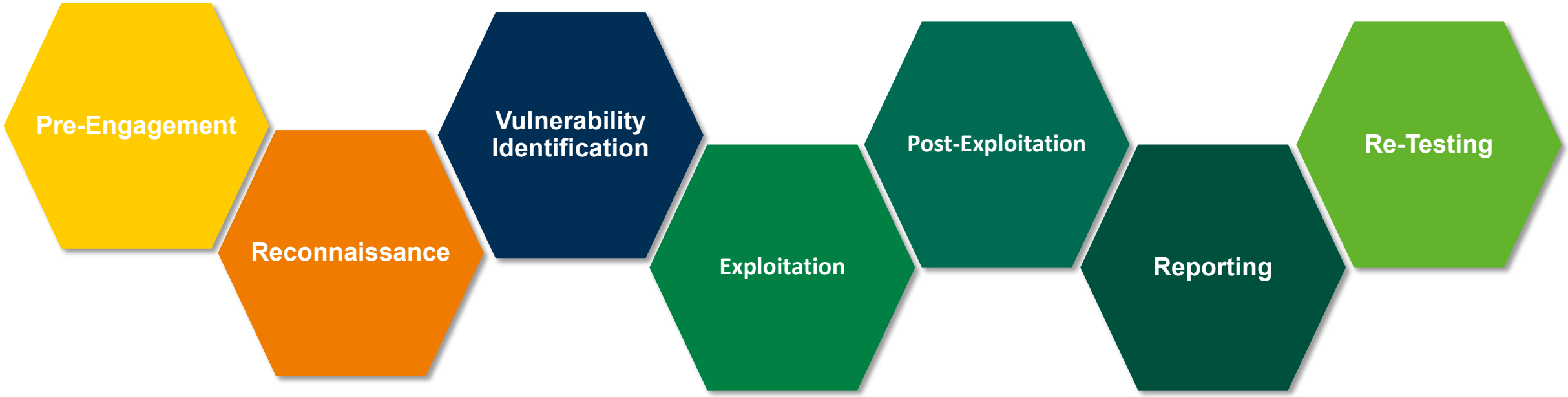
- Vehicle threat analysis
- Testbench simulating relevant ECUs
- Tasks included in 1st and 2nd phase of Component Penetration testing

Phase 2 - On-site

- Check lab findings
- Fuzzing
- Review of physical ports (e.g. OBD2) and Network security mechanisms (e.g. Sec. Gateways)
- Physical access review (wiring)

Phase 3 - Retest

- Verify remediation plans
- Check that security relevant vulnerabilities have been fixed


Pre-Engagement
Reconnaissance
Vulnerability Identification
Exploitation
Post-Exploitation
Reporting
Re-Testing

