HEADSTART Week:

Cybersecurity Validation In Automated Driving

Joaquim Maria Castella Triginer

Virtual Vehicle Research, Graz

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 824309.

Agenda

- ✓ Introduction of cybersecurity role in the HEADSTART project
- ✓ Presentation of the cybersecurity particularities and integration in HEADSTART method
- ✓ Cybersecurity coverage and integration in HEADSTART procedure
- ✓ Next steps, use cases and testing tool for HEADSTART validation
- ✓ Open questions

Introduction of cybersecurity

Safe Connected and Automated Driving (CAD) will require functionality:

- At vehicle level: The functionalities of the ego vehicle.
- At system level: Other vehicles, users and systems (User equipment)

Solving this will require certain Key Enabling Technologies (KETs). Three KETs were listed during the application phase:

- V2X communication
- Positioning
- **Cybersecurity**

Introduction of cybersecurity

Cybersecurity is the practice of protecting electronic systems, computers, mobile devices, networks and data from malicious attacks.

That includes technology aimed at reducing the impact of cyber risks by:

- Preventing security attacks
- Mitigating security attacks
- Detecting security attacks

Connected automated driving vehicles perspective:

- Cybersecurity is considered in this case a key technology as safety of the vehicle cannot be guaranteed without cybersecurity. However, cybersecurity needs a special treatment to be integrated into the safety assessment.

Introduction of cybersecurity

Cyber-security

7 entries

V2X communication:

- ETSI ITS-G5
  - Message signatures,
  - PKI for certificate management
- Cellular communication:
  - MQTT/AMQP with TLS

In-vehicle Security:

- Secure Boot and Updates,
- Authenticated messages

} Standard missing

Introduction of cybersecurity

Standards (automotive related):

- SAE J3061
- ISO 21434

General standards:

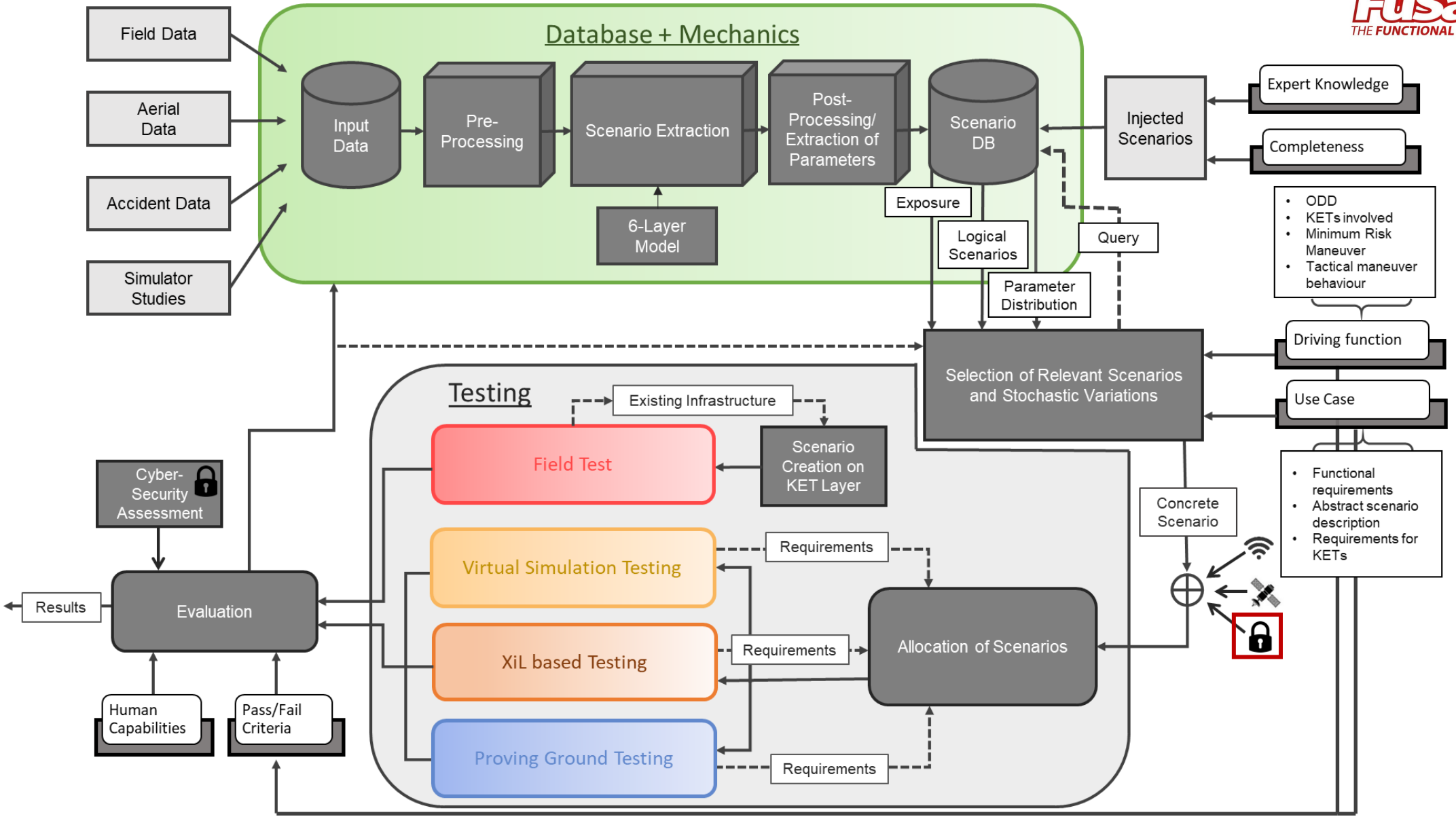
- ISO 27000-series
- NIST Cybersecurity Framework
- ISO 15408
- …

