Positioning, Communication (V2X) and Cybersecurity

integration of Key Enabling Technologies in a comprehensive assessment methodology

Jacco van de Sluis - TNO

Andrea Steccanella - CRF

Michael Schmeja, Joaquim Maria Castella Triginer – Virtual Vehicle

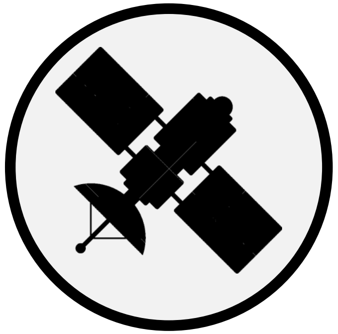
Event rules and process

- ✓ Webinar is being recorded
- ✓ Slides and recording **will be shared** and published on [HEADSTART website]
- ✓ 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.
- ✓ Do not wait until the end of the presentation! If you have questions, just send them to us!

- ✓ Please, avoid using the GoToMeeting chat as your question may not arrive to us

Key Enabling Technologies (KETs) in HEADSTART



Positioning for AD functions

Operational Design Domain extension with absolute (lane-level) positioning

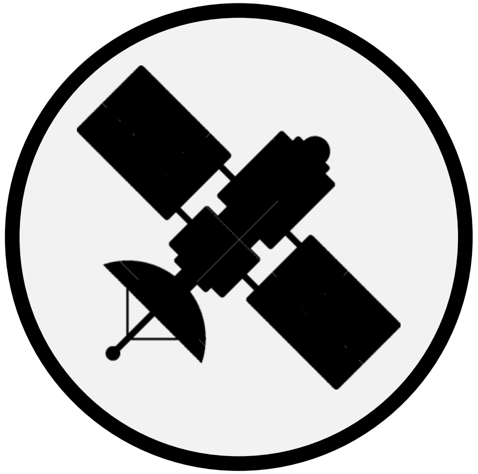
Communication (V2X) for AD functions

Additional information collected from external environment beyond current sensors sensing

Cybersecurity for AD functions

Identification of vulnerabilities capable to compromise the safety functions

Enhance current Automated Driving functions



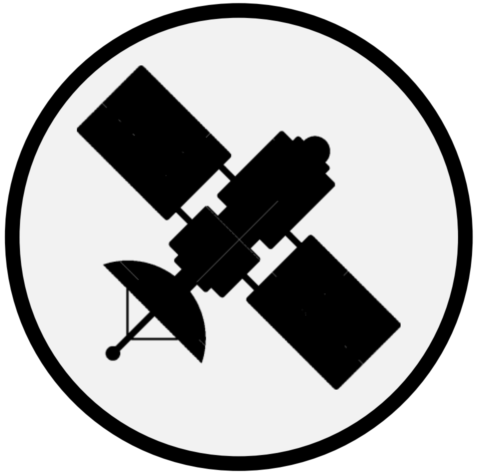
Positioning
Ego-Vehicle
Geo
Localization

Communication
(V2X)
Geo-localized data
from vehicles
& infrastructure

Improve AD functionalities:

- Highway pilot
- Truck platooning
- Traffic jam chauffeur

Enhance current Automated Driving functions



Positioning
Ego-Vehicle
Geo
Localization

Communication
(V2X)
Geo-localized data
from vehicles
& infrastructure

Improve AD functionalities:

- Highway Pilot
- Truck platooning
- Traffic jam chauffeur

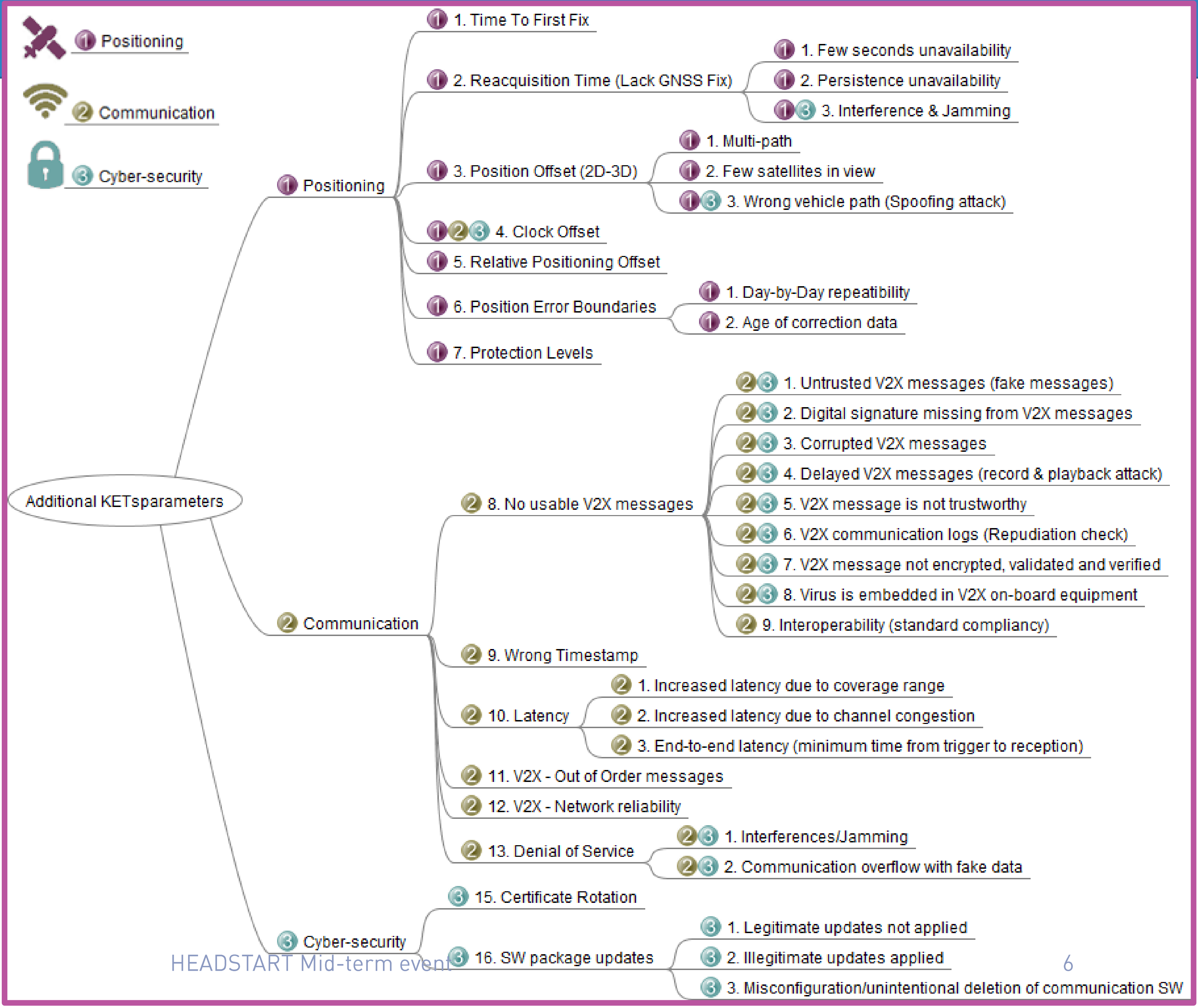
BUT
they rely on (external) data outside the normal vehicle design domain

