Continental Engineering Services

Cyber Security in Automotive - Zero to 100
23/24

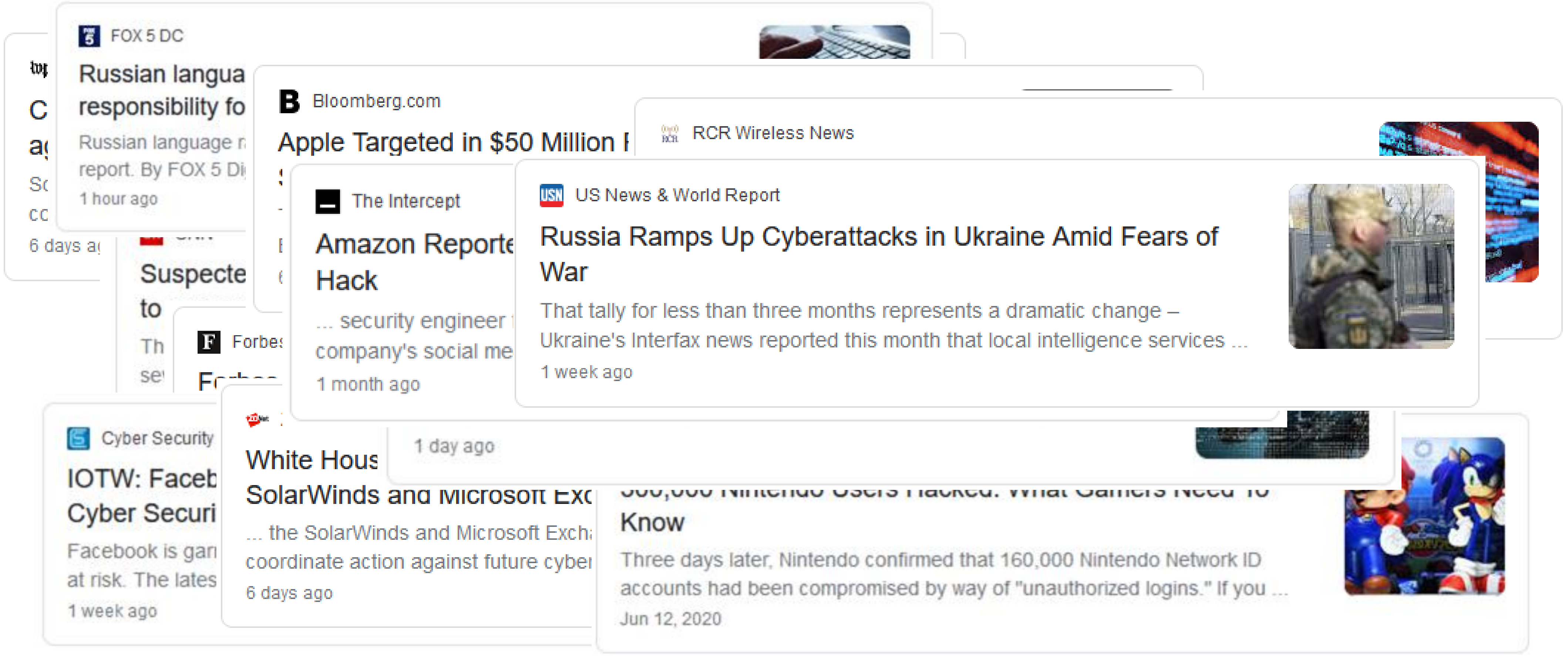
www.conti-engineering.com

Continental Engineering Services

Table of contents

What we see

Continental Engineering Services



FOX 5 DC
Russian langua
responsibility fo
Russian language r
report. By FOX 5 Di
1 hour ago

C
ag
Sc
cc
6 days ag

Bloomberg.com
Apple Targeted in $50 Million I

RCR Wireless News

The Intercept
Amazon Reporte
Hack
... security engineer
company's social me
1 month ago

US News & World Report
Russia Ramps Up Cyberattacks in Ukraine Amid Fears of War
That tally for less than three months represents a dramatic change – Ukraine's Interfax news reported this month that local intelligence services ...
1 week ago

Suspecte
to
Th
se

Forbes
Fo

Cyber Security
IOTW: Faceb
Cyber Securi
Facebook is gan
at risk. The lates
1 week ago

White Hous
SolarWinds and Microsoft Exc
... the SolarWinds and Microsoft Exch
coordinate action against future cyber
6 days ago

1 day ago

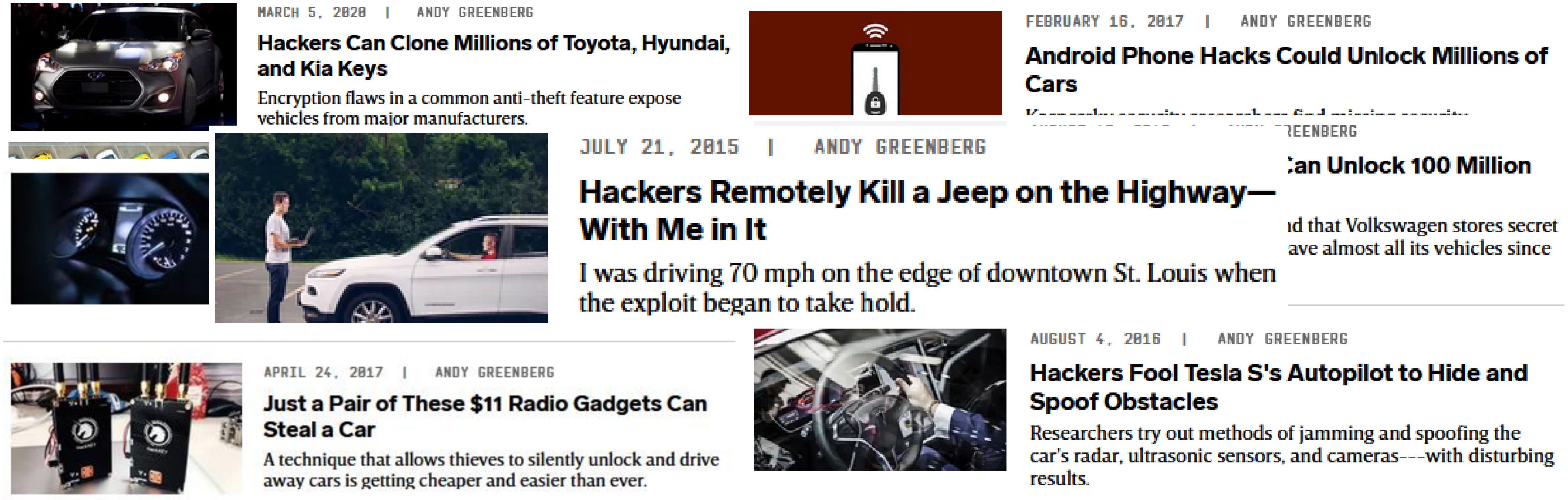
Know
Three days later, Nintendo confirmed that 160,000 Nintendo Network ID accounts had been compromised by way of "unauthorized logins." If you ...
Jun 12, 2020

Security in automotive

What about cars

What about cars …

Continental Engineering Services



MARCH 5, 2020 | ANDY GREENBERG

Hackers Can Clone Millions of Toyota, Hyundai, and Kia Keys

Encryption flaws in a common anti-theft feature expose vehicles from major manufacturers.

FEBRUARY 16, 2017 | ANDY GREENBERG

Android Phone Hacks Could Unlock Millions of Cars

Kaspersky security researchers find missing security

REENBERG

:an Unlock 100 Million

ıd that Volkswagen stores secret
ave almost all its vehicles since

JULY 21, 2015 | ANDY GREENBERG

Hackers Remotely Kill a Jeep on the Highway—With Me in It

I was driving 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

APRIL 24, 2017 | ANDY GREENBERG

Just a Pair of These $11 Radio Gadgets Can Steal a Car

A technique that allows thieves to silently unlock and drive away cars is getting cheaper and easier than ever.

AUGUST 4, 2016 | ANDY GREENBERG

Hackers Fool Tesla S's Autopilot to Hide and Spoof Obstacles

Researchers try out methods of jamming and spoofing the car's radar, ultrasonic sensors, and cameras---with disturbing results.

The worrying numbers

- **Collection and exchange** of data opens a security and privacy concern **to the future**
- **Cybersecurity** incidents are **increasing** dramatically
- **Careless development** opens new doors for black-hats

2010-2021
84.5% Remote

2022
63% Black Hat

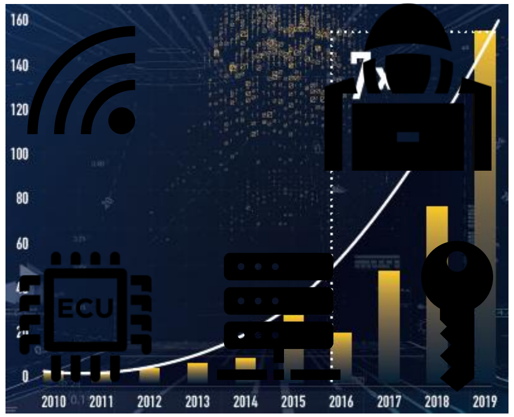
2016-2019
7x

2022
97% Remote

Servers 35%

ECU 14%

Keyless 18%



Top incidents in 2022

2022

Q1:

- Hacker remotely controls 25 American OEM EVs around the world.
- Several vulnerabilities were found in multiple charging stations which allowed remote attackers to impersonate charging station admin users and carry out actions on their behalf.
- Two major OEMs vulnerable to replay attacks let hackers remotely unlock and start vehicles

Q2:

- Chinese OEM vehicles were found to be vulnerable to attacks via update Processes.
- Hackers targeted vehicles of an American OEM through Bluetooth attacks.
- Japanese automotive supplier hit by ransomware attack.

Q3:

- A hacker gained control over a head unit of Japanese automotive through the dashboard's API.
- Popular vehicle GPS tracker gives hackers admin privileges.
- Three ransomware attacks were launched against a Tier-1 supplier.
- A new mobile app vulnerability was discovered, enabling man-in-the-middle attacks on EV OEMs.

