Paper ID 745

Technical and functional requirements for V2X communication, positioning and cyber-security in the HEADSTART project

Martin Skoglund[1*], Anders Thorsén[1], Alvaro Arrue[2], Jean-Baptiste Coget [3] Mohamed-Cherif Rahal [3], Camille Plestan [3]

1. RISE Research Institutes of Sweden, Sweden, * martin.skoglund@ri.se
2. Applus+ IDIADA, Spain, alvaro.arrue@idiada.com
3. Institut VEDECOM, France

Abstract

Connected and Automated Driving (CAD) features rely on several key technologies to function safely at the vehicle and component level. HEADSTART (Harmonised European Solutions for Testing Automated Road Transport) is a research project funded by the European Union that aims to define testing and validation procedures for CAD features with a focus on three Key Enabling Technologies (KETs): Vehicle-to-everything (V2X) communication, Positioning and Cyber-security. This paper presents the technical and functional requirements for these three KETs, including what is needed for these technologies to work correctly (at vehicle and component level) and what is needed to verify and validate them in proving ground and simulation environment. The final aim is to satisfy the safety requirements to protect the vehicle itself and the other road users.

Keywords: Connected and Automated Driving (CAD), V2X Communication, Positioning, Cybersecurity, Testing

Introduction

The purpose of the HEADSTART project is a harmonisation of existing testing and validation approaches. The project develops and demonstrates a methodology for testing and validating CAD, which builds upon existing initiatives and includes testing and validating three identified KETs (communication, positioning, and cyber-security). A scenario-based approach is used, throughout the whole methodology and toolchain, from input data to test validation. Moreover, the main goal is the harmonisation of existing other efforts in the area. The project aims to develop procedures to identify which scenarios to test and what testing environment should be performed. As physical testing is the most expensive and time-consuming to perform, procedures to select which scenarios to test is developed based on the representativeness of the scenario.

The overall concept of HEADSTART as described in the application is shown in Figure 1. Building from existing scenario descriptions for CAD functions currently under development in other initiatives, HEADSTART enhances them by including Vehicle-to-everything (V2X) communication, positioning, and cyber-security. In addition, HEADSTART includes KETs in the generally accepted scenario creation and definition process and addresses user group-specific requirements that impact the scenario descriptions. The considered user groups are categorised as Development testing, Consumer testing and Type approval testing.

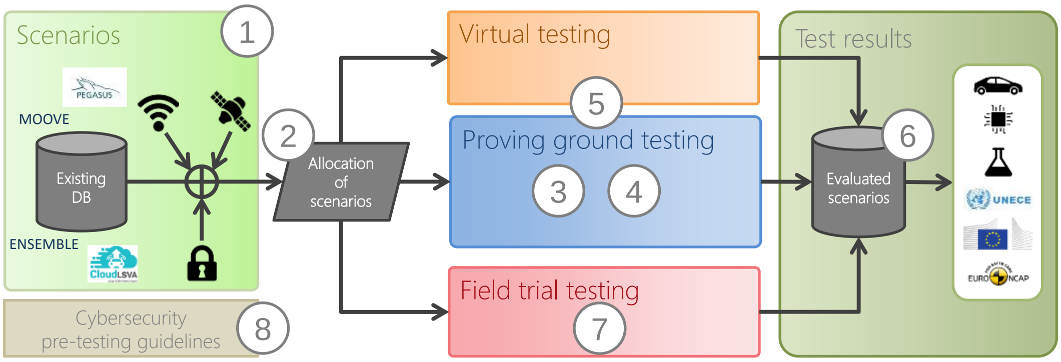

Figure 1: HEADSTART concept based on the Pegasus approach (simplification)

As part of the activities within the project, an assessment of the State-of-.the-Art was performed in different domains: scenario-based validation methodologies, e.g. KETs, regulation, consumer testing.

The HEADSTART project has been funded by the European Union under the H2020 funding program (Grant No. 824309). For more information on the project, please visit the webpage (https://www.headstart-project.eu/).

