HEADSTART:

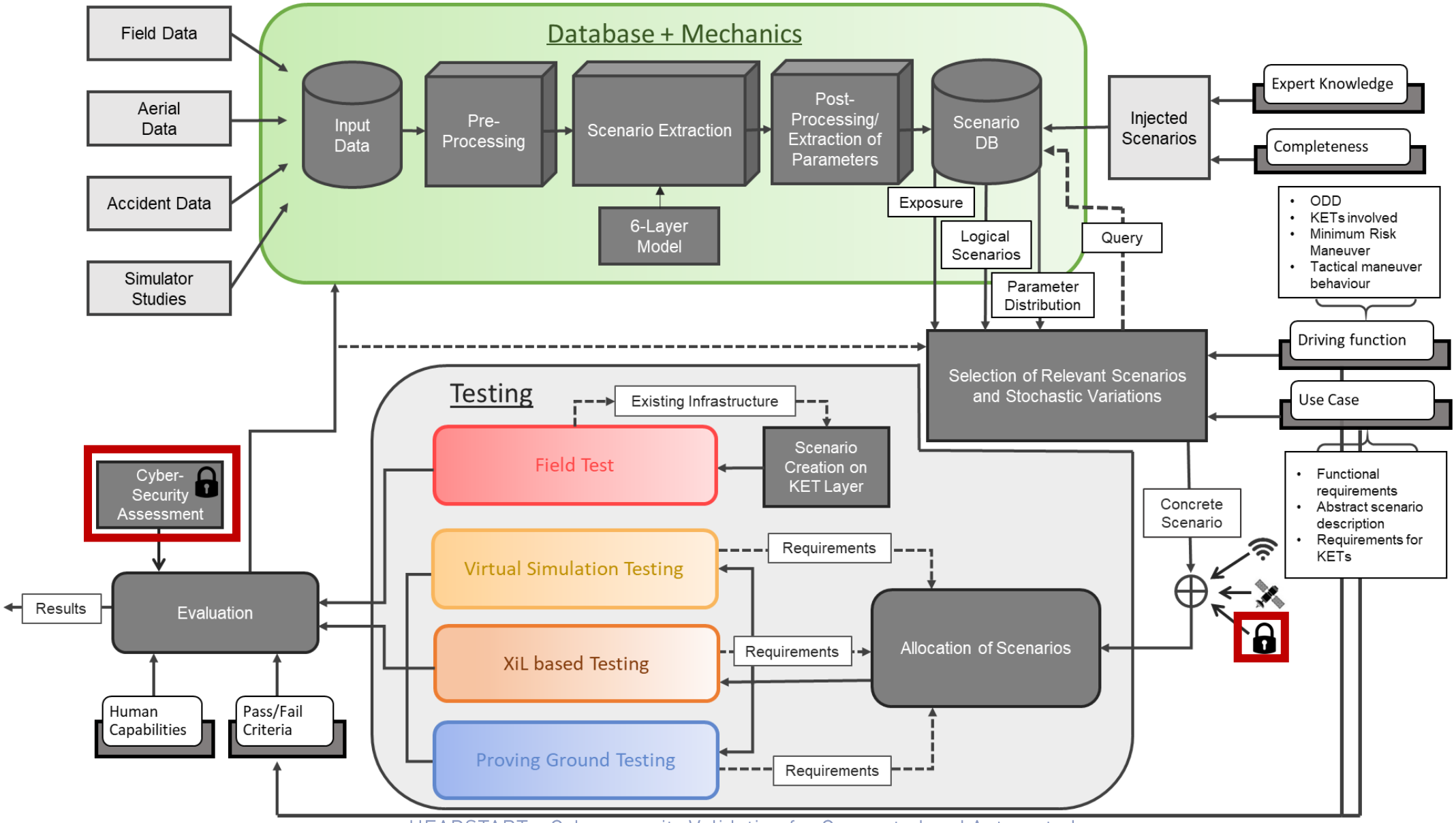
Cybersecurity

Joaquim Maria Castella Triginer [ViF]