Penetration Testing Phases – Reconnaissance

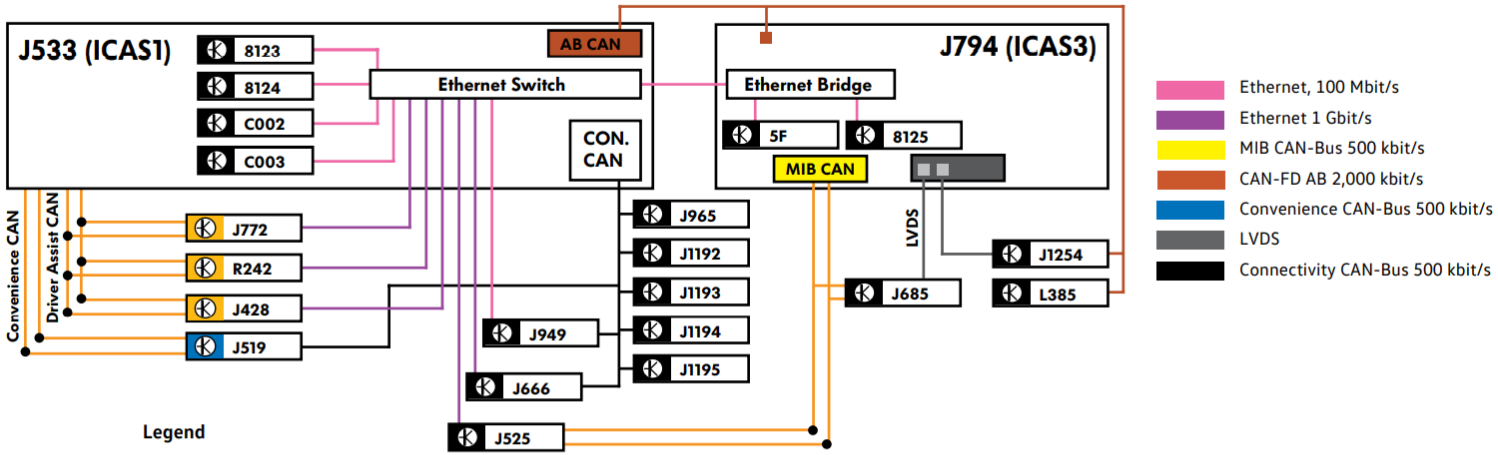
Vehicle Architecture

- Infotainment
  - MIB **CAN**
    - Front Info Display Control
    - Digital Sound System
  - **LVDS**
    - Front Info
    - Lighting
  - **Ethernet**
    - Infotainment Display Control
    - Application Server

- MIB CAN-Bus 500 kbits/s
- CAN-FD AB 2,000 kbits/s
- Convenience CAN-Bus 500 kbits/s
- Connectivity CAN-Bus 500 kbits/s

Networking in the ID.4

Two new control modules, the J533 (ICAS1) and J794 (ICAS3) are the primary processors. ICAS (In-Car Application Server) modules are central computers/servers that bring together a variety of basic services and vehicle functions to control the vehicle systems.



