



1st KETs workshop

Methodology for the validation of KETs in the context of CAD

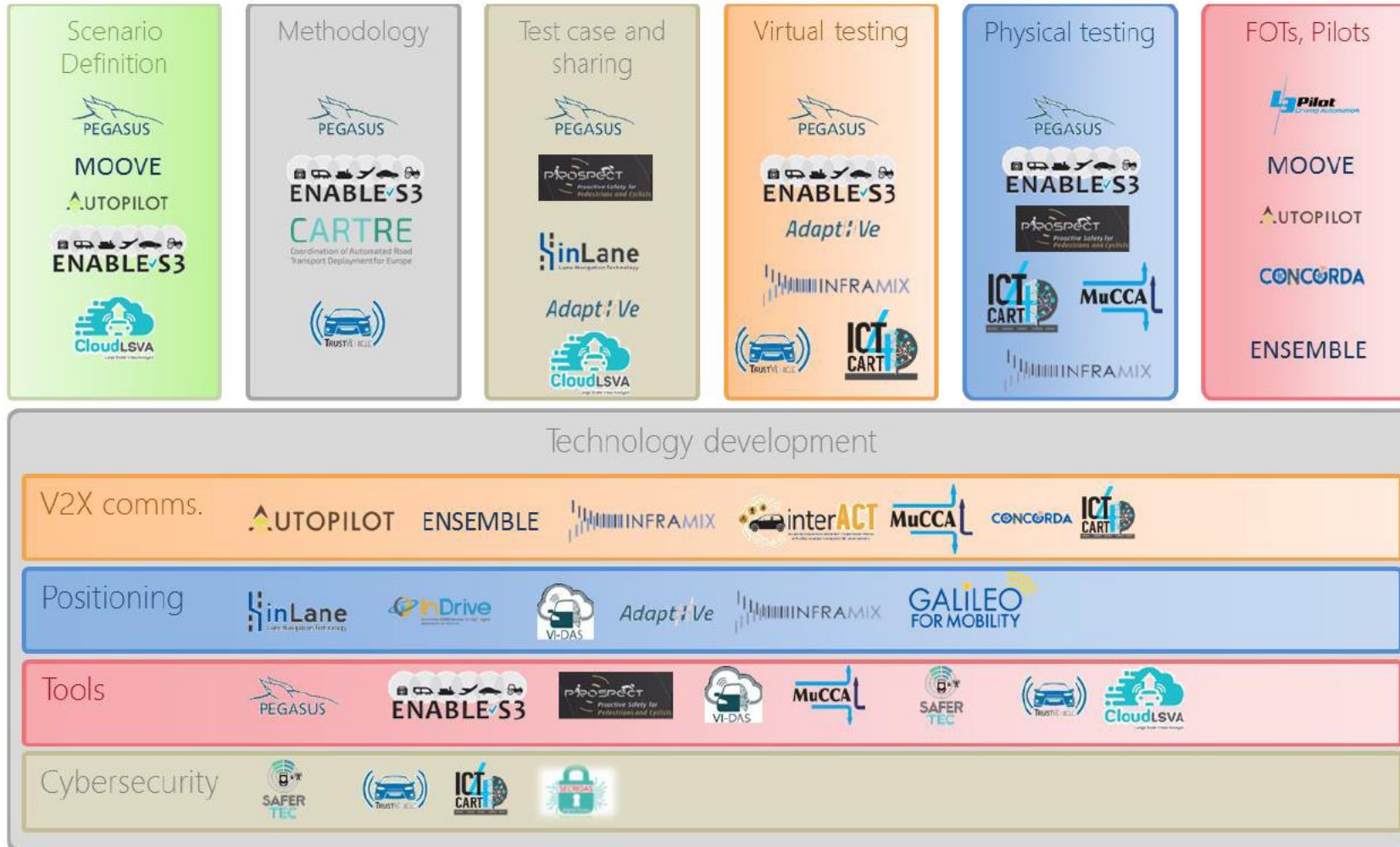
Andrea Steccanella, CRF



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



HEADSTART: built upon ongoing activities



Project liaisons in the original proposal:
28 projects



36 projects available in current list

WP5 – all project duration:

EXPERT GROUP PARTICIPATION

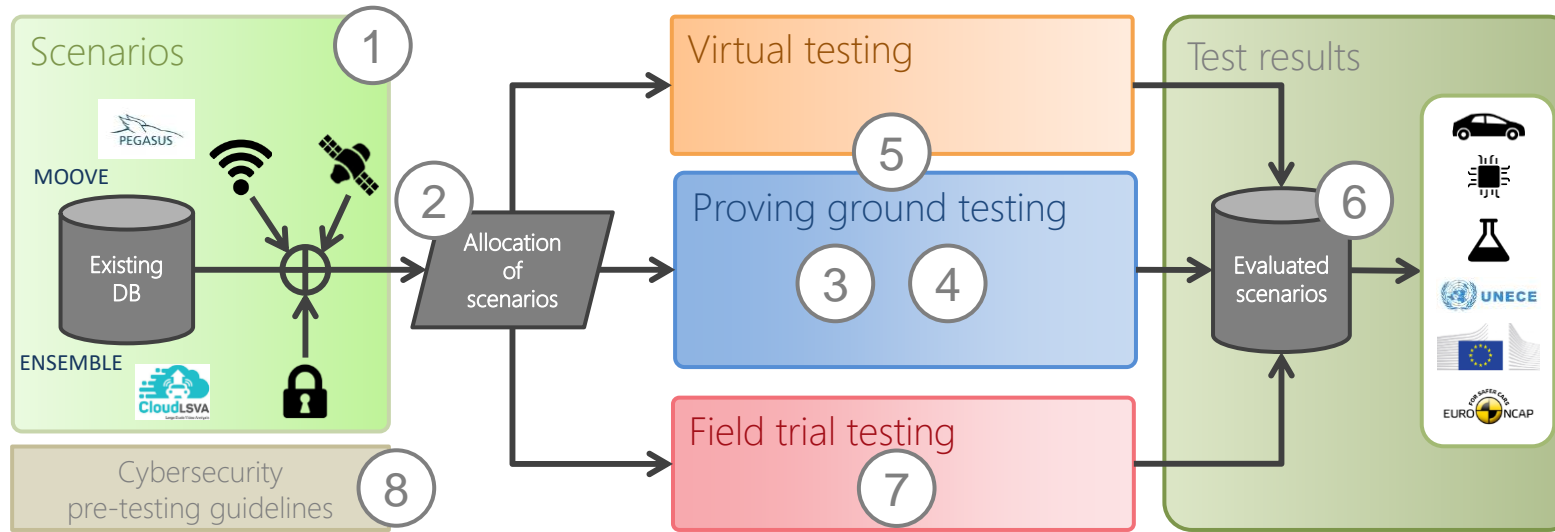
- Join as associated partner and our expert group
- Join the discussion group of your interest:
 - **Cyber-security**
 - **Communications (V2X)**
 - **Positioning**
 - Scenario selection
 - Consumer testing (NCAP)
 - Type approval
- Provide needs and requirements and evaluate project (intermediate) results