Other references:

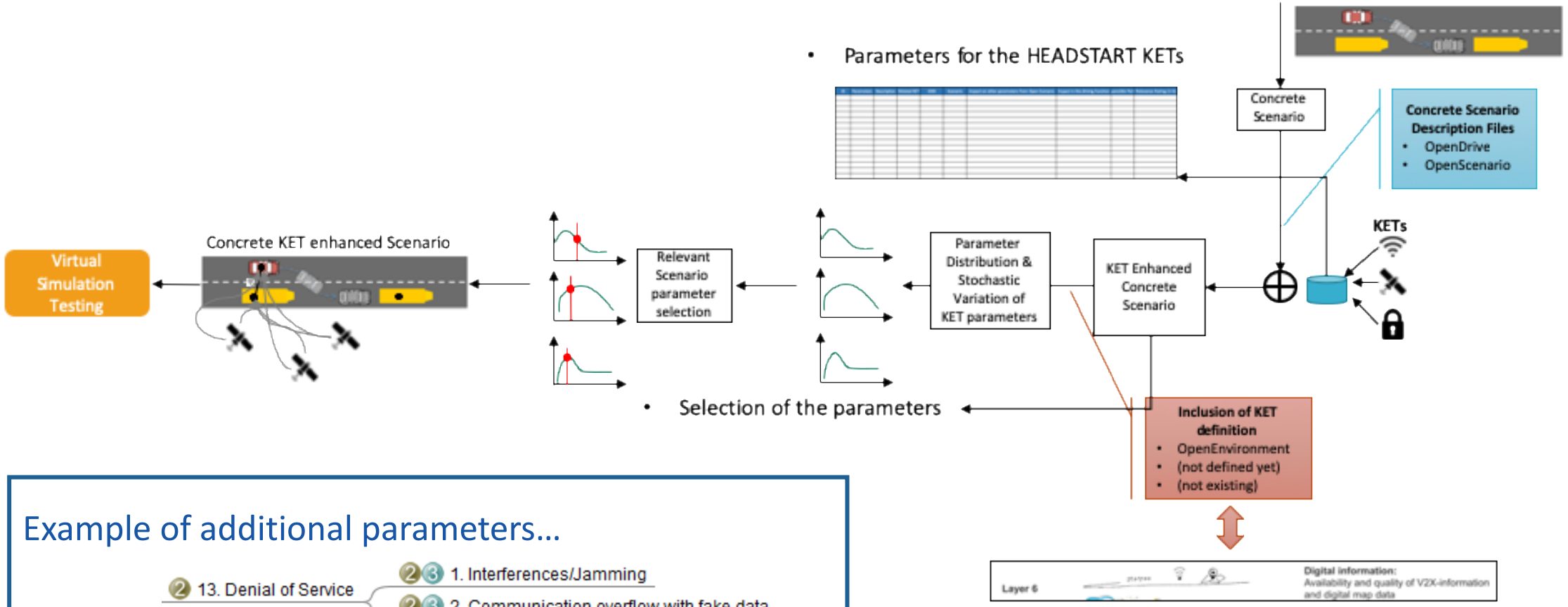
- IEEE1609.2
- ETSI
- NHTSA
- ENISA
- …

https://argus-sec.com/iso-sae-21434/

Methodology



Cybersecurity in the methodology



Example of additional parameters…

- 13. Denial of Service
  - 1. Interferences/Jamming
  - 2. Communication overflow with fake data

Cybersecurity in the methodology

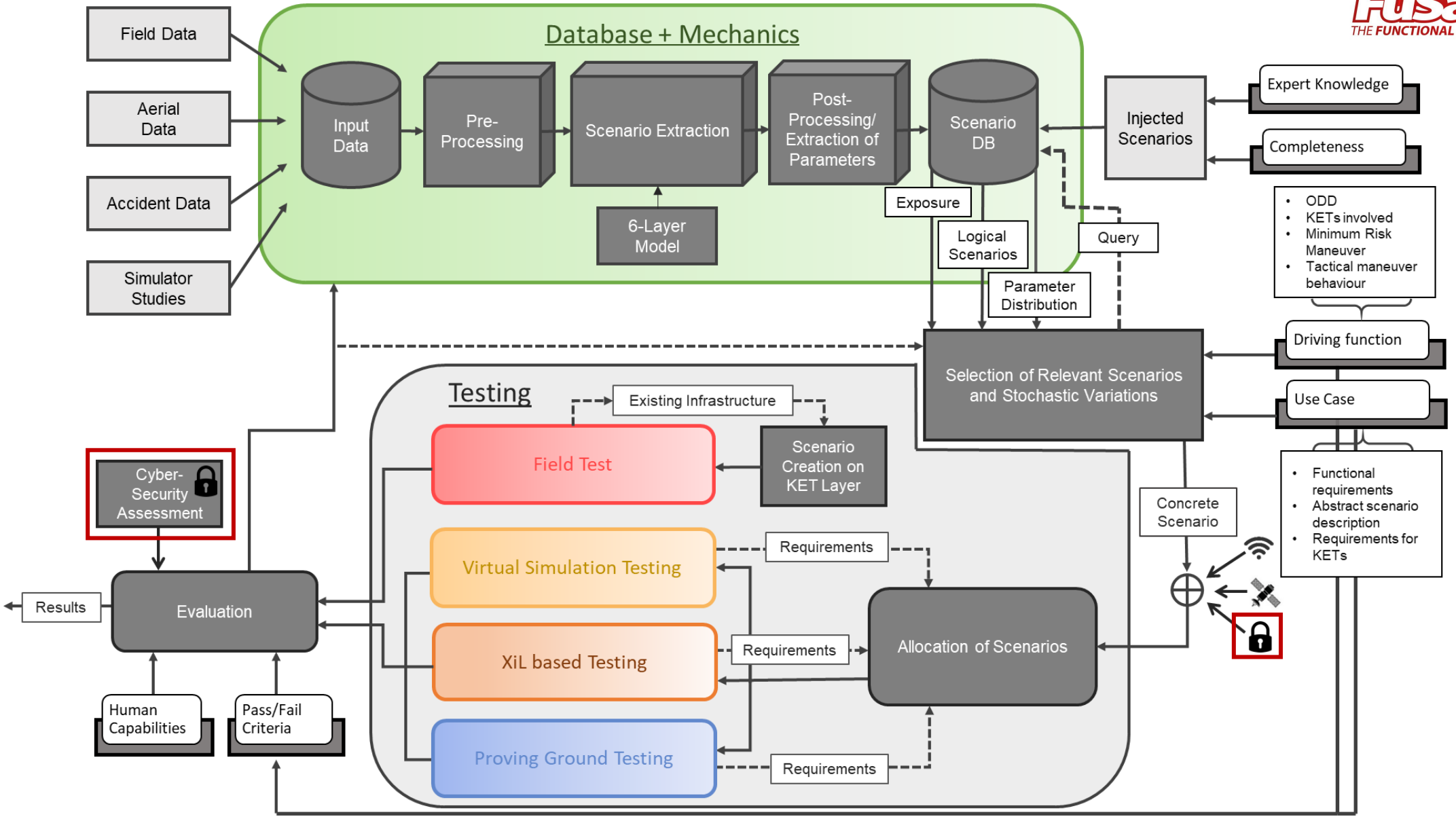
Question… Is the cybersecurity KET covered by the current methodology?