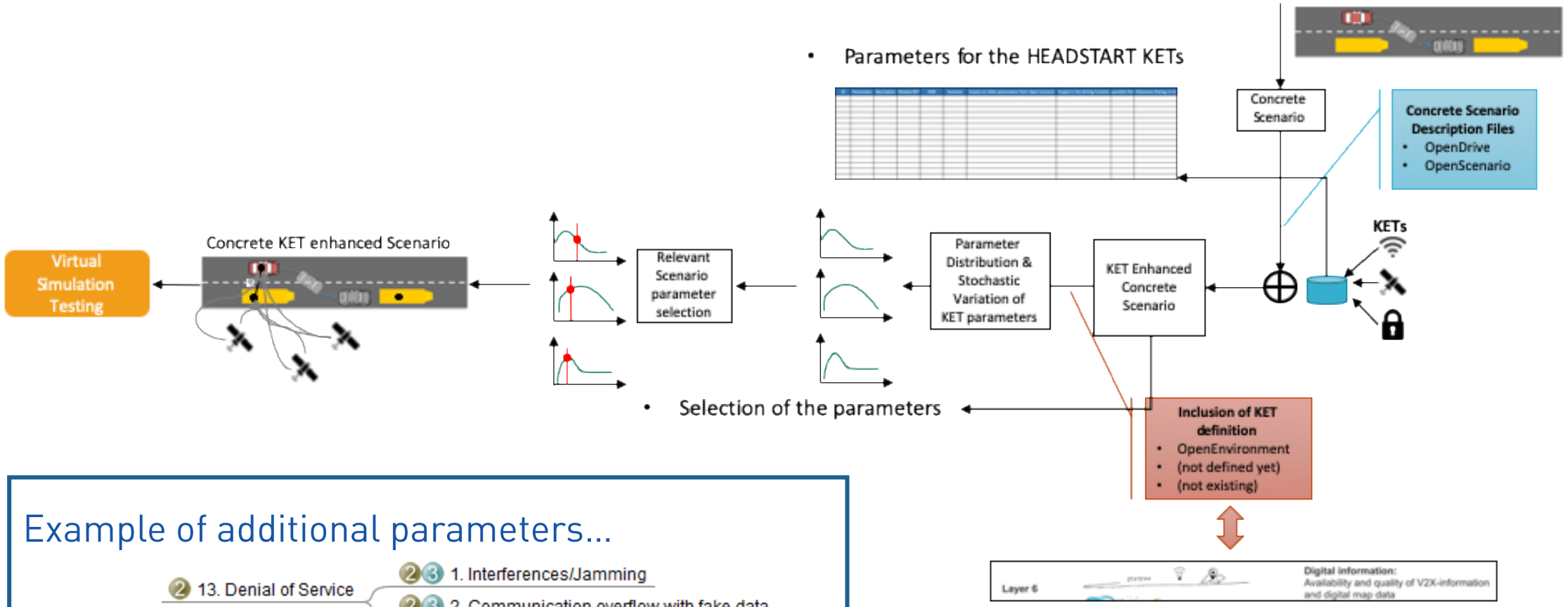
Athanasios Ballis [ICCS]