Three Key Enabling Technologies

Work together on:

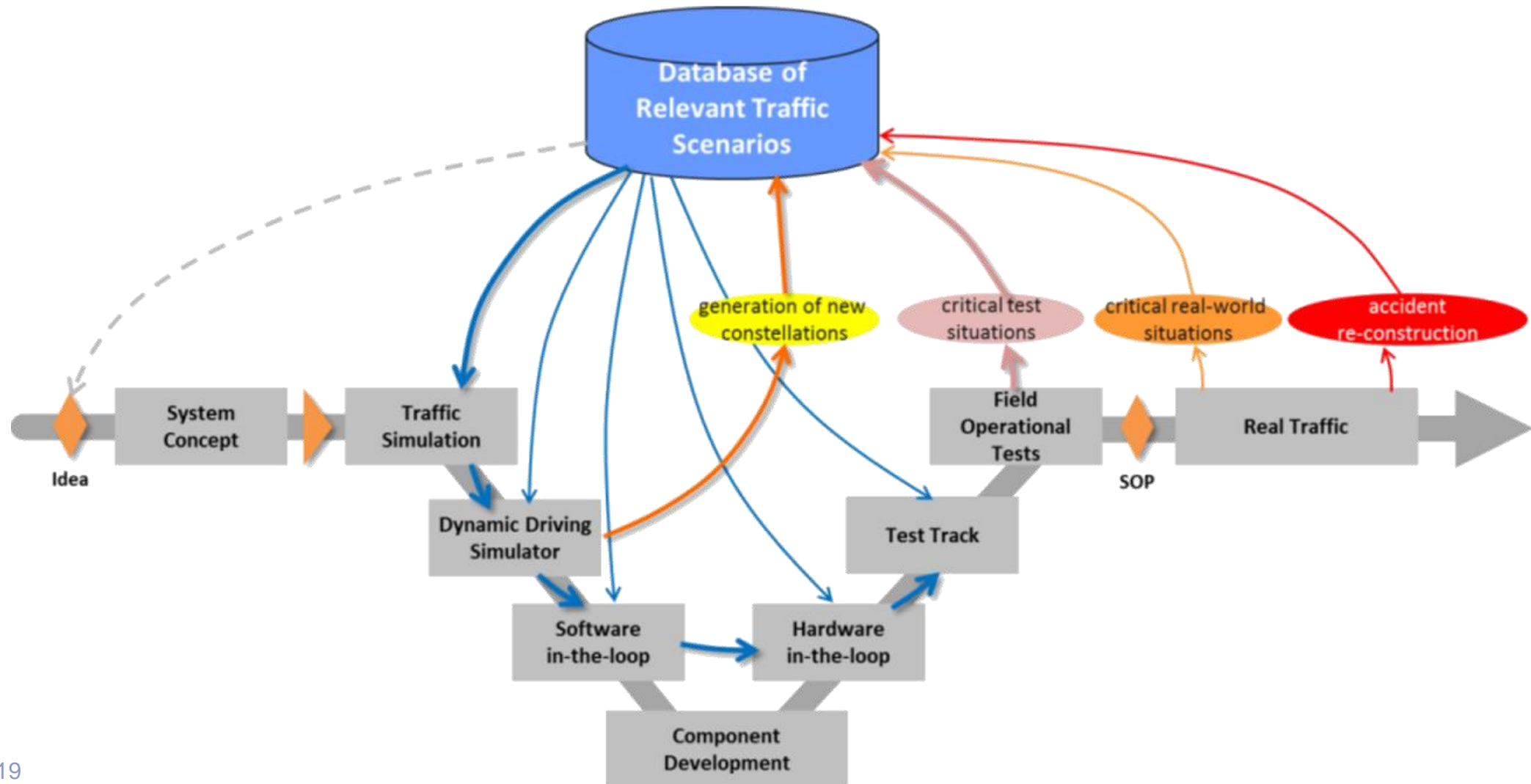
- ✓ Joint cooperation between projects for testing validation and certification purposes
- ✓ Align your project with the harmonized methodology and tools developed within HEADSTART
- ✓ Become one of our use cases!