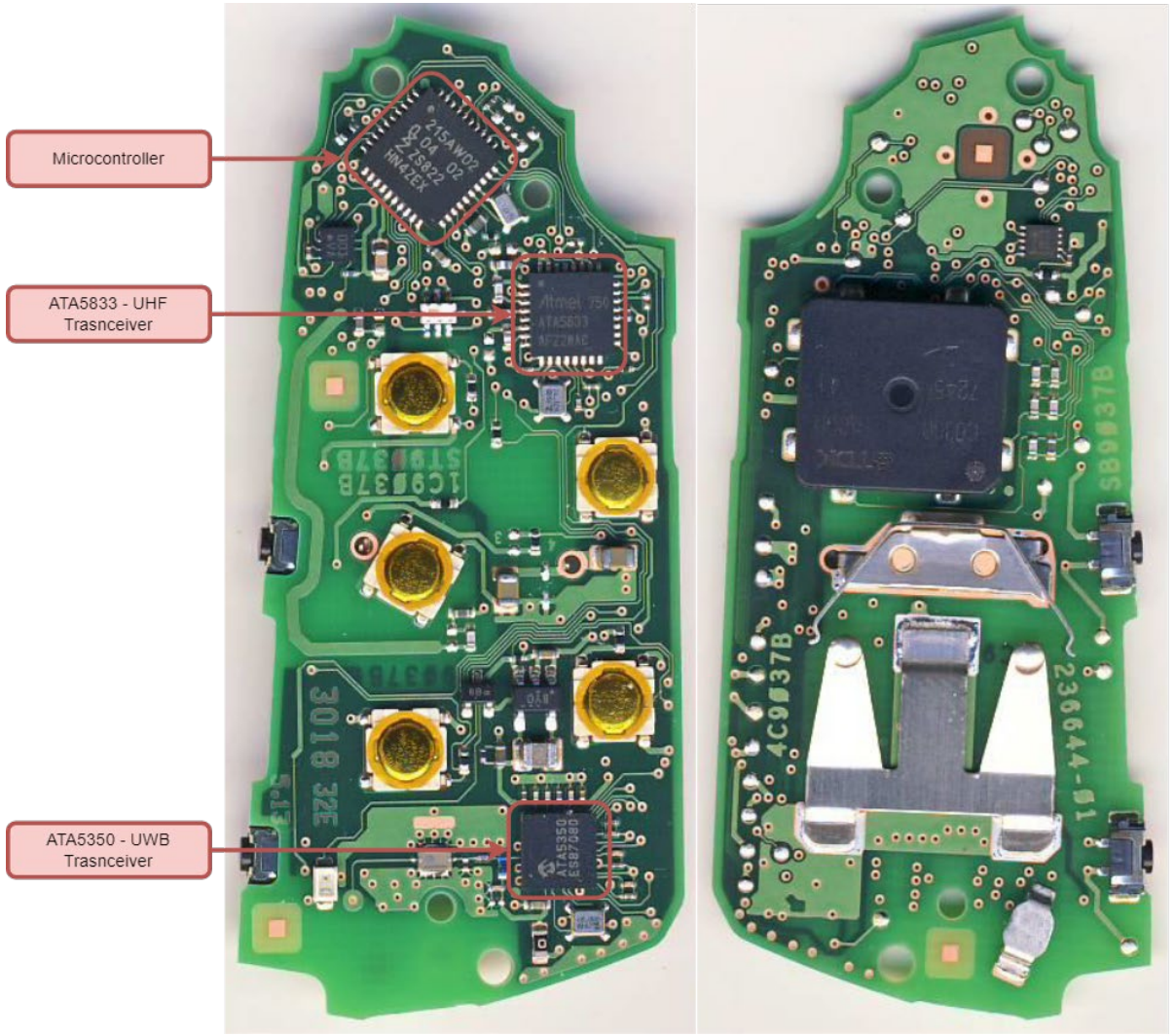
Legend

5F Information Electronics Display Control
8123 Application Server 1 System 1 Adaptive
8124 Application Server 1 System 2 Java
8125 Application Server 3, System 1 for Infotainment
C002 Software Cluster, Imbedded 1
C003 Software Cluster, Housekeeping 1
J428 Control Module for Adaptive Cruise Control
J519 Vehicle Electrical System Control Module
J525 Digital Sound System Control Module
J533 Data Bus on Board Diagnostic Interface (ICAS1)
J666 Internet Access Control Module
J685 Front Information Display Control Head
J794 Information Electronics Control Module 1
J949 Control Module for Emergency Call Module and Communication Unit
J965 Access/Start System Interface
J1192 Burglary Protection Control Module 2
J1193 Burglary Protection Control Module 3
J1194 Burglary Protection Control Module 4
J1195 Burglary Protection Control Module 5
J1254 Driver Information System Control Module with Display Unit
L385 Dynamic Lighting Strip 1 for Information in Instrument Panel
R242 Driver Assistance Systems Front Camera

Penetration Testing Phases – Reconnaissance

Keyfob system internals

- KeyFob
  - Information retrieved from FCC ID
    - https://fcc.report/FCC-ID/NBGFS19
  - Identified HW Components
    - MCU – NXP 2154W02
    - UHF Transceiver – ATA5833
    - UWB Transceiver – ATA5350