How can cybersecurity be covered?

We need…

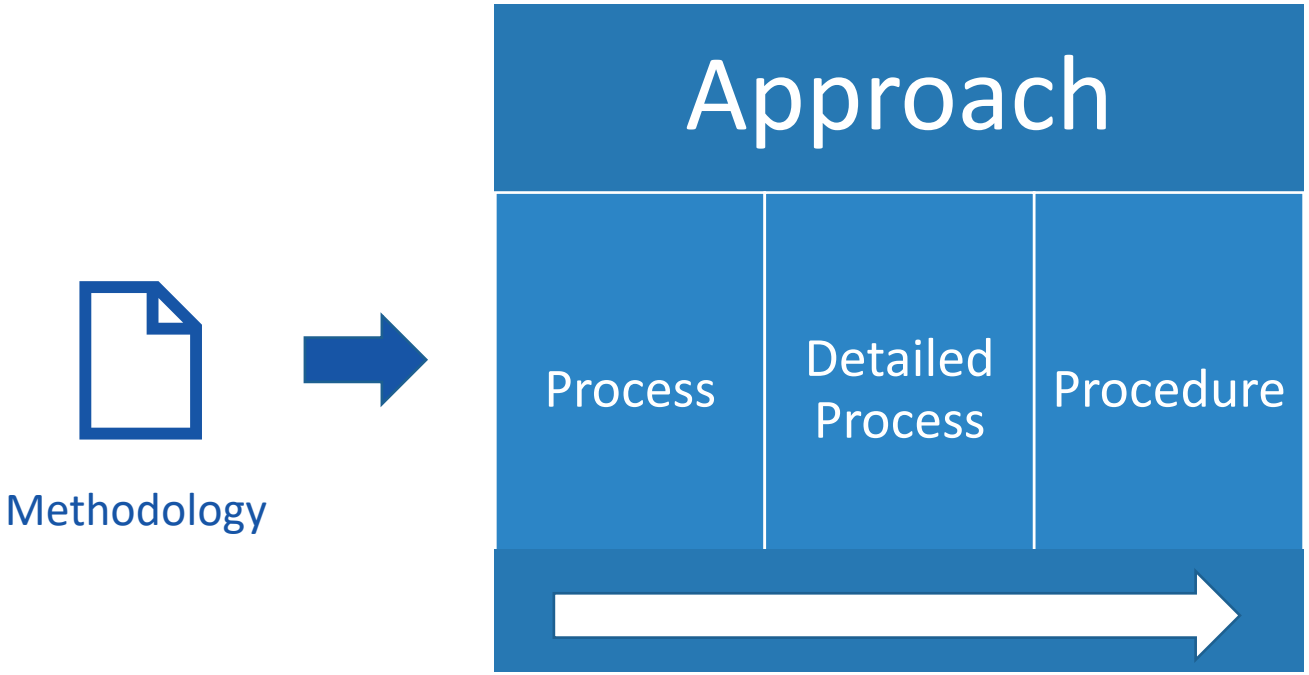
- Evaluation for connected automated driving
- Towards certification and type approval
- Connected to the methodology
- Adapted for the different Use Cases
- Covered by available tools

