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.

Join at
slido.com
#HEADSTART

Agenda

- ✓ Introduction webinar
- ✓ Introduction of HEADSTART project
- ✓ Introduction of cybersecurity role in the HEADSTART project
- ✓ Presentation of the cybersecurity particularities and integration in HEADSTART method
- ✓ Cybersecurity coverage and integration in HEADSTART process
- ✓ Next steps, cybersecurity framework refinement and testing tool for HEADSTRAT validation
- ✓ Open questions

- ✓ Wrap-up of the HEADSTART week

Introduction webinar

Webinar rules and process

- ✓ Webinar is being recorded
- ✓ Slides, voting results and recording will be shared and published on HEADSTART website
- ✓ Participants feedback anonymously gathered via www.slido.com with event code: *HEADSTART*
- ✓ Questions can be raised via www.slido.com with event code: *HEADSTART*

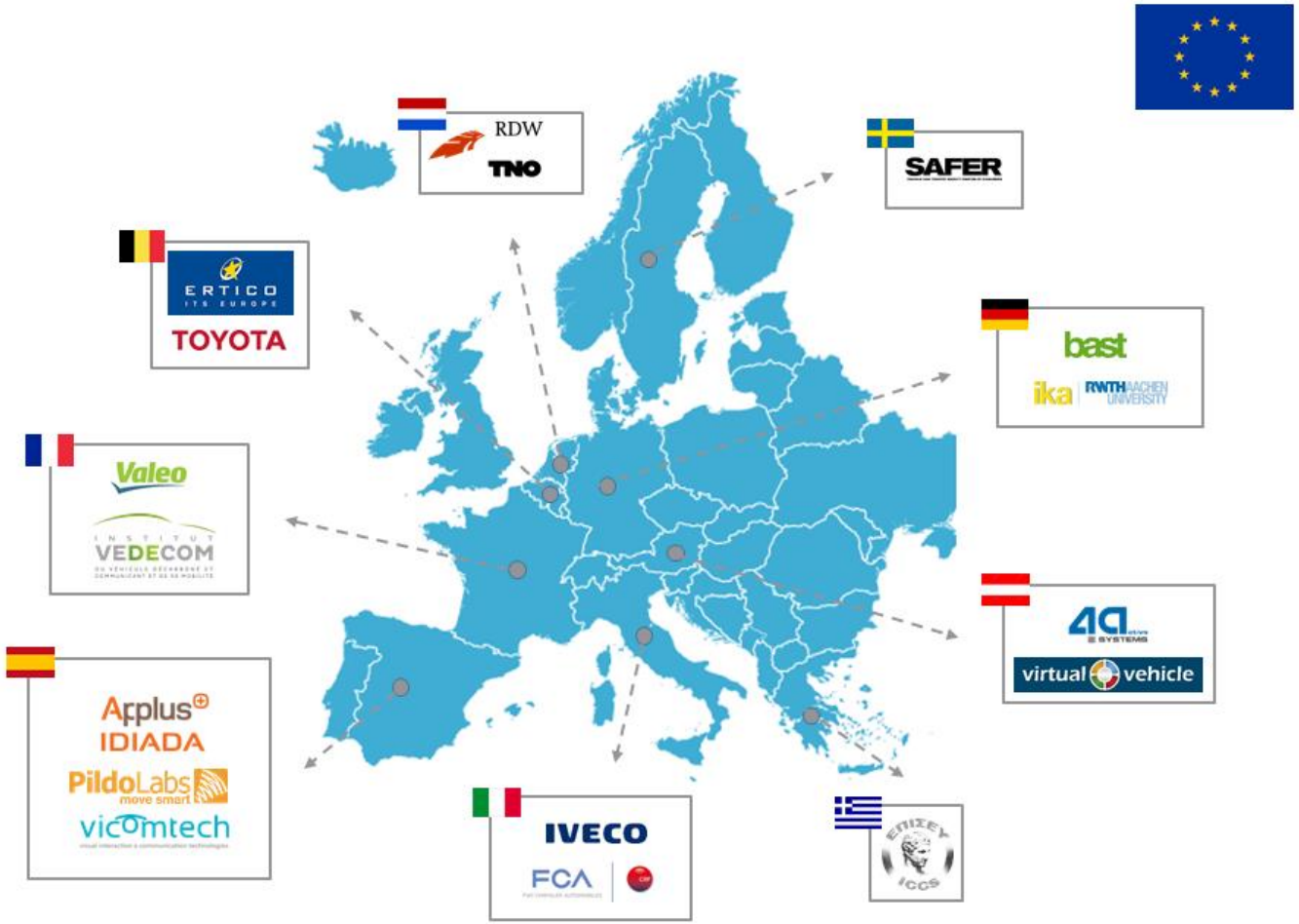
  The questions are gathered and where possible raised by the webinar moderator at fixed time slots during the webinar to the presenters.

Join at
slido.com
#HEADSTART

Introduction of HEADSTART project

- ✓ **Call identifier:** ART-01-2018
- ✓ **Type:** RIA
- ✓ **Duration:** 01.2019 – 12.2021 (36 months)
- ✓ **Budget:** 6M€
- ✓ **Consortium:** 17 partners
- ✓ **Coordinator:** Applus IDIADA, Mr. Álvaro Arrue, Project Manager
- ✓ **Dissemination Manager:** ICCS, Dr. Angelos Amditis, Research Director
- ✓ **Website:** https://www.headstart-project.eu
- ✓ **Social media:** / HEADSTART_EU
  / HEADSTART-PROJECT
  / HEADSTART project
  / @HeadstartEUproject