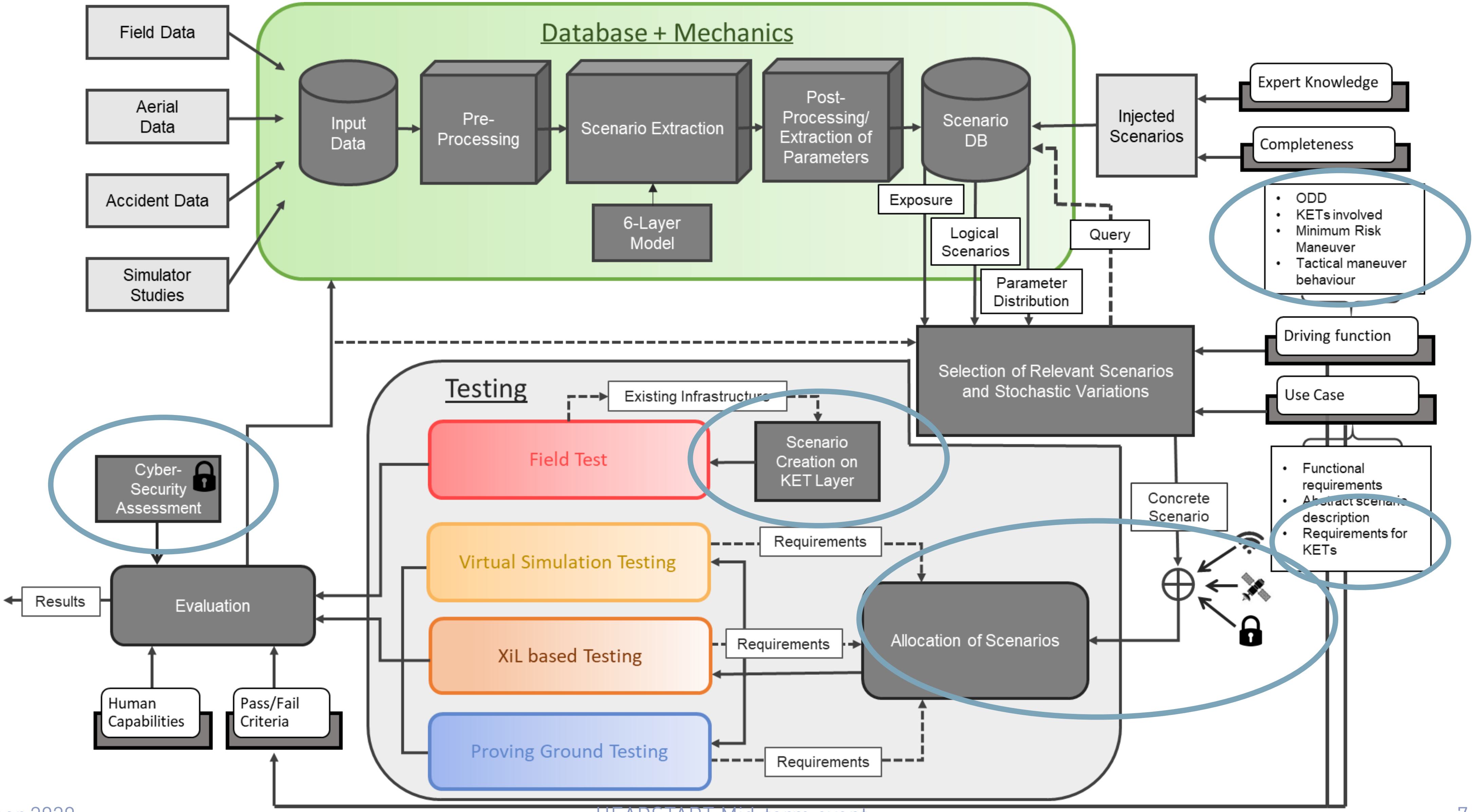
Cybersecurity
Information trust
is crucial

New information channels

New failure possibilities

- Additional parameters in the validation methodology
- Cross-dependencies between these parameters





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
Query
Parameter Distribution
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
XiL based Testing
Proving Ground Testing
Requirements
Requirements
Requirements
Allocation of Scenarios
Concrete Scenario
Functional requirements
Abstract scenario description
Requirements for KETs
Cyber-Security Assessment
Evaluation
Results
Human Capabilities
Pass/Fail Criteria

Positioning integration

1) Virtual Tests
   - Stochastic Variation of positioning parameters starting from Scenario DBs
2) Hardware & Software in the Loop
   - Creation of simulated GNSS/IMU signals starting from GNSS traces

Comparison of driving function performances; Improvement of positioning fidelity testing.

3) Proving Ground
   - Validation of driving function relying on the positioning module in a controlled environment
4) Field Tests
   - Validation of driving function relying on the positioning module in a real-world: interaction with unpredictable obstacles

Extraction of 'positioning profile' from Vehicle under Test

Creation of extended scenario DB

Replicate anomalies into Virtual & XiL test

Challenges for Positioning

✓System & Environment:

- **Functional requirements at vehicle level**
  - Detect and evaluate GNSS uncertainty from the vehicle under test.
- **Technical constrains at vehicle component level**
  - Capability to inject coherent positioning data:
    - GNSS signals: the vehicle under test might require GNSS corrections.
    - Coherence with other in-vehicle data.
- **Technical feasibility**
  - Day-by-day repeatability

✓Methodology, Testing & Assessment:

- **Potential physical constrains on test tracks**
  - A HD map of the test track area must be available.
- **How the technical requirements are expected to be partly verified by computer tools**
  - Capability to compare the performances of different implementations of the same vehicle function.

Communication (V2X) integration

1) Virtual Tests
   - V2X Communication 'as a sensor'
     - 'Simple' versus complex models
       - Logical testing: example V2X message exchange as part of platooning interaction protocol
     - Ideal, probabilistic, physical sensor models
2) Hardware & Software in the Loop
   - Communication software stack up to complete communication units (multiple radio technologies)
   - Include in scenarios the relevant 'V2X events'
     - communication loss, delays, errors
     - at application level (CAD under test): should detect and act accordingly
3) Proving Ground
   - Identification of V2X Communications anomalies in real-world (controlled environment)
   - Smart infrastructure, I2V deployment for logging, for generation of 'V2X events'
4) Field Tests
   - Identification of V2X Communication anomalies in real-world (interaction with dynamic environment)