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

Methodology



Cybersecurity in the methodology

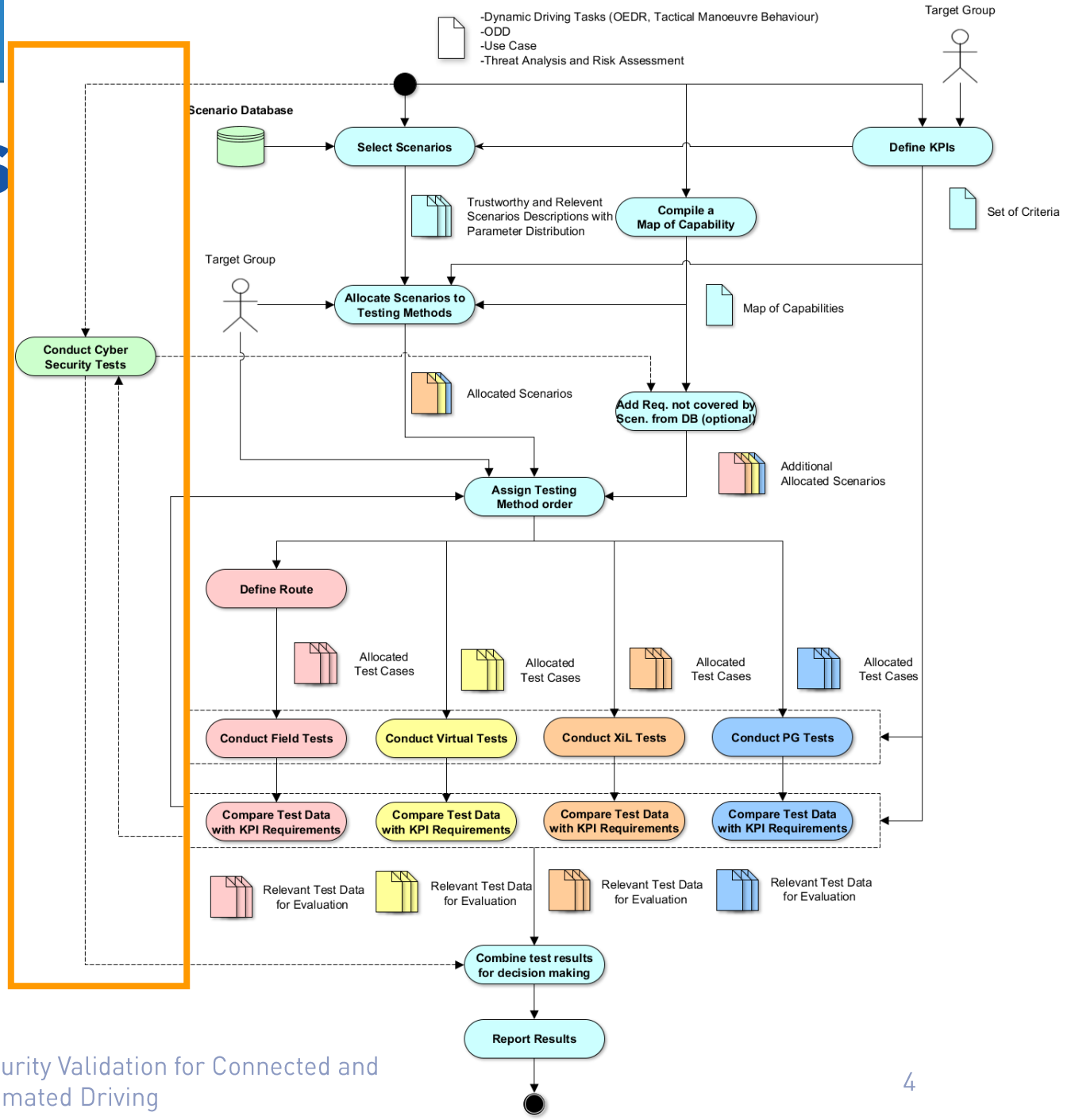


Example of additional parameters…

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

High-Level Process

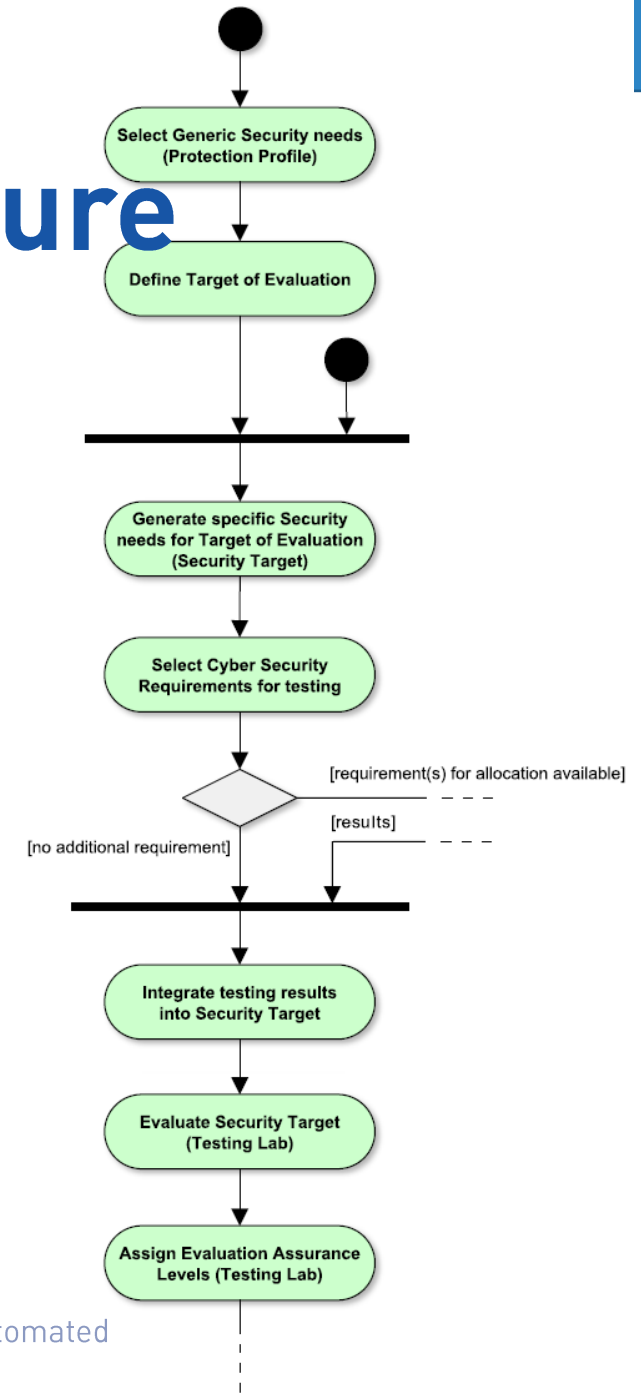
- ✓ Cyber Security
  - Optional side branch
  - Cybersecurity certification oriented
  - Linked to the scenario allocation phase for additional requirements that can be allocated to testing methods



