




Enhancing Safety Assessment of Automated Driving Systems with Key Enabling Technology Assessment Templates.

Martin Skoglund ^{1,*} , Fredrik Warg ^{1,†} , Anders Thorsén ^{1,†}  and Mats Bergman

¹ RISE - Research Institutes of Sweden, Borås, Sweden

² Telia Company, Stockholm, Sweden

* Correspondence: martin.skoglund@ri.se; Tel. +46 705 14 5949

† These authors contributed equally to this work.

Abstract: The emergence of Automated Driving Systems (ADSs) has transformed the landscape of safety assessment. ADSs, capable of controlling a vehicle without human intervention, represent a significant shift from traditional driver-centric approaches to vehicle safety. While traditional safety assessments rely on the assumption of a human driver in control, ADSs require a different approach that acknowledges the technology as the primary driver. Before market introduction, it is necessary to confirm the vehicle safety claimed by the manufacturer. The complexity of the systems necessitates a new comprehensive safety assessment that examines and validates the hazard identification and safety-by-design concepts and that the ADS meets the relevant safety requirements throughout the vehicle lifecycle. The presented work aims to enhance the effectiveness of the assessment performed by a homologation service provider using assessment templates based on refined requirement attributes that link to the Operational Design Domain (ODD) and the use of Key Enabling Technologies (KETs), such as communication, positioning, and cybersecurity, in the implementation of ADSs. The refined requirement attributes can serve as safety performance indicators to assist the evaluation of the design soundness of the ODD. The contributions in the paper are: (1) Outlining a methodology for deriving assessment templates for use in future ADS assessments, (2) demonstrating the methodology by analyzing three KETs with respect to such assessment templates, and (3) demonstrating the use of assessment templates on a use case, an unmanned (remotely assisted) truck in a limited ODD. By employing assessment templates tailored to the technology reliance of the identified use case, the evaluation process gained clarity through assessable attributes, assessment criteria, and general scenarios linked to the ODD and KETs.

Keywords: Safety assessment; Operational domain; Automated driving; Communication, Connectivity, Positioning, Cybersecurity

Citation: Lastname, F.; Lastname, F.; Lastname, F. Title. *Vehicles* **2022**, *1*, 1–21. <https://doi.org/>

Received:

Accepted:

Published:

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2023 by the authors. Submitted to *Vehicles* for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The introduction of Automated Driving Systems (ADS) has created a paradigm shift in the approach to safety assurance in the automotive industry. Contrasting to an advanced driver-assistance system (ADAS), an ADS can completely take over the driving task from the human driver for a portion of the trip [1]. Examples of ADS features include Traffic Jam Chauffeur, Highway Autopilot, Valet Parking, and Automated Truck Platooning.

Safety standards and regulation conformance form a basis for what needs to be satisfied by a vehicle before it can be commercially available. A successful fulfilment assessment, called type approval, must be made before the market introduction of any vehicle to ensure that it is safe for use on public roads, while using the new feature, e.g. Automated Lane Keeping Systems [2].

Introducing an ADS represents a significant change in the scope of the road vehicle approval procedures. Safety assurance claims made by original equipment manufacturers (OEM) must demonstrate that the ADS can operate safely in all traffic situations, including in rare circumstances such as sensor failures, cyberattacks, or environmental changes. Type

approval becomes particularly important to ensure that these systems are safe and reliable to build trust and acceptance in the eyes of the public for this emerging technology. Key entities in the new type approval process include the OEM, Homologation Authority, and Homologation Technical Service Provider seen in Figure 1.

The OEM is responsible for designing, developing, and producing the vehicle or automotive component, seeking type approval. They ensure compliance with regulations and standards, providing necessary documentation, test reports, and technical information. The Homologation Authority is the regulatory body granting type approval. They verify compliance with regulations, assessing safety, environmental impact, and legal requirements. They review documentation, conduct tests, and issue type approval certificates. The Homologation Technical Service Provider is an independent organization authorized by the Homologation Authority. They perform testing, evaluation, and certification services. Following standardized procedures, they assess product performance, safety, and environmental characteristics. Their reports and documentation support the type approval process.

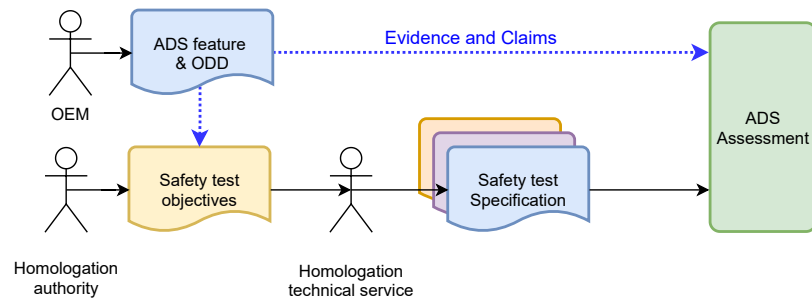


Figure 1. In the type approval process, key entities include the OEM, Homologation Authority, and Homologation Technical Service Provider.

An ADS assessment scheme must consider complex sensors, algorithms, and the decision-making process the vehicle employs to operate in automated mode. To meet the challenge of assessing an ADS, the United Nations Economic Commission for Europe (UNECE) World Forum for Harmonization of Vehicle Regulations (WP.29) has drafted a "New Assessment and Test Method" (NATM) that may become part of the future type approval for ADS. The NATM aims to assess the ADS's safety based on the high level safety requirements [3] and determine whether it can operate safely within its operational design domain (ODD) by examining scenarios linked to road users' behaviour, environmental conditions, and driver behaviour. NATM's multi-methodologies (pillars) approach includes a scenarios catalogue that combines accelerated (simulation) testing, test track, real-world testing, audit/assessment procedures, and in-service monitoring and reporting to validate the safety and performance of ADS. Accelerated testing is coupled with validity documentation in the audit and assessment procedure, covering system-related aspects as a complement to classical test track certification. A consensus exists that in order to evaluate an ADSs implementation reliably, there is a need to employ a combination of methods to validate the capabilities since it cannot be done comprehensively nor effectively through a single validation methodology. The procedural goal of NATM is to conduct an empirical, objective, practical, and repeatable independent safety assessment of any ADS while maintaining technology neutrality.

Independent safety assessment is a crucial gatekeeping function before releasing automated vehicles to the market. It involves evaluating and verifying the technology's safety and reliability by a neutral third party separate from the manufacturer. Manufacturers may make claims about the capabilities of their automated vehicle technology that do not reflect its real-world performance. Unvalidated claims create a significant risk of overreliance on technology and a false sense of security among drivers and other road users. Automated vehicles must operate safely in diverse conditions, including challenging

environments, complex traffic scenarios, and unpredictable events. Therefore, thorough testing and evaluation are necessary to establish the reliability and proper functioning of the technology in all possible situations. Current safety assessment approaches are not suited for complex automated systems as traditional testing and validation methods do not fully capture these systems' intricacies and potential failure modes. This work focuses on the challenges related to an independent assessment of the safety of automated vehicles and the importance of robust safety assessment frameworks. Such a testing framework must bridge the gap between the marketing portrayal and the actual performance of such systems in real operating conditions. It requires industry, government, and academia collaboration to develop a framework that ensures this technology's safe and responsible development and deployment.

Despite the existence of safety assessment frameworks, standards and guidelines, there is still a need for more practical guidance on conducting safety assessment for ADSs. This is especially true for the assessment tasks envisioned by a technical service provider, which are highly complex and require expertise in multiple domains, including technology, human factors, risk management, and safety regulations. Moreover, ADS technology is rapidly evolving, and new safety and performance requirements are emerging as the technology advances. However, a significant challenge arises due to the limited availability of information before the evaluation process begins, necessitating the need for proactive and forward-thinking guidance. By providing technical service providers with anticipatory practical guidance, they can better prepare and navigate the assessment process, identify relevant tests, and address the challenges of establishing confidence in ADS's safety and user awareness. An assessment template can be crucial in conducting comprehensive evaluations of ADSs by capturing all assessable attributes. Yet, given the complexity and evolving nature of ADSs, achieving a fully comprehensive and exhaustive evaluation using a single template is currently unattainable.