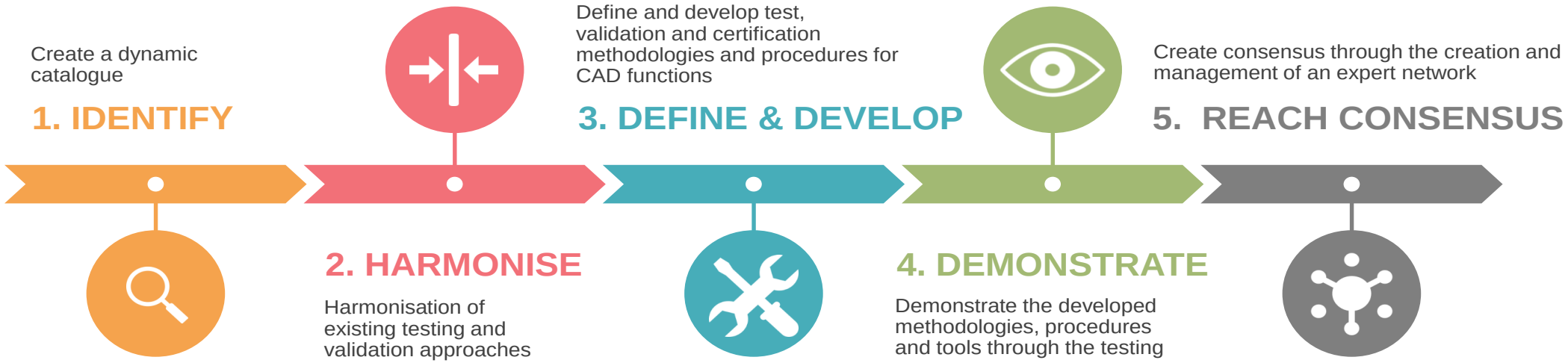
HEADSTART Consortium



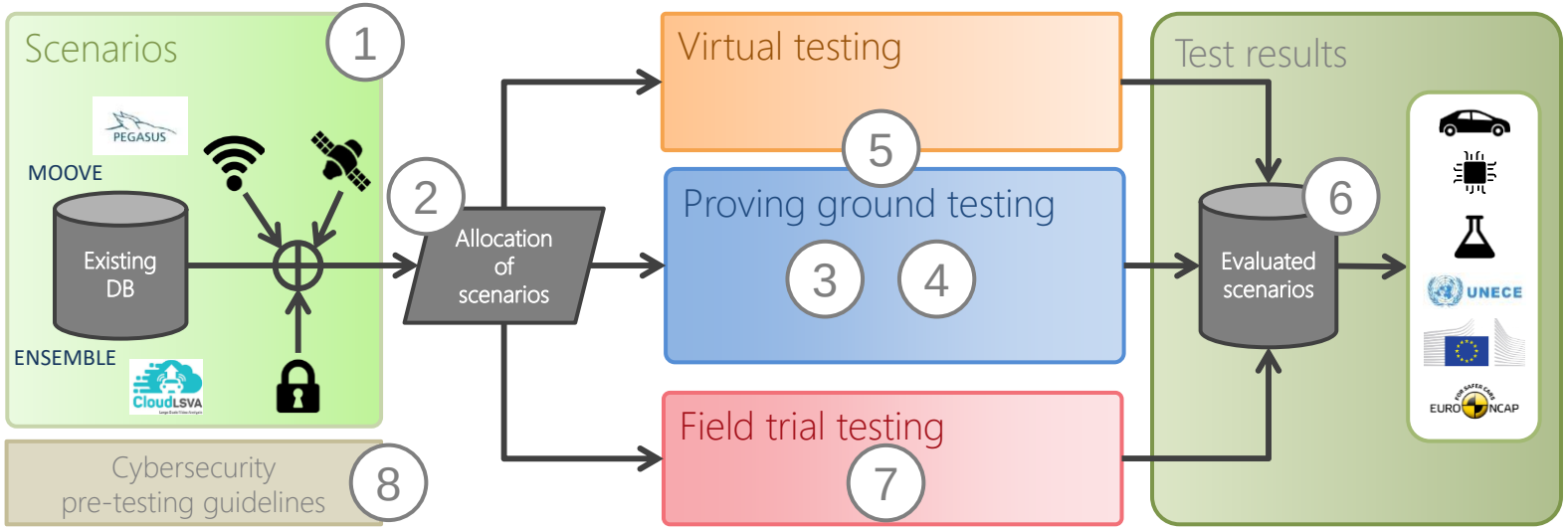
Project's Objectives

HEADSTART will define testing and validation procedures of CAD functions including:

- its key enabling technologies (i.e. communication, cyber-security, positioning)
- by cross-linking of all test instances such as simulation, proving ground and real world field tests
- to validate safety and security performance according to the needs of key user groups (technology developers, consumer testing and type approval)



Project's Concept



1. Integration of positioning, communications and cyber-security in CAD test scenarios
2. Comprehensive procedure for the allocation of test cases per testing platform
3. Selection criteria and specification for proving ground test scenarios taking into account criticality
4. Proving ground testing and evaluation
5. Correlation between simulation and proving ground results
6. Harmonised, open result compilation and sharing
7. Field trial test methodology description
8. Cyber-security principles and integration in the testing methodology

Cooperate with HEADSTART project

EXPERT GROUP PARTICIPATION

- Join as associated partner and our expert group
- Join the discussion group of your interest:
  - Cyber-security
  - Communications (V2X)
  - Positioning
  - Scenario selection
  - Consumer testing (NCAP)
  - Type approval
- Provide needs and requirements and evaluate project (intermediate) results

JOINT TESTING ACTION

- ✓ Joint cooperation between both projects for testing validation and certification purposes
- ✓ Align your project with the harmonized methodology and tools developed within HEADSTART
- ✓ Become one of our use cases!

Please let us know about your interest and join our distribution list.
Website: www.headstart-project.eu
Contact: info@headstart-project.eu

HEADSTART status update

- ✓ Available to be downloaded in www.headstart-project.eu
  - D1.1: State of innovation of existing initiatives and gap analysis
  - D1.2: Stakeholders and user group needs
  - D1.3: Technical and functional requirements for KETs
  - D1.4: Functional requirements of selected use cases
  - D2.1: Common methodology for test, validation and certification
  - D2.2: Criteria to choose optimal scenarios and tests for each KET
- ✓ HEADSTART Week
  - WC20: 11/05 – 15/05: A dedicated webinar + discussion every day from 10-11:30 CET
  - WB1: Methodology; WB2: Truck platooning; WB3: Traffic Jam assist; WB4: Cybersecurity
- ✓ International cooperation
  - Engage with US and Japan projects in a Project-2-project basis
  - Already discussing interaction with European initiatives

Introduction of HEADSTART project

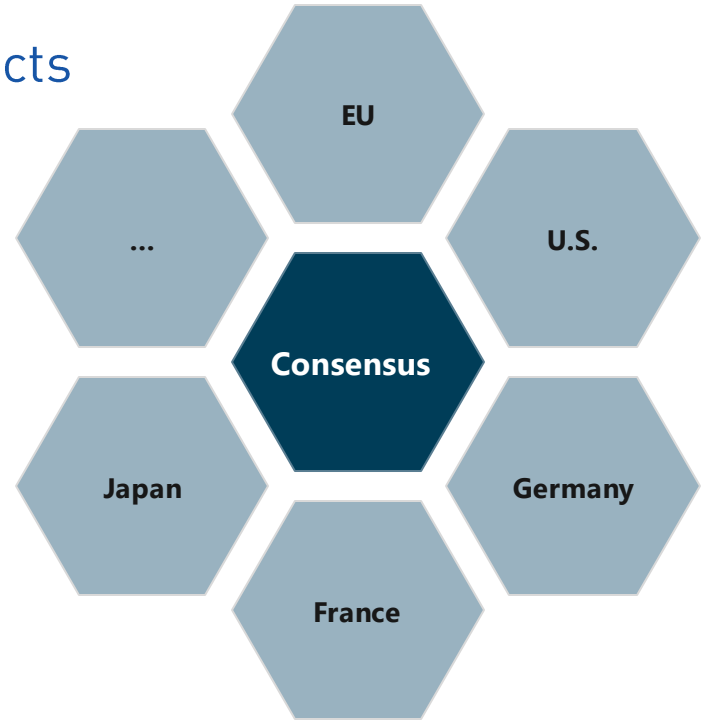
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 824309.