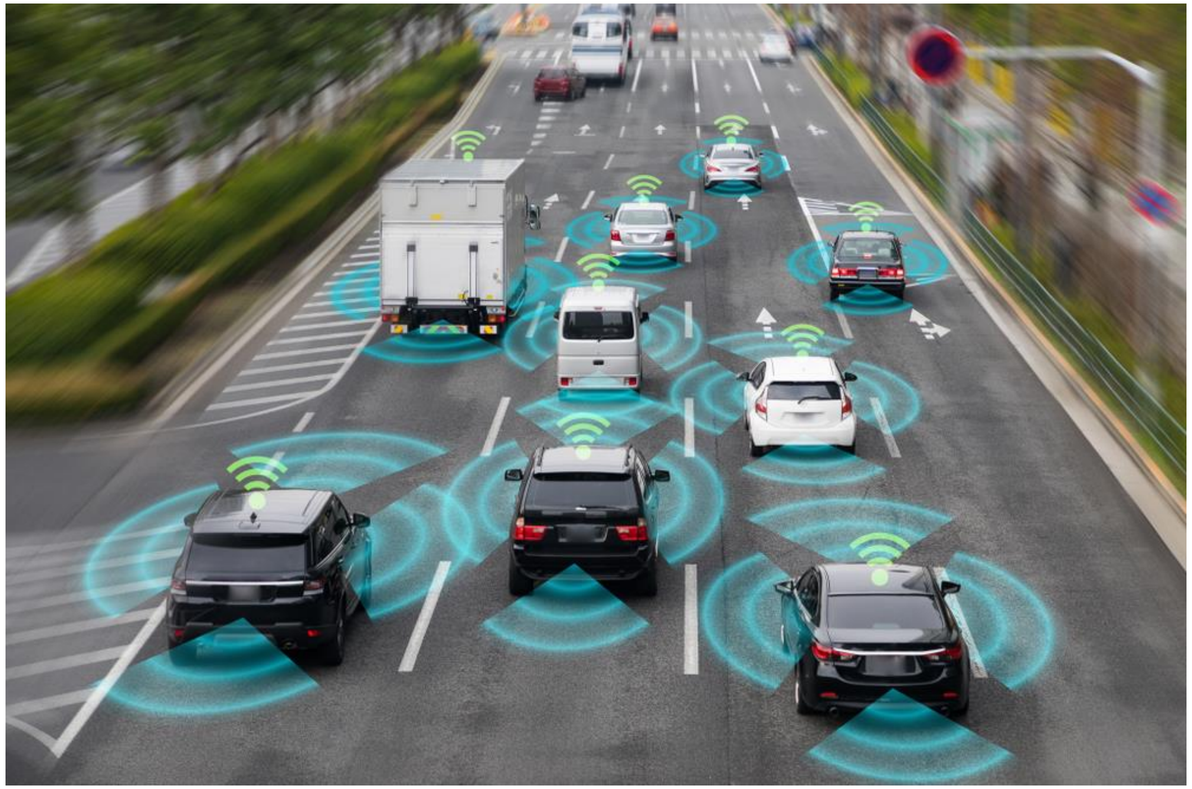
Q4:

- Italian OEM hit by ransomware attack.
- Japanese OEM customers affected by data breach in its mobile app
- Cyber attack shuts down Denmark's largest train company.
- Chinese EV OEM impacted by a data breach and ransomware demand of $2.25 million in Bitcoin.

How it started ...

Continental Engineering Services

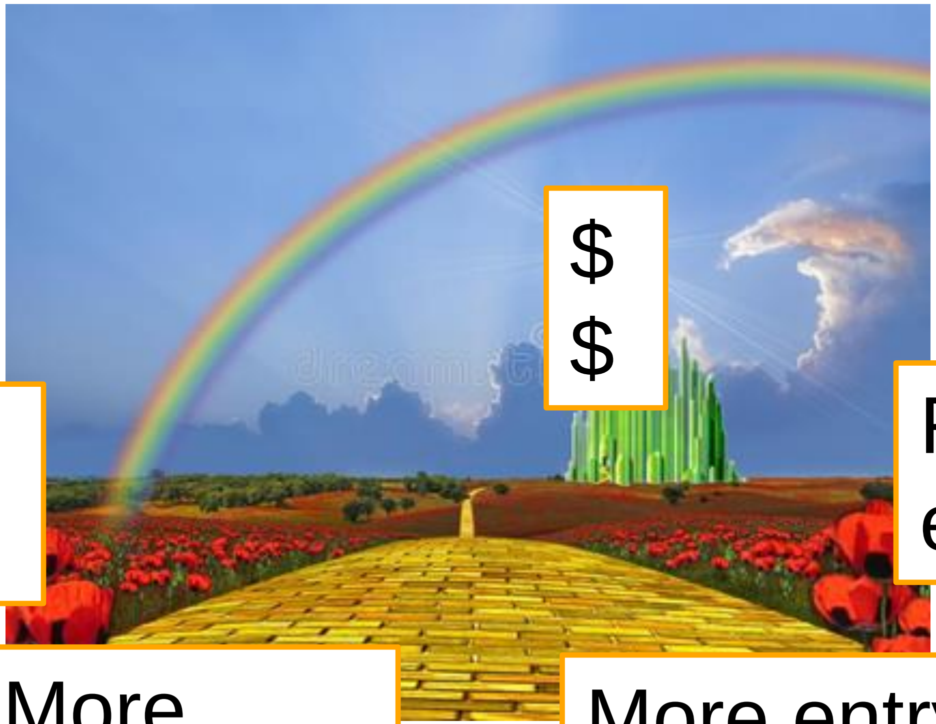
How it will be in the future ...



Automotive Connectivity

Continental Engineering Services

What do hackers see ?



Easier access

$ $

Remote exploits

More bugs

More entry points

Anything is possible

- We can make someone just **UNCOMFORTABLE**
- Or make them go **CRAZY**
- Or just make it **STOP**

- Video

Which type of attack do you know in the automotive area?

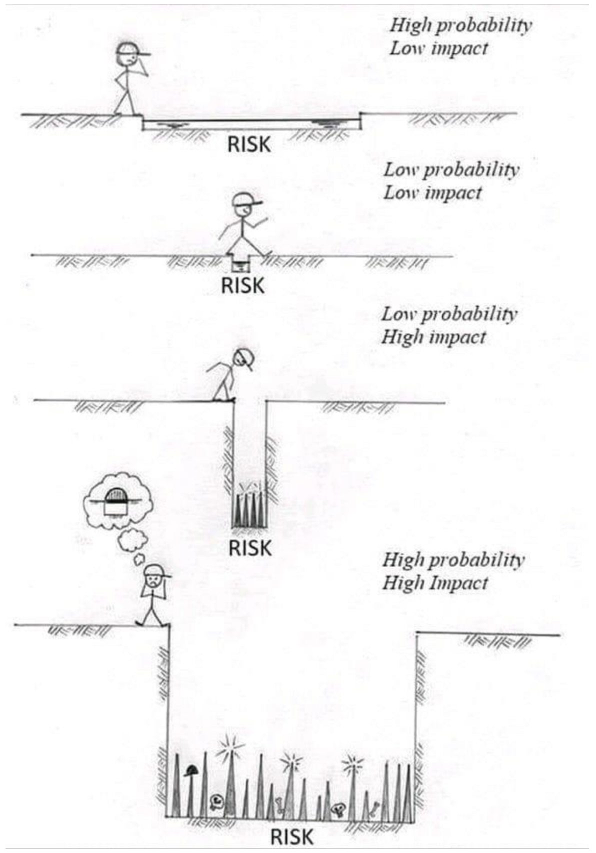
- Video

Standards, Regulations and Framework and

- ISO/SAE 21434
  - Guidance the best practice for automotive CS development
- UNECE R155
  - Threat categories
- AUTomotive Open System Architecture (AutoSAR)

ISO/SAE 21434

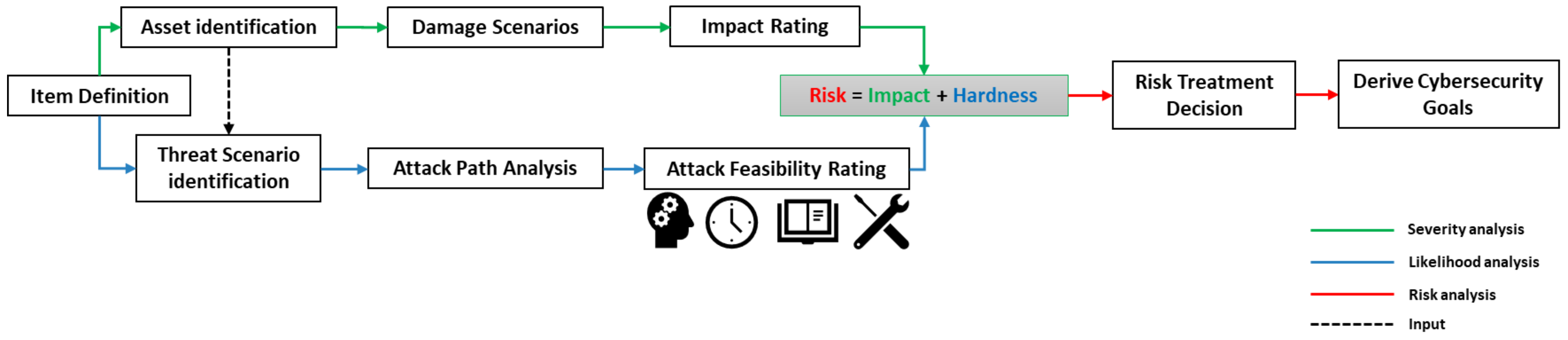
- Standard for automotive cybersecurity
- Security Development Lifecycle (SDL) process
- Threat Analysis and Risk Assessment (TARA) detailed

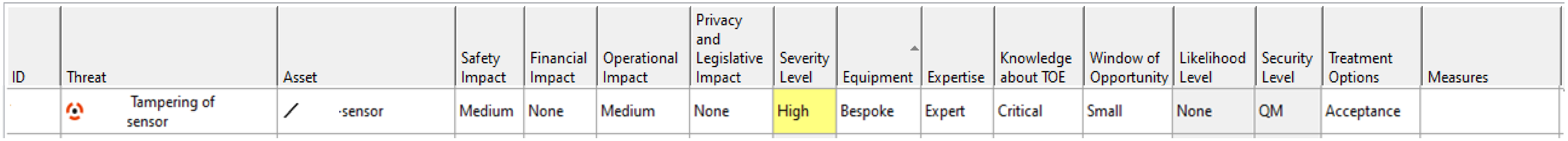


ISO/SAE 21434 - STRIDE

Threat	Desired property	Threat Definition
Spoofing	Authenticity	Pretending to be something or someone other than yourself
Tampering	Integrity	Modifying something on disk, network, memory, or elsewhere
Repudiation	Non-repudiability	Claiming that you didn't do something or were not responsible; can be honest or false
Information disclosure	Confidentiality	Providing information to someone not authorized to access it
Denial of service	Availability	Exhausting resources needed to provide service
Elevation of privilege	Authorization	Allowing someone to do something they are not authorized to do

ISO/SAE 21434 - TARA





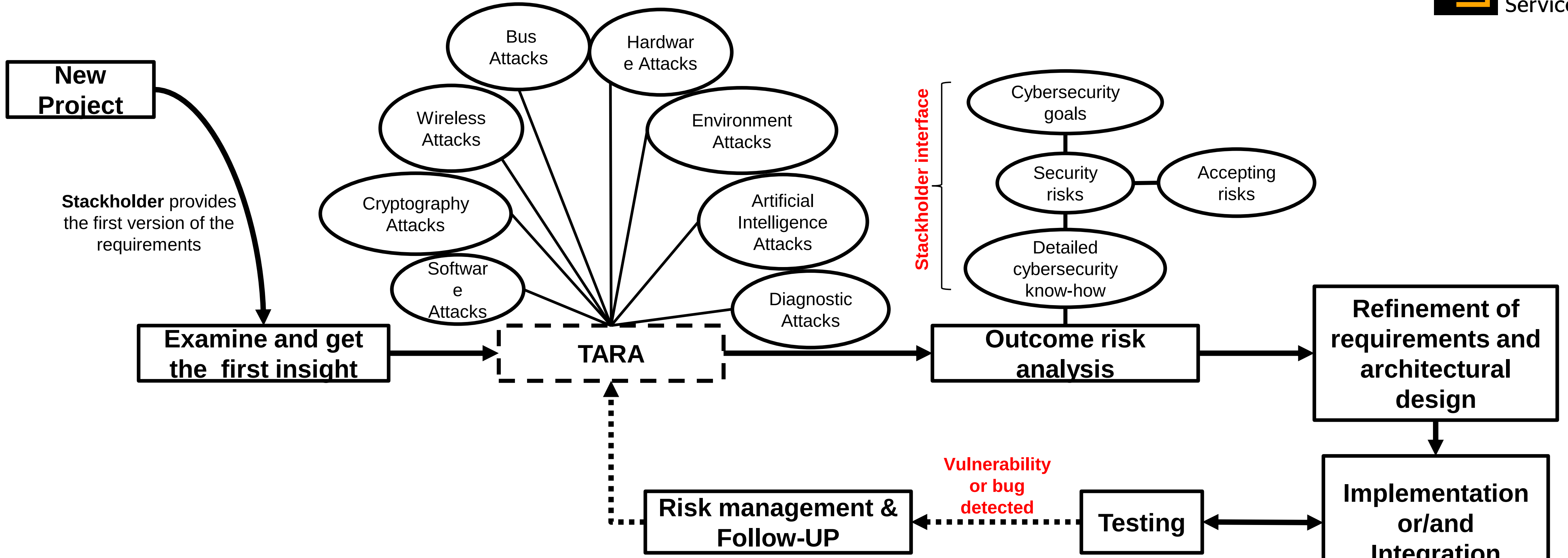
ID	Threat	Asset	Safety Impact	Financial Impact	Operational Impact	Privacy and Legislative Impact	Severity Level	Equipment	Expertise	Knowledge about TOE	Window of Opportunity	Likelihood Level	Security Level	Treatment Options	Measures
	Tampering of sensor	·sensor	Medium	None	Medium	None	High	Bespoke	Expert	Critical	Small	None	QM	Acceptance	