Requirements for KETs

An essential part of HEADSTART project work is identifying and collecting key enabling technologies (KETs) to achieve safe automated functions. Initial gap analysis showed that the KETs are excluded in most state-of-the-art approaches and scenario concepts. Projects are dealing with cyber-security, but these approaches do not include the entire chain of safety assurance with a scenario database. A three-step approach was used to identify the requirements for these KETs; **(1)** ongoing activities in standardisation organisation and similar were investigated, **(2)** a series of interviews, surveys and questionnaires with various stakeholders (e.g., OEMs, Tier 1 suppliers, Regulatory entities) were performed to identify user needs, and **(3)** collect requirements and needs from other identified relevant research projects.

Standardisations efforts are ongoing for all three KETs. For V2X communication, there are many activities, and for testing specifically, it involves organisation like 3GPP, 5GAA, ETSI, GCF, IEEE, OmniAir, SAE, C-ITS, C-SAE and NTCATS. Testing equipment vendors are also active in designing instruments for V2X testing; most also address GNSS testing. Positioning is more differentiated since many different technologies are included, but GNSS standardisation is ongoing in ETSI and testing equipment vendors works actively with GNSS. Cybersecurity is challenging since it involves defence against techniques that may not be understood when the system is created. It is recommended to follow published best practices, including recommended testing. SAE and ISO jointly work with standardisation activities targeting vehicle cyber-security [12].

The **survey of the stakeholders needs** revealed a mixture of high-level and low-level user needs. For the responders, Communication and Positioning were higher ranked than Cyber-security, but that may more reflect the personal interest of the responders and what phase in the development cycle they are currently engaged. The main interest relates to verification and validation. The **project's analysis** revealed many specific requirements for the KETs, and if a number is given for a requirement, it is usually strongly connected to a specific use case. The requirements are generally formulated, and more details likely need to be added for specific use cases. A challenge is that the requirements are based on what is wanted and needed but not necessarily is available today as development is ongoing in all the KETs. Adoption of the requirements may be needed to demonstrate use cases with today's technology. Identified requirements and constraints relevant for three KETs have been compiled from [1,2] into tables presented here and acts as the minimum specification to develop a harmonisation testing and validation procedure within the HEADSTART [15, 14] project.

Requirements for positioning

Positioning is the ability of an actor in the traffic system to decide its position and estimate and track the object's position in the proximity of the ego vehicle (ego vehicle is the vehicle under test and/or executing a particular driving function).

Technical and functional requirements for positioning

Different applications within the scope of CADs have different needs for a position, but the main aspects are absolute and relative positioning. Sub-categories for these aspects are accuracy, reliability, update rate, confidentially, integrity and availability. Also, the measurement of the physical dimensions of the object with the estimated position is of interest. High definition (HD) maps and relative measurements can be used for absolute positioning. Significant points of interest like traffic signs, beams, or poles, retrieved from the HD map, can be used as trust anchors to determine the vehicle's position without active connections. V2X communications also offer a channel to transfer information that can be used to improve positioning, provide there is a mechanism to establish sufficient trust in the data.

Table 1 - Functional requirements relevant for positioning at the vehicle level

#	Description
1	The vehicle should be equipped with positioning capabilities.
2	The positioning module shall have HD map of the area in which it will be operating.
3	The system shall be able to provide positioning data at 10 Hz.
4	Detect and evaluate GNSS uncertainty
5	The automated vehicle must have a strategy to handle the loss of GNSS positioning.
6	The positioning system must handle GNSS jamming and spoofing.

Table 2 - Technical constraints at vehicle component level relevant for positioning

Type	Description
Accuracy	Positioning accuracy within urban environment less than 20 cm The system shall be able to provide longitudinal positioning with 10 cm accuracy The system shall be able to provide lateral positioning with 10 cm of accuracy
Integrity	Reliability and availability are also crucial though no specific numbers come out from this survey.
In the case of positioning using C-V2X	A relative lateral position accuracy of 0.1 m between user equipments (UEs) shall be supported. For platooning, the relative longitudinal position accuracy of less than 0.5 ms for UEs supporting V2X application for platooning.