Penetration Testing – Vulnerability Identification

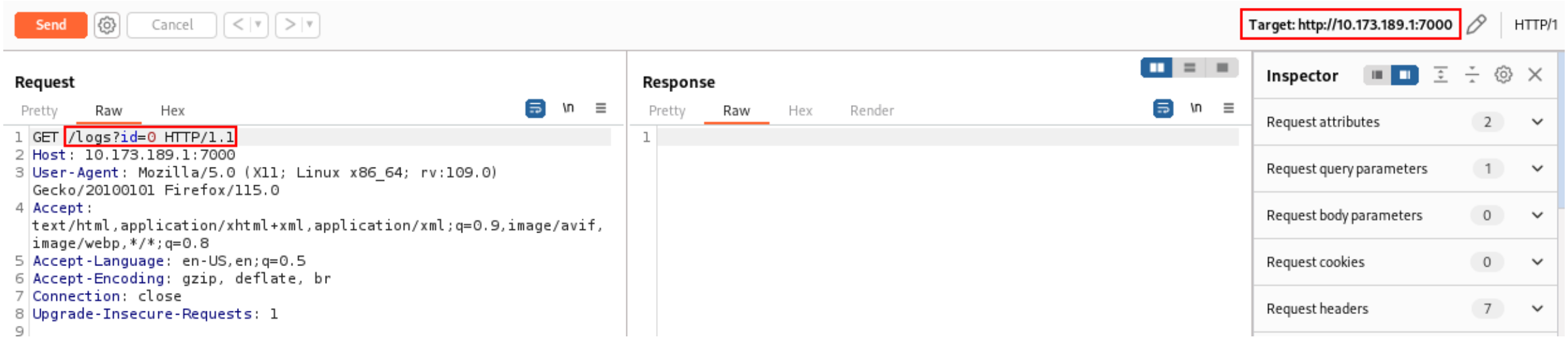
- RTSP port for Apple Car play running on IPv4 of IVI Hotspot Wi-Fi network.
- Affected by CVE-2023-28898
  - https://nvd.nist.gov/vuln/detail/CVE-2023-28898

```
└─$ nmap -sV -sC [redacted] -T4 -p-
Starting Nmap 7.92 ( https://nmap.org ) a[redacted]
Nmap scan report for [redacted]
Host is up (0.0029s latency).
Not shown: 65528 filtered tcp ports (no-response)
PORT      STATE  SERVICE       VERSION
80/tcp    closed http
443/tcp   closed https
5000/tcp  closed upnp
5001/tcp  closed commplex-link
6030/tcp  closed x11
7000/tcp  open   rtsp
|_rtsp-methods: ANNOUNCE, SETUP, RECORD, PAUSE, FLUSH, TEARDOWN, OPTIONS, POST, GET, PUT
|_irc-info: Unable to open connection
| fingerprint-strings:
|   FourOhFourRequest, GetRequest:
|     HTTP/1.1 404 Not Found
|     Content-Length: 0
|     Server: AirTunes/320.17.7
|   HTTPOptions:
|     HTTP/1.1 200 OK
|     Public: ANNOUNCE, SETUP, RECORD, PAUSE, FLUSH, TEARDOWN, OPTIONS, POST, GET, PUT
|     Server: AirTunes/320.17.7
|   RTSPRequest:
|     RTSP/1.0 200 OK
|     Public: ANNOUNCE, SETUP, RECORD, PAUSE, FLUSH, TEARDOWN, OPTIONS, POST, GET, PUT
|     Server: AirTunes/320.17.7
|   SIPOptions:
|     RTSP/1.0 200 OK
|     Public: ANNOUNCE, SETUP, RECORD, PAUSE, FLUSH, TEARDOWN, OPTIONS, POST, GET, PUT
|     Server: AirTunes/320.17.7
|_    CSeq: 42 OPTIONS
49150/tcp closed inspider
```

Penetration Testing - Exploitation

Exploitation through WiFi Hotspot

- **Exploit**: https://www.pcautomotive.com/vulnerabilities-in-skoda-and-volkswagen-vehicles
- Try to exploit vulnerabilities through open ports in WiFi interfaces.
    - It was possible to perform a DoS in the Infotainment by sending crafted RSTP request - *CVE-2023-28898*