ISO/SAE 21434 – Security Goals

Requirements:

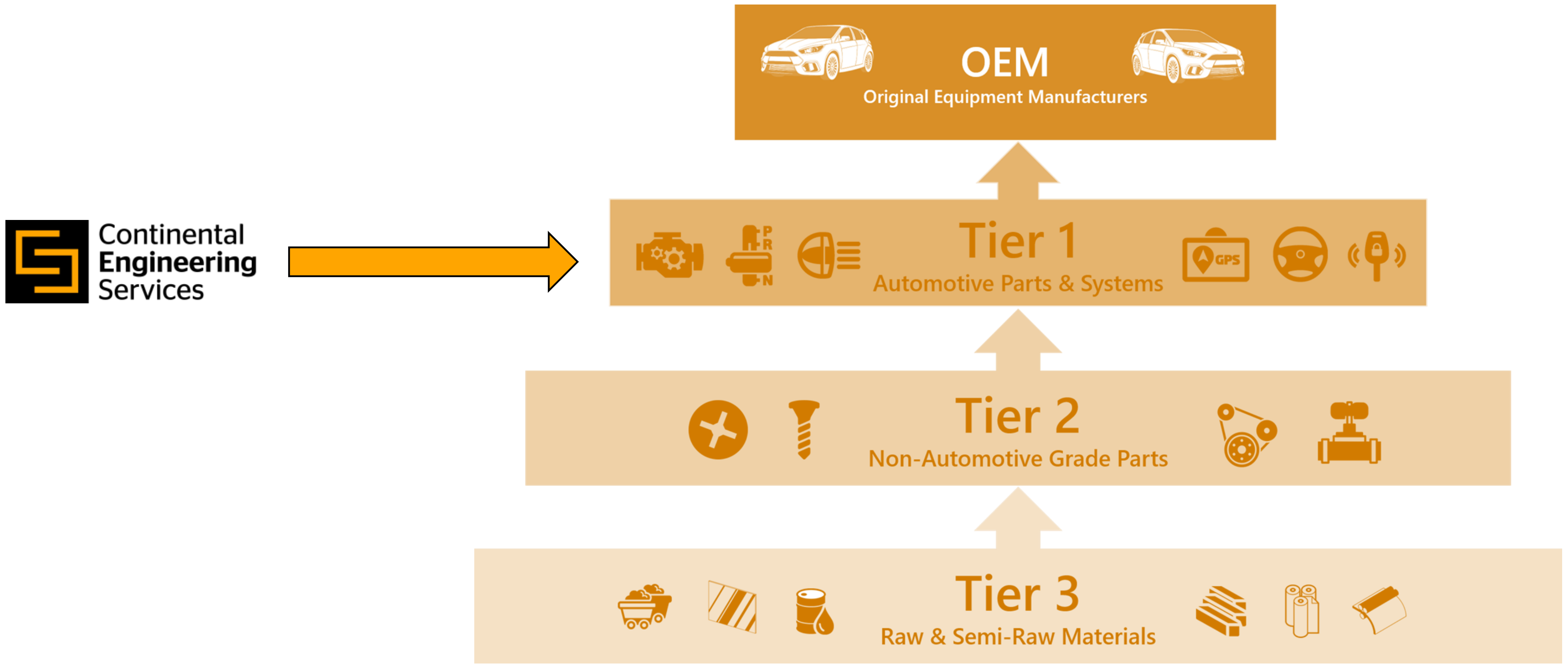
1. Secure Mileage
2. Secure ECU Modes
3. Secure Boot
4. Secure Flashing/Update
5. Secure Communication with other ECUs (Live Demo)
6. Secure Diagnostics
7. Secure Debug

…


New Project
Stackholder provides the first version of the requirements
Examine and get the first insight
Bus Attacks
Hardware Attacks
Wireless Attacks
Environment Attacks
Cryptography Attacks
Artificial Intelligence Attacks
Software Attacks
Diagnostic Attacks
TARA
Stackholder interface
Cybersecurity goals
Security risks
Accepting risks
Detailed cybersecurity know-how
Outcome risk analysis
Refinement of requirements and architectural design
Implementation or/and Integration
Testing
Vulnerability or bug detected
Risk management & Follow-UP

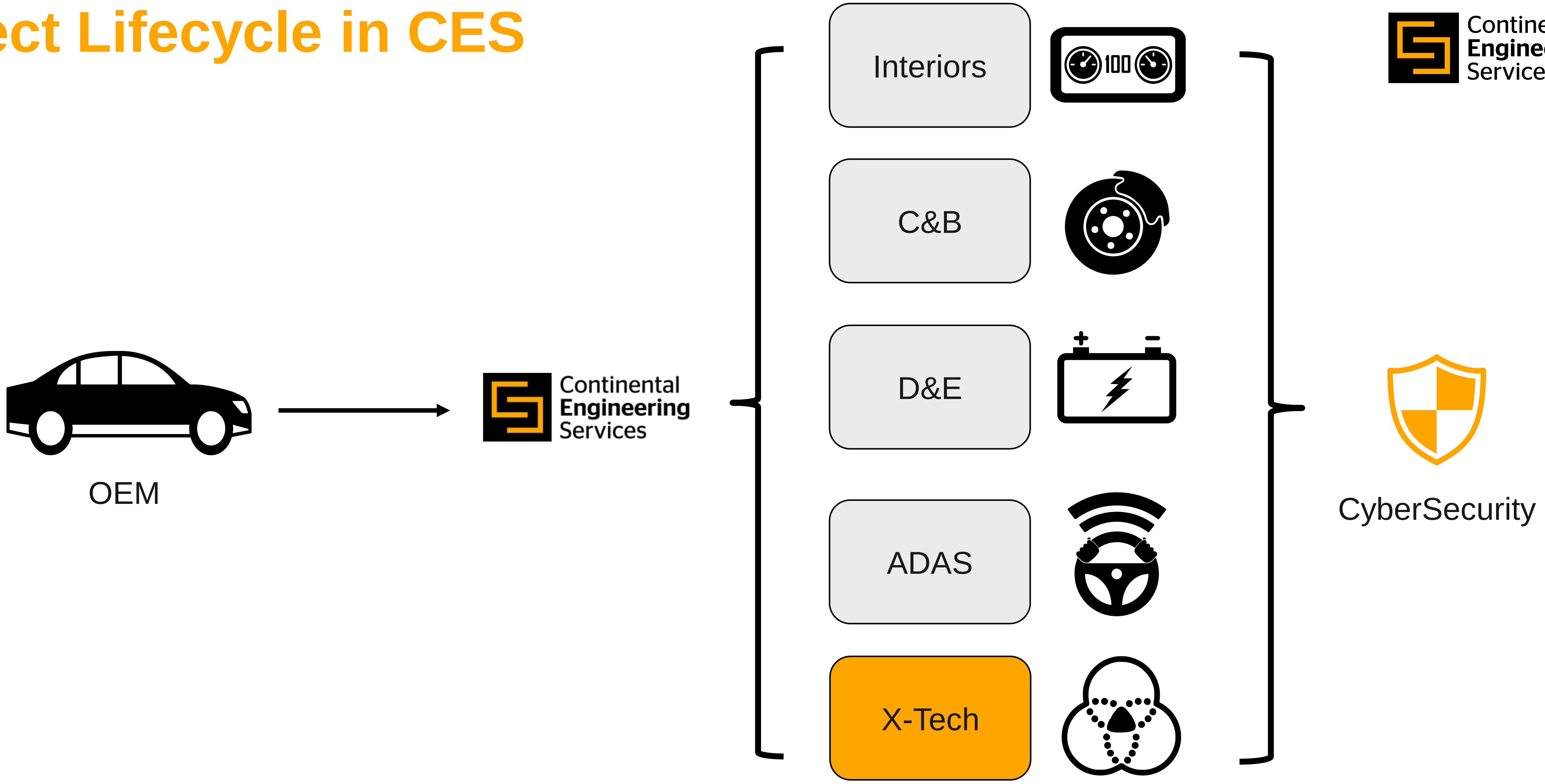
Cybersecurity in CES

Where is CES in the automotive industry supply chain?

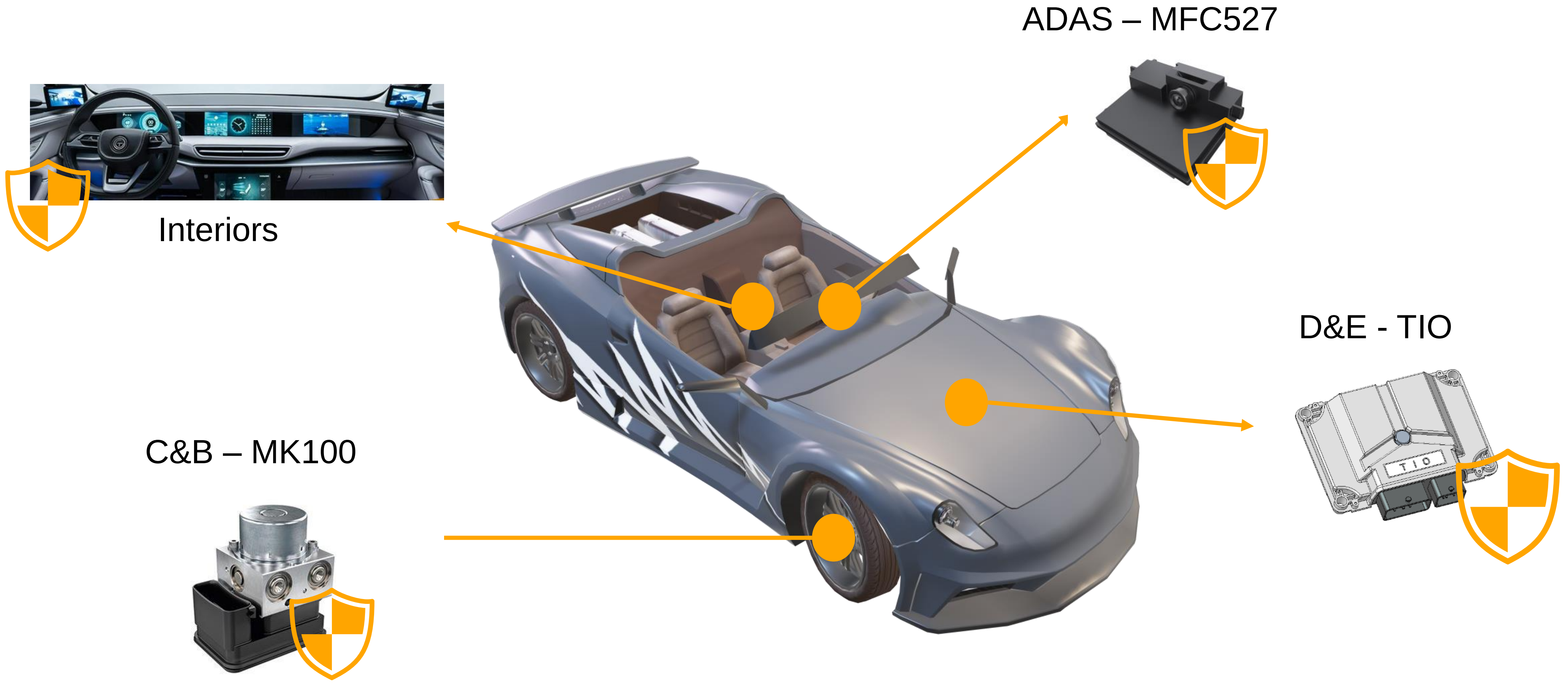

Continental Engineering Services
OEM
Original Equipment Manufacturers
Tier 1
Automotive Parts & Systems
Tier 2
Non-Automotive Grade Parts
Tier 3
Raw & Semi-Raw Materials