Creation of extended scenario DB, includi ng V2X messages

Challenges for Communication (V2X)

✓ System & Environment:

- Functional requirements at vehicle level
  - Connected infrastructure, e.g., traffic lights, should be able to communicate through different technologies.
- Technical constrains at vehicle component level
  - The radio system must support high connection density for congested traffic.
- Technical feasibility
  - V2X is still in being developed and devices meeting the 'requested requirements' may not be available

✓ Methodology, Testing & Assessment:

- Safety requirements
  - A vehicle must be able to reach a safe state if it has a critical failure (eg. loss of V2X communication).
  - To ensure safety when testing of non-deterministic algorithms (e.g. High-speed Truck Platoon and AI).
- How the technical requirements are expected to be partly verified by computer tools
  - Tooling should be able to define and re-use test sequences of V2X messages
- Potential physical constrains on test tracks
  - With V2X Communication testing in open air, no other radio transmission must influence the testing.
  - Limited/blocked radio coverage

Cybersecurity integration

Cybersecurity testing:

Asset identification (Target of Evaluation definition)

TARA analysis (and generic threat list) -> Threat list

Selection of security requirements to test

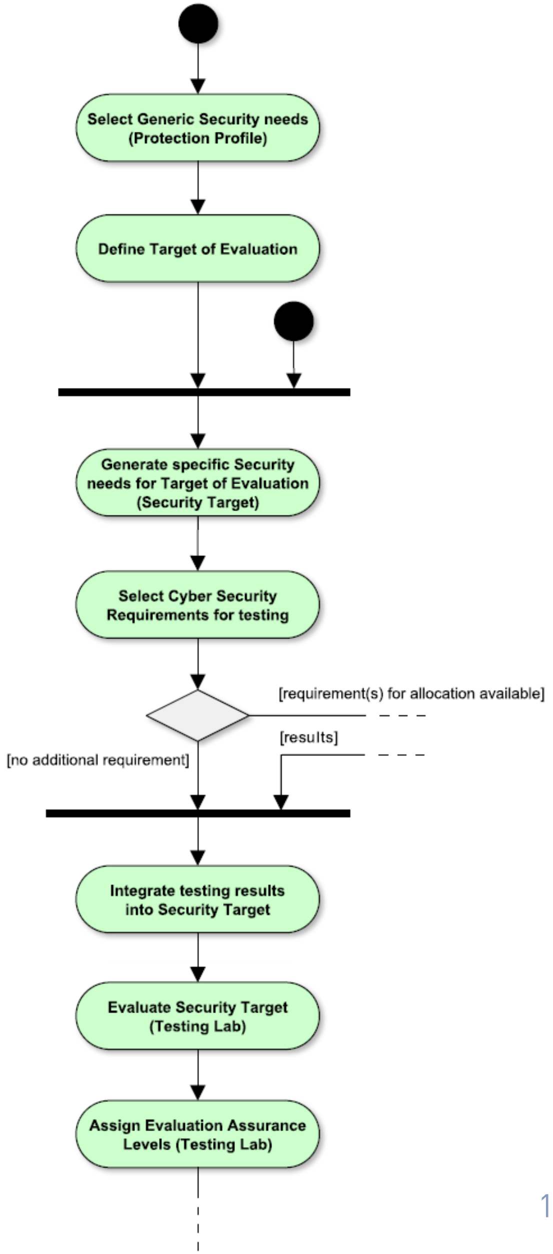
Preparing security scripts for different test scenarios

Performed cyber security testing (e.g. Penetration testing, Fuzz testing,...)

1) Virtual Tests
2) Hardware & Software in the Loop
3) Proving Ground
4) Field Tests

Cybersecurity integration

- ✓ Cybersecurity assessment:
  - ✓ For the entire lifecycle
  - ✓ For safety validation
- ✓ Cybersecurity assessment:
  - ✓ Identifies generic security requirements for a group of security devices (Protection profile)
  - ✓ Description of the Target of Evaluation (TOE)
  - ✓ Generation of specific needs for the target of evaluation (Security Target)
  - ✓ Selection of cybersecurity requirements for testing
  - ✓ Integration of the testing results into the Secure Target
  - ✓ Evaluation of the Security Target
  - ✓ Assignment of the Evaluation Assurance Levels (EALs)



Challenges for Cybersecurity

✓ System & Environment:

- Functional requirements at vehicle level
  - V2X message reception shall be signed by a trusted third-party (message shall have valid and verified certificate and signature).
  - Adopt high levels of Confidentiality, Integrity and Availability.
- Technical constrains at vehicle component level
  - Measures should be applied for all components in the system (e.g. vehicles involving network and infrastructure) to ensure an end-to-end cybersecurity
- Technical feasibility
  - Cybersecurity in the system has been developed following existing best practices for cybersecurity.
  - Sensitive to attack GNSS systems in non-shielded environment.