To address this challenge, our contribution is threefold. First, we propose a method for constructing specialized subsets of assessment templates tailored to ADSs and their specific reliance on key enabling technologies (KETs). Requirements are collected through stakeholder surveys and use cases, and relevant attributes are derived from these requirements groups. In this context, requirement attributes are defined as properties of a requirement that capture essential information suitable for evaluation. Secondly, we apply the proposed method to investigate requirements for two common enabling technologies in ADS: positioning and communication, focusing on the additional quality attribute of cybersecurity. The result is specialized templates that offer a more focused and targeted approach, providing forward-thinking practical guidance for assessing ADSs effectively. Third, we demonstrate the effectiveness of the assessment templates through a specific use case involving a remotely assessed truck. This practical application showcases the template content of attributes and assessable performance indicators in general test scenarios.

KET-specific assessment templates contribute to structured technology-aware evaluations of ADS safety and performance, establishing a knowledge-driven consistent and repeatable assessment framework. The assessment template approach has limitations as it primarily relies on predefined scenarios, and is thus intended as a complement to data-driven methodologies, incorporating real-world data, for a comprehensive assessment. The templates should also be continuously updated and refined to keep up with technology development.

The paper is organized as follows: the problem is introduced in Section 1, the background and related works are presented in Section 2, the method to produce templates is introduced in Section 3, the creation of fit-for-purpose templates for the considered KETs is elaborated upon in Section 4, the templates are utilized and evaluated in Section 5, and the results and future work are discussed in Section 6.

2. Background and related work

Automated driving technology, also known as autonomous or self-driving vehicle technology, use a combination of complex sensors and advanced algorithms to navigate and interact with their surroundings without human intervention. As with any new technology, the development and deployment of automated vehicles come with potential risks and challenges that must be addressed. These risks and challenges are related to the safety and reliability of the technology, the ethical and legal implications of its use, and the overall impact on society and the environment [4].

SAE J3016 is widely recognized as a taxonomy and definition reference for Automated Driving Systems (ADSs) [1]. ADSs are categorized under SAE automation levels 3 to 5. These systems are designed to take over the driving task for a portion of a trip, performing operational functions such as vehicle motion control (lateral and longitudinal) and tactical functions like route planning, following, and object and event detection and response (OEDR). Similar to a human driver, ADSs must be able to perceive their location and surroundings, which requires various functionalities. These functional, non-functional, and technical requirements are crucial considerations throughout the development, type approval, and consumer testing of ADSs. The assessment of ADSs is significantly influenced by the concept of Operational Design Domain (ODD) [5,6]. ODD refers to the specific operating conditions in which an ADS is designed to function and must be integrated into safety-related functions. The dynamic driving task (DDT) encompasses the real-time operational and tactical functions necessary to operate a vehicle within the ADS's ODD. Several efforts have been made and are ongoing to define and describe an ODD, including standards such as those by the British Standards Institution (BSI) [7] and the International Organization for Standardization (ISO) [8], and Association for Standardization of Automation and Measuring Systems (ASAM) OpenODD [9].

Another important aspect is the use of scenario-based testing [10,11]. Scenario-based testing focuses on specific scenarios and edge cases essential for ensuring automated vehicles' safe operation [12]. This approach complements real-world testing and allows for a more comprehensive evaluation of the system's capabilities and limitations. By systematically designing and evaluating scenarios representing realistic and critical situations, developers can gain valuable insights into the system's performance and identify potential failure modes. Safety assessment approaches for autonomous systems encompass a range of methodologies and techniques, but many are at least relatable to scenario-based testing and the SAE taxonomy. Other safety assessment approaches include real-world testing, distance-based evaluation, staged introduction, function-based testing, shadow mode evaluation, formal verification, and traffic simulation-based testing [13]. These approaches all enable the assessment of system safety and performance in various contexts. However, ensuring that autonomous systems meet the necessary requirements and can operate safely in diverse requires a holistic approach.

There are several efforts to develop standardized testing methodologies for ADSs, and some focused on assessment [14]. Examples of standardized testing is the National Highway Traffic Safety Administrations (NHTSA) Framework for Automated Driving System Testable Cases and Scenarios ([15], and the New Assessment/Test Method for Automated Driving (NATM) [16] proposed by the United Nations Economic Commission for Europe (UNECE). We primarily concentrate on NATM due to its significance in the European context.

The procedural goal of a method like NATM is to conduct an empirical, objective, practical, and repeatable safety assessment of any ADS while remaining technology neutral. Within the NATM certification process, accelerated testing is combined with validity documentation supplied by the manufacturer in the audit and assessment procedure to cover system-related aspects. However, it is important to note that this is meant to complement, rather than replace, classical test track certification. Combining multiple methods, as depicted in Figure 2, is recommended to comprehensively validate the capabilities of an ADS [14].

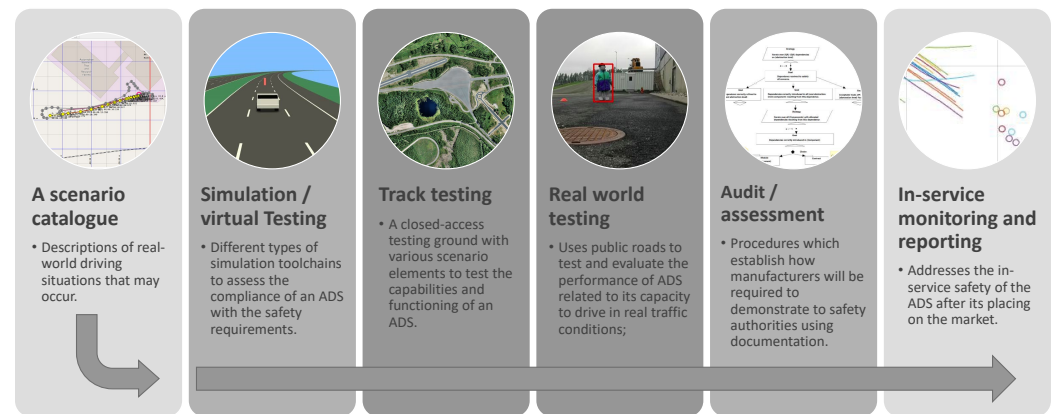


Figure 2. The envisioned procedural instance of the assessment framework. General scenarios related to KETs can be added to the scenario catalogue.

While the NATM certification process is a step forward in developing safety assessment frameworks for automated vehicles, it is not without limitations. One limitation is that NATM is still in the proposal stage and has not been widely adopted or implemented. As a result, limited data are available to assess its effectiveness and suitability [17] for different automated driving systems.

NATM is general and technology-neutral, meaning it does not provide specific guidance on assessing the safety of different automated driving systems or technologies. As a result, it may be difficult for assessors to apply the framework consistently and effectively across different ADS applications. Another difficulty is the dynamic nature of automated systems and the rapid pace of technological advancements. Safety assessments must keep up with the evolving technology, requiring continuous updates and adaptations to assessment frameworks and standards. The emergence of new sensor technologies, AI algorithms, and connectivity features further complicates the assessment process. We believe the method of using assessment templates proposed in this paper can help mitigate these limitations. An assessment template can add general scenarios that cover conditions in the ODD by examining scenarios linked to road users' behaviour, environmental conditions, driver behaviour and technology reliance, and provides some consistency of evaluation across applications.

3. Method to derive assessment templates

Our thesis asserts that analyzing KETs is fundamental to developing practical guidance for evaluating the soundness and comprehensiveness of the ODD and general test scenarios for automated vehicles. This guidance, in the form of requirement attributes, serves as safety performance indicators that enable the examination and evaluation of automated vehicle systems. Analyzing all major KETs is essential in providing complete guidance for evaluating any use case of automated vehicle systems. We believe this approach should be prioritized regardless of the technologies being analyzed. The process to derive assessment templates can be summarized as follows:

1. Collect ADS use case requirements: Engage with stakeholders, including manufacturers, researchers, regulators, and industry experts, to gather their requirements and perspectives. Identify and analyze various use cases to understand the specific technology reliance and testing needs. Assess the reliance of each requirement on KETs.
2. Allocate requirements based on technology reliance: Determine which requirements are directly or indirectly dependent on specific KETs. Allocate and associate the requirements with the corresponding KET.
3. Derive attributes for KET category: For each category, derive attributes that capture the essential characteristics. These attributes should primarily reflect safety considera-

tions, but functionality, reliability, and other relevant technological group aspects can also be considered.

4. Establish safety performance indicators: Based on the derived attributes and safety objectives, establish safety performance indicators that can be used to assess and measure the safety performance of the automated system. These indicators should provide quantifiable and meaningful measures to evaluate the system's compliance with safety requirements. Create general test scenarios that cover diverse operational conditions and situations to be added to the scenario database. These scenarios should exercise the system's capabilities and evaluate its performance against the safety indicators.