Source: “https://www.indx.com/”

Project Lifecycle in CES



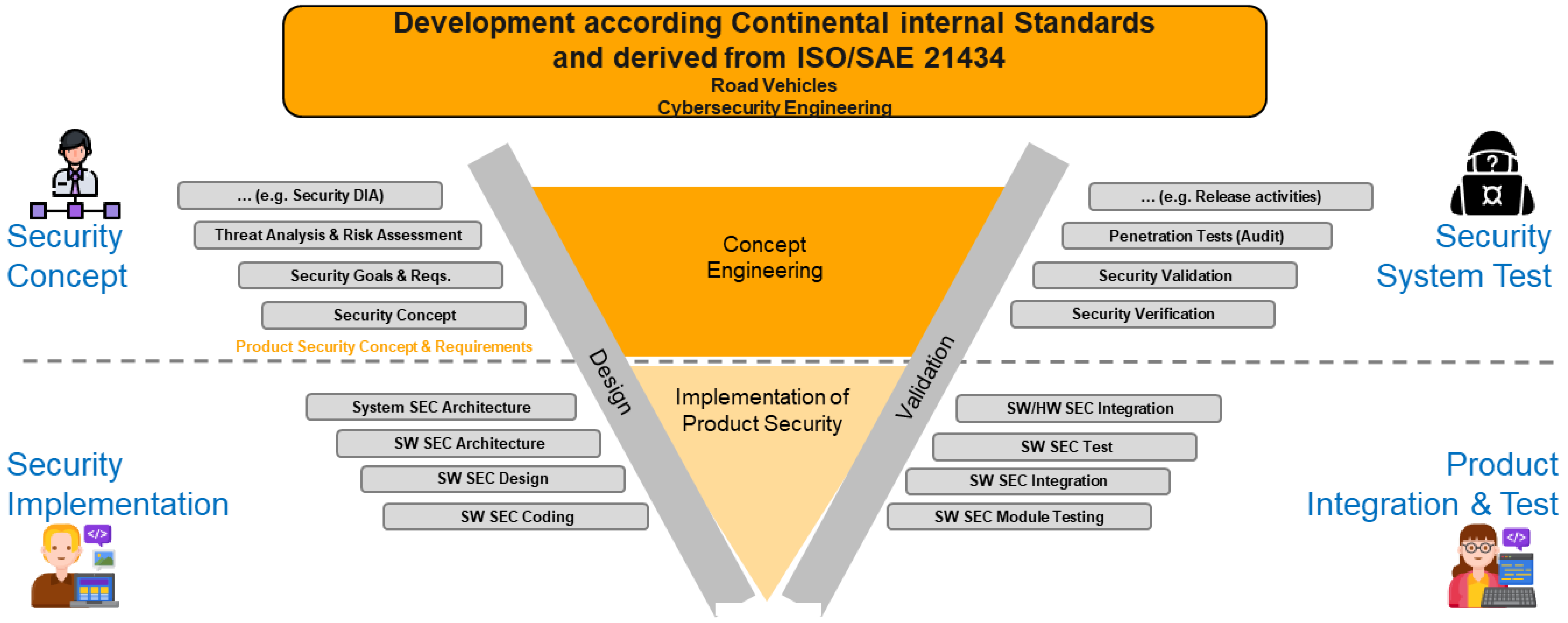
Cybersecurity is transversal to all segments



Automotive security in CES, why?

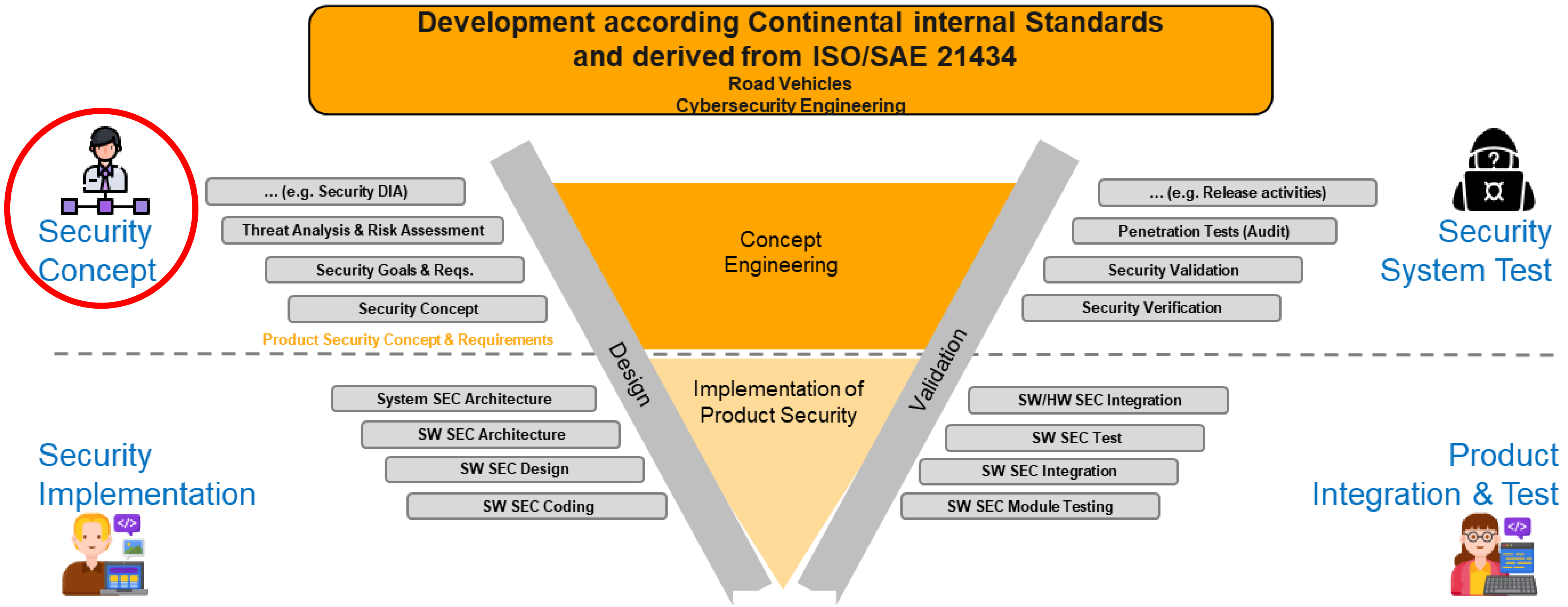
- Brands are focus on new features/functionality
- Lack of awareness, everyone always think their implementation is good
- These is a lack of people with experience/knowledge in security
- Few security standards and regulations for the automotive world