Testing and validation requirements for positioning

Testability of positioning concerns test objects such as the ego vehicle and the surroundings, e.g. static objects such as landmarks, and dynamic ones, such as other vehicles, pedestrians. Testing the position means measuring the absolute or relative position. Absolute position is relative to a global reference frame with its orientation and origin fixed to the earth, e.g., using Global Navigation Satellite Systems (GNSS). There are now several satellite constellations that are often used in conjunction. Relative position is defined as the distance between the test object and another object, e.g. vehicles and road markers; continuous tracking is essential here.

Table 3 - Testing and validation requirements relevant for positioning

Domain	Requirement
Potential physical constraints on test tracks (e.g. radio interference)	"Simulate" different environments regarding GNSS quality on the proving ground. Positioning signal quality varies in different urban environments; therefore, handling multipath is required—the necessity to "simulate" multiple vehicles with synchronised trajectories. The proving grounds must allow GNSS testing and simulate degradations. Infrastructure must provide base stations for RTK-GPS and UWB. HD map of the test track area must be available.
How can simulation verify the requirement	"Simulate" different environments regarding GNSS quality on the proving ground—proper simulation under weather conditions.
Safety requirements for road-users	The vehicle must be possible to bring to a safe state when positioning is degraded/lost.

As for V2X communication, testing of positioning must be based on simulations, laboratory tests, proving ground tests, and public road tests. For GNSS based solutions, vendors engaged in V2X communication testing primarily also includes testing of GNSS. That must be combined with suitable methods for other positioning technologies.

Technical and functional requirements for V2X communication, positioning and cyber-security in the HEADSTART project

Requirements for V2X communication

Communication technologies suitable for CAD is what usually is called Vehicle-to-everything (V2X) communication. V2X communication enables a vehicle to communicate wirelessly with any entity that may affect the vehicle; vehicle-to-infrastructure (V2I), vehicle-to-network (V2N), vehicle-to-vehicle (V2V), vehicle-to-pedestrian (V2P), vehicle-to-device (V2D) and vehicle-to-grid (V2G). It is an enabler for cooperative driving and optimises collective behaviour concerning throughput, fuel consumption, emissions and Safety [5]. There are two main types of V2X communication technologies associated with the automotive industry; WLAN-based (IEEE 802.11p, used in ETSI ITS G5 and DSRC); Cellular based (3GPP defined C-V2X includes short distance communication using PC5 sidelink and traditional cellular interface through 3G/4G/LTE/5G.

Technical and functional requirements for V2X communication

V2X communication might involve 3 different types of use cases (Road safety, Traffic management and efficiency, Infotainment) where the first one, road safety, likely is most relevant for HEADSTART [5]. The main objective of road safety application is to reduce traffic collision, improve road safety, and listed its general requirement (Coverage, latency, reliability, throughput, predictability, range, velocity, operation). The second one, traffic management and efficiency, is also relevant for CAD and may be relevant for HEADSTART to gain CAD's system-level advantages. According to the assessment of the state of the art activity achieved in HEADSTART, Table 4 and

Table 5 summarise requirements at the vehicle and component level.

Table 4 - Functional requirements at vehicle level relevant for V2X communications.

#	Description
1	Communication may be applied through ITS-G5, 4G/LTE, 5G/LTE.
2	Automotive OEM Clouds should communicate (registration and data exchange) with service providers (e.g. parking, charging, etc.) through a standard interface.
3	V2V communication means must integrate authentication and encryption components. Based on the data to be exchanged between vehicles (V2X) and their communication needs, requirements for Confidentiality, Integrity and Availability of the information to be exchanged can be derived. Possible solutions for achieving the correct level of protection are authentication, encryption etc.
4	Connected infrastructure, e.g., traffic lights communicating through ITS-G5, 4-5G/LTE.
5	The system must support high connection density for congested traffic.
6	In terms of function requirements, low latency and high reliability, including availability, would be the two key aspects to be considered from the communication point of view.
7	Predictability: it is vital to get information about when and where network KPI can't be fulfilled.
8	The supported Vehicle velocity needs to be specified. On German's autobahn, it may be as high as 250 km/h. The relative velocity that must be supported is twice the absolute velocity.
9	Multi-operator's operator: the communication system must support communication between vehicles, pedestrians and RSUs served by different operators.