Methodology



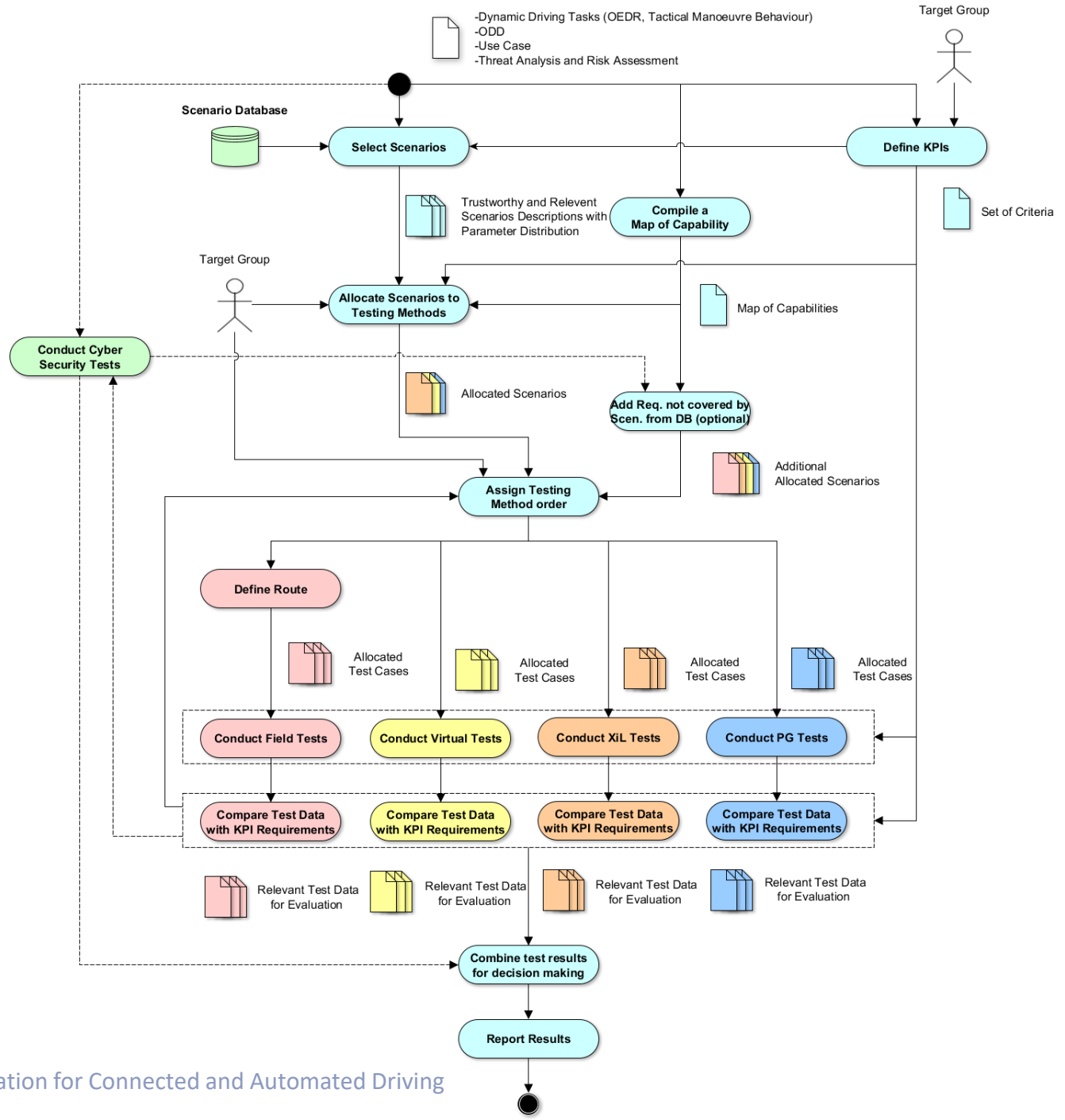
Cybersecurity in the procedure

- ✓ **A process** is a set of interrelated or interacting activities which transforms inputs into outputs. It's about **what to do.**
- ✓ **A procedure** is a specified way to carry out an activity or a process. It's about **how to do it**.