CES Environment

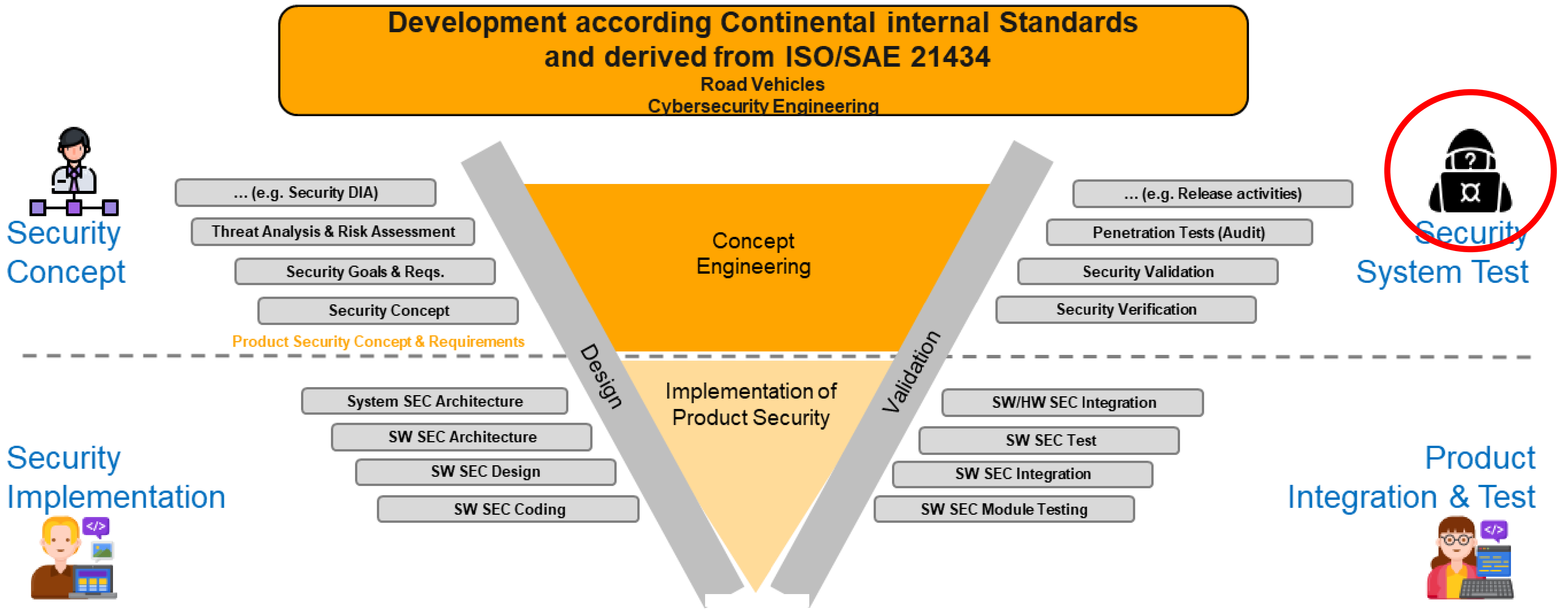


CES Environment

Continental Engineering Services



CES Environment

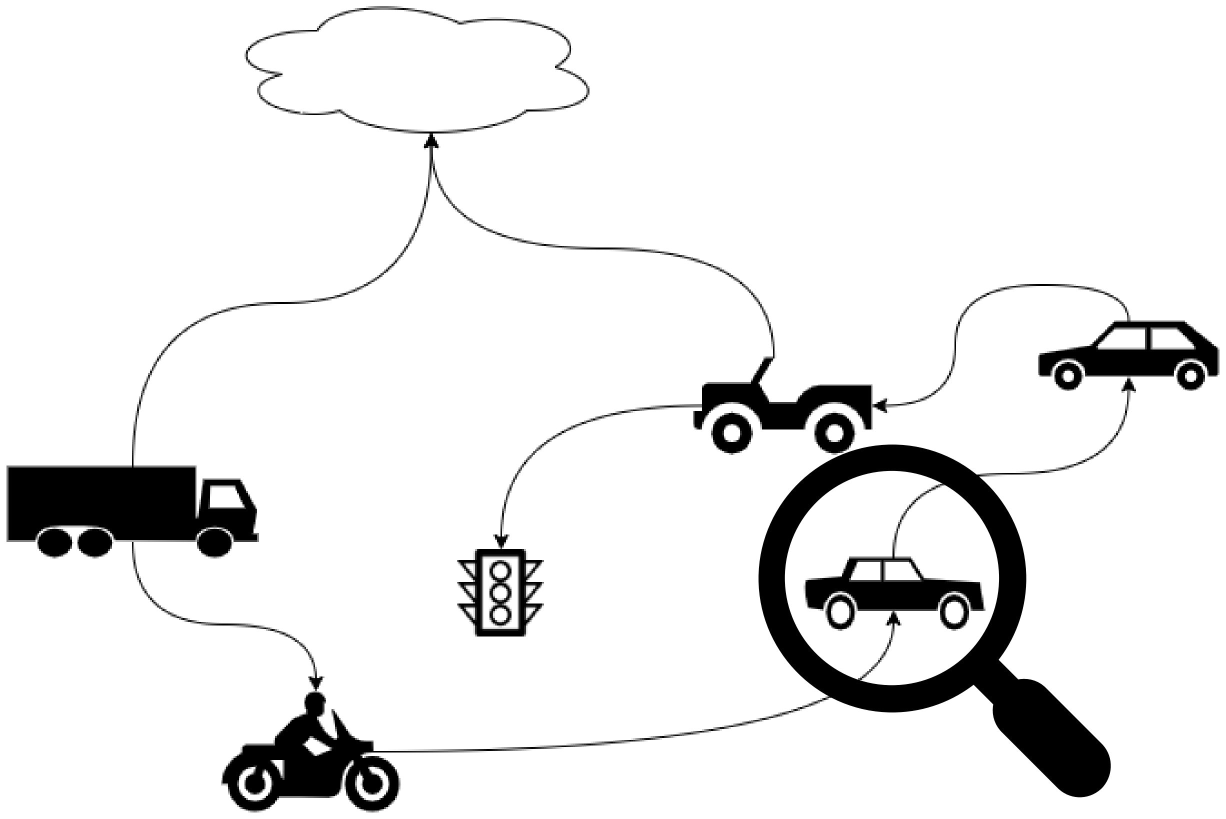


Project Security and Privacy manager (Security Concept)

- The key interface to the customer
- Studies the threats and defines strategies to reduce the risk (TARA)
- Plan and organize all the security-related topics of a project (e.g Technical Security Concept)
- Supports the developers and testers during the development of the projects

Let's get technical

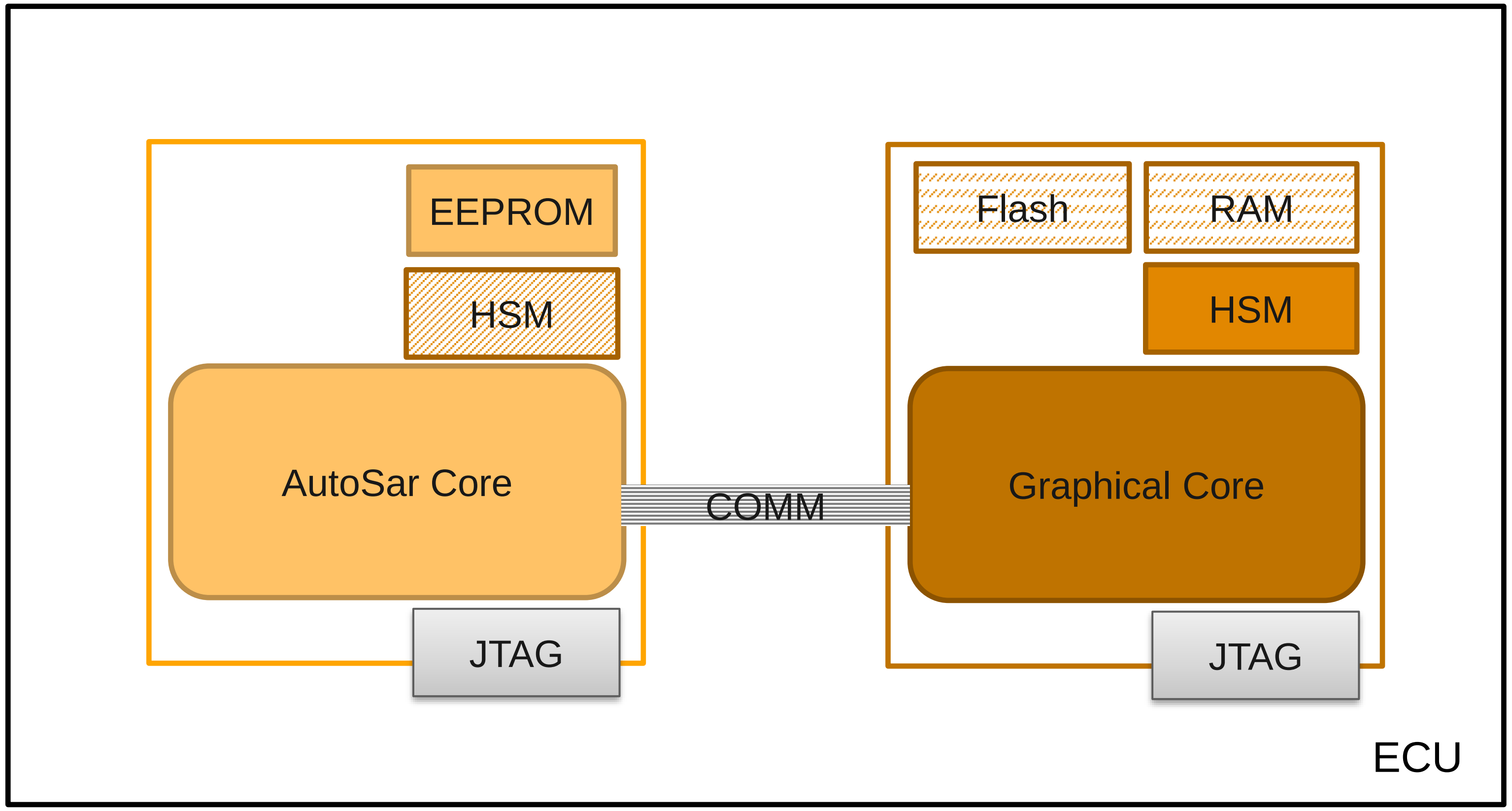
Where to start ?



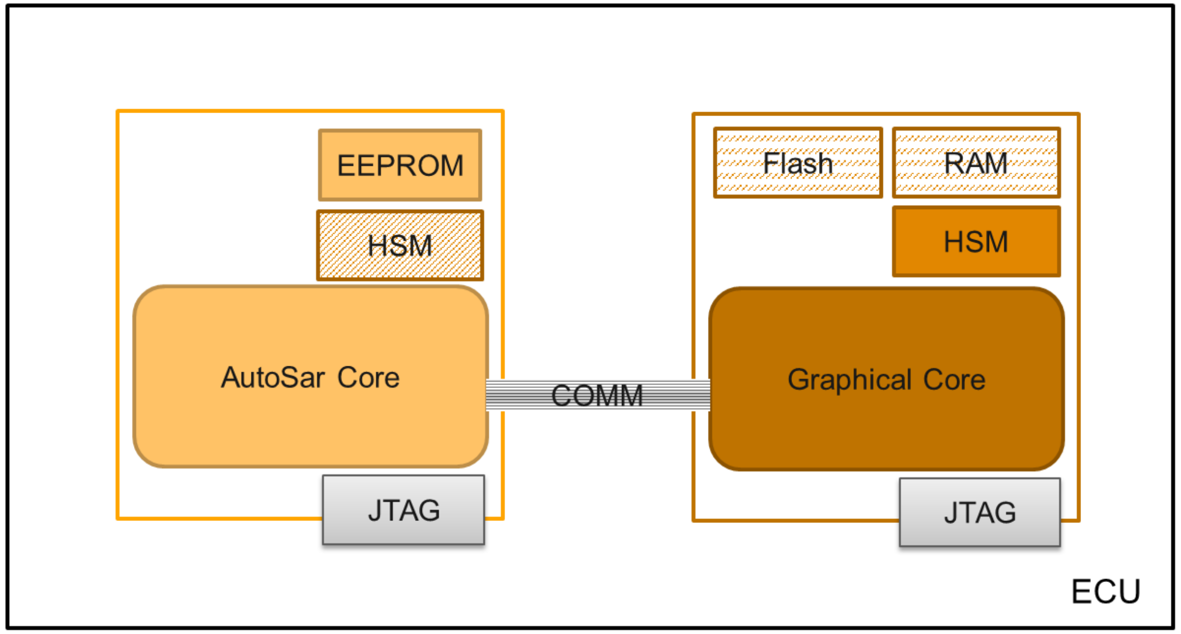
Where to start ?

How do we achieve security on ECU level?

Example - Electronic Control Unit (ECU)



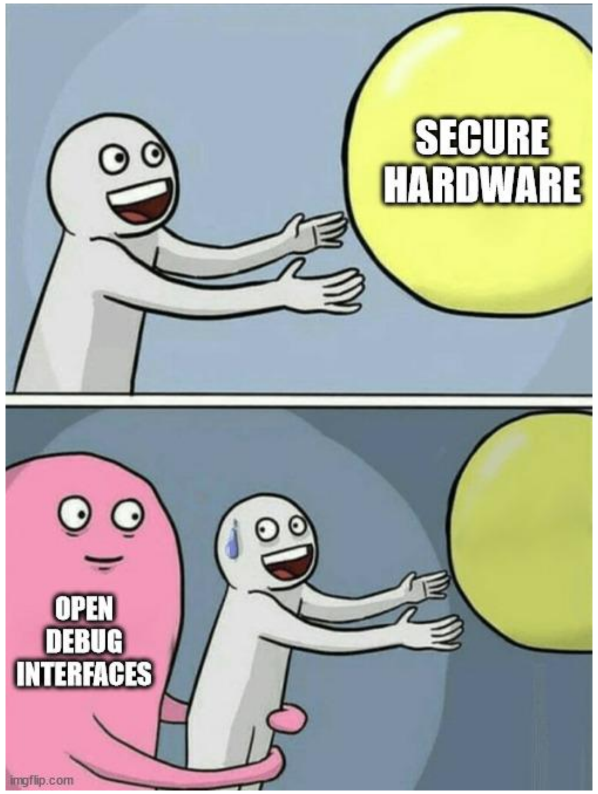
Example ECU



Requirements:

1. Secure Mileage
2. Secure ECU Modes
3. Secure Boot
4. Secure Flashing/Update
5. Secure Communication with other ECUs (Live Demo)