A panel of experts refines the collected requirements into attributes for the collected requirements per KET; the schematic process with inputs and outputs is depicted in Figure 3. Such an approach has certain limitations. Limitations include subjectivity, as attribute selection relies on expert opinions, leading to variations in definitions and importance. Limited representation of diverse stakeholders may overlook essential requirements. Lack of standardization can result in inconsistent attribute definitions, making comparisons difficult. Nonetheless, the practical evaluation in Section 5 shows the approach to be viable and valuable.

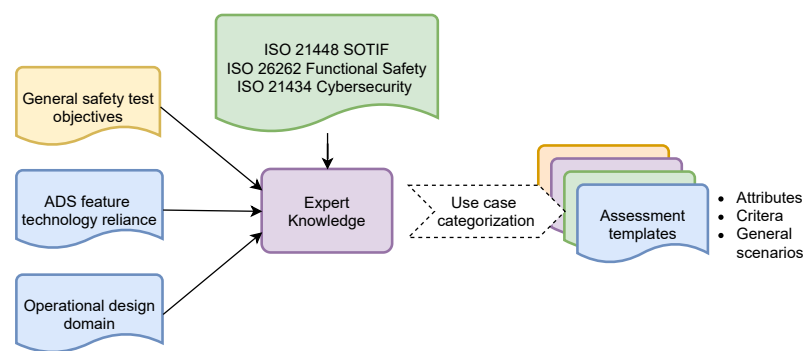


Figure 3. Schematic assessment templates creation process.

Following this process, stakeholders can systematically collect requirements, identify technology dependencies, and derive requirement attributes per KET and safety performance indicator. This structured approach helps ensure that safety considerations are adequately accounted for and enables a more comprehensive and consistent assessment of the automated system's safety performance.

4. Derive assessment templates

The method, delineated in Section 3, serves as a blueprint for crafting assessment templates. This section provides a condensed overview of the template creation steps for the KETs *communication*, *positioning*, and *cybersecurity*. These KET categories were integral to the HEADSTART [18] project. While we touch upon the rudimentary aspects of requirement collection and allocation to categories, our main focus lies in elaborating on the attributes and assessment templates, which represent an extension of this foundational work. Subsequent sections and Figure 4 delve into these steps, underscoring their significance. Our analysis zeroes in on these three KETs, illustrating how they were employed to validate our hypothesis concerning the role of technology-aware guidance in ADS assessment. This approach underscores the importance of encompassing a complete array of KETs when evaluating ODDs and general test scenarios for automated vehicles.

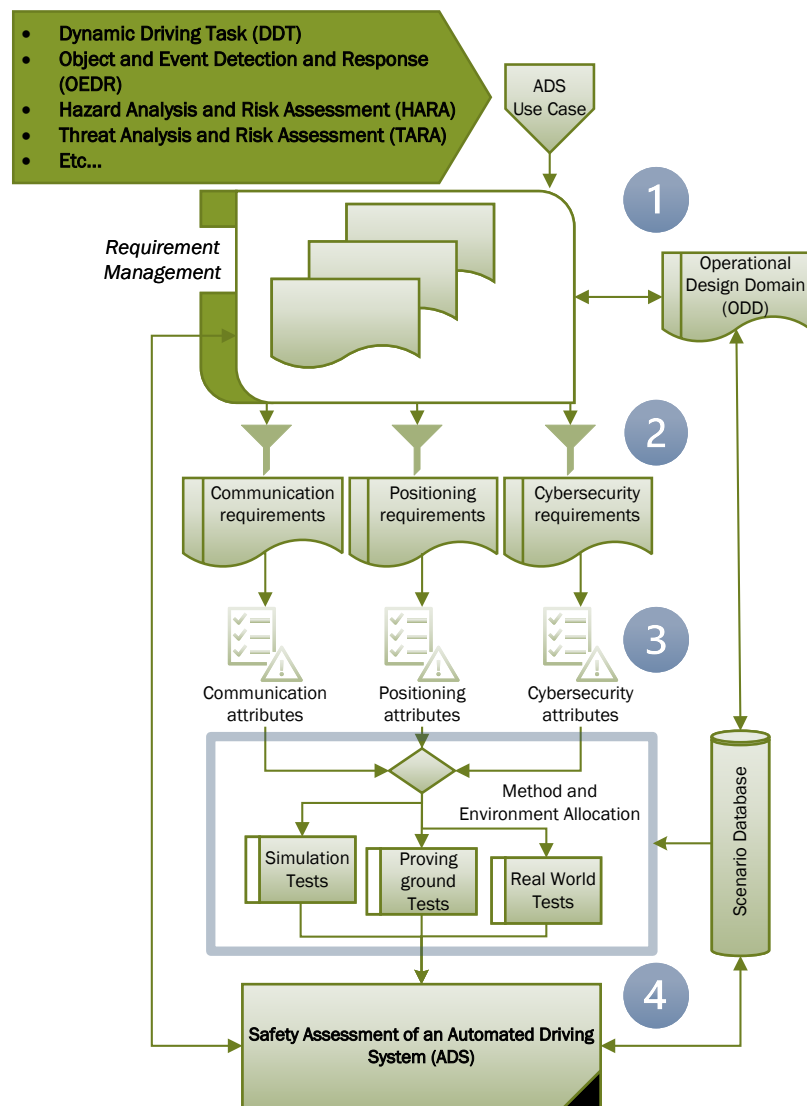


Figure 4. Method to derive assessment attributes for KETs.

4.1. Collect requirements

The first step (denoted 1 in Figure 4) is requirements collection. Our previous work [19], conducted within the HEADSTART project, extensively gathered functional and technical requirements related to the three KETs, as these technologies play a critical role in the functionality and safety of automated vehicles.

A three-step approach was followed to identify the relevant requirements for the KETs. Firstly, ongoing activities in standardization organizations and other interest groups were investigated. Secondly, a series of interviews, surveys, and questionnaires were conducted with various stakeholders, including OEMs, Tier 1 suppliers, and regulatory entities, to understand their needs and perspectives. Lastly, requirements and insights from other relevant research projects were also incorporated into the analysis. This comprehensive approach ensured a comprehensive collection of requirements and needs related to the KETs.

The data collection efforts were conducted in collaboration with stakeholders, participants or those affiliated with the HEADSTART project from the industry, research institutes, and policymakers. The survey of the stakeholder's considerations revealed a mixture of high-level and low-level requirements. The intended use of the testing was also considered in the survey and was categorized as development, consumer, and type approval testing. The project's analysis revealed many specific requirements for the KETs, usually strongly

connected to a specific use case. A challenge is that the requirements are based on what is wanted and needed but not necessarily available today as development is ongoing in all the KETs. Adapting the requirements may be needed to demonstrate use cases with today's technology. Identified requirements and constraints relevant to these KETs have been documented and presented in various publications [19–21] that describe the specification to develop a harmonization testing and validation procedure within the HEADSTART [22] project.

The use cases analyzed in the project, e.g., highway pilot and highway truck platooning, play a crucial role in exploring various aspects of critical enabling technologies. The variation in reliance on these underlying technologies is crucial in developing a practical assessment procedure. By understanding the specific requirements and challenges associated with each use case, a comprehensive assessment procedure can be developed to ensure the safety and performance of automated vehicles. The derived attributes presented in Section 4.3 are based on these collected requirements.

4.2. Allocate requirements based on technology reliance

As indicated in Step Two in Figure 4, the method integrates the gathered and categorized requirements, guaranteeing the inclusion of all pertinent technology-specific parameters within the ODD and scenario specifications. The framework includes a separate analysis of the KETs to address their requirements comprehensively. Doing so ensures that the framework considers each technology's specific attributes and considerations. The effects of these technology-specific requirements are continuously monitored as they propagate and permeate the framework and give rise to attributes, performance indicators and general test scenarios.