Join at
slido.com
#HEADSTART

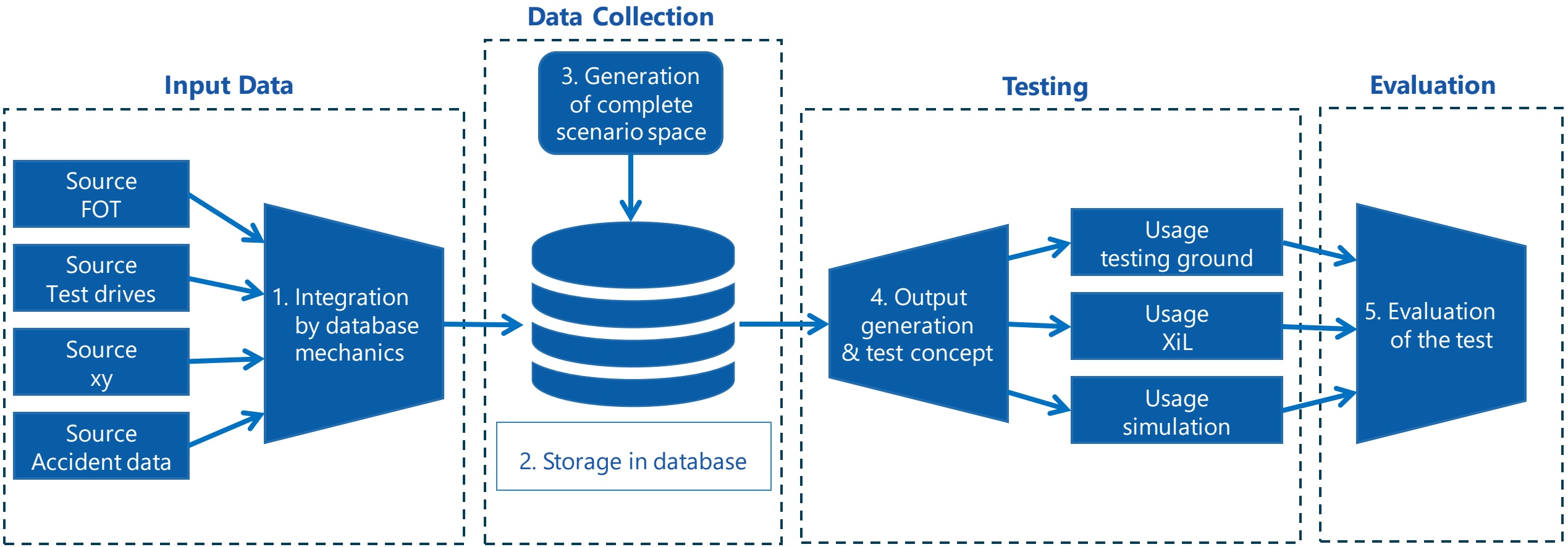
Overall Methodology

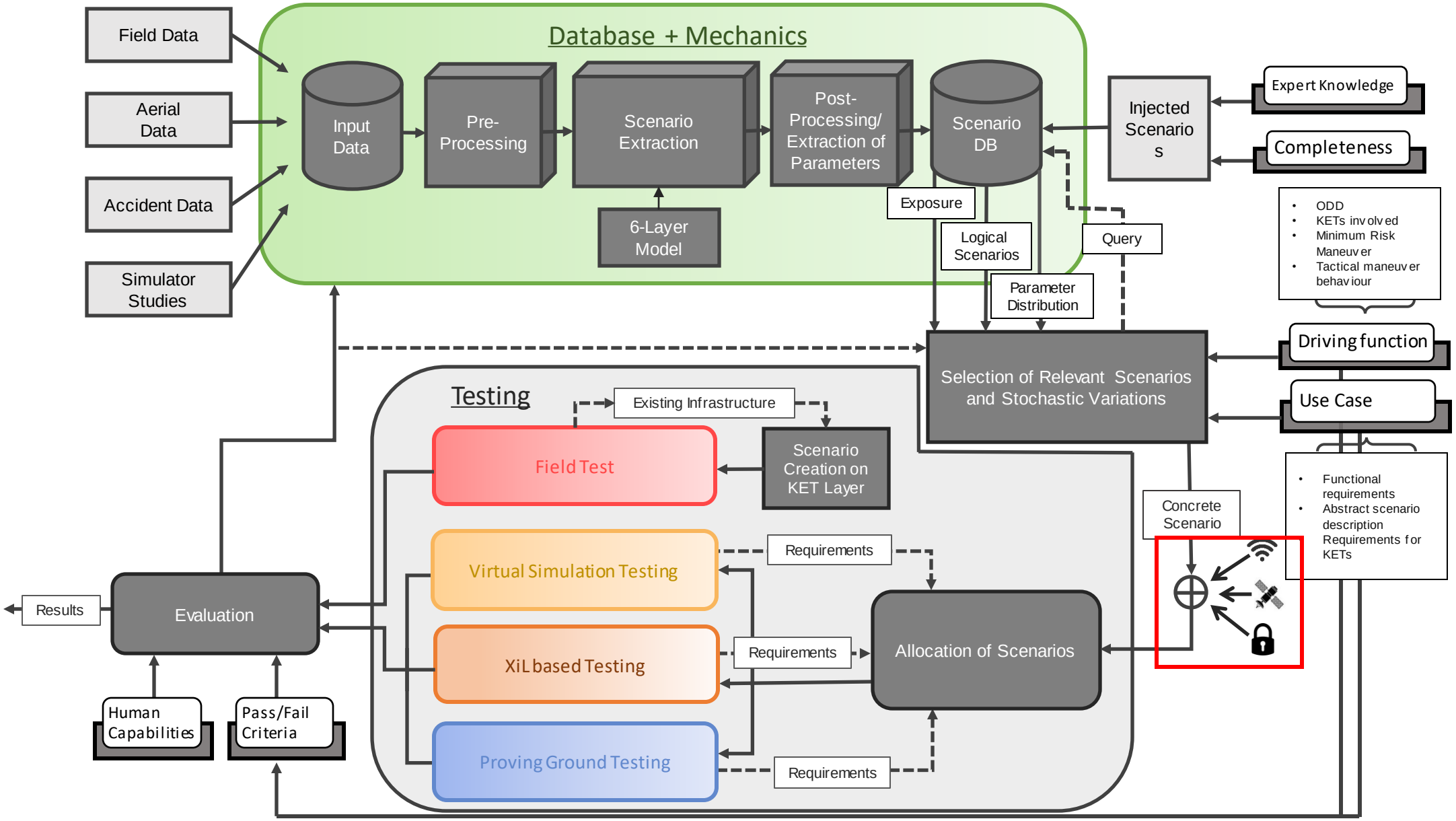
Where does the HEADSTART Methodology come from?