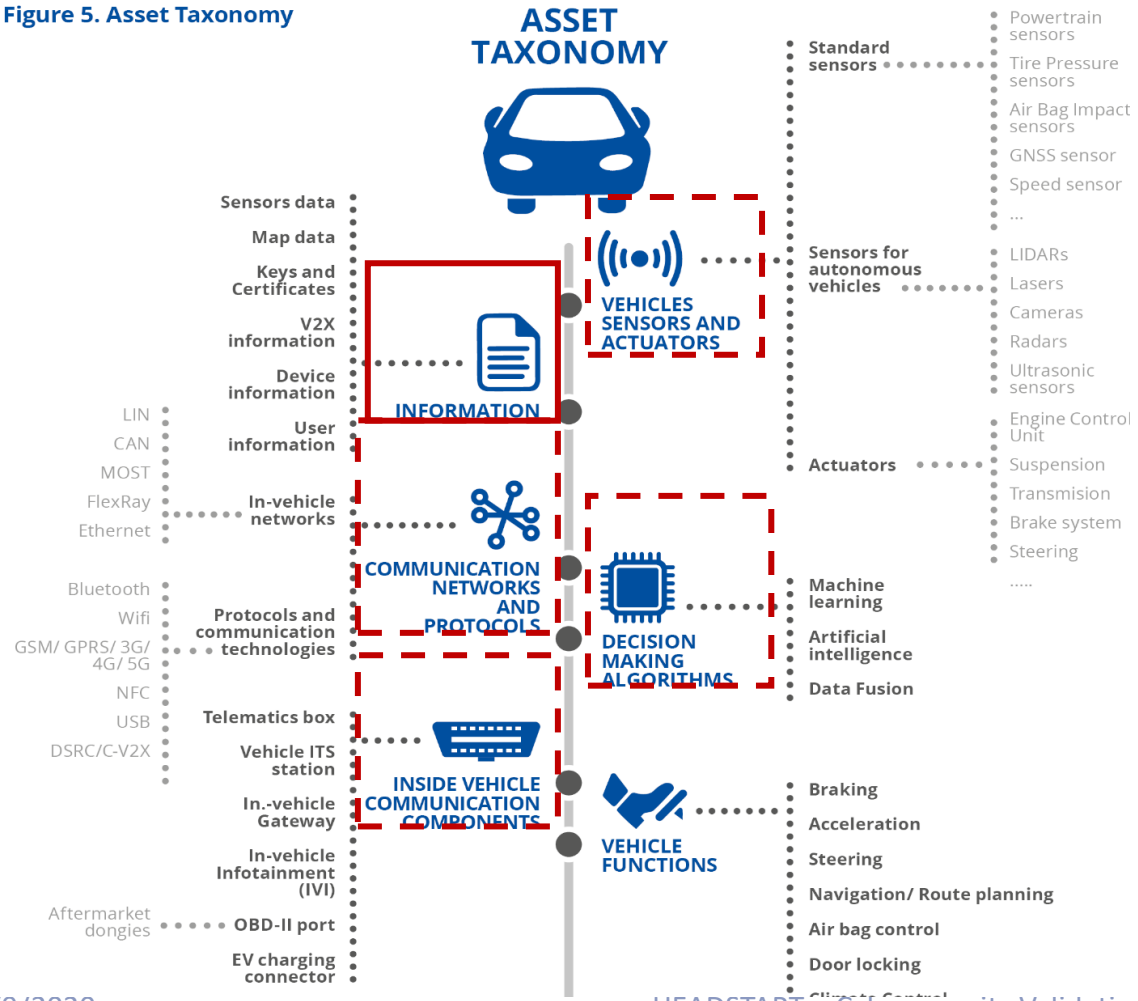
High-Level Process

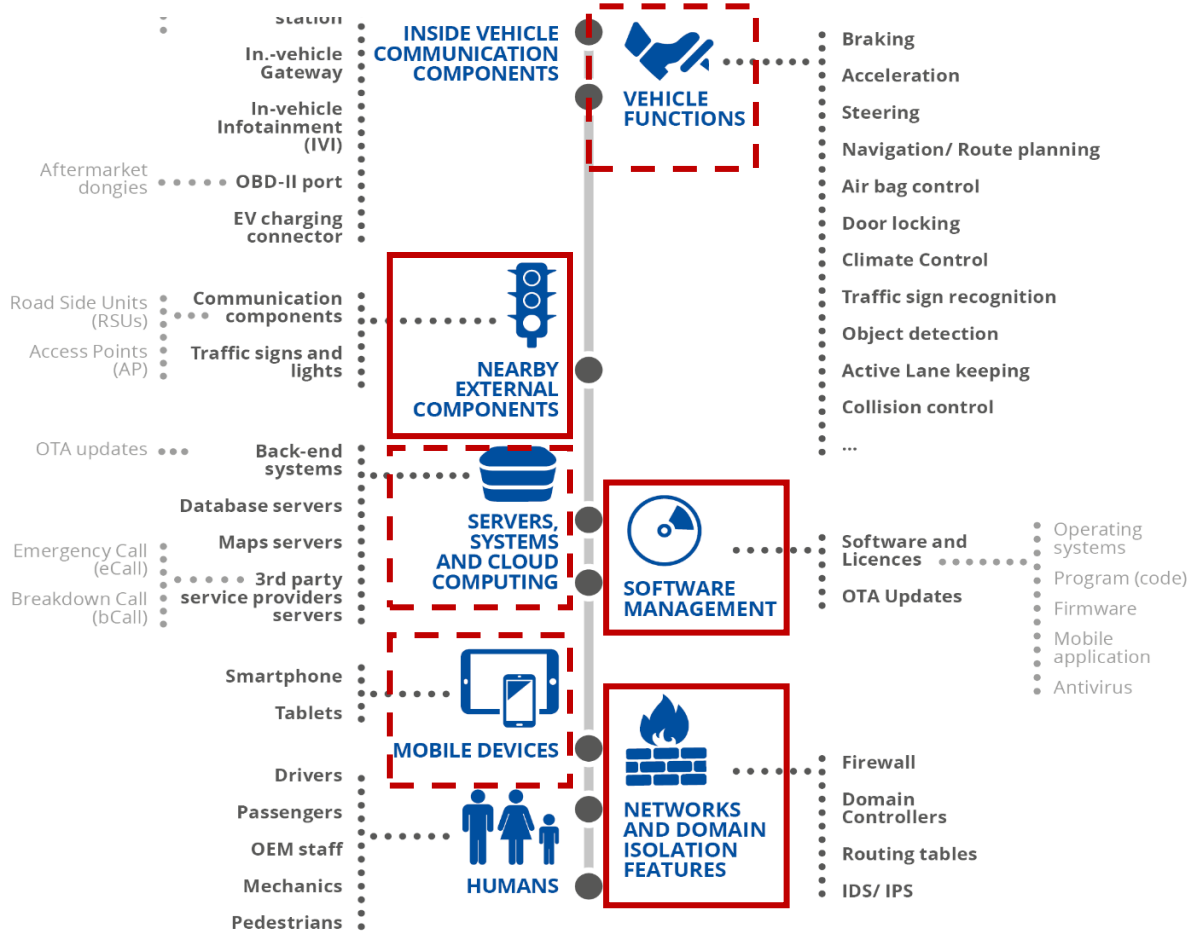
- ✓ Scenario Selection
- ✓ Scenario Allocation
- ✓ Testing Method Coordination
- ✓ Field Testing
- ✓ Virtual Testing
- ✓ XiL Testing
- ✓ Proving Ground Testing
- ✓ Cyber Security
- ✓ Evaluation



Cybersecurity in the procedure

Figure 5. Asset Taxonomy





ENISA GOOD PRACTICES FOR SECURITY OF SMART CARS

Cybersecurity in the procedure

Cybersecurity as a KET:

1. Different testing methods like penetration test, fuzzy test, vulnerability scanning, functionality testing, etc. defined by the requirements (scenario parameters)

Testing of cybersecurity is challenging and differs from safety testing. Cybersecurity relies on:

- Attack (vulnerability) testing
- Penetration testing
- Functional Testing
- Interface Testing
- Fuzz Testing