Project's Concept



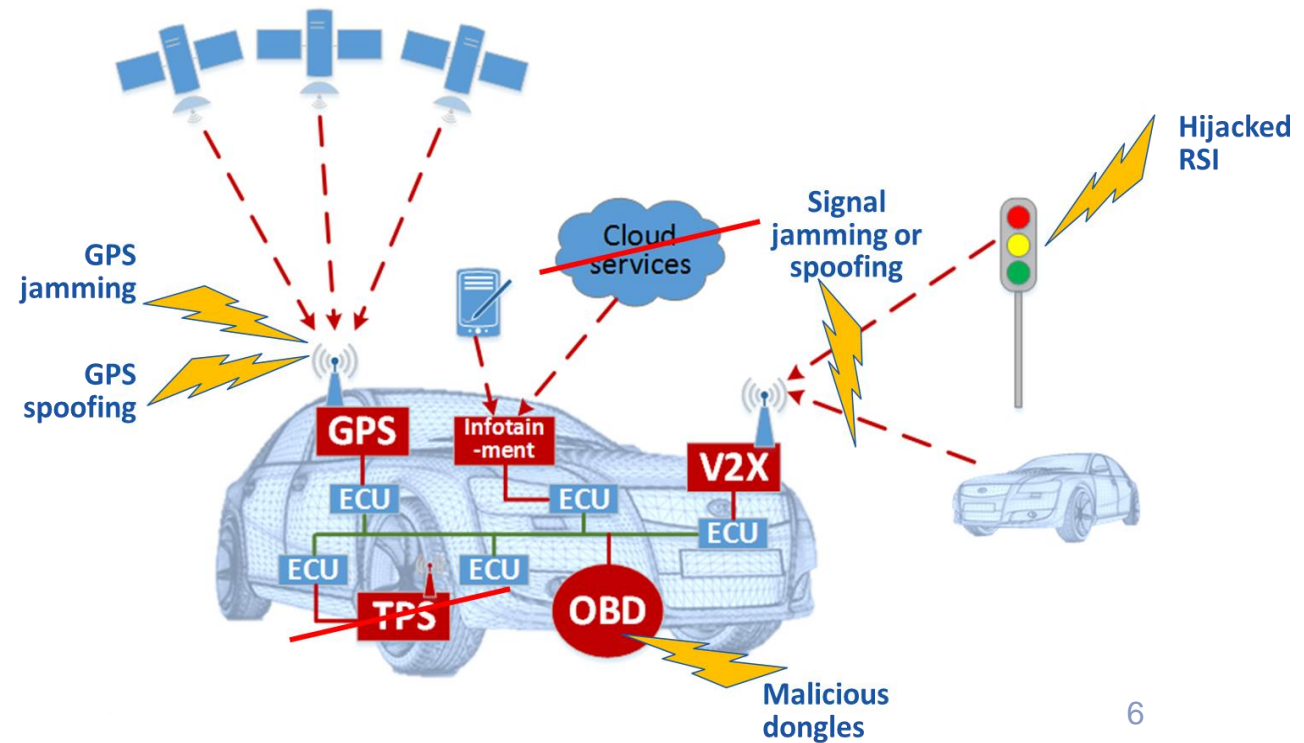
- ① Integration of positioning, communications and cyber-security in CAD test scenarios
- ② Comprehensive procedure for the allocation of test cases per testing platform
- ③ Selection criteria and specification for proving ground test scenarios taking into account criticality
- ④ Proving ground testing 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

HEADSTART approach



Motivation for the KETs

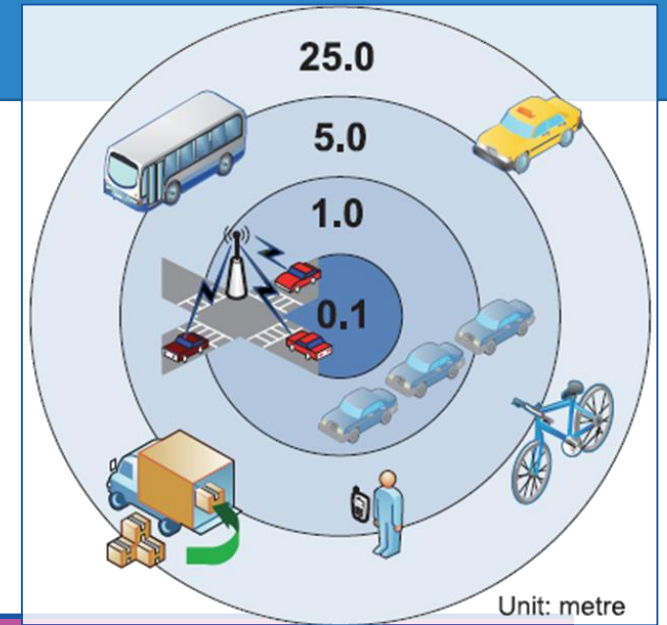
- HEADSTART will enhance current Connected Automated Driving (CAD) testing methods dealing with cyber-security, V2X Communications and Positioning.
- Digitalization of the automotive industry is the main enabler for technologies such as V2X communication and High Precision Positioning, key for CADs functions but at the same time pose a great challenge in terms of cyber-security.
- HEADSTART will deliver new testing procedures and tools for assessing connected and automated vehicles to guarantee safe operations in every condition.
- Strong interconnections on the other two KETs (Positioning & Communication) as they are both potential sources for attacks



What we mean by KETs in HEADSTART

- Positioning for CAD functions
 - ✓ Detection systems able to improve CAD safety
 - “relative” & “absolute” positioning systems
- Communication for CAD functions
 - ✓ Additional information collected from external world that cannot be directly senses by current sensors
 - Vehicle to Vehicles (or Infrastructure) Communication via ETSI ITS-G5 or Cellular-V2X (LTE-V2X or 5G-PC5)
- Cyber-security for CAD functions
 - ✓ Identification of failures capable to compromise the safety of CAD functions