4.2.1. V2X Communication

Communication and associated requirements can play a crucial role in ADS. Vehicle-to-everything (V2X) communication technologies enable vehicles to wirelessly communicate with various entities that can impact their operation, including vehicle-to-infrastructure (V2I), vehicle-to-network (V2N), vehicle-to-vehicle (V2V), vehicle-to-pedestrian (V2P), vehicle-to-device (V2D), vehicle-to-grid (V2G), and Tele-operated Driving (ToD). This communication capability facilitates cooperative driving, optimizing collective behavior regarding throughput, fuel consumption, emissions, and safety [23]. In the automotive industry, there are two main types of V2X communication technologies: WLAN-based, which utilizes IEEE 802.11p and is used in standards such as ETSI ITS G5 and DSRC, and cellular-based, which is defined by 3GPP and includes short-distance communication using PC5 sidelink and traditional cellular interfaces through 3G/4G/LTE/5G networks. The testing of V2X communication involves various organizations such as 3GPP, 5GAA, ETSI, GCF, IEEE, OmniAir, SAE, C-ITS, C-SAE, and NTCATS. Test equipment vendors are actively developing instruments designed explicitly for V2X testing, with many of them also incorporating Global Navigation Satellite System (GNSS) testing capabilities.

4.2.2. Positioning

Positioning is another crucial capability required for ADS. It involves determining the position of the ego vehicle (the vehicle under test) and estimating and tracking the position of objects in its vicinity within the traffic system. Different applications within the scope of connected ADSs have varying positioning needs, with the main aspects being absolute and relative positioning. Accuracy, precision, refresh rate, and integrity are sub-attributes associated with these aspects. Additionally, there is an interest in measuring objects' physical dimensions and estimated positions. Global Navigation Satellite System (GNSS) based positioning and High Definition (HD) maps can be utilized for absolute positioning. HD maps provide relevant information, such as traffic signs, beams, or poles, which can be trust anchors to determine the vehicle's position without active connections. V2X communications can also improve positioning by transferring information, provided a

mechanism exists to establish sufficient trust in the received data. HD maps and relative measurements are employed to achieve accurate positioning. Ongoing standardization efforts related to GNSS are being carried out in organizations such as ETSI, and test equipment vendors actively develop GNSS testing capabilities. The interrelation between cybersecurity and GNSS positioning in Intelligent Transportation Systems (ITS) systems is discussed in [24].

4.2.3. Cybersecurity

Cybersecurity is a critical quality attribute that significantly affects the safety of ADS applications. Unlike safety, cybersecurity risks continuously evolve as attackers develop new techniques and capabilities, making it essential to address cybersecurity concerns throughout the system's lifecycle. When defining cybersecurity requirements, it is essential to consider potential threats. The NIST FIPS 199 [25] defines three commonly used aspects of cybersecurity, known as CIA:

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

The identified technical and functional requirements emphasize the two latter aspects as more safety-related and the importance of following best practices for cybersecurity throughout product development.

Defining cybersecurity requirements differs from communication and positioning, as it is a vital quality attribute for both aspects. V2X communication should establish a chain of trust using verified signatures and certificates, and state-of-the-art cybersecurity testing should be performed for all aspects. Best practices and design principles for cybersecurity in-vehicle systems exist, including those outlined in standards such as SAE J3061 [26], NIST FIPS 2004 [25], and ISO/SAE 21434 [27]. These practices encompass governance, awareness and training, security by design, risk assessment and management, threat detection and protection, incident response, and collaboration with relevant stakeholders. General guidelines for automotive cybersecurity can be found in [27], and there are various studies and discussions on security and privacy in Connected Vehicle-to-Everything (C-V2X) communications [23,28,29]. Standardization activities related to vehicle cybersecurity are jointly conducted by SAE and ISO [27]. Cybersecurity is challenging because it involves defending against evolving techniques and addressing threats that can impact safety. It is recommended to adhere to published best practices and recommended testing, including ISO/SAE 21434 [27]. ISO TR 4804 [30] is a technical report that connects ISO/SAE 21434, ISO 26262, and ISO/PAS 21434.

4.3. Derive attributes for KETs

The general safety objectives include potential hazards during a generalized ADS operation, including internal system and external environmental hazards. The process denoted three in Figure 4 deals with assessing the risks associated with identified hazards [27,31,32], relevant to the reliance of KETs, by analyzing the likelihood and severity of potential incidents or accidents. Furthermore, strategies and measures, such as safety implementation, are devised to alleviate these identified risks.

To evaluate the influence exerted by KET on the ODD of an ADS, the ISO 34503 "Test scenarios for automated driving systems — Specification for operational design domain" is used as a baseline [8]. ISO 34503 applies to ADS levels 3-4 and provides requirements for a hierarchical taxonomy that identifies the ODD, considering both static and dynamic attributes.

ISO 34503 proposes dividing the operating conditions into three primary attributes: scenery, environmental conditions, and dynamic elements. Scenery refers to non-moving elements, dynamic elements represent moving elements in the operating environment,

and environmental conditions encompass factors between geographical and temporal attributes, including meteorological weather parameters relevant to the ODD. The hierarchy in ISO 34503 provides a base set of attributes that can be expanded based on stakeholder needs. To better incorporate KETs into the ODD taxonomy, the connectivity category in ISO 34503 can be refined to include communication, positioning, and cybersecurity. Communication requirements can include coverage, latency, throughput, and predictability, as listed in Table 1. Positioning requirements encompass absolute and relative positioning with sub-attributes like accuracy, precision, and refresh rate integrity, as shown in Table 2. Cybersecurity requirements can be derived based on the categorization proposed by Firesmith [33], as presented in Table 3.

Table 1. When assessing a V2X communication solution, the following attributes should be considered.

Attributes	Indication description
Coverage	The geographic area or range within a carrier's defined service. Indicates the solution's ability to establish and maintain connectivity.
Latency	Time delay between sending a message from a sender to its reception by the intended recipient. Indicates the responsiveness of communication solution.
Throughput	Number of data packets that can be transferred within a specific time. Indicates the solution's capacity to handle data traffic.
Predictability	Consistency, and reliability of solution performance. Indicates the ability to preempt and plan for degraded coverage, latency, and throughput.

Table 2. When assessing a positioning solution, the following attributes should be considered.

Attributes	Indication description
Position priority	Absolute, relative. Possible refinements: lateral, longitudinal or elevation position.
Accuracy	How close measurements are to the true position. Indicates the solution's capability to determine an object's location accurately.
Precision	How close measurements are to each other. Indicates the consistency of the solution in providing consistent position measurements.
Refresh rate	How close measurements are to each other in time. Indicate the solution's responsiveness.
Confidence	Confidence reflects the ability to quantify the uncertainty in measurements. Indicates the ability to handle and preempt degraded service. Confidence and integrity are closely related indicators.
Integrity	Integrity refers to the reliability and availability of the solution. Indicates the solution's ability to function correctly and consistently, providing accurate and trustworthy position information.

Table 3. Additional quality attributes to assess when considering cybersecurity .

Type ¹	Description
Prevention	Measures that reduce the security risks. It's preferable to stop risks realising than repair the damage after an incident.
Detection	Mechanisms to discern malicious activity from normal use.
Reaction	Strategies to employ after detecting malicious activity to minimise the harm.
Adaptation	Modification to improve prevention, detection, or reaction.

¹ Inspired by Firesmiths defensibility solution types [33]

Numerous vital questions still need to be addressed and recognized, including supporting cooperative functions and allocating responsibilities to ensure a safe implementation across multiple brands. Additionally, considerations of interdependence within the ODD

must be examined, including the specification and testing of supported vehicle velocities and establishing a trusted chain of external data sources. These external data sources should have a seamless chain of trust and consistent uncertainty measurements—also, assessment of common time base solutions for synchronized cooperative ADS.

While the attributes presented in the Tables 1, 2 and 3 may not cover all gathered requirements, and in all likelihood, not all relevant concerns are addressed, they provide useful patterns and attribute families for analyzing the performance of KETs and mapping them to the ODD. Additional research is required to delve into coverage and comprehensiveness when mapping an ODD to specific isolated technology elements, encompassing specification and testing. However, it is crucial to initiate the process of providing proactive and practical guidance to technical service providers to enhance their preparedness and streamline the assessment process.

4.4. Establish safety performance indicators and general scenarios

Much effort has been spent on the development of performance indicators [34,35] and scenario databases [36,37] focusing on data-driven aspects like longitudinal control (acceleration, braking and road speed, lateral control (lane discipline) and environment monitoring (headway, side, rear) as single aspects and when moving into more complex scenarios, in combination. This combination poses a challenge to proving ground capabilities due to the high level of coordination needed to realize the scenarios. As it is virtually impossible to evaluate an automated vehicle against all possible scenarios it will face in real-world traffic, balancing the representativeness of the tests and the reliable safety performance indicators is necessary.