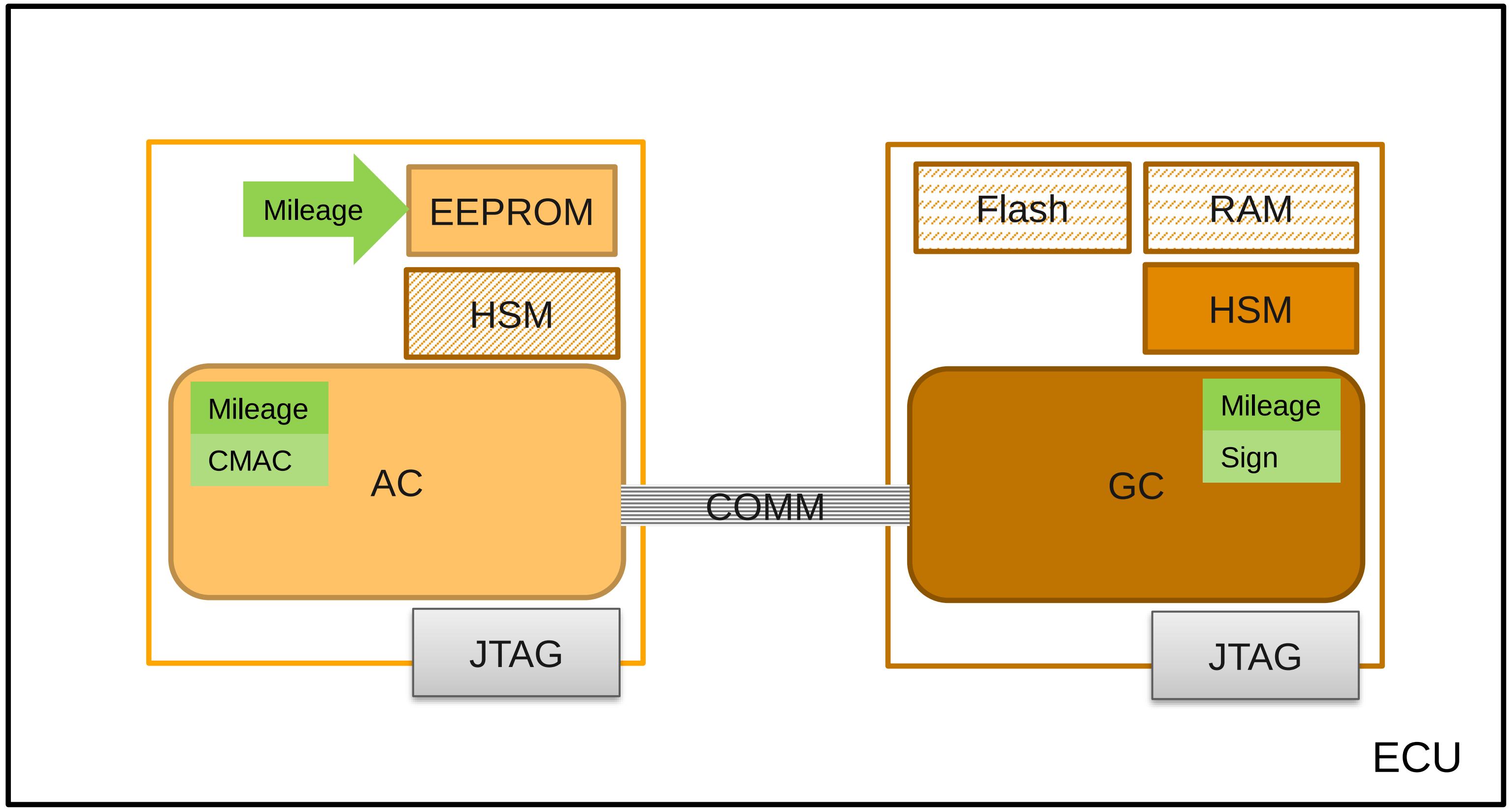
Even if the costumer does not request ...



ALWAYS CLOSE/DISABLE THE JTAG

Secure Mileage

Example ECU



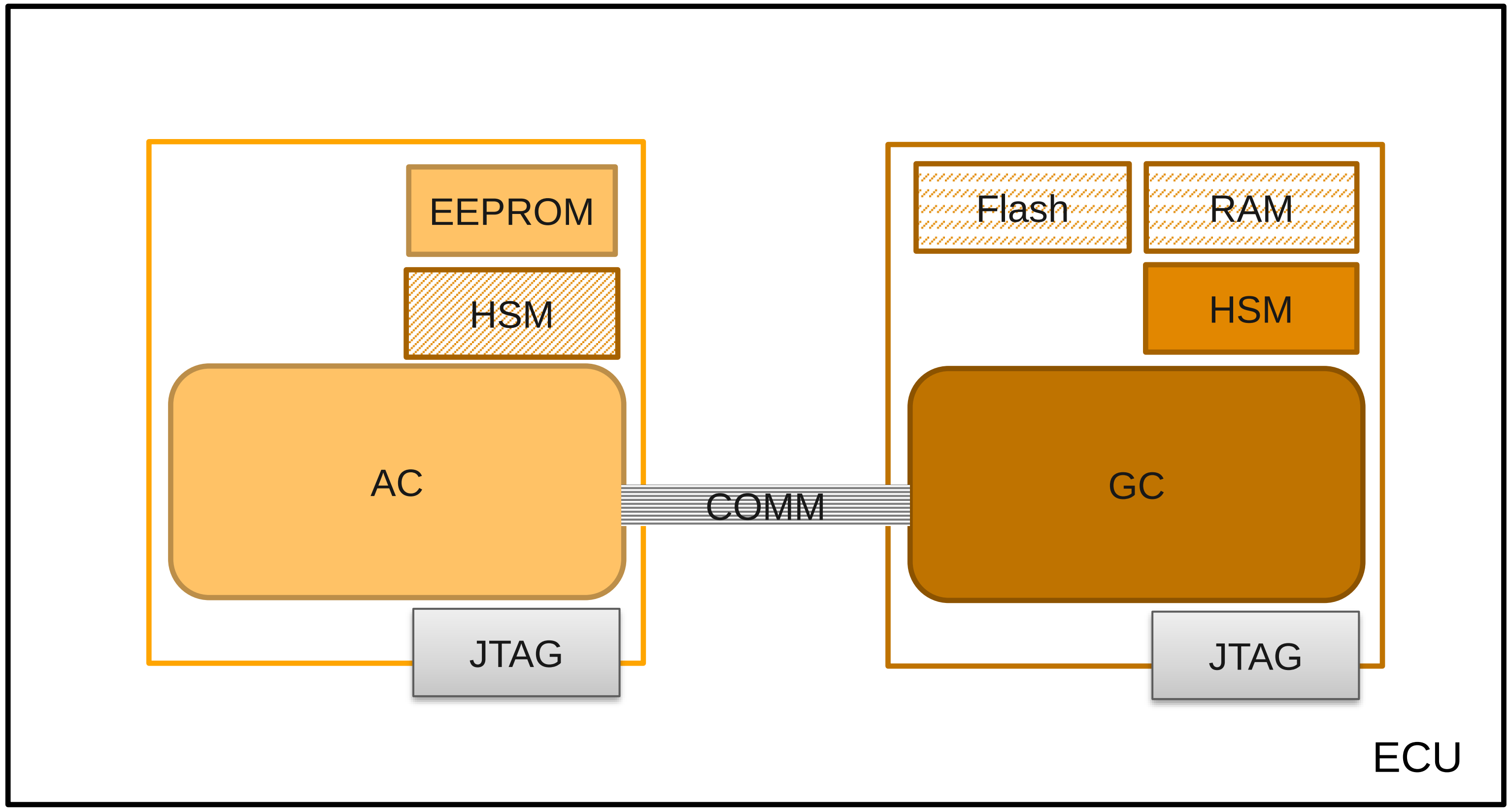
Mileage
EEPROM
HSM
Mileage
CMAC
AC
JTAG
COMM
Flash
RAM
HSM
Mileage
Sign
GC
JTAG
ECU

BLACK FRIDAY
~~457.000 km~~
176.000 km

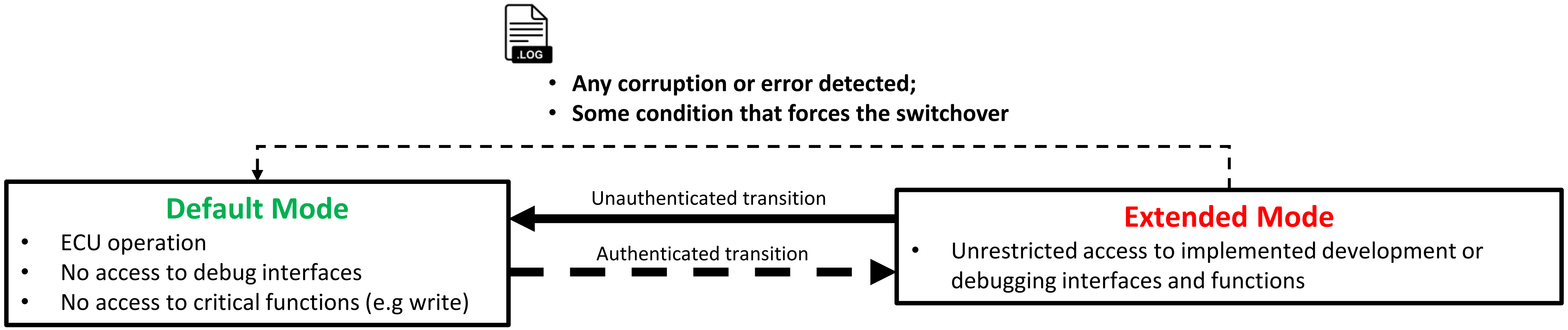
Continental Engineering Services

Secure ECU Mode

Example ECU



Dedicated Modes



- **Any corruption or error detected;**
- **Some condition that forces the switchover**

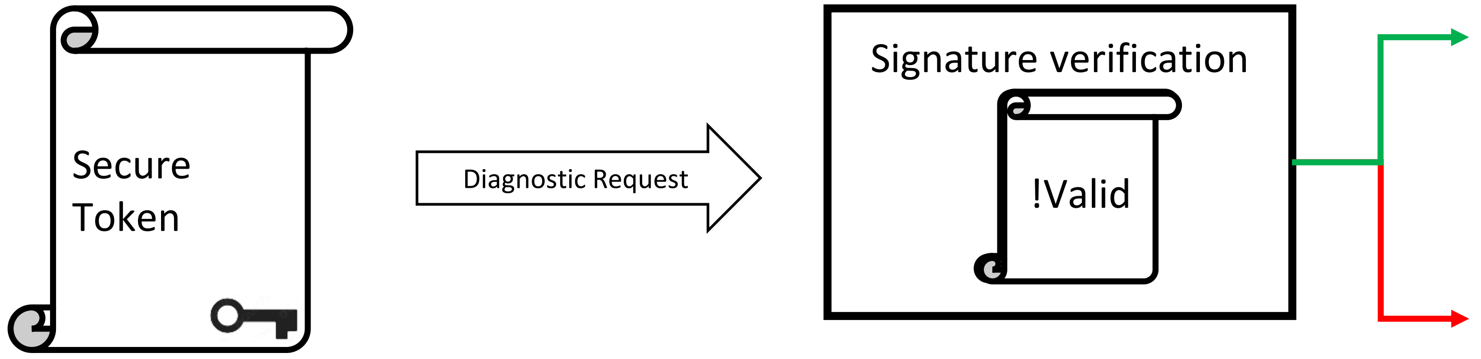
Default Mode

- ECU operation
- No access to debug interfaces
- No access to critical functions (e.g write)

Extended Mode

- Unrestricted access to implemented development or debugging interfaces and functions