The need for “Positioning” for road user services



Services			Acceptable value
GNSS only	Trip travel information	Stolen vehicle recovery	25 meters (95% confidence)
	Fleet management	Dynamic route guidance	
	In-car navigation	Emergency call	5 meters (95% confidence)
	Urban traffic control	Road-user charging	
Integration with other sensors mandatory	Intelligent Speed Adaptation (ISA)	Collision avoidance	1 meters (95% confidence)
		Restraint deployment	
	Automated highway	Lane control	0.1 meters (95% confidence)

HEADSTART objective

International standard are emerging:

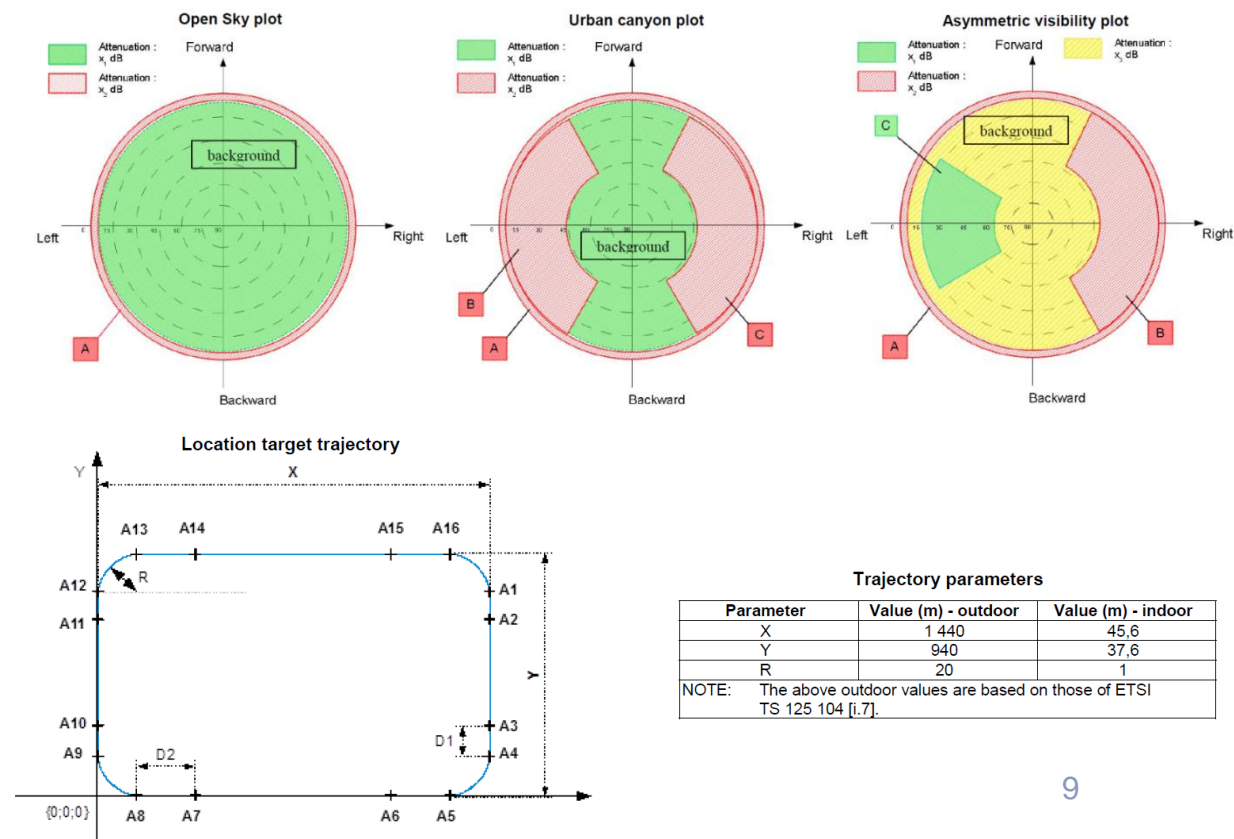
- CEN/CENELEC, EN16803: “Use of GNSS-based positioning for road Intelligent Transport Systems (ITS)”,
- ETSI TS 103 246 1-5: “Satellite Earth Stations and Systems (SES), GNSS-based Location Systems (GBLS)”.

✓ Sky attenuation conditions:

- Model definition for:
Open-sky, Urban canyon,
Asymmetric sky visibility.

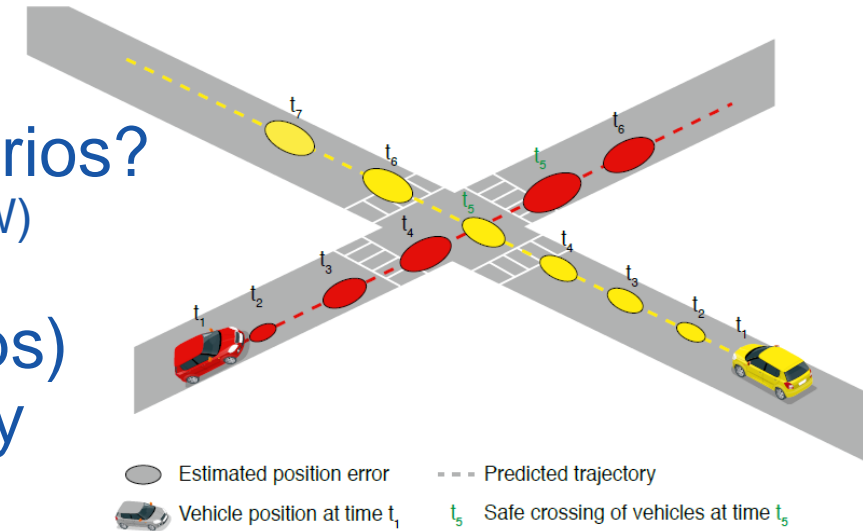
✓ Moving Location Target Scenario - Track trajectory

- Simulated trajectory to assess the positioning performances.