Conversely, we talk about the assessment criteria subset that can be created for the attributes derived previously for the enabling technologies, positioning, communication (V2X) and cybersecurity. Knowledge-driven indicators that can be assigned elementary behavioural aspects of the automated function that must be assessed with scenarios linked to the ODD and its monitoring, e.g.,

- Conditions for activation
- Minimum risk manoeuvres
- External and internal human-machine interfaces

The assessment criteria are partly based on the existing automotive safety assessment methods (See Figure 3), as also discussed in Section 2. In the assessment framework, we describe activities as denoted (4); see Figure 4. i.e. new assessable criteria related to KETs.

There are two main criteria for scenario-based testing: pass/ fail and metric criteria. Both types are based on objective observation of the executed scenario. For success criteria and metrics, different context-specific safety performance indicators need to be defined, which gather the necessary data to evaluate and compare the expected and executed behaviour of the automated vehicle.

The derived attributes for each KET have an operating condition that needs to be fulfilled. A failure to uphold the conditions often leads to a minimal risk manoeuvre (MRM) activation to reach a minimal risk condition. Many failures, including attacks on vehicle control, environmental monitoring, and external and internal human-machine interface (HMI) interaction, trigger an MRM and HMI interaction whose appropriateness needs to be assessed [38].

For example, in the case of communication, metrics such as coverage, latency, throughput, and predictability can be used to assess the effectiveness of the communication system. The acceptable values for these metrics can be defined based on the ADS's safety requirements and ODD. These values should be determined through extensive research, analysis of existing standards and guidelines, and consideration of real-world operating conditions.

Similarly, for positioning, metrics like accuracy, precision, refresh rate, and integrity can be used to evaluate the ADS's ability to determine its position and track objects in its environment. The acceptable values for these metrics will depend on the specific use case and safety-critical requirements.

Regarding cybersecurity, metrics can include factors such as robustness against cyber-attacks, resistance to unauthorized access, and integrity of data transmission. Again, the acceptable values for these metrics need to be determined based on industry best practices, relevant standards, and the criticality of the ADS's functions. In conclusion, when addressing the requirements posed by the KETs, the number of scenarios with attached assessment criteria for minimum risk manoeuvres, transition hand-over, HMI (internal and external), and driver monitoring will expand, and the representatives and completeness must rigorously be checked for in the scenario catalogue.

5. Evaluation of the use of assessment templates

Analyzing how each use case relies on support technology building blocks, which are implementing the KETs, helps identify the specific requirements and dependencies of different technological components. Understanding these dependencies allows determining which assessment templates are relevant and how they should be applied (Figure 5). It also becomes possible to tailor the assessment process to the specific needs and requirements of the system in terms of functional requirements on the ODD and general scenarios to test or assess. Furthermore, it is essential to consider the interdependencies between different technology building blocks and how they collectively contribute to the overall functionality and safety of the automated driving system. In contrast, some assessment templates may address multiple technology components simultaneously.

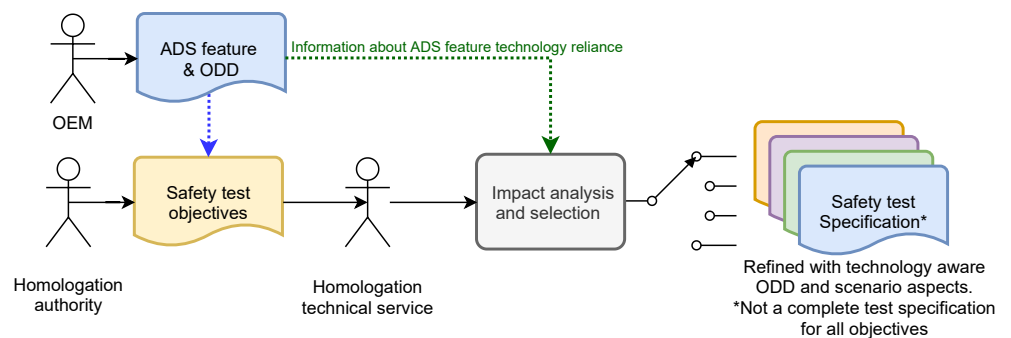


Figure 5. Schematic selection process of assessment templates.

5.1. ADS feature and ODD under evaluation

The evaluation centers on highly automated freight vehicles in a dedicated urban area, aiming for SAE Level 4 automation using remote assistance functionality. It involves automated freight transport within a controlled environment, specifically for potentially uncrewed vehicles. Design options include vehicles with or without a driver's cab, focusing on lower speeds for fuel efficiency.

As depicted in the Figure. 5 the input is the safety objectives, function description, and intended ODD. The description of the ADS features describes the system utilized, including the functions of remote assistance automated vehicle features and the infrastructure deployed within the trial environment.

The safety objectives align with the guidelines outlined by the Swedish Transport Agency (TSFS 2022:82 [39]), emphasizing including a traffic safety analysis and an independent risk assessment in all exemption applications. These safety objectives ensure that the evaluation process addresses and fulfills the requirements for risk assessment, guaranteeing the safety and reliability of testing the automated freight transport system on public roads. They serve as representative surrogates for the envisioned safety objectives of future type approval.



Figure 6. Potential ODD at Lindholmen. The geofenced route is denoted by green.

A potential site for conducting the ADS feature trials has been identified in the urban traffic environment at Lindholmen, Gothenburg, Sweden. The intended route can be seen in Figure 6. The ODD is relevant to this specific ADS feature and can be generally described as a route encompassing parking lots and streets with parked cars on either or both sides. Traffic in the area generally operates at low speeds, with few vulnerable road users (VRUs) except during lunch and rush hours. VRUs are expected to walk and cycle throughout the area.

- Road conditions: Public urban roads, going straight, intersection and turns.
- Geographical area: Lindholmen, Sweden. Exact geographic site with Geofence.
- Environmental conditions: Daylight, good visibility, no or light rain, little or no water on the road surface
- Velocities: Speed restricted to lower ranges < 15 km/h.
- Other constraints: Conditions must be fulfilled for the safe operation.

To ensure the trial operation of the vehicle maintains a traffic-safe environment, the assessment plan considers multiple aspects. These include adhering to regulatory requirements within the ODD, establishing safety and security objectives for remotely assisted automated functions, and ensuring seamless control transitions during operation.

A geofence solution utilizing GNSS acts as a safety and cybersecurity mechanism to mitigate vehicle operating risks beyond the defined ODD. While geofencing is partially rooted in threat analysis, additional cybersecurity assessment currently falls beyond the scope of this study. Maintaining precise positioning within the ODD is crucial, fulfilling a critical system safety and security requirement. This investigation primarily centers on KET's assessment guidance.

Hence, the relevant assessment templates encompass V2X communication, its interdependencies with cybersecurity in the context of 5G connectivity, and its position within the broader assessment plan, particularly regarding geofencing.

5.2. Guided assessment plan

This study primarily focuses on the interdependence between positioning, V2X communication, and their interplay with cybersecurity. It leaves significant portions of object detection and event response without specific assessment guidance.

Integrating 5G communication into the Operational Design Domain (ODD) expands the evaluation of operational conditions. The ODD's boundaries are extended by incorporating 5G communication attributes to encompass connectivity considerations. This evaluation encompasses system performance and safety scenarios like network congestion or communication disruptions.

Including 5G communication attributes in the assessment process aids in identifying potential risks and challenges. It evaluates the system's capability to handle situations involving degraded connectivity, assesses the impact of communication delays on decision-making processes, and tests the system's resilience against potential cybersecurity threats targeting the 5G infrastructure.

Therefore, compared to existing standards like ISO 34503, which includes attributes such as Vehicle-to-Infrastructure (V2I) and 5G, we propose a refinement of operating conditions to focus on attributes like network coverage, latency, throughput, and predictability.

These refined attributes are designed to serve as performance indicators. The assessment metrics and use-case-specific conditions were derived from the Safety Case for Autonomous Trucks (SCAT) project [40].

The real-time demands within the control loop necessitate precise latency requirements. Ensuring comprehensive coverage using minimum throughput or bandwidth is vital for the safe control of remote operations and for enabling actionable minimal-risk maneuvers. The guarantee of this minimum throughput holds utmost importance throughout the entire ODD. Maintaining high service availability is critical to preempting potential service congestion and counteracting inadequate coverage, especially in adverse weather conditions, emphasizing the need for predictability. This comprehensive coverage requirement must be consistently met within the ODD in alignment with the communication attributes specified in Table 1.

Furthermore, the Quality of Service (QoS) functionality within the network can address specific service congestion, regardless of whether it results from natural factors or intentional actions. Predictability can be further achieved by implementing multiple redundant 5G carrier networks and real-time performance monitoring.