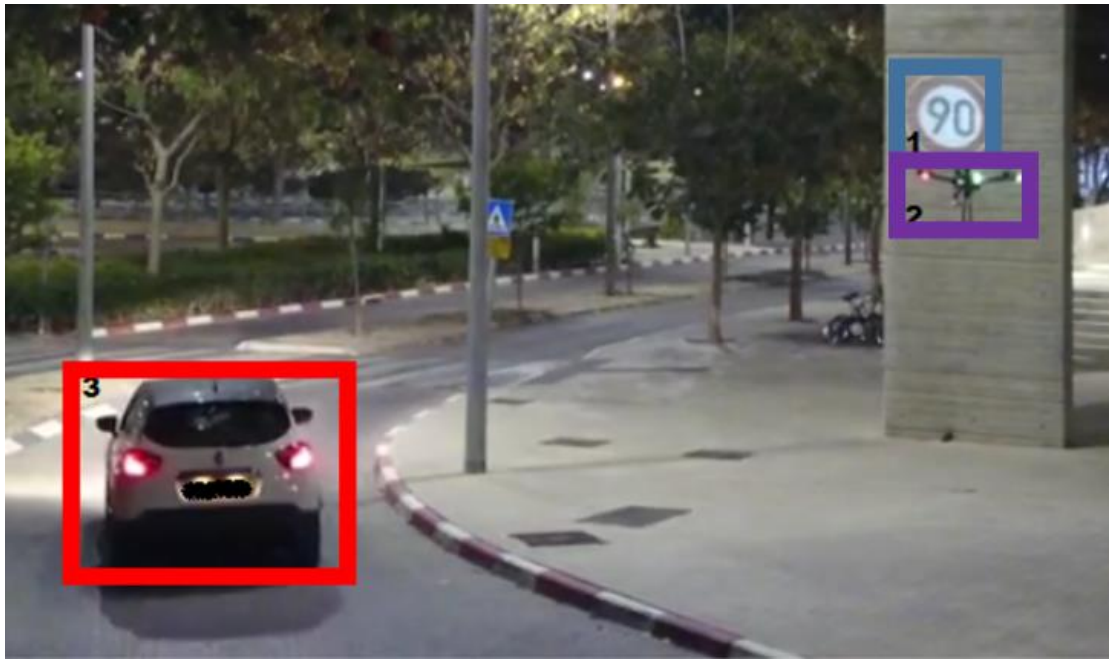
Based on a performed:

- Threat Analysis & Risk Assessment (TARA)
- Cybersecurity Requirements

Cybersecurity in the procedure

Cybersecurity as a KET:

2. Testing intended functionality/cybersecurity related (e.g. creating interferences of a sensor, in case of positioning by interference to GNSS)



https://arxiv.org/pdf/1906.09765.pdf

Cybersecurity in the procedure

Cybersecurity as a KET:

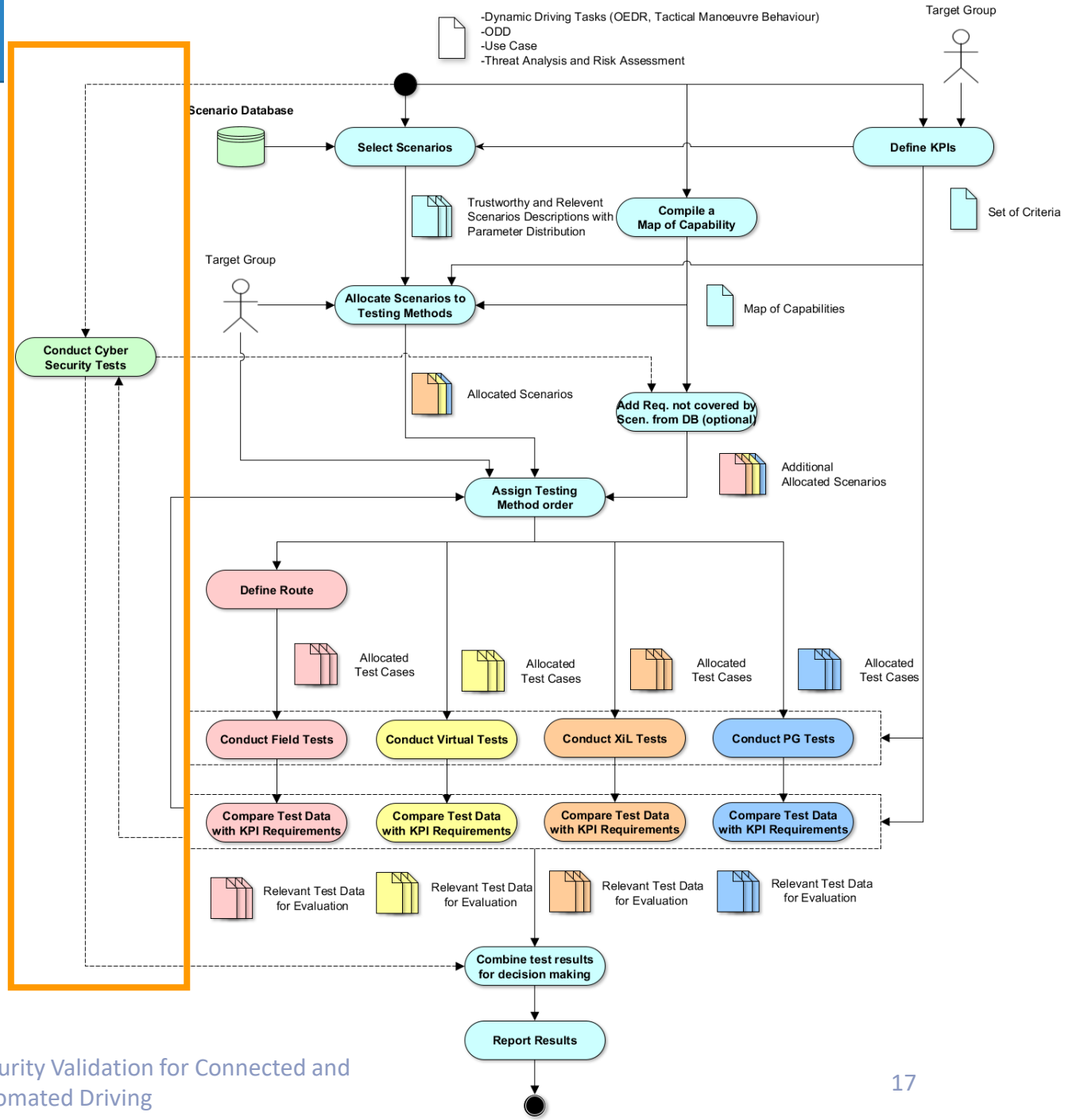
3. Evaluation of the cybersecurity coverage during the lifecycle of the item:

Relevant activities from the ISO 21434 (ISO/SAE DIS 21434 Road vehicles — Cybersecurity Eng.):

- Overall cybersecurity management
- Project dependent cybersecurity management
- Concept phase
- Product development phases
- Post-development phase
- Continuous cybersecurity activities
- Risk assessment methods

High-Level Process

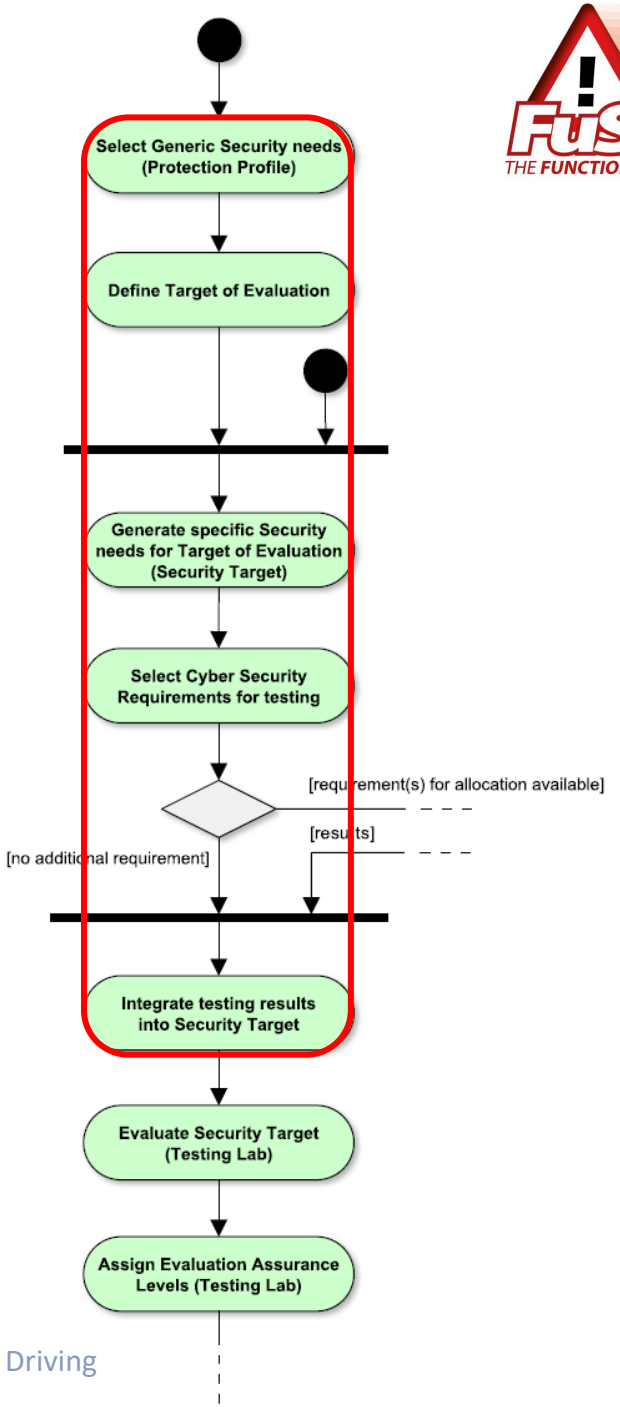
- ✓ Cyber Security
  - Optional side branch
  - Cybersecurity certification oriented
  - Linked to the scenario allocation phase for additional requirements that can be allocated to testing methods