- ✓ State of the art analysis of international and national projects
- ✓ **Harmonization** of present and past projects
- ✓ Utilizing **common databases** to analyse data
- ✓ Testing of selected **relevant scenarios**



Overall Methodology

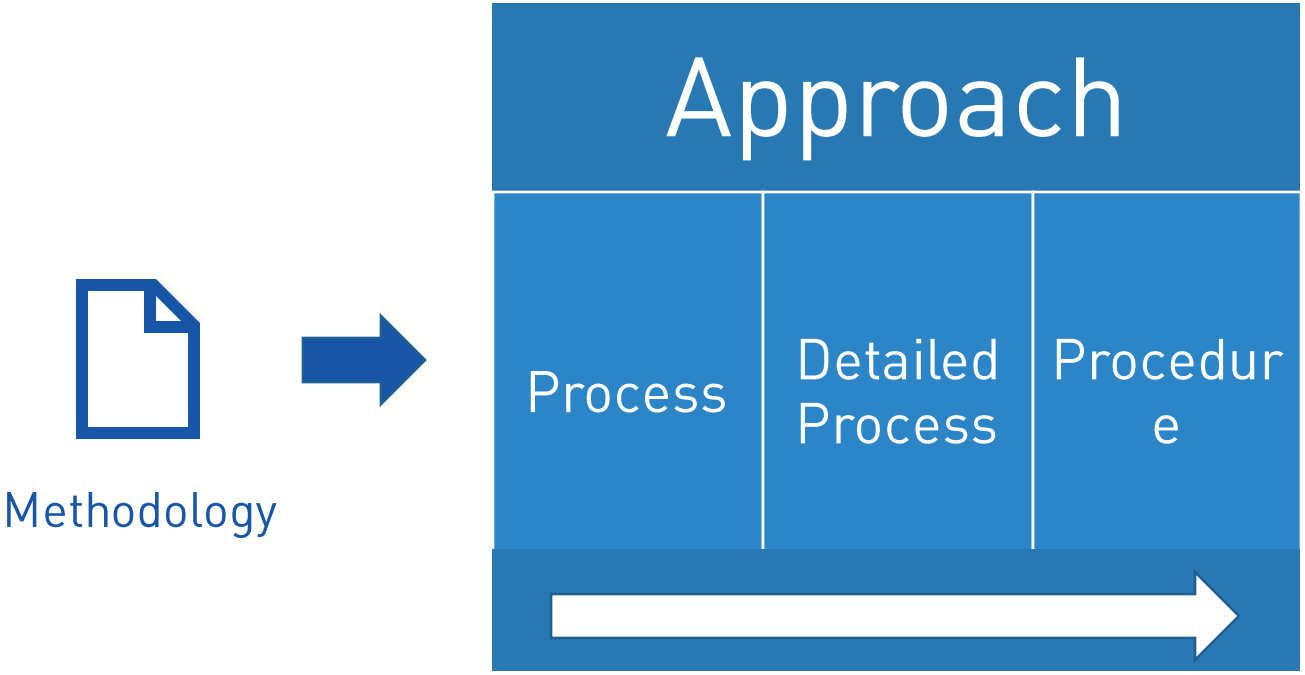



Field Data
Aerial Data
Accident Data
Simulator Studies
Database + Mechanics
Input Data
Pre-Processing
Scenario Extraction
Post-Processing/ Extraction of Parameters
Scenario DB
6-Layer Model
Exposure
Logical Scenarios
Parameter Distribution
Query
Injected Scenarios
Expert Knowledge
Completeness
ODD
KETs involved
Minimum Risk Maneuver
Tactical maneuver behaviour
Driving function
Use Case
Selection of Relevant Scenarios and Stochastic Variations
Testing
Existing Infrastructure
Field Test
Scenario Creation on KET Layer
Virtual Simulation Testing
Requirements
XiL based Testing
Requirements
Allocation of Scenarios
Proving Ground Testing
Requirements
Concrete Scenario
Functional requirements
Abstract scenario description
Requirements for KETs
Results
Evaluation
Human Capabilities
Pass/Fail Criteria