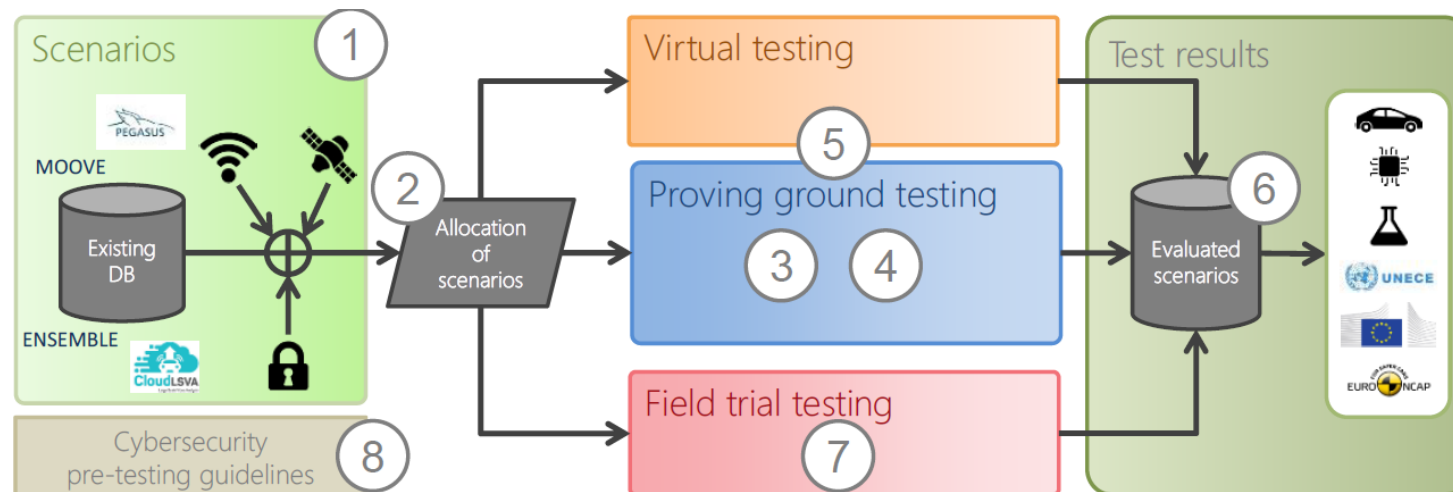
What's missing?

- A unified testing methodology able to represents real environment conditions based on virtual scenarios for Connected Automated Driving (CAD) functions
 - ✓ What happen to GNSS signals in critical scenarios?
 - ETSI TS 101 539-2 V2X Intersection Collision Risk Warning (ICRW)
 - ✓ How vehicle sensors (camera, radar, lidar, maps) can be modeled into the testing methodology to improve the positioning performances?
 - ✓ How to compare solutions relying on different positioning architectures?



HEADSTART approach

- Starting from a database of CAD scenarios;
- Include the environmental conditions into the communication channel and perception layers of the device under test:
 - ✓ GNSS: introduce range errors due to environment conditions (urban canyons, interference levels).
 - ✓ Camera: obstruction of lane marking information.
 - ✓ Others...



Goals for *V2X Communication*

- In HEADSTART available V2X communication technologies will be analysed and elaborated:
 - ✓ ETSI ITS-G5 - IEEE 802.11p,
 - ✓ Cellular C-V2X: LTE-V2X→3GPP Rel.14, 5G-V2X→PC5
- Relevant use cases for V2X communication for CAD are being identified based on use cases from other projects.
- Transfer V2X testing and assessments methods, tools and approaches and adapt it to the specific needs of the CAD functions testing methodology

V2X based assessment means?

What do we want to assess? What can we assess?

■ Low-level communication functions:

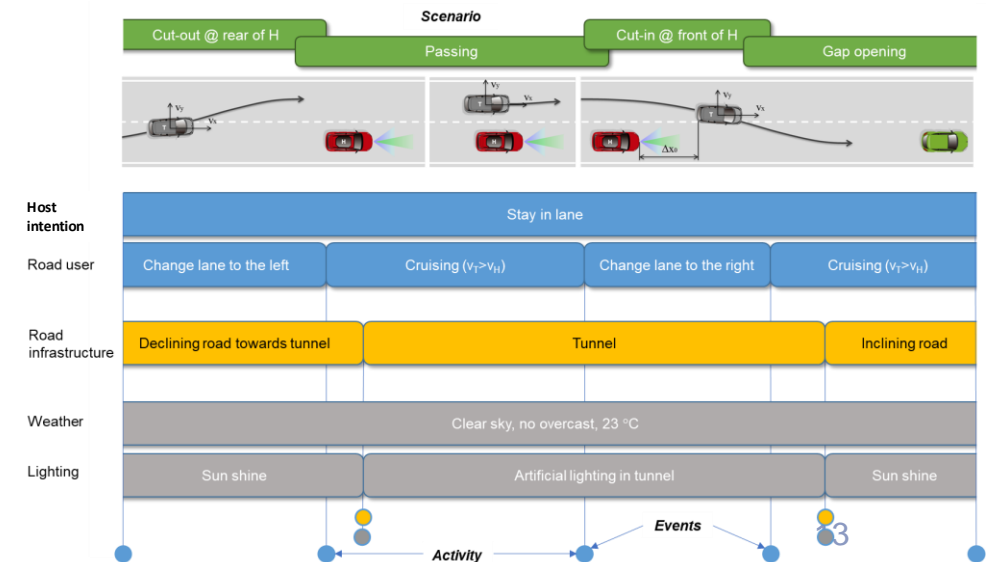
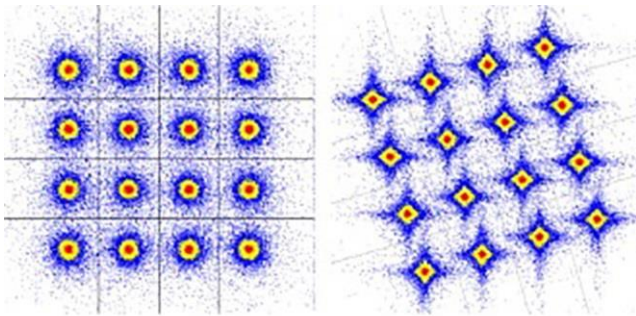
✓ Propagation/physical layer/media related