Cybersecurity in the procedure

Cybersecurity branch

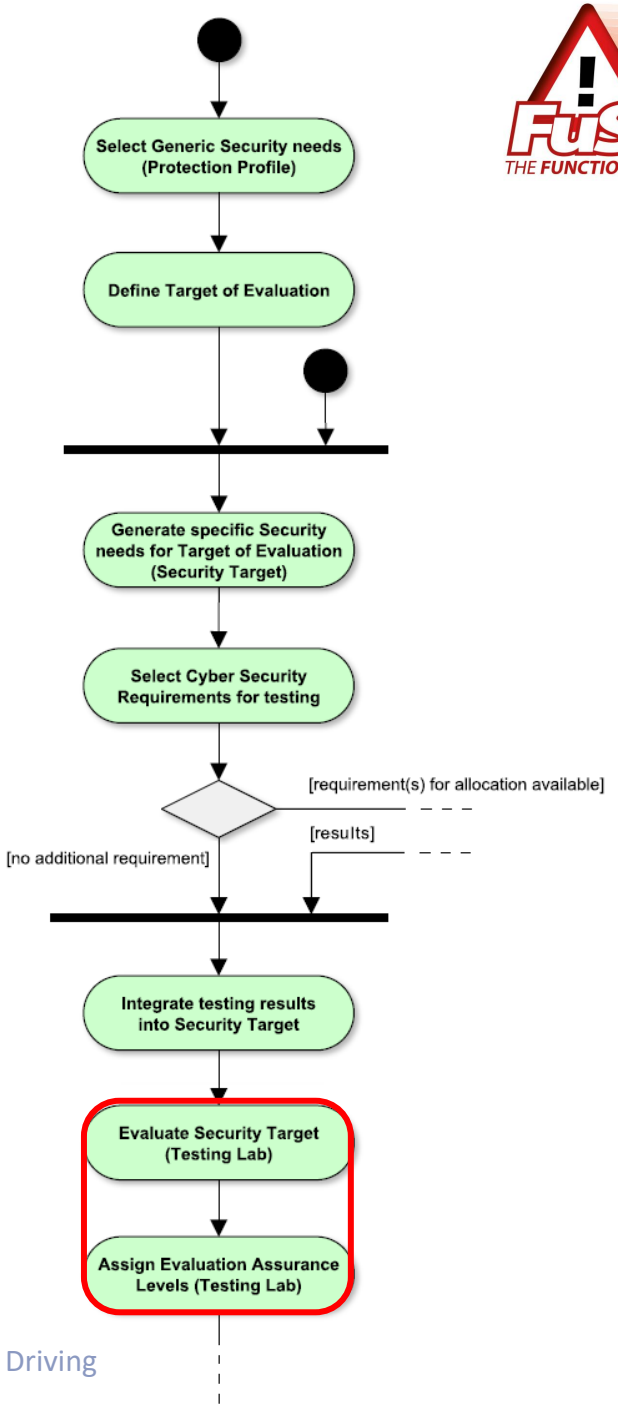
- Developer part (for OEMs and TIERs)
  1. Identifies generic security requirements for a group of security devices (Protection profile)
  2. Description of the Target of Evaluation (TOE)
  3. Generation of specific needs for the target of evaluation (Security Target)
  4. Selection of cybersecurity requirements for testing
  5. Integration of the testing results into the Secure Target



Cybersecurity in the procedure

Cybersecurity branch

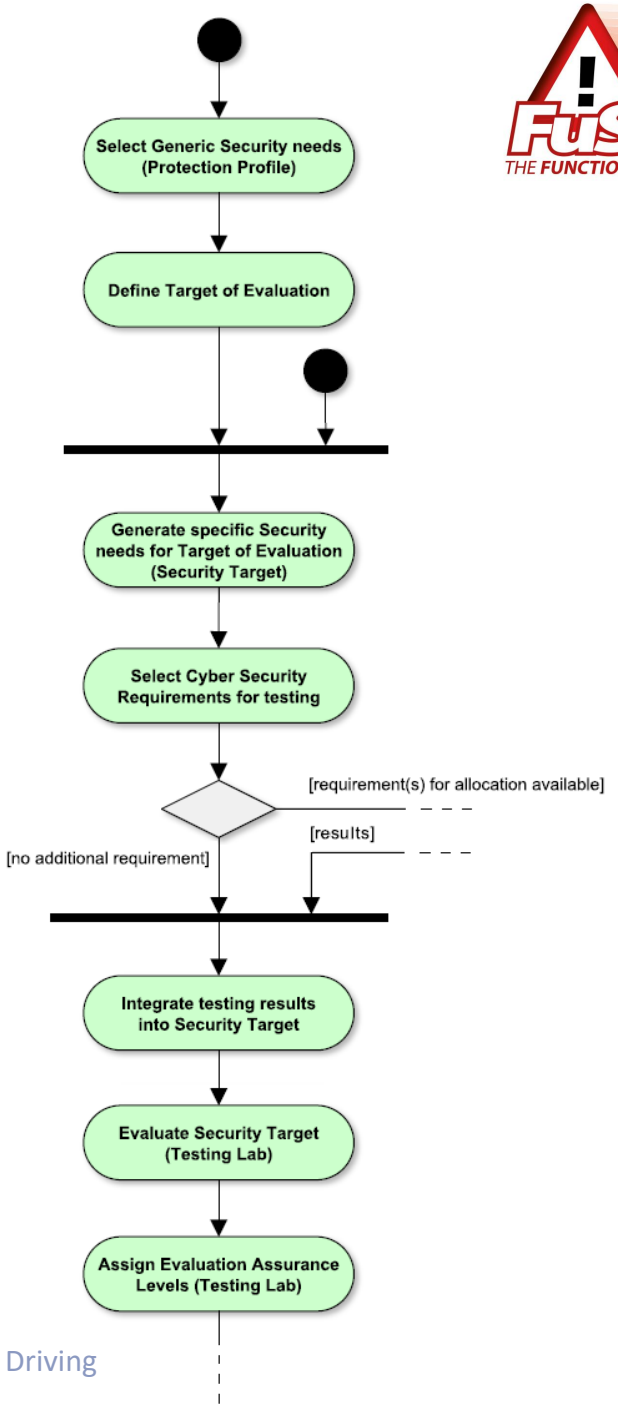
- Independent testing labs (for independent OEMs and TIERs)
  - Evaluation of the Security Target
  - Assignment of the Evaluation Assurance Levels (EALs)



Cybersecurity in the procedure

Cybersecurity branch

- Results
  - Evaluation and validation scheme (Validation Body)
  - United States is the National Security Agency
  - Germany the “Bundesamt für Sicherheit in der Informationstechnik”
  - And so on…



Next steps

Testing tool:

- Generic security need protection (Protection Profile)
- ISO 21434 (ISO/SAE DIS 21434 Road vehicles — Cybersecurity Engineering) integration
- Target group adaptation

SAFER TEC

Security Assurance Framework
for Networked Vehicular Technology

Next steps

Truck Platooning

Highway pilot

Traffic-jam chauffeur

Thank you!

Any questions?

Joaquim Maria Castella Triginer

Joaquim.castellatriginer@v2c2.at

Researcher / Dependable systems

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 824309.