10	The automated vehicle must have a strategy to handle the loss of V2X communication. Application-level: robustness of the CAD system/application, reduced functionality, graceful degradation. System/Technology level: redundancy: multiple channels, multiple radio's, multiple radio technologies.
11	Seamless communication with Real/Virtual Cars.
12	Communication between the in-car system and a remote server/cloud.

Table 5 - Testing and validation requirements for V2X communication.

#	Description
1	Low latency required for operational data for automated driving functions/application ≤ 60 ms per case (typically 5 ms).
2	High reliability (99.00-99.99%).
3	Data Rate (128kbps-29Mbps per case).
4	Communication range: Typical values <300m for a short distance It may be needed to distinguish between short and long-distance communication. Possible downscaling, from a vehicle perspective, to communicate with its direct neighbours.
5	One Road-Side Unit shall be able to communicate with up to 200 UEs.
6	In platooning, a specific UE shall be able to communicate with up to 19 other UEs.

Testing and validation requirements for V2X communication

Testing V2X communication must be done using simulations, laboratory tests with cables and over-the-air tests in laboratories, proving ground tests and field tests on public roads. An overview of simulation tools is included in [8]. Vendors already engaged in the Wi-Fi or cellular industry usually have shown solutions for V2X testing or are working on it. However, testing on test tracks requires infrastructure, and work is continuously building cellular networks on the test track to enable testing using communication. Furthermore, with the fast technological progress, it is expected that the test tracks need close collaboration with the companies developing equipment for V2X communication.

Table 6 - Technical constraints at vehicle component level relevant for V2X communication.

Domain	Requirements
Technical feasibility	A challenge is that V2X, especially C-V2X, is still in the development phase, and devices meeting the requested requirements may not be available.
Potential physical constraints on test tracks	The test tracks must be equipped with relevant infrastructures for V2X communication to perform the tests—information congestion in a v2x setting in an urban environment. For example, if V2X communication testing is carried out in the open air or a shielded chamber, no other radio transmission must exist.

How the requirement is expected to be partly verified by computer tools	A V2X communication simulator sends pre-defined messages to the vehicle under test, and dynamic messages based on GPS data feeds/replays/path generation. The tool should make it possible to define and re-use test sequences of V2X messages and record and replay messages received from the vehicle under test. If available, data from Field Operational Tests may be used as input.
Safety requirements for road-users	The ADS feature must always meet functional safety requirements based on performed Hazard and Risk Analysis (HARA), e.g. vehicle must have measures to attain a safe state in case of critical failures.

Requirements for Cybersecurity

From a CAD perspective, the interplay between Cybersecurity and Safety – a malicious attack may be a hazard from a Safety perspective, cybersecurity that protects information technology resources must be handled in parallel. A challenge for Cybersecurity compared with Safety is that Cybersecurity risks evolve as attacker's motivations and capabilities change, i.e., Cybersecurity involves defence against techniques that may not be understood when the system is created [3]. An extensive State-of-the-Art about vehicular security is available from the HoliSec project [4]. Overview, review and discussions concerning security and privacy in C-V2X are found in, e.g., [5,6,7]. How Cybersecurity is interrelated GNSS positioning in ITS systems can be found in [13]. When defining Cybersecurity requirements, it is essential to understand potential threats that need to be considered when designing the system, for this CIA is commonly used, defined by NIST FIPS 199 [9]:

- **Confidentiality:** "Preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
- **Integrity:** "Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity."
- **Availability:** "Ensuring timely and reliable access to and use of information."

Many best practices and design principles for cyber vehicle physical systems exist, e.g., [3,9–12]. The best practices cover what is included in the Auto-ISAC best practice [11], that in addition to governance and awareness & training, defines five guiding principles affecting motor vehicle cybersecurity; security by design, risk assessment and management, threat detection and protection, incident response, and collaboration and engagement with appropriate third parties.