- Propagation: LoS aspects, reflections, scattering, delays, path loss
- Channel: availability, contention, congestion
- SNR, BER
- Encoding/decoding delays/errors

✓ High-level communication functions:

■ Application level

- Logical testing
- Event based, sharing intentions, interaction protocol

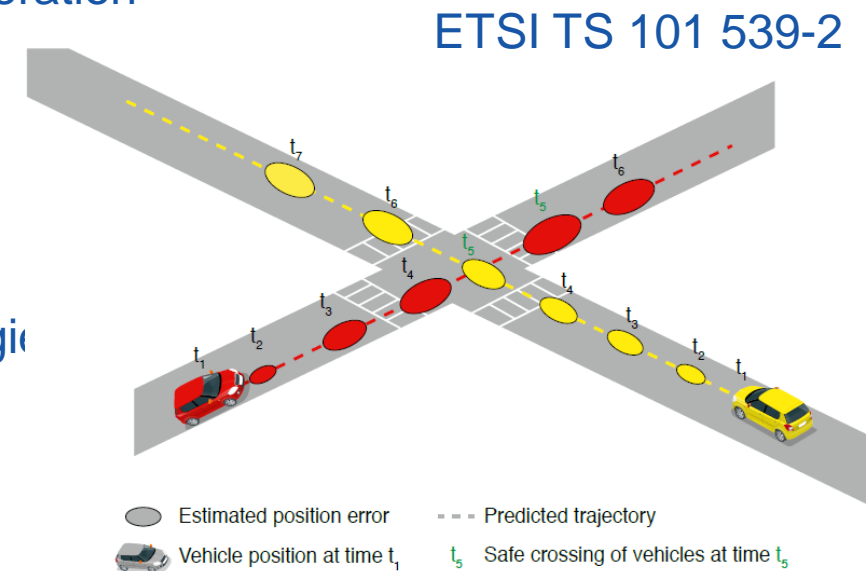


V2X communication approach

- Creation and use of Expert Network:
 - ✓ Consultation with stakeholders from the industry, research and standardization bodies to identify strengths and weaknesses of current V2X communication systems and their performance.
 - ✓ Lessons learned and knowledge transfer: adapt procedures successfully used in other domains, other project.
- Integration of V2X communication into CAD scenario tooling
 - ✓ Define operational settings and metrics for V2X communication (ongoing)
- V2X testing in HEADSTART
 - ✓ Use case(s) allowing to apply developed V2X communication assessment tests

V2X extension for scenario assessment


- Can we make this generic within one V2X Communication assessment scenario
 - Will we always need more specific communication scenarios depending on:
 - ✓ Type of application, type of deployment
 - ✓ RF-Obstacles: Urban, Non-urban, Highway
 - ✓ Number of vehicles to be simulated
 - ✓ Channel degradation
- Scalability problems in RF-simulation generation
- Multiple connected vehicles communicating (V2V)
 - ✓ System-of-system (multiple vehicles: Platooning application)
 - ✓ Multiple radio systems (ETSI ITS-G5, Cellular-V2X, new technologies)
 - ✓ Mixed traffic conditions: unequipped vehicles
 - How to integrate existing tools?
 - ✓ Radio simulators, Network simulators, Application simulators, Traffic simulators.




Cybersecurity Motivation

Digitalization of CADs features imposes to car makers to protect the vehicles against Cyber attacks.


- Connected vehicle provides opportunities for a malicious hacker to disrupt normal vehicle operations without the need of direct access into the car

 The attacks can range from annoyances:

- ✓ Sounding the horn,
- ✓ Turn on the radio.

 To small damages and anomalies into car operation:

- ✓ Collision at slow speed during parking manoeuvre,
- ✓ Malfunctioning fuel pump.

 But can impact on the safety of the car:

- ✓ Turning the steering wheel at high speed,
- ✓ Perform harsh braking.



Cybersecurity in HEADSTART terms

✓ What are the possible cyber threats?

- Define the potential threats and types of attacks that directly affect CADs

✓ What are potential consequences of cyber attacks?

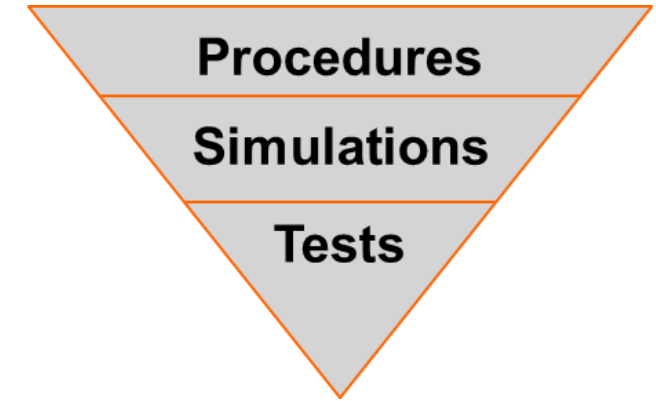
- different kind of consequences which can be triggered directly or indirectly by attackers
- In HEADSTART potential consequences of driving function fails are most important