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
- Independent testing labs (for independent OEMs and TIERs)
  - Evaluation of the Security Target
  - Assignment of the Evaluation Assurance Levels (EALs)
- Results
  - Evaluation and validation scheme (Validation Body)
  - Certification schemes in Europe



WP4 - Application and demonstration

Linked projects issues:

- No truly cybersecurity-oriented linked projects
- Integration of cybersecurity for the different use cases in early stages
- Other KETs are more developed and with more linked projects
- Low effort within the project

Linked project – ENSEMBLE

ENSEMBLE project paved the way for the adoption of multi-brand truck platooning in Europe to improve fuel economy, traffic safety and throughput.

- Linked project connected to communication KET
- Partially connected to cybersecurity KET -> ENSEMBLE includes a security framework of platooning
- Unsuccessful for cybersecurity KET:
  - Missing security concept "security by design"
  - Pure technical oriented (D2.9 Security framework of platooning)
  - Prioritization on V2X communication

Linked project – RISE SDVP

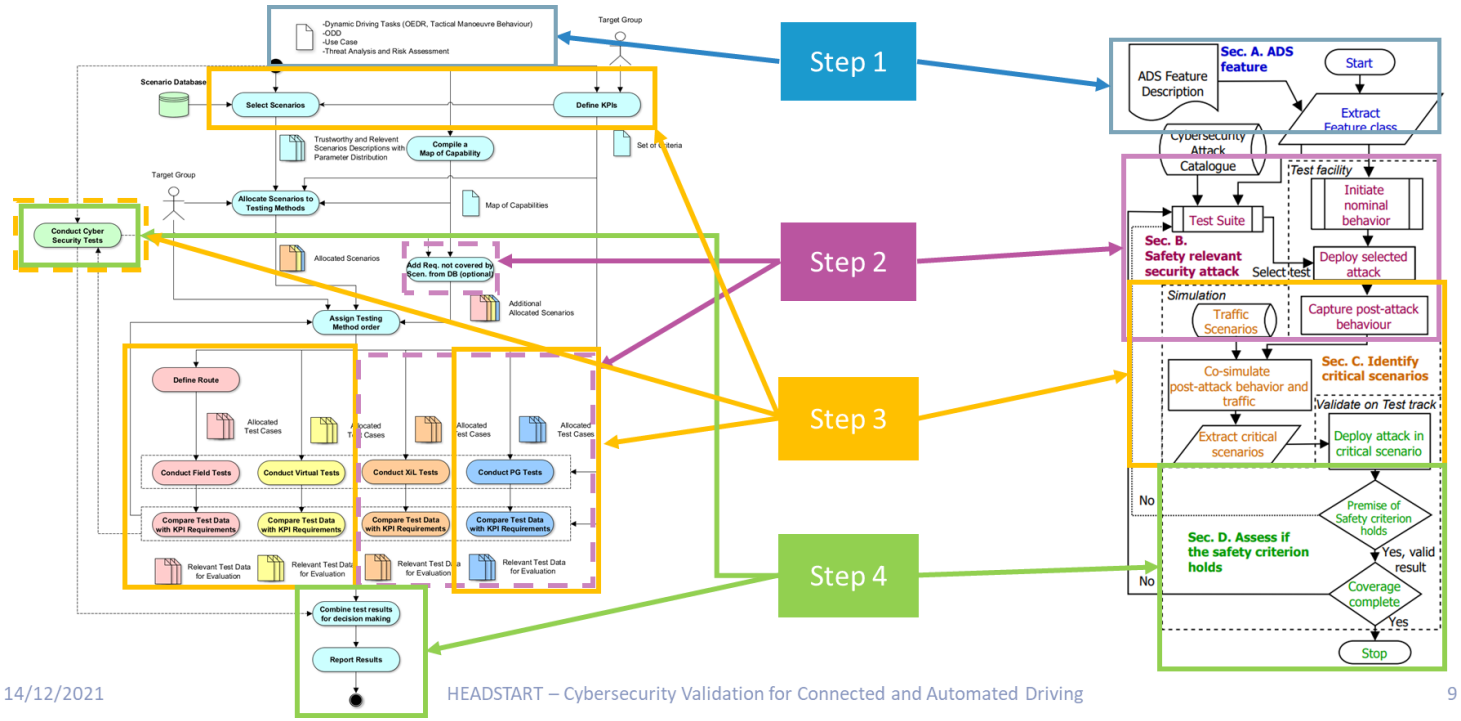
RISE Self-Driving Model Vehicle Platform