Source: https://blog.triaster.co.uk/blog/procedure-vs-process-what-is-the-diffe

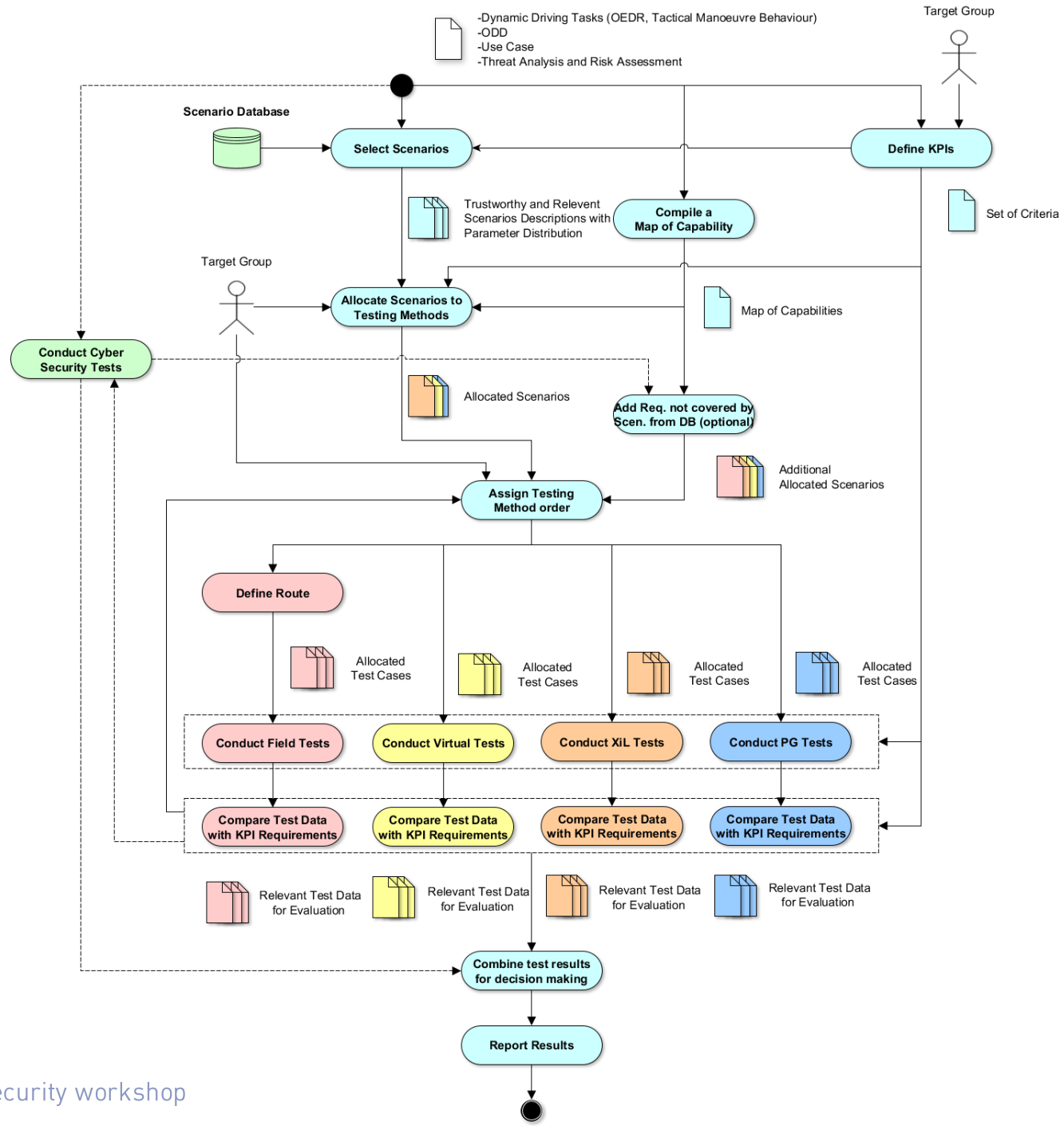
Approach

- ✓ **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



Introduction of cybersecurity role in the HEADSTART project

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

Join at
slido.com
#HEADSTART

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

AUTOPILOT
ENABLE-S3
ENSEMBLE
AutoSec
ICT4CART
SAFER TEC
SECREDAS

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/

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.

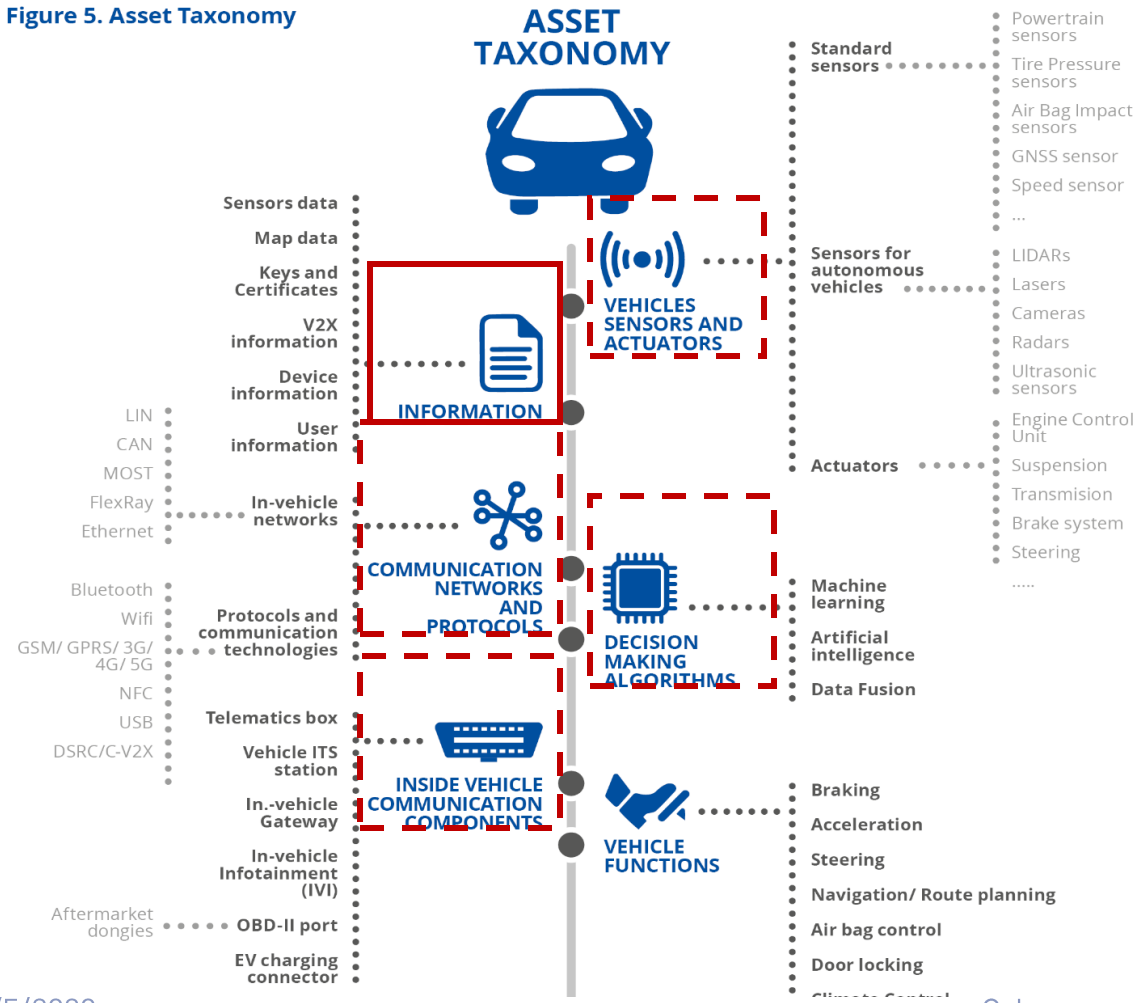
Presentation of the cybersecurity particularities and integration in HEADSTART method