Testing of Cybersecurity is challenging and differs from safety testing. Cybersecurity relies on attack (vulnerability) testing or penetration testing and is usually based on a Threat Analysis & Risk Assessment (TARA). The TARA results drive future analysis activities by focusing future analyses on the highest risk Cybersecurity threats. Threat Analysis and applied to all external data interfaces. Generally, there are three primary settings for testing- Black Box testing – where little or no pre-disclosed information is available, White Box testing – the tester has access to all information about the system and Gray Box testing somewhere in between. Vulnerability testing can be conducted by either scanning methods that can detect vulnerabilities to be exploited by exploratory testing methods used to detect and probe for vulnerabilities. Aggressive testing aiming to break, bypass, or tamper with the cybersecurity controls and demonstrate potential misuse of the system or feature. In contrast, Fuzz testing bombards the feature or system with data with the purpose to see if it responds in an unspecified way. All described methods should be used to test Cybersecurity in vehicles with CAD functions; Appendix I in SAE J3061 [3] lists examples of security test tools.

Technical and functional requirements for Cybersecurity

The results from the investigations of standardisation work, other research projects and collected user needs from stakeholders were used to summarise the identified main technical and functional requirements for KETs as presented in Table 7. The main requirement is that product development follows best practices for Cybersecurity and that all potentially cyber-attacks are considered. For V2X communication, there shall be a chain of trust using verified signatures and certificates. For all products, state-of-the-art cybersecurity testing shall be performed. A noteworthy response to the questionnaires' is that Cybersecurity is ranked third in importance among the KETs, even though Cybersecurity can be critical during the whole lifetime of the vehicle. It seems reasonable to assume that most stakeholders are in the early phases of the development cycle and focus on getting V2X communication and positioning to work rather than testing.

Table 7 - Technical and functional requirements for Cybersecurity.

Type	Description
General	• Make use of best practices for Cybersecurity. • All cybersecurity issue shall be monitored and continuously assessed. • Potential cyber-attacks shall be dually analysed; from the "Defenders" and the "Attackers" point of view.
Functional requirements at the vehicle level	• Adopt high levels of Confidentiality, Integrity and Availability. • V2X message reception shall be signed by a trusted third party (message shall be valid and verified with certificate and signature). • Messages shall be predictable and uncorrupted. • All components in the system must support end-to-end Cybersecurity, even involving network and infrastructure like, e.g., traffic lights.
Technical constraints at vehicle component level	• Potential physical constraints on test tracks (e.g. radio interference) o It must be possible to conduct penetration testing in dynamic conditions in specific scenarios and environments. • How the requirement is expected to be partly verified by computer tools (simulation) o Performed cybersecurity testing: o Attack (Vulnerability) testing o Penetration testing o Fuzz testing

Testing and validation requirements for Cybersecurity

Regarding requirements for testing and validation for Cybersecurity, HEADSTART focuses on vehicle level tests and that component system-level tests are out of the scope. The latter tests are assumed already performed by the suppliers, following well-established and standardised practices, and is reflected in the safety and security documentation. However, independent tests at the vehicle level must be conducted for certification and type approval. Testing and validation requirements allocated to the four-testing block identified by HEADSTART are summarised in Table 8.

Table 8 - Testing and validation requirements for Cybersecurity.

Domain	Sub-category	Requirements
Proving ground testing	GNSS jammer	• GNSS generator (to be connected directly) to the GNSS receiver to evaluate the performance of the positioning system
	V2X jammer	• Overflow communication channel with fake data. • V2X generator able to generate fake vehicles around the DuT
Virtual testing	NA.	• No specific related parameters for virtual testing were found.
XiL-Based testing Scenarios	Conformance	• Conformance testing to relevant Cooperative-ITS security standards. E.g. ETSI Plug Test events or a similar approach. • Testing of CAD application performance/robustness/resilience against external attacks (V2X, wireless comm.) (e.g. Jamming V2X, DoS Tx/Rx V2X messaging, spoofing V2X messages).
	Interoperability	• Interoperability testing to relevant Cooperative-ITS Security Standards. E.g. ETSI Plug Test events or a similar approach (testing, tools, evaluation).
Real-world testing scenario	NA.	• No specific requirements for Cybersecurity on open road testing were found.