Penetration Testing – Reporting – Based on ISO 17025 best practices

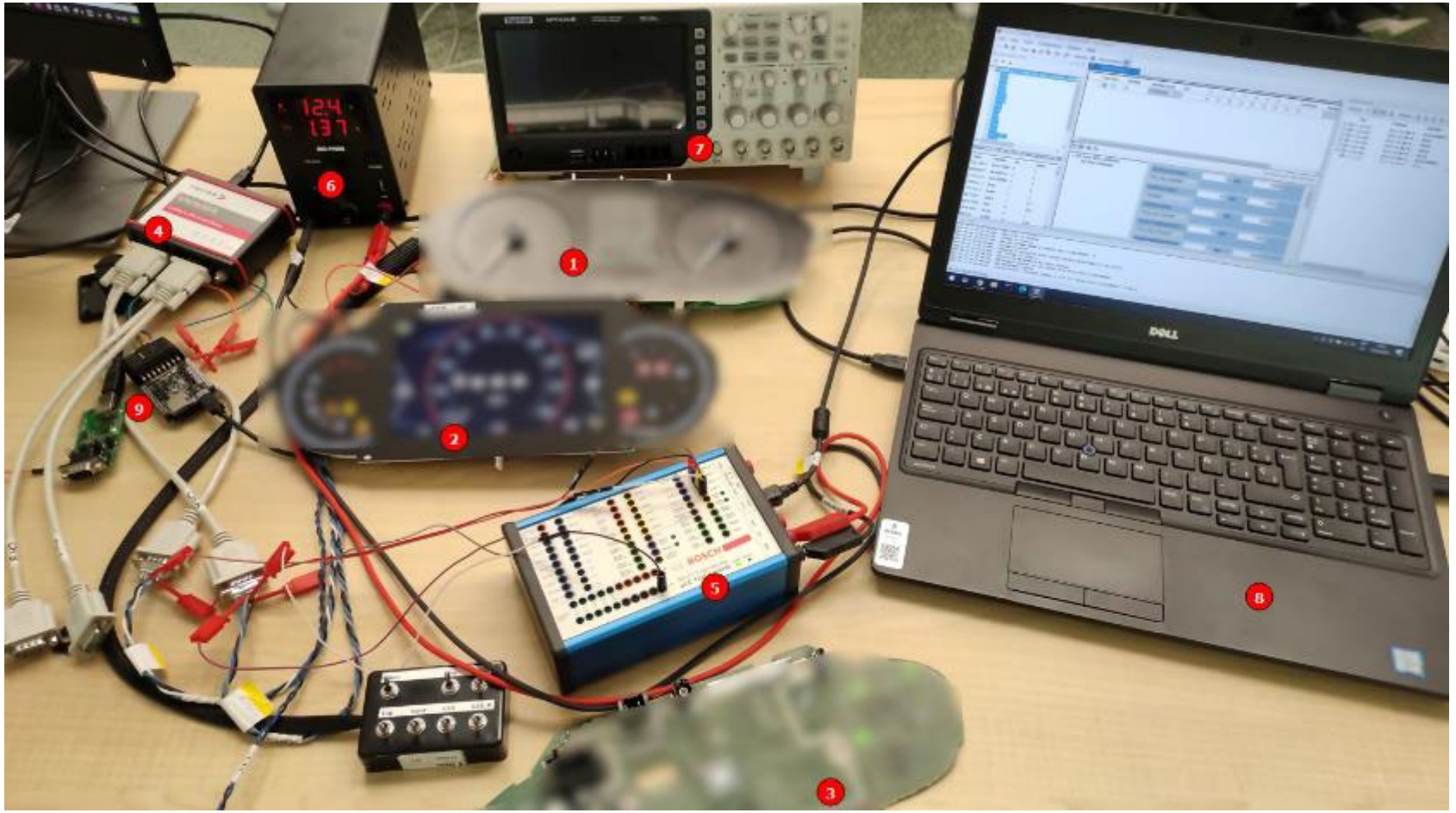
- ISO 17025 is the international standard that specifies the general requirements for the competence, impartiality, and consistent operation of laboratories.
- A key component of ISO 17025 compliance is the proper documentation and reporting of evaluation results.
  - Title
  - Unique identifier
  - Name and address of the laboratory
  - Customer information
  - Description of the item tested (Type, Model, FW, HW, …)
  - Testing period and location
  - Identification of methods used
  - Results of the evaluation
  - Signature, Name and position of Authorizing personnel
  - Environmental conditions (if applicable)
  - Tools
  - Competences and guarantees
  - Remarks and Comments