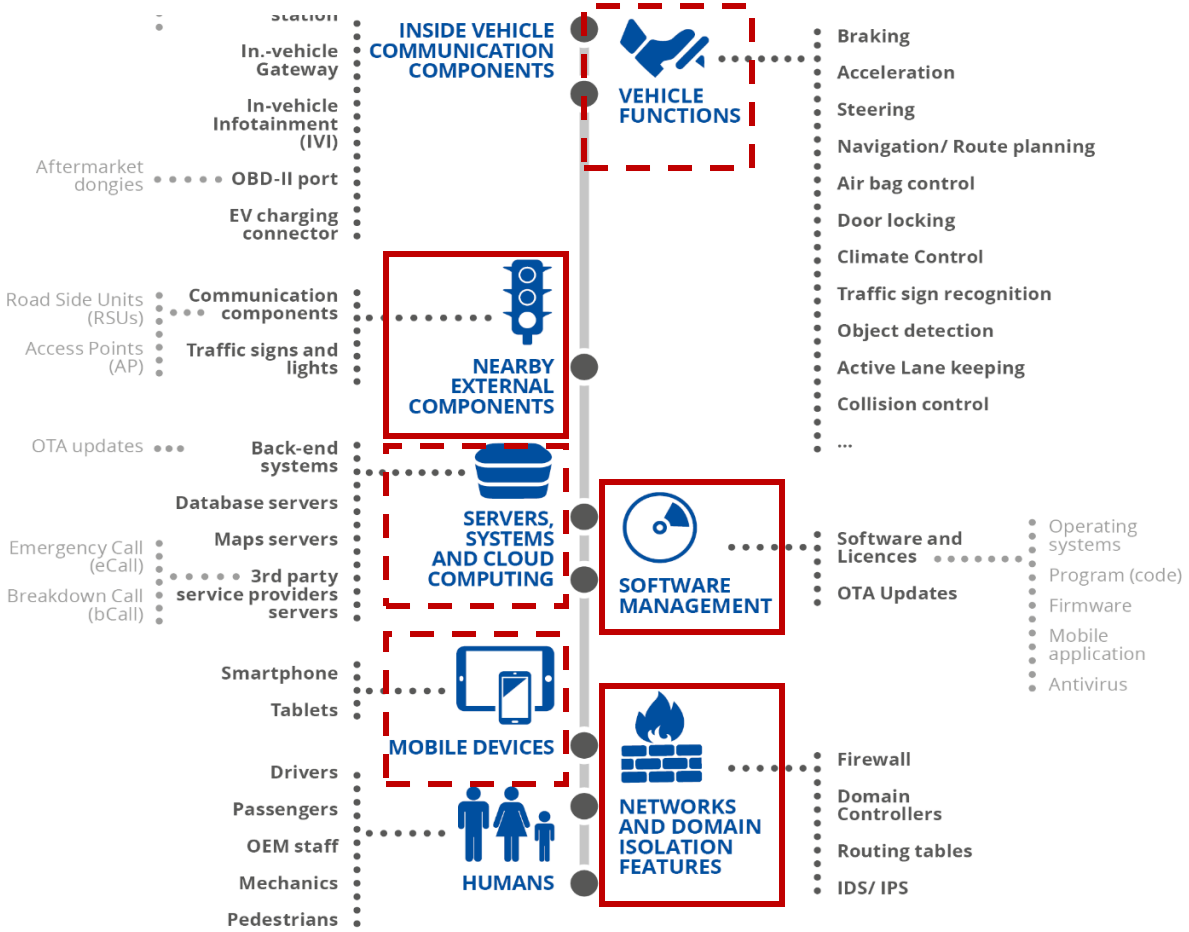
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 824309.

Join at
slido.com
#HEADSTART

Cybersecurity in the methodology

Figure 5. Asset Taxonomy





ENISA GOOD PRACTICES FOR SECURITY OF SMART CARS

Cybersecurity in the methodology

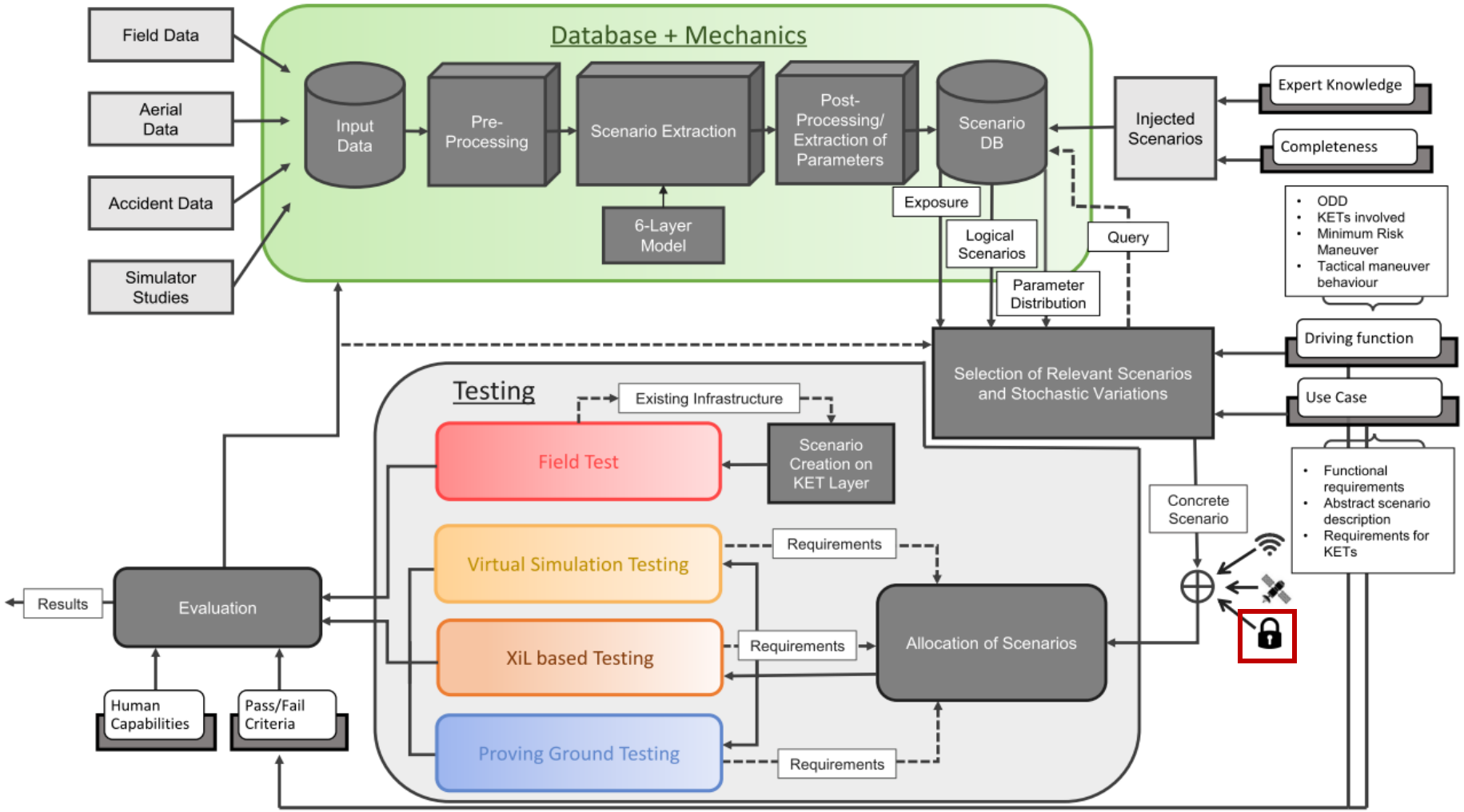
Testing of cybersecurity is challenging and differs from safety testing. Cybersecurity relies on:

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

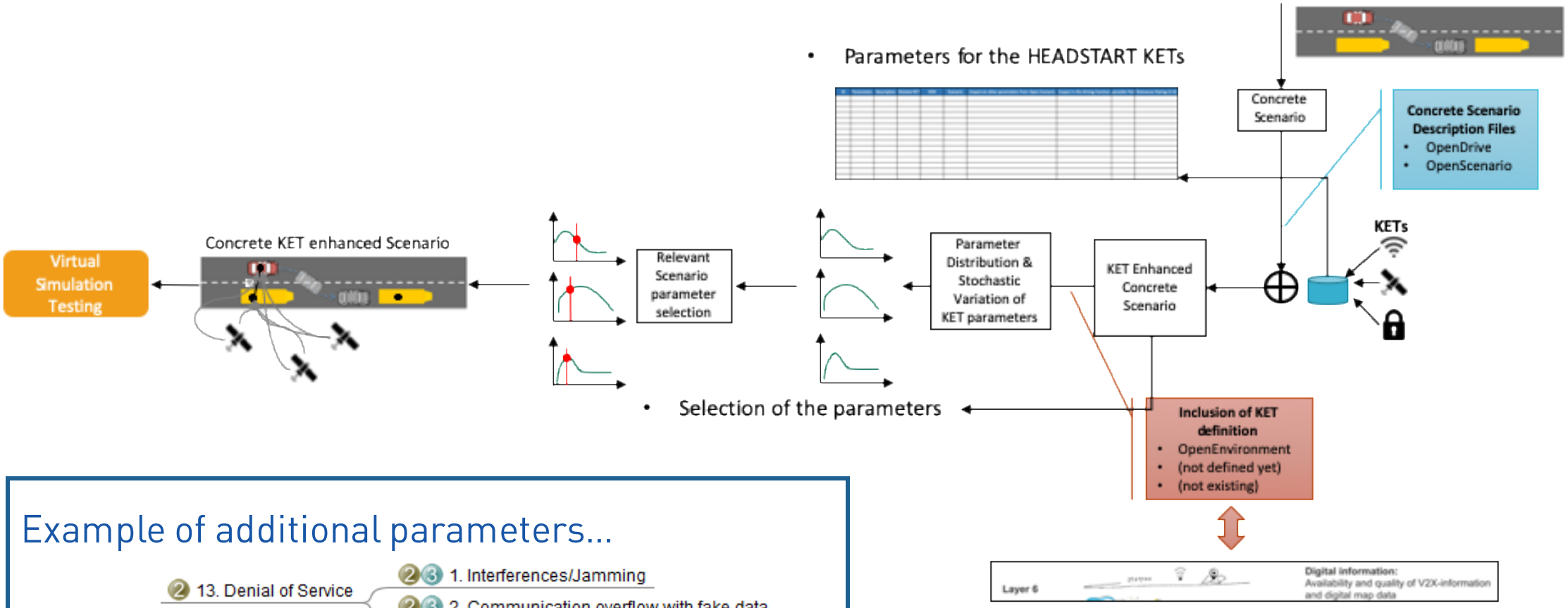
Based on a performed:

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

Cybersecurity in the 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

Cybersecurity coverage and integration in HEADSTART process

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

Join at
slido.com
#HEADSTART

Cybersecurity coverage

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

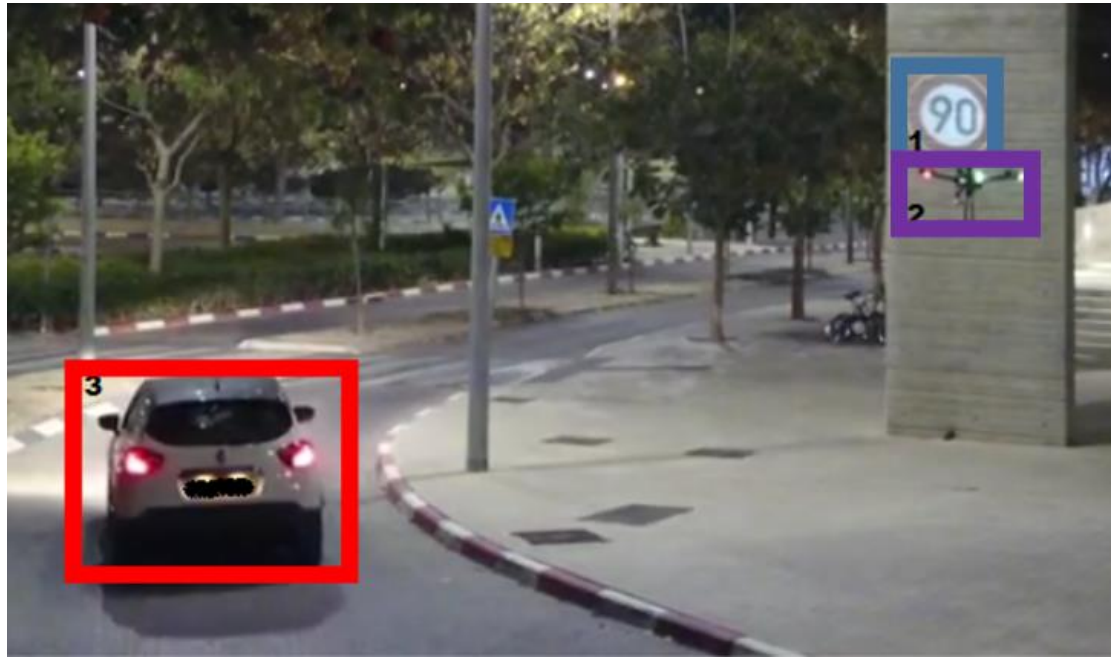
Based on a performed:

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

Cybersecurity coverage

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 coverage

Cybersecurity as a KET:

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

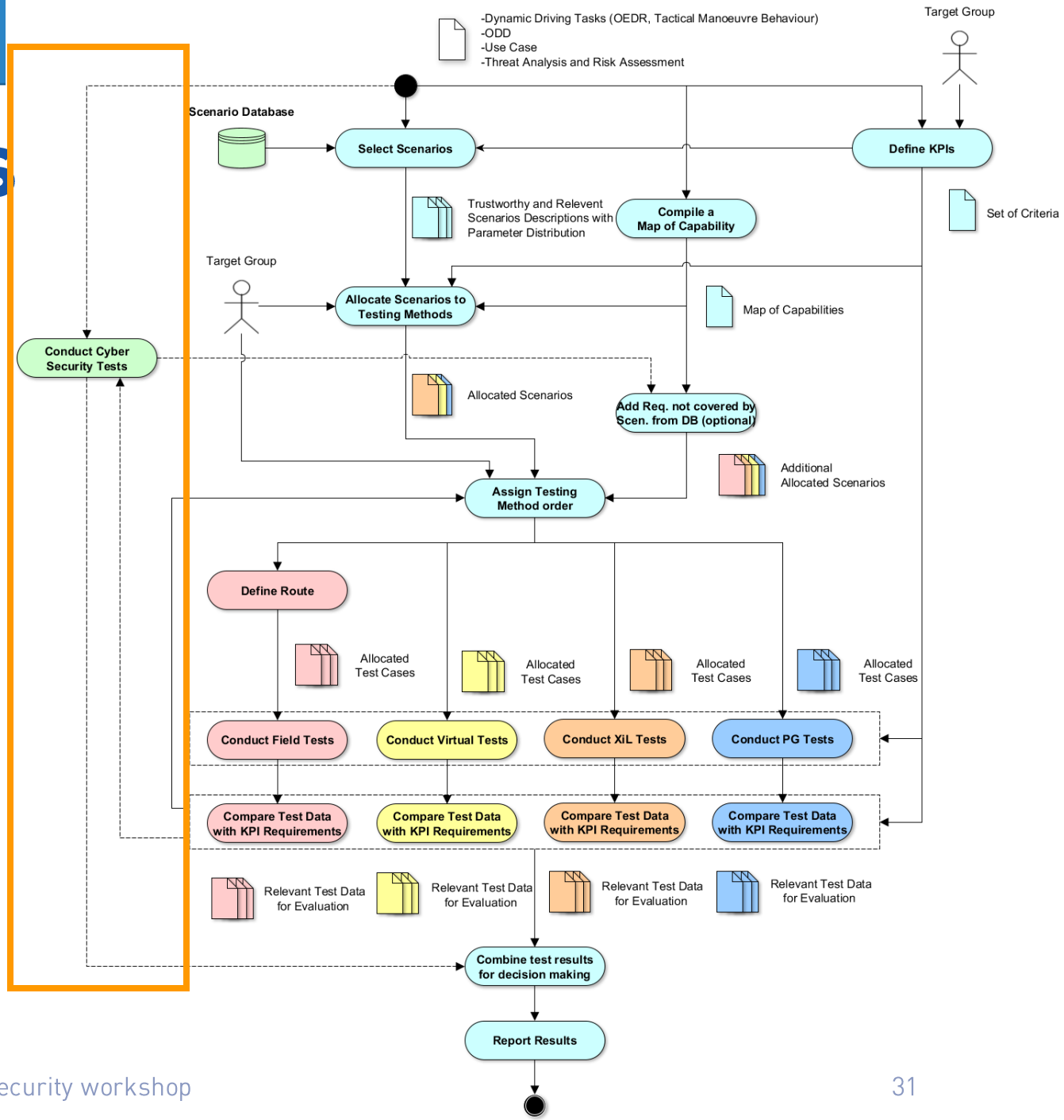
Relevant activities from the ISO 21434 (ISO/SAE DIS 21434 Road vehicles — Cybersecurity Eng.):