✓ Methodology, Testing & Assessment:

- Safety requirements for road-users
  - Cybersecurity must protect the road-users and vehicle occupants from intentional attacks
- How the technical requirements are expected to be partly verified by computer tools
  - Cybersecurity framework tool to support the entire lifecycle of the vehicle
  - Performed cybersecurity testing (e.g. TARA analysis, Penetration testing, Fuzz testing)
- Potential physical constrains on test tracks
  - Potential cyberattacks shall be dually analysed; from the "Defenders" and the "Attackers" point of view.

Example: Truck Platooning Use Case

Two or more cooperative trucks driving together in a line, maintaining a close distance enabled by vehicle-to-vehicle (V2V) communication

✓ Relevance for:

- Communication (V2X)
- Positioning (GNSS)
- Cybersecurity

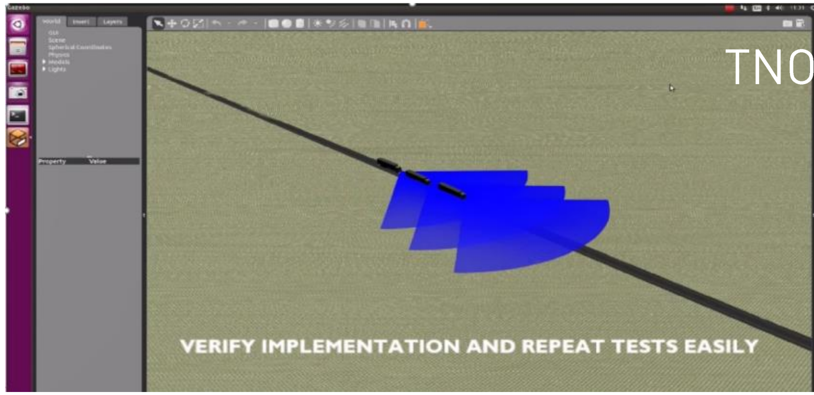
✓ Functional requirements

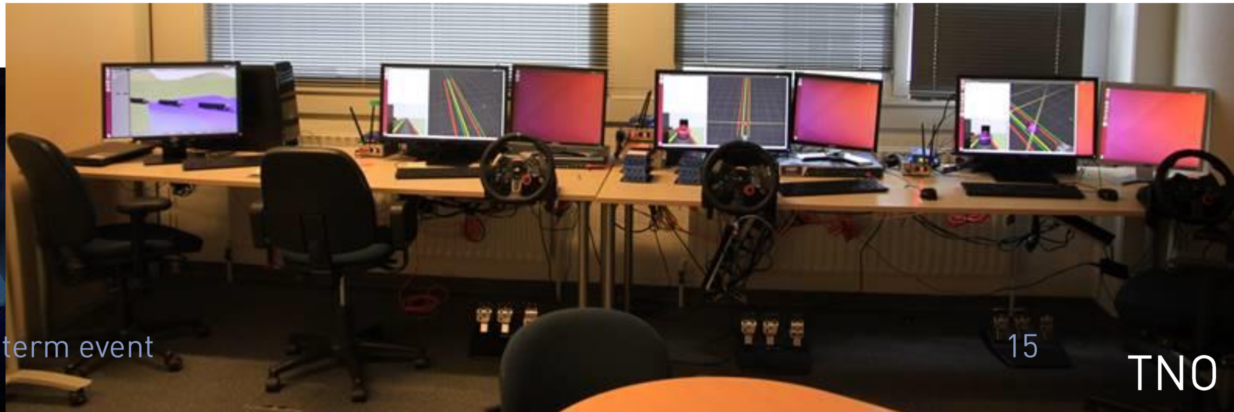
- Operation Design Domain (ODD)
- Object and Event Detection and Response (OEDR)
- Tactical manoeuvre behaviour

KET parameters are modelled and integrated into testing scenarios

- Virtual testing
- Hardware/Software in the Loop
- Proving Ground
- Field testing

Secure Assurance Framework implementation





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

Thank you!

Any questions?

Communication (V2X)
Jacco van de Sluis
TNO Automotive
Jacco.vandesluis@tno.nl

Cybersecurity
Joaquim Maria Castella Triginer
Virtual Vehicle Graz
joaquim.castellatriginer@v2c2.at

Positioning
Andrea Steccanella
CRF
andrea.steccanella@crf.it