Table 4. Assessment criteria for operating conditions within the Lindholmen ODD for 5G communication.

Attributes	Indication description
Coverage	5G communication coverage present in the whole Lindholmen ODD. Coverage is achieved by several cells. Handover must not affect Throughput.
Latency	Here assessed to be subsumed by 5G coverage and validated by video performance tests.
Throughput	Target bandwidth 20 Mbit/s. Unsafe < 1 MBit/s and 15 frames per second.
Predictability	Deployment-site test measurements and Quality of Service (QoS).

The assessment of GNSS-based geofence considerations follows a similar approach. It employs the prototype template in Table 2, focusing on absolute positioning by relying on GNSS. GNSS guarantees precise location information for the geofence system. Achieving accuracy within a meter is pivotal, and this level of precision can be attained by implementing a real-time kinematic (RTK) solution.

Precision is a critical factor in the geofence solution. Consistently delivering real-time kinematic (RTK) based position measurements ensures the system's reliability and accuracy in pinpointing an object's location within the geofence.

The refresh rate holds significant importance in geofence systems. It determines how frequently the position measurements are updated. In geofencing, a refresh rate exceeding 1 Hz is generally preferred. Incorporating odometric data with GNSS measurements can help achieve this, enhancing system redundancy and accuracy.

Maintaining confidence in the measurements is vital. The system should be capable of quantifying the uncertainty associated with position measurements. This quantification aids in assessing the reliability and robustness of the geofence solution.

To ensure the integrity of the geofence system, a recommended strategy is to employ a multiple-constellation solution. This approach enhances both reliability and availability. Incorporating a second observer plausibility check and dual-frequency receivers, alongside RTK technology, further bolsters the integrity of the geofence solution. The accuracy and reliability of GNSS-based geofence solutions can be assessed by evaluating these criteria.

The assessment template underscores the necessity of evaluating test scenarios that directly relate to dependency checks and ODD monitoring. These scenarios encompass a range of aspects, such as control transition demands, minimal risk maneuvers, and considerations regarding internal and external HMI interactions.

Regarding activation scenarios, these tests ensure that all KET ODD conditions are met before activation occurs. Conversely, deactivation scenarios assess the appropriateness of both internal and external HMI responses when deactivation is required. This deactivation can be initiated gracefully through control transition demands or via minimal risk maneuvers, ensuring safety is maintained.

Using the prototype assessment templates in conjunction with general scenarios (e.g. control transition demands, minimal risk maneuvers, activation, deactivation) proposes evaluating 40 distinct test scenarios. These scenarios are supported by ten indicators that focus on the fundamental behavioral aspects of the automated function. These indicators are particularly pertinent to 5G communication and geofence conditions. They are organized into various categories, covering activation conditions, minimal risk maneuvers, and external and internal HMI conditions. The number of conditions within each category may vary, with at least four conditions related to 5G communication and six conditions for geofence considerations.

5.2.1. Cybersecurity of 5G

When applying the derived cybersecurity attributes outlined in Subsection 4.3, we gain insights into essential prevention measures for ensuring the authenticity of service subscribers. Paramount among these measures is the prevention of unauthorized vehicle control. To achieve this, communication must be authenticated and encrypted, safeguarding the integrity, confidentiality, and authenticity of the entities involved.

Detection mechanisms between the remote assistance and the vehicle are crucial to discern malicious activity from regular use. In case of failure or an attack, the reaction strategy should follow a fail-safe approach, transitioning the system into a safe operating mode with reduced functionality. Furthermore, considerations for system adaptation may extend to communication coverage, where an over-the-air update could be necessary to patch any identified security vulnerabilities.

As depicted in Table 5, assessing the presence and appropriateness of cybersecurity measures, even in conjunction with quality attributes linked to another KET (such as V2X communication), is paramount. Though not directly part of the ODD, this consideration adds a robust layer to the evaluation process. By incorporating an evaluation of threat agents and potential attack surfaces within the ODD, a more robust connection is forged between the ODD and activities tied to threat analysis and risk assessment. Such an assessment guides the implementation of necessary safeguards against possible attacks and the potential consequences of breaches to the system.

Table 5. Cybersecurity example considerations per attribute of 5g connectivity.

Attributes	Prevention	Detection	Reaction	Adaptation
Coverage	Implementation of strong authentication protocols. Regular security audits and vulnerability assessments.	Intrusion detection systems (IDS). Network traffic monitoring.	Immediate incident response and mitigation. Isolation of affected components.	Upgrading security protocols based on emerging threats. Continuous monitoring and updates.
Latency	Network optimization for reduced latency. Use of caching and content delivery networks (CDNs).	Anomaly detection algorithms. Latency monitoring tools.	Timely notification and escalation procedures. Remediation actions to mitigate latency-related threats	Adoption of emerging technologies to minimize latency. Performance optimization strategies.
Throughput	Bandwidth management and allocation. Quality of Service (QoS) prioritization	Traffic analysis for abnormal patterns. Throughput monitoring tools.	Traffic filtering and blocking of malicious connections. Throttling or rate limiting for suspicious activities	Capacity planning and scaling to meet increasing throughput demands. Optimization of network resources.
Predictability	Robust network architecture and routing protocols. Redundancy and failover mechanisms.	Behavior analytics for anomaly detection. Predictability monitoring and analysis.	Incident response plans and playbooks. Business continuity strategies for predictable disruptions.	Continuous improvement based on predictive analytics. Adaptive network configurations.

Through integrating cybersecurity measures, the assessment plan significantly more comprehensively assesses the system's safety and resilience, aligning with future type approval requirements.

The attributes derived in Section 5 proved invaluable for enriching assessment planning and analyzing use cases. They highlighted the importance of ensuring 5G communication coverage with QoS bandwidth priority to maintain bandwidth during congestion, whether from natural factors or malicious actions. Further assessment of the attributes' utility for proving-ground testing is yet to be undertaken.

5.3. Test scenarios for communication

The assessment template emphasizes crucial test scenarios, particularly those directly tied to KET ODD dependencies and their monitoring through performance indicators. These scenarios ensure the availability of all necessary conditions for activating and maintaining the ADS feature throughout the ODD, here focusing on connectivity. Conducting tests allows for assessing system functionality and performance within defined ODD, offering valuable insights into its strengths and limitations.

Evaluating cellular coverage at the test site is paramount to ensure dependable communication and data exchange between the vehicle and infrastructure. This is vital for the seamless operation of the monitored ADS feature, encompassing functionalities like assistance and monitoring links. Maintaining a bidirectional stream with balanced symmetric bandwidth and low latency for the control channel requires consistent capacity to attain robust connectivity. By gaining a comprehensive understanding of the test site's capabilities and limitations, effective planning and preparation for operational deployment become achievable. This involves identifying areas that require enhancement or optimization and ensuring that the essential infrastructure and connectivity requirements are met to showcase the ADS feature successfully.

Remote assistance and monitoring, especially video streaming, necessitates low latency and high uplink bandwidth. The adaptive video codec should accommodate varying bitrates based on availability. Additionally, the uplink is typically more constrained than

the downlink, making it a critical consideration. The site assessment has concentrated on available uplink capacity, likely to be the limiting factor in this scenario.

The assessment predominantly focused on measuring Reference Signal Received Power (RSRP). RSRP is a reliable indicator for predicting radio uplink capacity since it gauges the cell's proximity from a radio standpoint. Up-link radio interference is mainly due to other handsets moving within the cell, making it more dynamic and harder to predict than downlink interference.

The site assessment employed a low adaptive latency User Datagram Protocol (UDP) stream to validate video performance. This helped estimate the traffic that could be sent on the uplink without causing delays or overloading the network. Unlike network speed test tools prioritizing high bandwidth, this approach considers absolute latency and latency variation (jitter).

The test utilized a handheld terminal with a specialized carrier company application (Telia). This application collected and reported essential radio measurements, including Reference Signal Received Power (RSRP), Reference Signal Received Quality (RSRQ), Signal-to-noise ratio (SNR), frequency, cell information, and absolute position using GNSS (Global Navigation Satellite System). Figure 8 showcases RSRP as a performance indicator for coverage, while Figure 9 illustrates the related general handover scenario.

An adaptive UDP stream, emulating adaptive video, was used to measure real-time bandwidth (RT BW) up to a target level. Laps 1 and 2 employed a 20 Mbit/s target bitrate, with later laps using 50 Mbit/s. RT BW serves as a performance indicator for throughput, as depicted in Figure 10, and the related scenarios are portrayed in Figure 11.