- 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 coverage

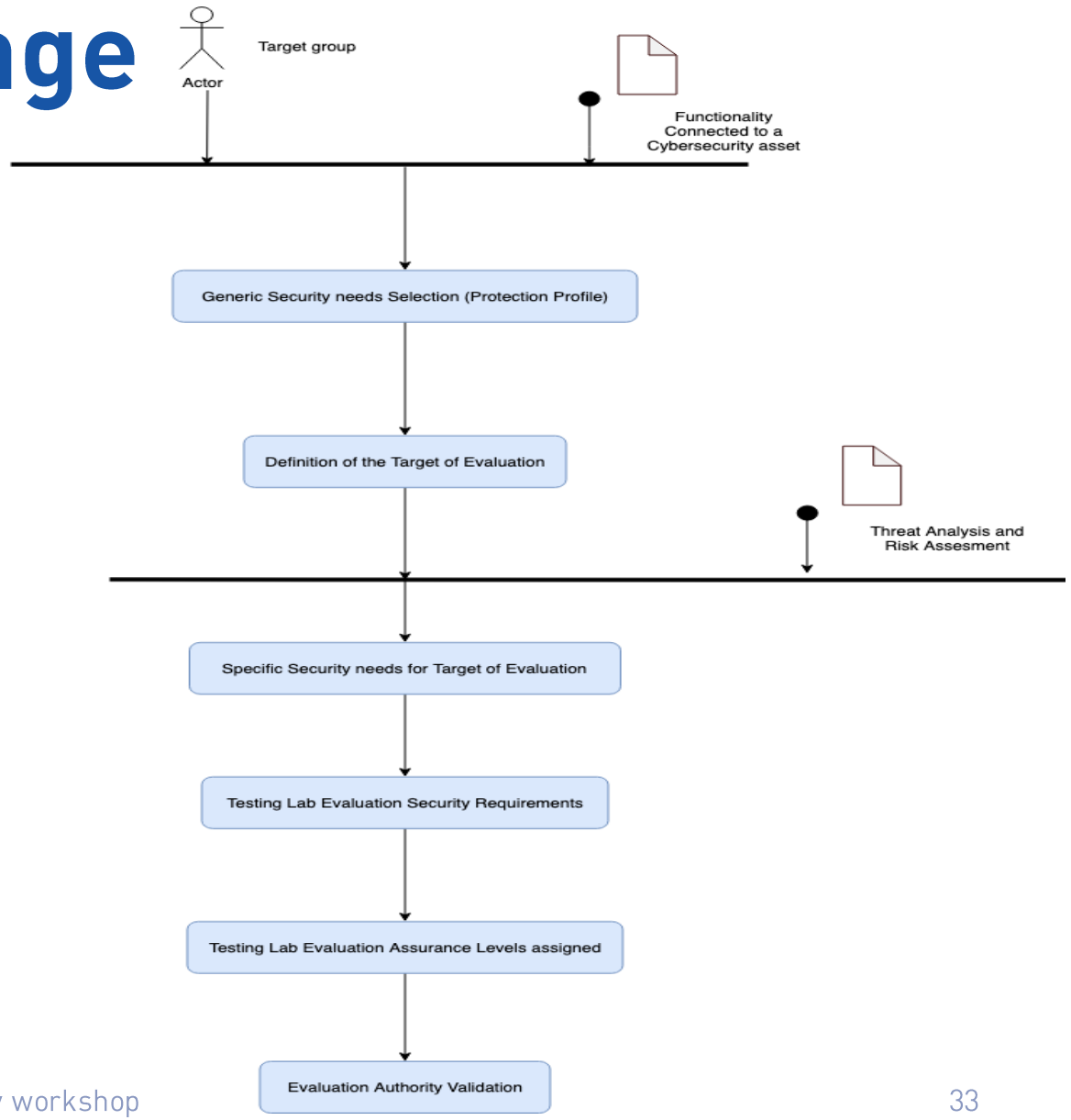
Common Criteria

The Common Criteria for **Information Technology Security Evaluation** (referred to as Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security certification.

Common Criteria is a framework in which computer system users can specify their ***security functional and assurance requirements*** in a ***Security Target*** taking as a reference the selected Protection Profiles. Developers can then implement or make claims about the security attributes of their products, and testing laboratories can evaluate the products to determine if they actually meet the claims.

Common Criteria provides **assurance** that the **process of specification, implementation and evaluation** of a computer security product has been conducted in a rigorous and standard and repeatable manner at a level that is commensurate with the target environment for use.

Cybersecurity coverage



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 coverage

Evaluation methodology

Scope of evaluation (what part of product is evaluated)

Functional requirements (which functions are evaluated)

- Security by construction (defined security function)
- Security by design (consistency between SF)

Assurance requirements (what evidences are evaluated)

- By documentation inspection
- By product testing
- By product vulnerability assessment
- By usage environment analysis
- By development and production environment analysis

Evaluation Methodology (how evidences are checked);

Next steps, cybersecurity framework refinement and testing tool for HEADSTRAT validation.

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

Join at
slido.com
#HEADSTART

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.