Scenario 1: Inter-component bus data sniffing

ITEMS

1. Canoe VECTOR PC
2. Vector tool
3. Saleae Logic Analyzer
4. Arduino SPI Sniffer / Replay
5. Saleae Logic PC
6. TOE
7. Microscope
8. Power Source

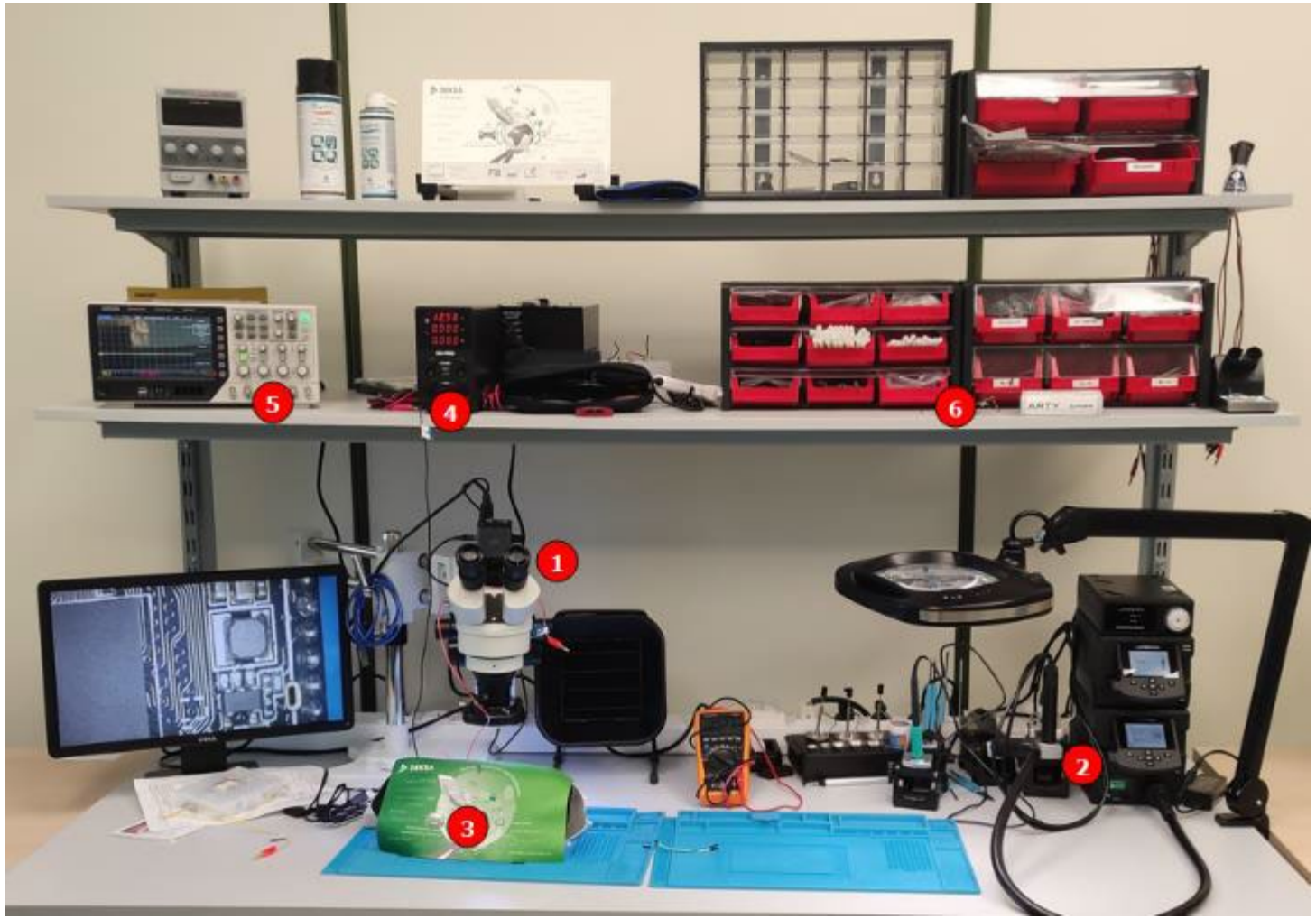
Scenario 2: Setup for automotive / CANbus