Authenticated transition



- Switchover authorized
- The Extended Mode value will be stored in the EEPROM

- The ECU will continue in the Default mode
- The token will not be stored

Concerns

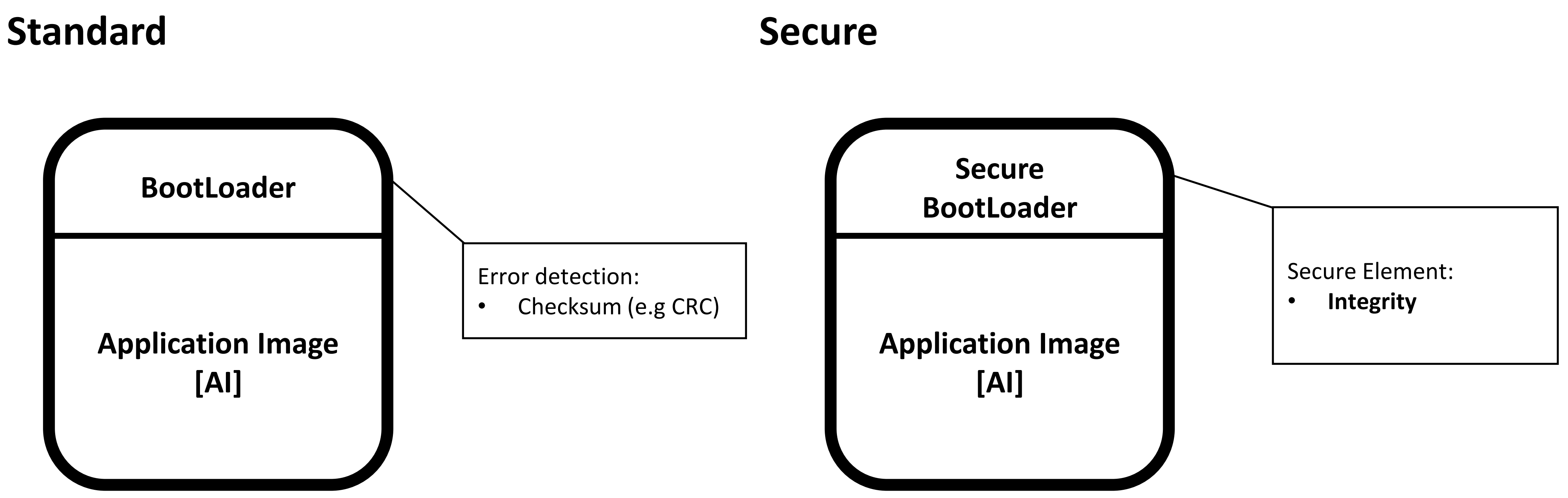
- **How do we ensure an attacker cannot exchange the key on the ECU by its own?**
  - The keys are part of a certificate chain integrated into the Software

- **How do we protect against replay attacks?**
  - Each token signed has a timestamp, which is then compared. Only if the timestamp is newer than the one stored, the token is accepted

- **How do we reduce the exposure of the key used?**
  - We do not directly sign with the certificates in the SW, we use an intermediate one that is sent with the token

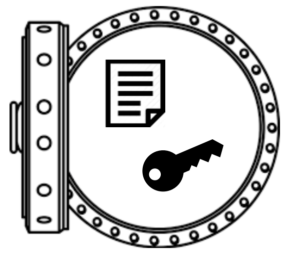
Secure Boot

Secure boot

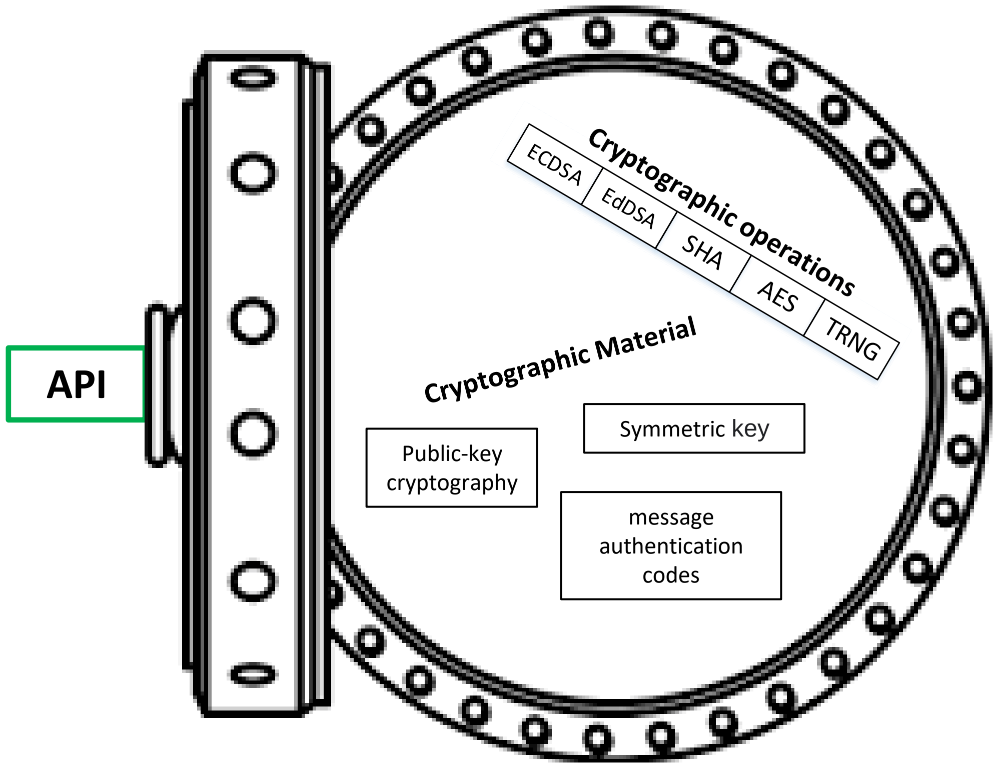

Standard
BootLoader
Application Image [AI]
Error detection:
• Checksum (e.g CRC)
Secure
Secure BootLoader
Application Image [AI]
Secure Element:
• Integrity

Secure element

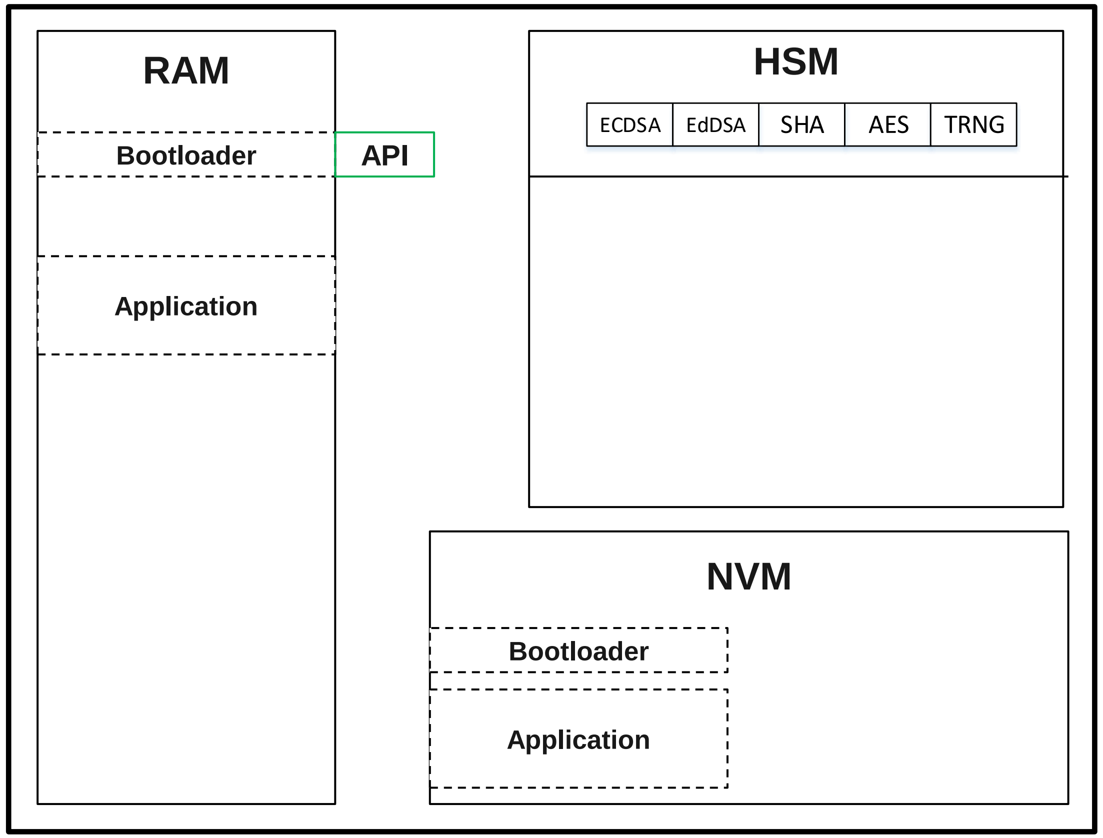
- **Integrity**
  - One-way function (e.g SHA) or Symmetric Key Cryptography (e.g AES-CMAC)
  - The secret (e.g key) is stored in a trustable physical computing device (e.g HSM)