Source: Cyber Security Threats of Connected Vehicles – Consequences and safety solutions, Dr. Housseem Abdellatif, TÜV SÜD



- ✓ Standardization on cyber-security ongoing but not focused specifically to CADs functions yet: EU Cyber-security Act, SAE J3061 "Cybersecurity Guidebook for Cyber-physical systems", ISO/SAE 21434 "Road vehicles – Cybersecurity engineering"

Cybersecurity approach 1/2



- Following functional safety approach
 1. Well defined development process (e.g., ISO 26262 for safety)
 - Risk/vulnerability assessment covering a wide range
 2. Simulations (on component level) targeting several scenarios and test cases
 3. Physical/real tests: a set of specific tests carried out on vehicle level
 - For safety: “Handful well-defined tests → vehicle safe”
 - Same approach for cybersecurity?
- Lessons learned and knowledge transfer
 - ✓ Adapt procedures successfully used in other domains; learn from best practices from ICT
 - ✓ Analyse security known flaws
- Cybersecurity testing in HEADSTART
 - ✓ At least one Use case allowing to apply developed cyber-security assessment procedures/tests

Cybersecurity approach

Security goals
are categorized in:

- ✓ Integrity
- ✓ Authenticity
- ✓ Availability
- ✓ Confidentiality

Examples for Security Controls				L3 & L4 functions	
Security Goal	Environmental Level Security Controls	Vehicle Level Security Control	Component Level Security Controls		
Integrity	<ul style="list-style-type: none"> Integrity management of access rights 	<ul style="list-style-type: none"> Secure communications, TLS, IPsec, etc. Functional separation and a trusted execution of the control flow 	<ul style="list-style-type: none"> Access control Control flow integrity (CFI) Trust anchor 		
Authenticity	<ul style="list-style-type: none"> Access control to development and production sites Secure communications 	<ul style="list-style-type: none"> Message authentication codes etc. 	<ul style="list-style-type: none"> Secure boot with a trust anchor, e.g. public keys in OTP 		
Availability	<ul style="list-style-type: none"> Intrusion detection mechanisms to react to potential attacks 	<ul style="list-style-type: none"> Congestion control on gateways/routers 	<ul style="list-style-type: none"> Rate limiting on networking interfaces Deterministic scheduling 		
Confidentiality	<ul style="list-style-type: none"> Access control to documentation 	<ul style="list-style-type: none"> Encryption of data in flight TLS, IPsec, etc. 	<ul style="list-style-type: none"> Encryption of data at rest Secure storage 		

Source: Safety First for Automated Driving, White Paper, Aptiv et.al.

Exploitation of the initiatives: SAFERtec project

- Cyber-security insights from SAFERtec project
 - Attackers do not have physical access on the Infrastructure
 - Distinction on communication: roadside units vs cloud-based services
- Identification of threats via the ETSI TR 102 893 TVRA Method (Threat, Vulnerability and Risk Analysis)