- Used to demonstrate the adaptation of the test procedure in the HEADSTART methodology
- Tests cases for a traffic jam chauffeur based on ALKS regulation
- Extendable to cybersecurity KET:
  - Focus on Black-Box Testing for Security-Informed Safety
  - Testing GNSS availability -> based on GNSS attacks
  - Proposed methodology of tests that could support establishing cybersecurity informed safety in an ADS.

Cybersecurity KET - RISE SDVP

RISE SDVP - cooperation projects:

- Validation comparing approaches
- Enhanced with the attack catalog
- Missing the assurance level criteria and target groups integration



HEADSTART – methodology assessment

✓L3pilot "Code of Practice for the Development of ADF"

- Alignment between cybersecurity best practices:
  - Established and followed cybersecurity process within the organization
  - Security by design
  - Asset management and threat analysis and risk assessment performed
  - Cybersecurity requirements identified
  - Review of the considered architectural design based on refined requirements
  - Cybersecurity Incident Response process established
  - Cybersecurity validation process clearly defined

HEADSTART goal

HEADSTART – methodology assessment

✓L3pilot "Code of Practice for the Development of ADF"

- HEADSTART cybersecurity KET achievements:
  - Procedure based on well established IT security evaluation framework (Common Criteria)
  - Separated Cybersecurity assessment activity
  - Threat analysis on vehicle level with an asset identification
  - Cybersecurity requirements provided for communication KET
  - Evaluation of requirements using HAL (HEADSTART Assurance Level)
  - Integration of cybersecurity in HEADSTART safety validation process

HEADSTART – Conclusion and challenges

- ✓Cybersecurity KET seed towards scenario-based approach integration
- ✓Cybersecurity KET integrate type approval user group
- ✓HAL for communication KET

What is next?

- ✓“Reference for linked projects to consider c/s in their security by design processes“
- ✓"Invest resources to create detailed Protection Profiles“
- ✓"Thorough analysis and extraction of SFRs“
- ✓"Selection of external Certification body to officially validate the process“

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.

HEADSTART Assurance Level – HAL

- ✓ HAL value
  - SFR: Security Functional Requirement
  - CC: Common Criteria
  - ϕ: function to indicate testing depth
  - k: freedom parameter
  - $0 \leq HAL_{VALUE} \leq 3$

$$\boxed{HAL = InitialAssurance + ListBreadth + TestingDepth}$$

$$InitialAssurance = \frac{SFRs\ met}{total\ SFRs} \quad (1)$$

$$ListBreadth = \frac{CC\ funct.\ classes\ coverd\ by\ SFRs}{total\ CC\ funct.\ classes} \quad (2)$$

$$TestingDepth = \phi\left(\frac{Vulnerabilities\ fixed}{SFRs\ tested}\right) \quad (3)$$

$$\phi(\alpha) = \begin{cases} 0 & \alpha < k \\ 0.5 & k < \alpha < 1 \\ 1 & \alpha > 1 \end{cases} \quad (4)$$