ITEMS

1. TOE 1
2. TOE 2
3. TOE 3
4. VECTOR tool
5. uLC BOSCH tool
6. Power Source
7. Oscilloscope and Logic Analyzer
8. Canoe Software and others
9. Auxiliary CANbus sniffers

Scenario 3 - Setup for IC techniques



ITEMS

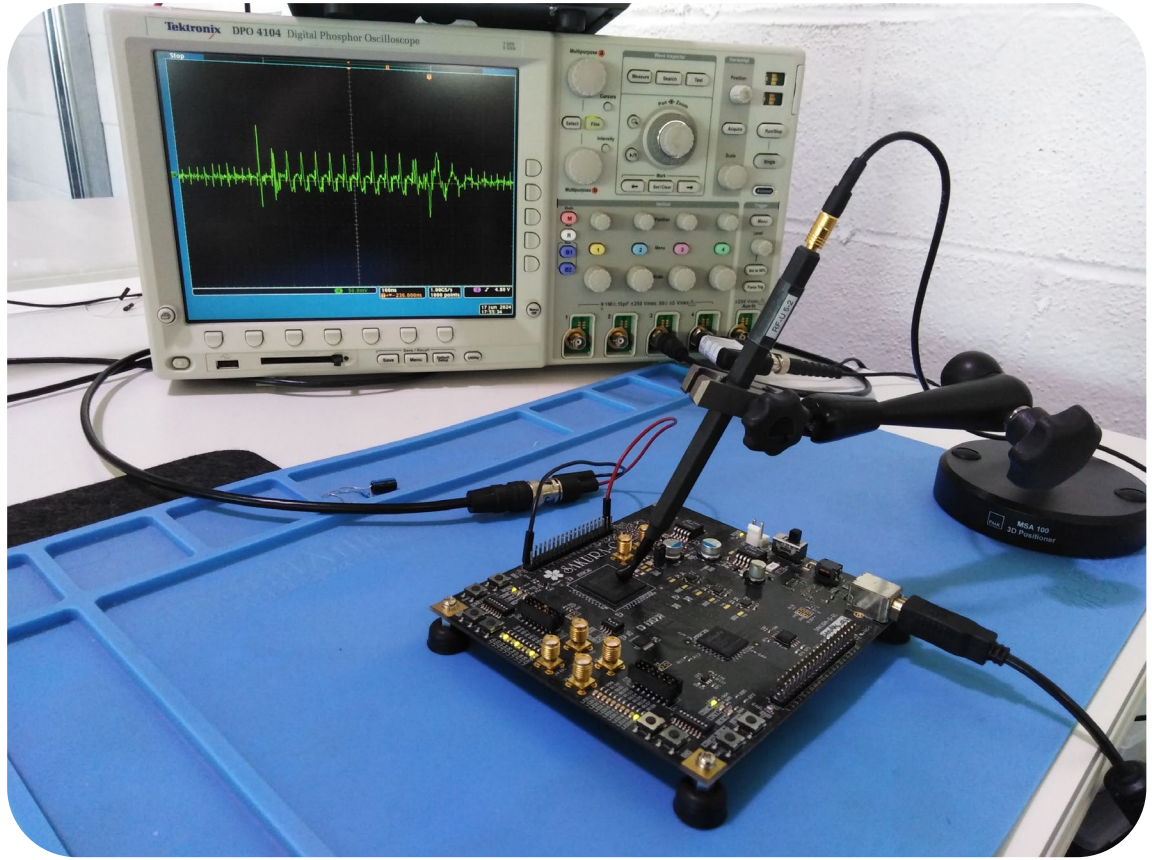
1. Microscope
2. Solder station
3. TOE
4. Power source
5. Oscilloscope
6. Other tools, fluxes and remover glues.