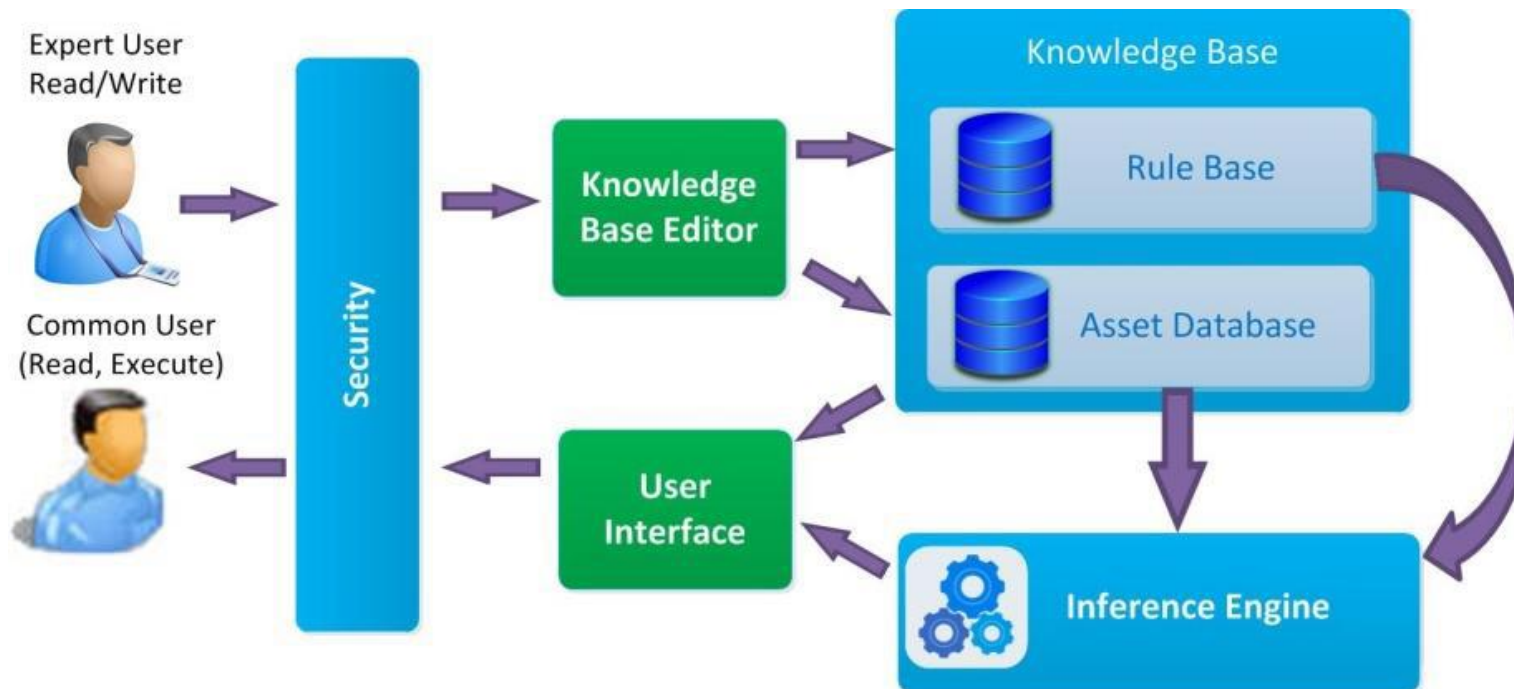
- Threats from SAFERtec

Electromagnetic communication interference disturbance (intentional)
Link layer flooding
Equipment spoofing
Data manipulation
Data leakage
Sabotage
Firmware/Application alteration
Firmware/Application reverse engineering
Extreme solicitation
System unauthorised access

Network unauthorised access
Downgrade attack on the mobile communication link
Data breaches
Account hijacking
Advanced persistence threats
Abuse of cloud services
Data loss
Malicious Insider

SAFERtec Assurance Framework Toolkit

- SAFERtec will provide a security Assurance Framework Toolkit by December 2019
 - ✓ Are there any other similar tools already available?
 - ✓ How can they be optimally used for HEADSTART?



KETs discussion groups

■ Positioning

- ✓ The need for “Absolute Positioning”
- ✓ Localization assessment for automotive

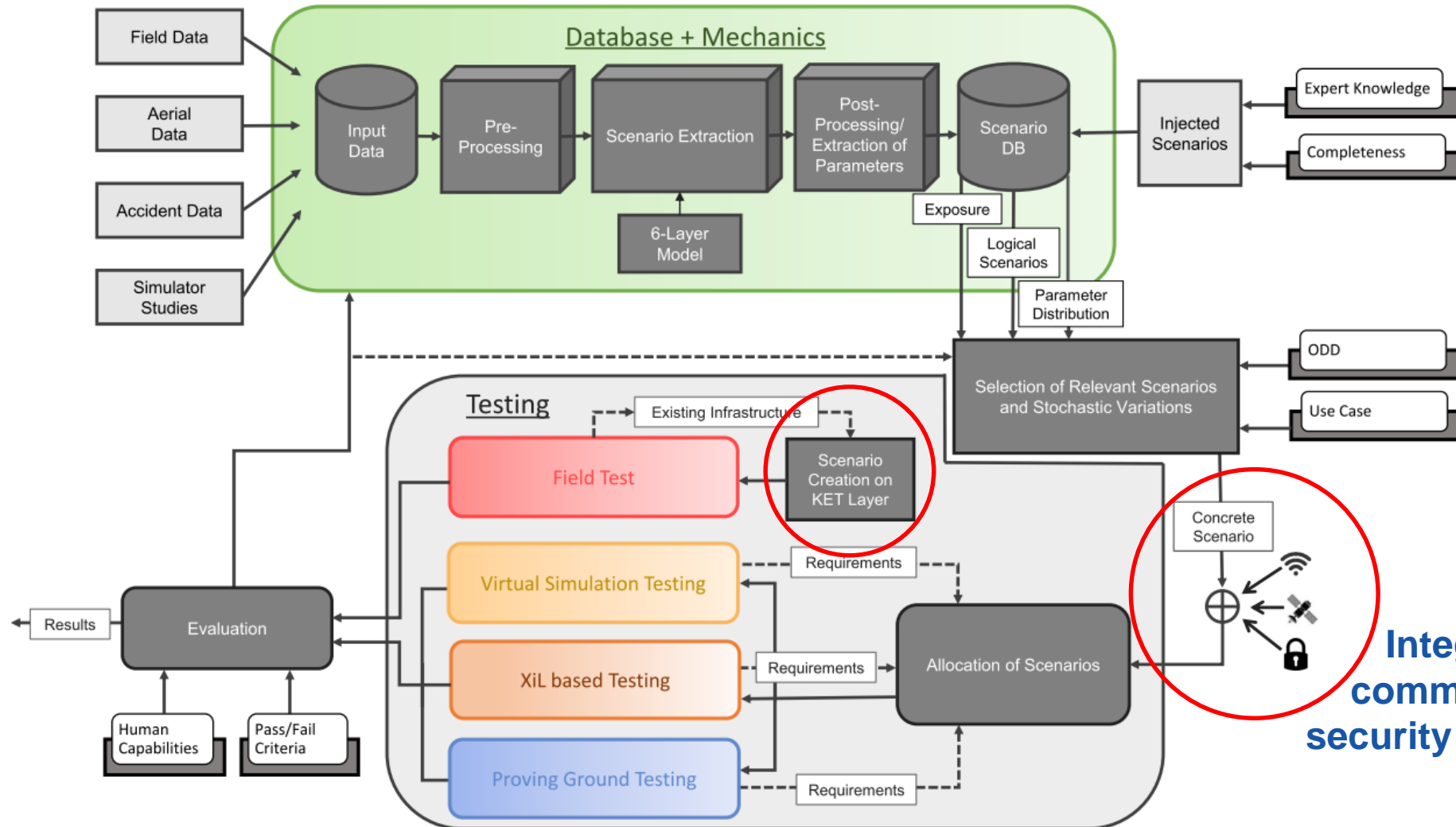
■ Communication

- ✓ Is V2X communication becoming reality?
- ✓ Simulation environment and tools: HEADSTART integrated approach

■ Cyber-security

- ✓ Cyber-security for other CADs functions assessment
- ✓ Potential approaches for HEADSTART procedures

Definition of an Overall Methodology



Integration of positioning, communications and cyber-security in CAD test scenarios