Conclusion

The main objective of the HEADSTART project is to develop a harmonised scenario-based testing approach for CADs, building on previous initiatives while catering to the largely unaddressed collective need for verification and validation of key enabling technologies (communication, positioning and cyber-security). The requirements and constraints presented in this paper act as a specification for the testing, relevant for the three KETs, and is essential for developing a verification and validation procedure within the project. Furthermore, the collected data is of import since it represents a collective understanding of the prerequisites for testing CADs gathered from key European stakeholders and is helpful as a stepping stone for similar initiatives.

References

1. G. Morandin, M Skoglund, N. Wagener, E. Martinez, O. Flix, C. Lujan, J. Coget, L. Bonic, A.

Bracquemond, J. Castermans, Á. Arrúe, HEADSTART Deliverable "D1.2 Stakeholders and user group needs" https://www.headstart-project.eu/results-to-date/deliverables/

2. A. Thorsén, M. Skoglund, F. Warg, J. Jacobson, R. Hult, N. Wagener, A. Ballis, J. van der Sluis, J. Pereze , A. Steccanel, HEADSTART Deliverable "D1.3 Technical and Functional requirements for KETs" https://www.headstart-project.eu/results-to-date/deliverables/
3. SAE. (2016). Cybersecurity Guidebook for Cyber-Physical Vehicle Systems (Surface Vehicle Recommended Practice No. J3061_201601). SAE Int., http://standards.sae.org/wip/j3061/
4. A. Lautenbach, T. Olovsson, & T. Rosenstatter. (2017). A State-of-the-Art Report on Vehicular Security (Holisec Deliverable No. D1.2). Vinnova/FFI, Sweden. Retrieved from https://autosec.se/wp-content/uploads/2018/04/1.2-holisec-state-of-the-art.pdf
5. NGMN V2X Task Force. (2018). V2X White Paper v1.0. NGMN. Retrieved from https://www.ngmn.org/fileadmin/ngmn/content/downloads/Technical/2018/V2X_white_paper_v1_0.pdf
6. Lonc, B., & Cincilla, P. (2016). Cooperative ITS security framework: Standards and implementations progress in Europe. In 2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM) (pp. 1–6). Coimbra, Portugal,
7. Marojevic, V. (2018). C-V2X Security Requirements and Procedures: Survey and Research Directions. arXiv:1807.09338. Retrieved from http://arxiv.org/abs/1807.09338
8. Storck, C., & Duarte-Figueiredo, F. (2019). A 5G V2X Ecosystem Providing Internet of Vehicles. Sensors, 19(3), 550. https://doi.org/10.3390/s19030550
9. NIIST. (2004). Standards for security categorisation of federal information and information systems (No. NIST FIPS 199). Gaithersburg, MD: NIST. https://doi.org/10.6028/NIST.FIPS.199
10. National Highway Traffic Safety Administration. (2016). Cybersecurity best practices for modern vehicles (No. DOT HS 812 333). Washington, DC, USA.
11. Auto-ISAC. (2016, 2019). Best Practices – Auto-ISAC.
12. ISO/SAE. (Under development). ISO - ISO/SAE CD 21434 - Road Vehicles -- Cybersecurity engineering. Retrieved from https://www.iso.org/standard/70918.html
13. EN 16803-1:2016 - Space - Use of GNSS-based positioning for road Intelligent Transport Systems
14. Wagener.; Weißensteiner, P.; Coget, J.-B.; Eckstein, L.; Common Methodology for Data-Driven Scenario-Based Safety Assurance in the HEADSTART Project, 27th ITS World Congress 2020
15. B. Hillbrand, P. Weissensteiner, J. Castella Triginer, M. Skoglund, M Nieto, O. Otaegui, X. Sellart, A. Ballis, HEADSTART deliverable, D3.1 Guideline of a comprehensive validation and certification procedure to ensure safe CAD systems, https://www.headstart-project.eu/results-to-date/deliverables/