Side-channel Analysis

Introduction

What is it?

- **A side-channel** is any kind of physical measurement during a device's operation that reveals information about the device or its data
- **Side-channel analysis** consists of extracting cryptographic keys or other valuable information from the side-channels of a device



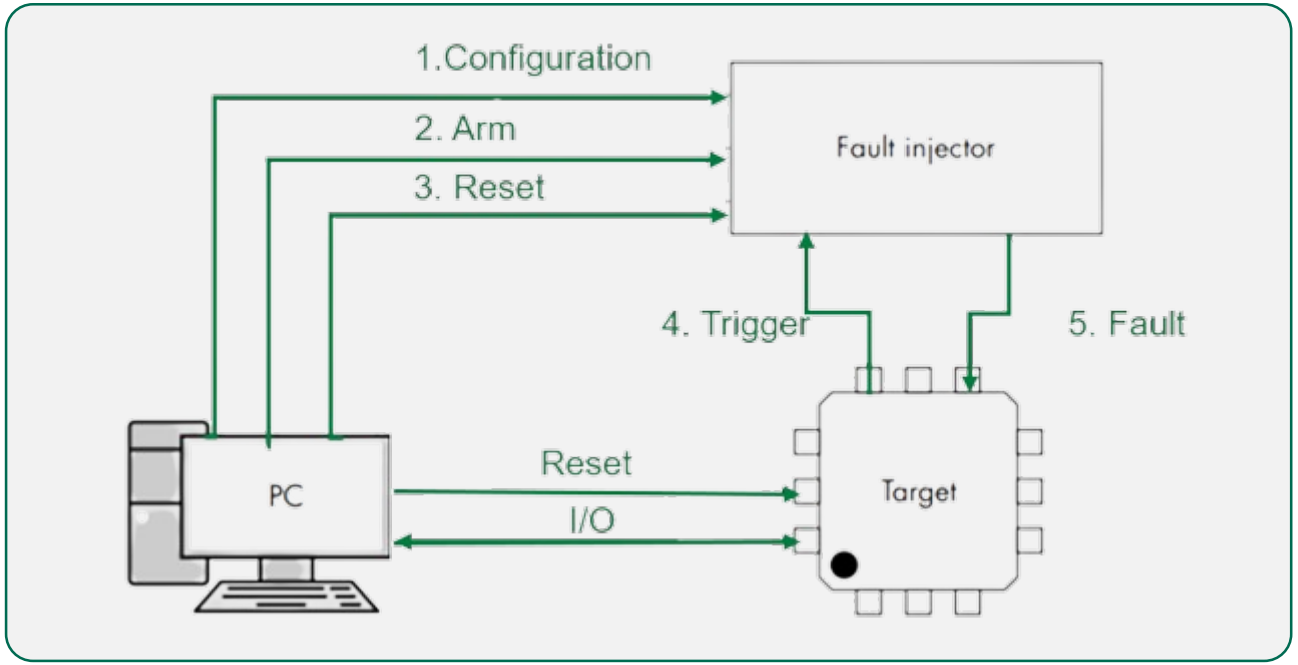
Fault Injection

Introduction

What is it?

- Induce incorrect operation in the circuit under analysis, in order to exploit different characteristics of it
- Used for bypassing security functions to e.g. extract firmware, attack secure boot or privilege escalation

Typical setup



Types

- Clock glitching
- Voltage glitching
- Electromagnetic fault injection (EMFI)

Backup: Other Regulations

- EU CCMS & CPOC (EU)
- RED Delegated Act (EU)
- NIS2 (EU)
- BIS (US)

Q&A

Thank you!