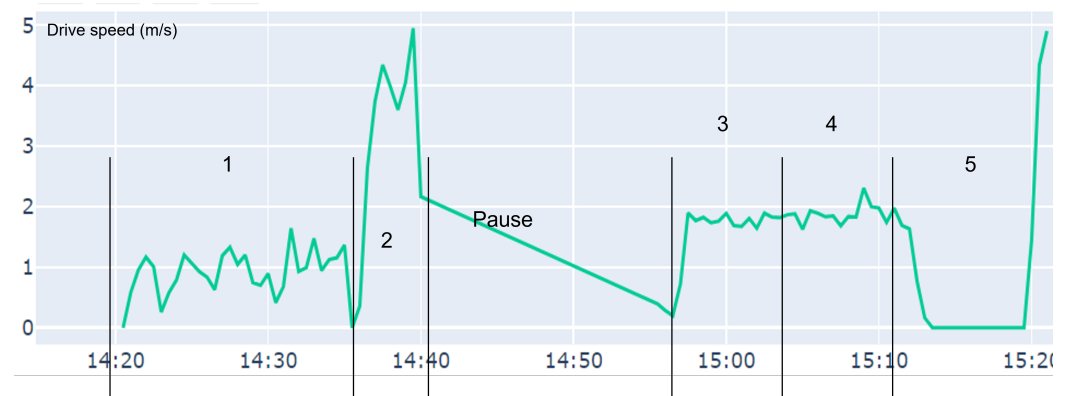


Figure 7. Data was collected over a total of 5 laps at the route at Lindholmen.

The tester held the terminal during the initial lap shown in Figure 7. For laps 2 to 5, the handheld device was positioned between the front seats of a car driving along the track. The first two laps utilized a target bitrate of 20 Mbit/s, while the subsequent laps were conducted with a higher target bitrate of 50 Mbit/s.

In an unloaded network, latency remains consistent at a specific location. The latency measured by the tool reflects the delay of the transmitted data stream. A significant relationship exists between traffic load and latency, as increased load results in network queues. The concept of real-time bandwidth aims to maximize bandwidth while preserving low latency.

The measurement tool employs Ericsson's SCReAM algorithm [41], a mobile-optimized congestion control algorithm. SCReAM dynamically adjusts bandwidth based on various metrics, including Round Trip Time (RTT). As depicted in Figure 11, SCReAM responds by reducing bandwidth when RTT increases, effectively minimizing latency. Therefore, RT BW refers to data delivered within a reasonably bounded RTT delay. Both bandwidth and throughput serve as indicators of network performance. While bandwidth indicates the available or predicted network capacity, throughput represents the transmitted data. Given the susceptibility of intended networks to congestion, mainly as they are not private, throughput is a more pertinent measurement in this context.

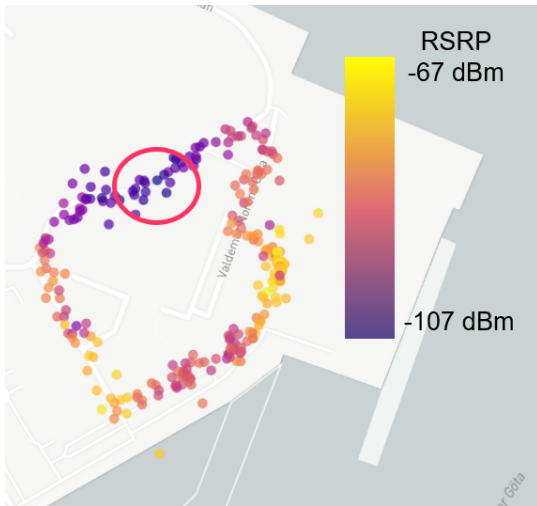


Figure 8. Reference Signal Received Power (RSRP) primary cells.

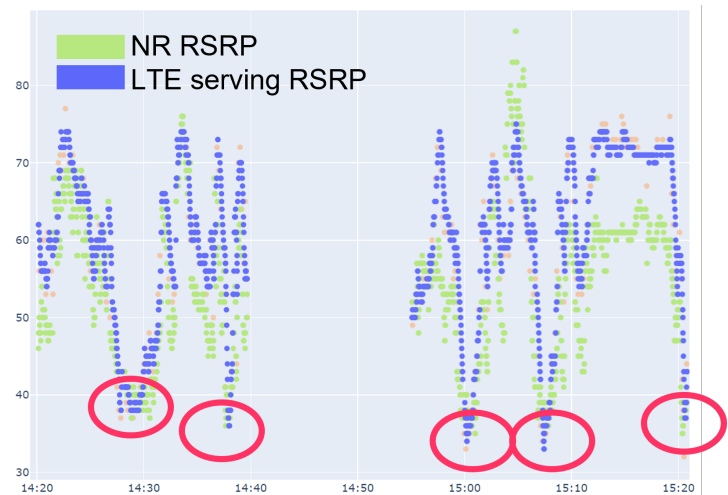


Figure 9. NR and LTE Reference Signal Received Power (RSRP) over time. Points of interest are circled in red in both graphs.

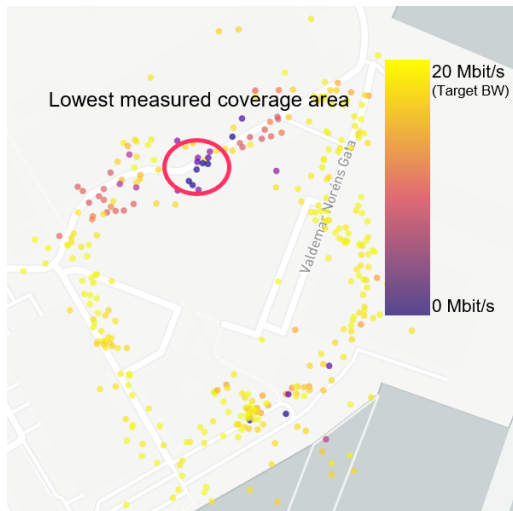


Figure 10. Measured bandwidth in the demonstration area.

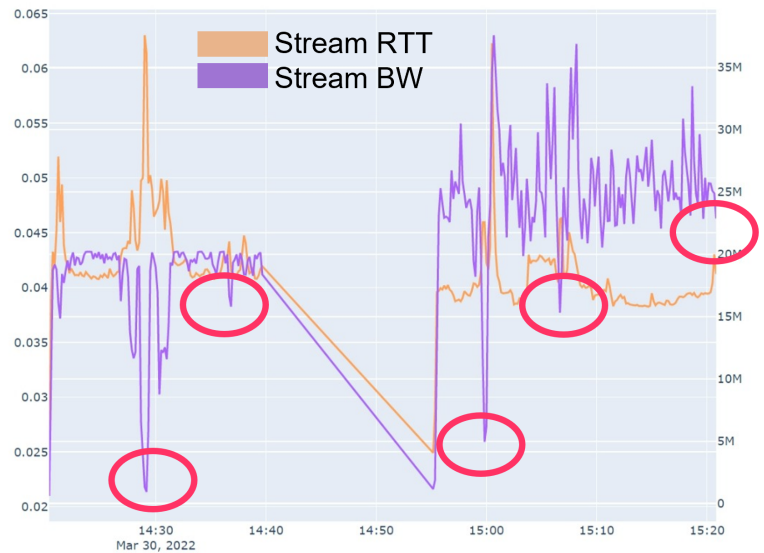


Figure 11. Stream round trip time (RTT) and stream bandwidth (BW) over time. Points of interest are circled in red in both graphs.

Accurately predicting handover issues between cells holds significant importance in the coverage testing of cellular networks. This prediction entails assessing elements such as signal strength, quality, and latency to detect potential challenges during the handover procedure, as exemplified in the problematic region between cell 1 and cell 2 in Figure 12. Operators can enhance handover algorithms and configurations through scenario simulations and an in-depth network performance analysis to achieve uninterrupted connectivity. However, conducting a dedicated ODD assessment is imperative to validate and assess the results. In summary, a site assessment guided by the relevant assessment templates, where predefined performance indicators tied to general scenarios served as a foundational framework, saving a lot of effort. This baseline approach provides a starting point for a more customized and specific assessment strategy.