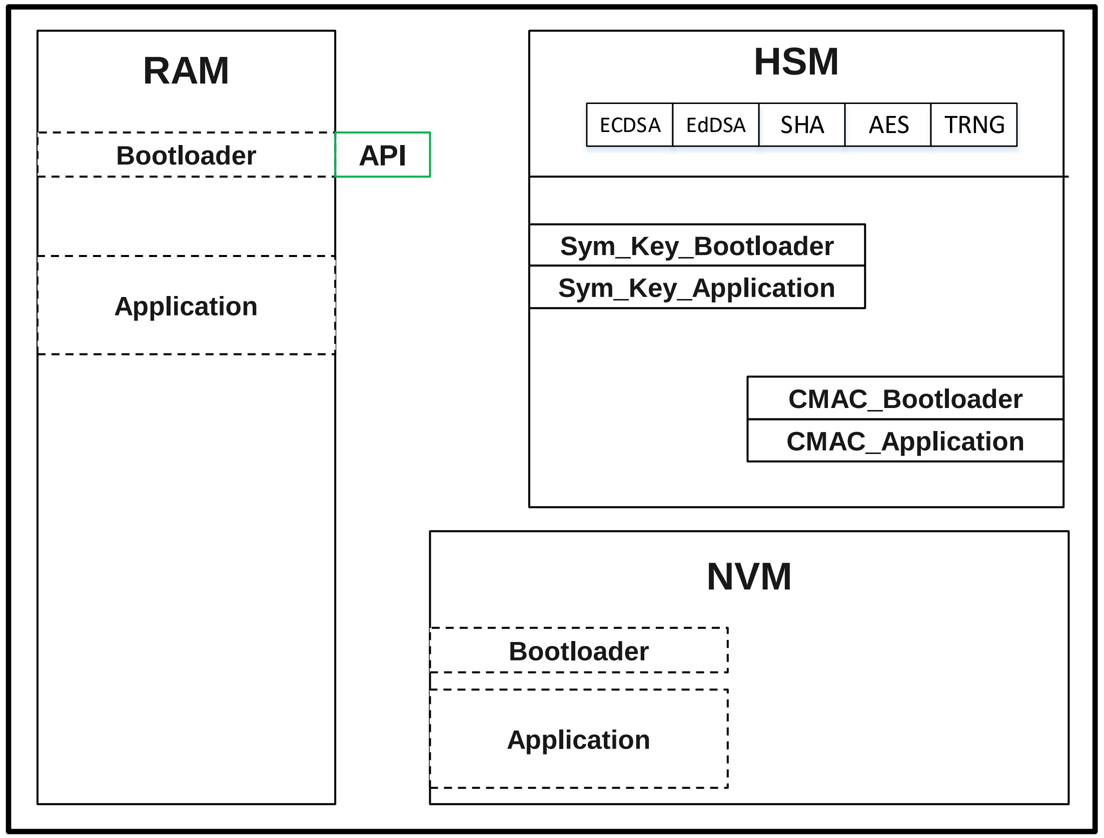
Handle secure elements



Secure Boot

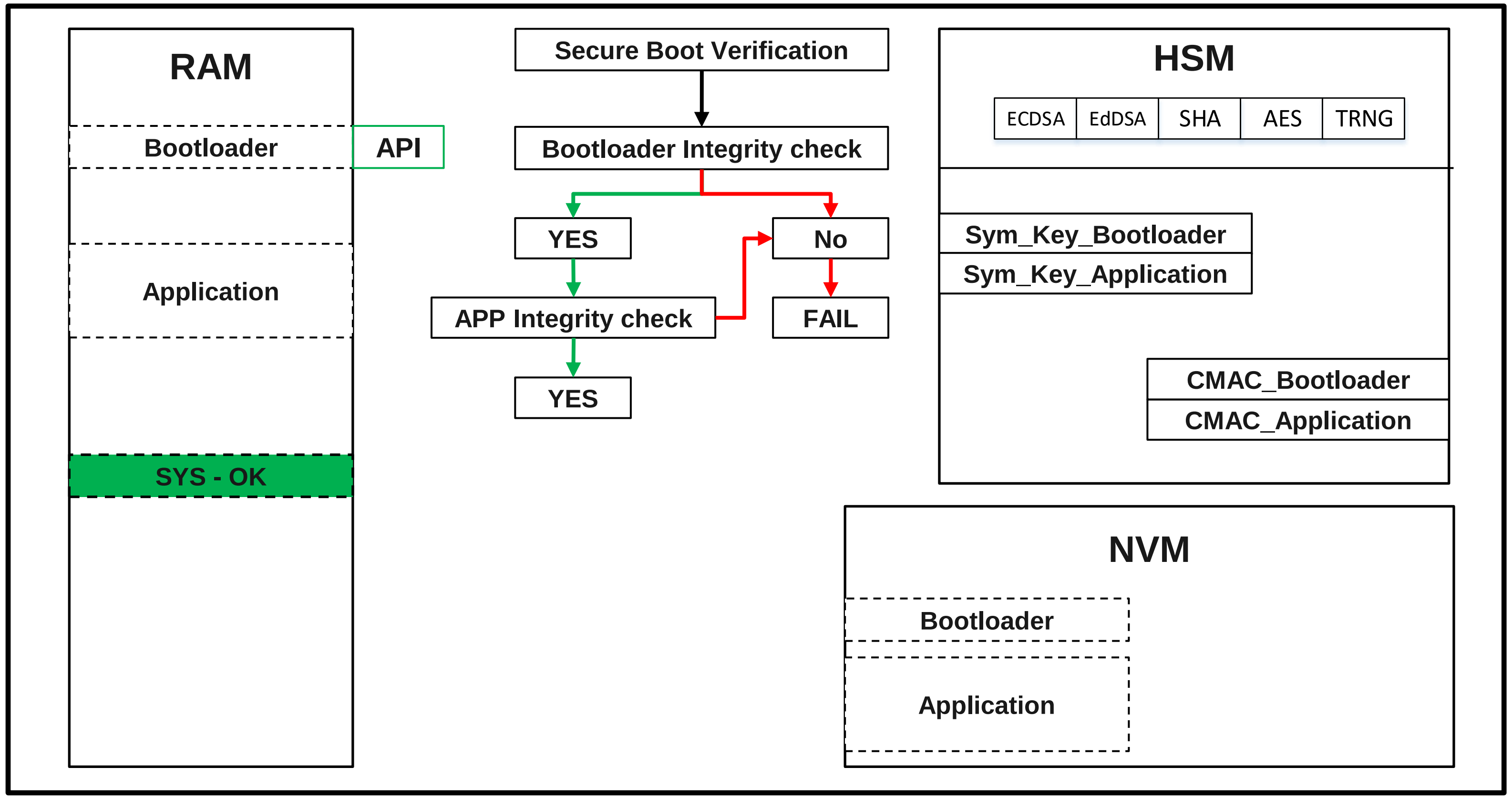

RAM
Bootloader
API
Application
HSM
ECDSA
EdDSA
SHA
AES
TRNG
NVM
Bootloader
Application

Secure Boot



1. Production environment is considered secure and trustable
2. Request the Gen of Sym keys for secure boot (API Call)
3. Trigger the Secure Boot procedure to start (API Call)
4. The Secure Boot procedure shall generate 2 CMAC's (e.g CBC-MAC)

Secure Boot


RAM
Bootloader
API
Application
SYS - OK
Secure Boot Verification
Bootloader Integrity check
YES
No
APP Integrity check
FAIL
YES
HSM
ECDSA
EdDSA
SHA
AES
TRNG
Sym_Key_Bootloader
Sym_Key_Application
CMAC_Bootloader
CMAC_Application
NVM
Bootloader
Application

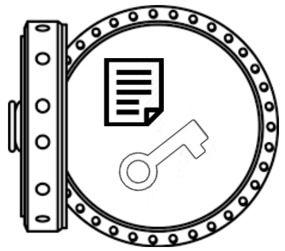
Secure boot challenges

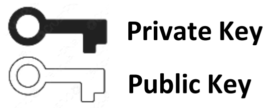
- **What problems are introduced in development due to secure boot ?**
  - Developers can not flash locally built software
- **Why not simply bypass secure boot altogether during development ?**
  - Because it will never be tested
  - Possible impact with other applications will go unnoticed

Secure Flashing/Update

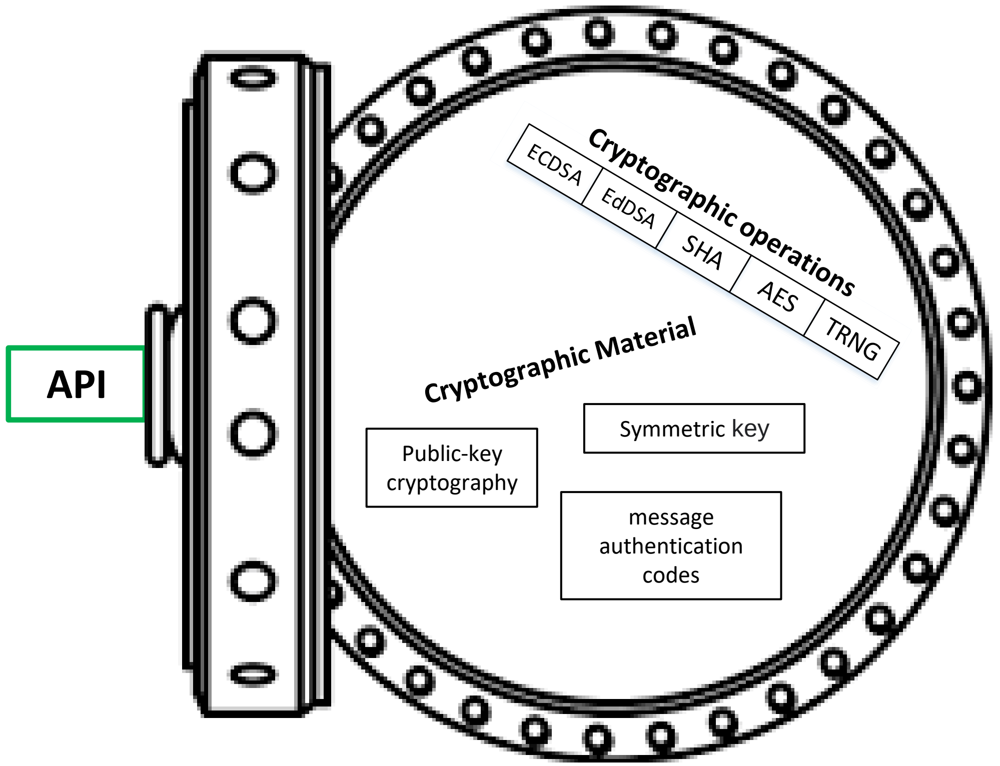
Secure element

- **Integrity**
  - One-way function (e.g SHA) or Symmetric Key Cryptography (e.g AES-CMAC)
  - The secret (e.g public key) is stored in a trustable physical computing device (e.g HSM)
- **Non-repudiation**
  - Digital signatures (e.g ECDSA) offers non-repudiation when it comes to binary exchange





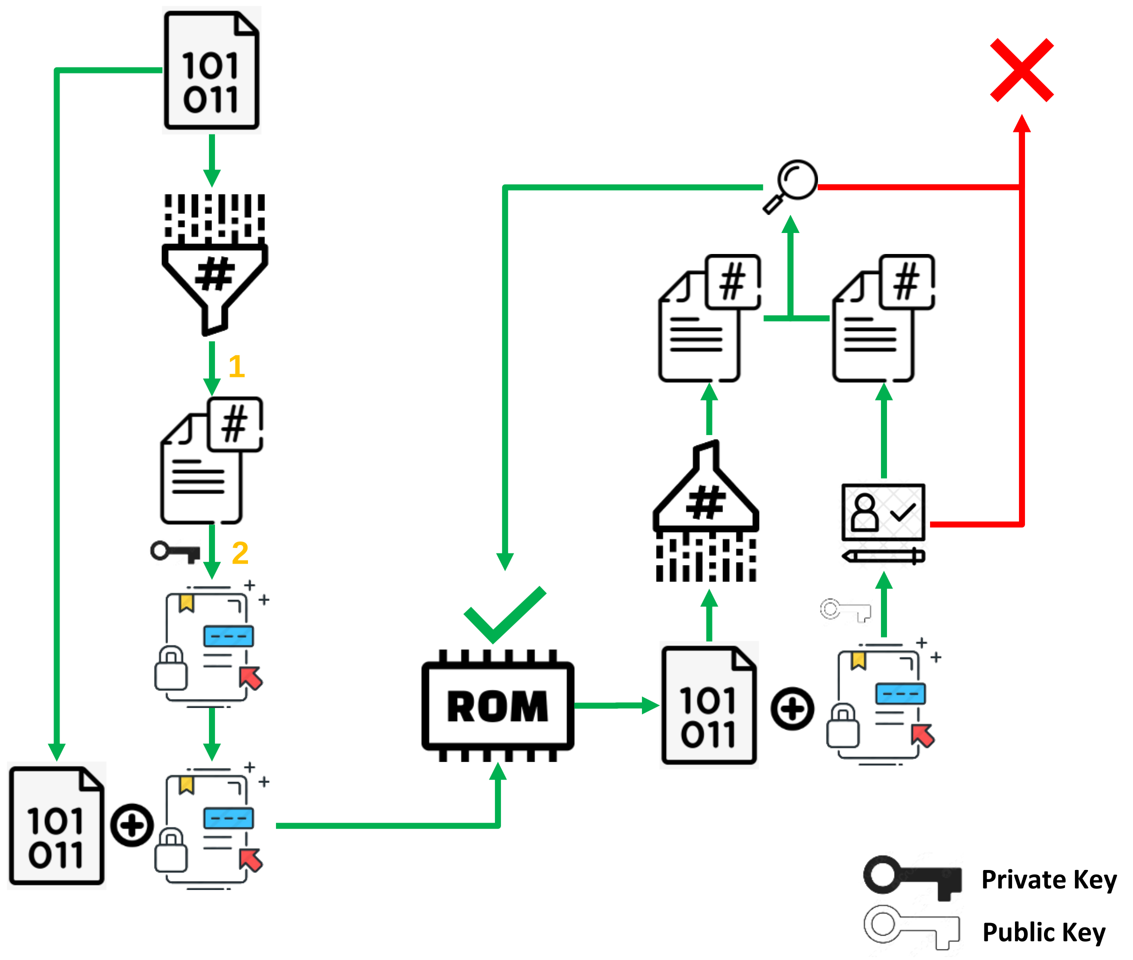
Handle secure elements



Secure Flashing/Update

The secure flashing will try to ensure that only trustable and reliable Software is flashed into memory

1. A **hash** of the binary is generated
2. The **digested binary** requires to be **signed**
3. The **original binary** and the resulting **signed** hash of the binary are sent out to **memory**
4. The received data will be **parser** and a **reverse process** validates the data



Secure flashing/updates challenges

- **What problems are introduced in development due to secure flashing/update ?**
  - Developers depend normally on an external source to get the necessary ingredients to be able to flash a new software version
- **Why not simply bypass secure flashing/update procedure during development ?**
  - Because it will never be tested

Continental Engineering Services

Questions?

Continental Engineering Services

Live demo

Continental Engineering Services

Questions?