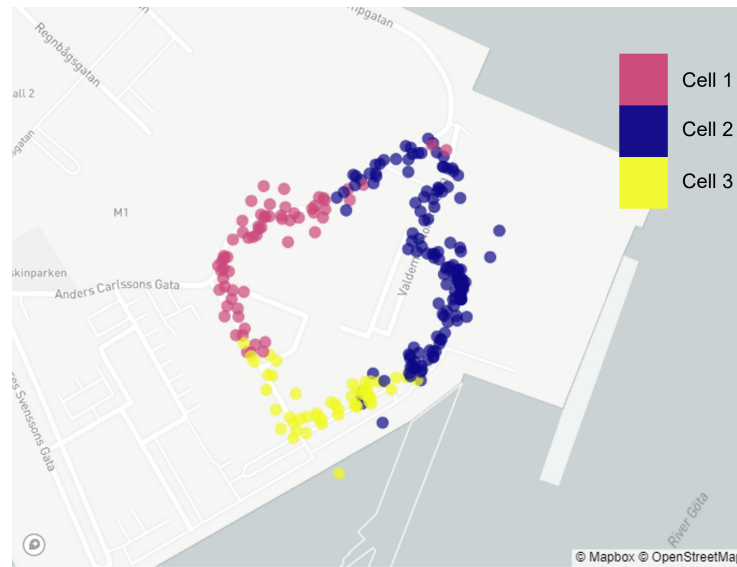


Figure 12. Three cells are involved in the coverage

6. Conclusion

In conclusion, while notable strides have been taken in safety assessment strategies for automated vehicles, certain limitations linked to the practical assessment endeavor still require attention. The proposed approach underscores the significance of technology-aware practical guidance within the assessment process, which should seamlessly integrate into a comprehensive and adaptable framework.

The primary contribution of this study lies in proposing the augmentation of existing scenario-based testing frameworks with a detailed examination of the underlying supporting technologies. This approach enriches the test suite employed in scenario-based testing by factoring in the specific attributes of test scenarios linked to the Key Enabling Technologies (KETs). By blending this bottom-up analysis with the top-down scrutiny focused on potentially hazardous traffic scenarios at the vehicle level, a more comprehensive understanding of the system's performance can be achieved.

While the method outlined in this study demonstrates practicality and efficacy, certain areas warrant further exploration. Subsequent research should investigate the extent of coverage and completeness when mapping the ODD to precise technological elements in specification and testing. The amalgamation of knowledge-driven and data-driven approaches could yield a more holistic assessment framework, drawing from existing knowledge and real-world data. Particularly, when substantial real-world data is unavailable, the integration of prior knowledge becomes pivotal.

Therefore, developing technology-aware assessment criteria for attributes derived from enabling technologies holds paramount importance. These criteria should complement the overarching high-level requirements and encompass the fundamental behavioral facets of the automated function within the defined ODD. This involves appraising the proper functionality of sensors and communication devices, adherence to protocols and standards, and effective mitigation of potential cybersecurity threats. By assimilating technology-aware assessment criteria, a more comprehensive evaluation of the automated function's performance can be achieved.

Author Contributions: Conceptualization and methodology, Martin Skoglund; validation measurements, Mats Bergman; investigation, Martin Skoglund and Anders Thorsén and Fredrik Warg; writing—original draft preparation, Martin Skoglund and Anders Thorsén and Fredrik Warg; writing—review and editing, Martin Skoglund and Anders Thorsén and Fredrik Warg; supervision, Fredrik Warg. All authors have read and agreed to the published version of the manuscript.

Funding: The SUNRISE project (www.ccam-sunrise-project.eu) has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 101069573. The JU receives support from the

European Union's Horizon 2020 research and innovation programme. The SCAT project (2020-04205) has received funding from Vinnova, Sweden's innovation agency. Content reflects only the authors' view and European Commission nor Sweden's innovation agency is not responsible for any use that may be made of the information it contains.

Institutional Review Board Statement: Not Applicable.

Informed Consent Statement: Not Applicable.

Data Availability Statement: Not Applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

- SAE. SAE J3016 - Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles. Surface Vehicle Recommended Practice J3016 APRIL2021, SAE International, 2021.
- UN Regulation No 157 – Uniform Provisions Concerning the Approval of Vehicles with Regards to Automated Lane Keeping Systems [2021/389], 2021.
- WP.29/GRVA. Current Draft of the Guidelines and Recommendations Concerning Safety Requirements for ADS (FRAV). <https://unece.org/transport/documents/2022/05/informal-documents/frav-current-draft-guidelines-and-recommendations>, 2022.
- Chan, C.Y. Advancements, Prospects, and Impacts of Automated Driving Systems. *International journal of transportation science and technology* **2017**, *6*, 208–216.
- Chen, C.; Qidong, Z.; Tong, Z.; Yang, Z.; Xianglei, Z. The Research on Current Automated Driving ODD Regulations, Standards and Applications. In Proceedings of the 2022 IEEE International Conference on Real-Time Computing and Robotics (RCAR), 2022, pp. 744–747. <https://doi.org/10.1109/RCAR54675.2022.9872246>.
- Gyllenhammar, M.; Johansson, R.; Warg, F.; Chen, D.; Heyn, H.M.; Sanfridson, M.; Söderberg, J.; Thorsén, A.; Ursing, S. Towards an Operational Design Domain That Supports the Safety Argumentation of an Automated Driving System. In Proceedings of the 10th European Congress on Embedded Real Time Systems (ERTS 2020), 2020.
- BSIGROUP. PAS 1883:2020 Operational Design Domain (ODD) Taxonomy for an Automated Driving System (ADS) – Specification. Technical report, BSIGROUP, 2020.
- "International Organization for Standardization". ISO 34503 Road Vehicles — Test Scenarios for Automated Driving Systems — Specification for Operational Design Domain. <https://www.iso.org/standard/78952.html>.
- Association for Standardization of Automation and Measuring Systems. ASAM OpenODD. <https://www.asam.net/standards/details/openodd>.
- Ulbrich, S.; Menzel, T.; Reschka, A.; Schuldt, F.; Maurer, M. Defining and Substantiating the Terms Scene, Situation, and Scenario for Automated Driving. In Proceedings of the 2015 IEEE 18th International Conference on Intelligent Transportation Systems, 2015, pp. 982–988. <https://doi.org/10.1109/ITSC.2015.164>.
- Menzel, T.; Bagschik, G.; Maurer, M. Scenarios for Development, Test and Validation of Automated Vehicles. In Proceedings of the 2018 IEEE Intelligent Vehicles Symposium (IV). IEEE, 2018, pp. 1821–1827.
- Koopman, P.; Wagnier, M. Autonomous Vehicle Safety: An Interdisciplinary Challenge. *IEEE Intelligent Transportation Systems Magazine* **2017**, *9*, 90–96.
- Riedmaier, S.; Ponn, T.; Ludwig, D.; Schick, B.; Diermeyer, F. Survey on Scenario-Based Safety Assessment of Automated Vehicles. *IEEE Access* **2020**, *8*, 87456–87477. <https://doi.org/10.1109/ACCESS.2020.2993730>.
- Laboratories, U. UL 4600: Standard for Evaluation of Autonomous Products. Technical report, Underwriters Laboratories, 2020.
- Thorn, E.; Kimmel, S.C.; Chaka, M.; Virginia Tech Transportation Institute.; Southwest Research Institute.; Booz Allen Hamilton, Inc. A Framework for Automated Driving System Testable Cases and Scenarios. Technical Report DOT HS 812 623, National Highway Traffic Safety Administration, 2018.
- 183rd WP.29. New Assessment/Test Method for Automated Driving (NATM) (Proposal). Informal Document WP.29-183-05, 183rd WP.29, 9 - 11 March 2021 Agenda items 2.3 and 3.5.5, 2021.
- Cieslik, I.; Expósito Jiménez, V.J.; Martin, H.; Scharke, H.; Schneider, H. State of the Art Study of the Safety Argumentation Frameworks for Automated Driving System. In Proceedings of the Computer Safety, Reliability, and Security. SAFECOMP 2022 Workshops; Trapp, M.; Schoitsch, E.; Guiochet, J.; Bitsch, F., Eds.; Springer International Publishing: Cham, 2022; Lecture Notes in Computer Science, pp. 178–191. https://doi.org/10.1007/978-3-031-14862-0_14.
- HEADSTART Project. <https://www.headstart-project.eu/>.
- Skoglund, M.; Thorsén, A.; Arrue, A.; Coget, J.B.; Plestan, C. Technical and Functional Requirements for V2X Communication, Positioning and Cyber-Security in the HEADSTART Project. In Proceedings of the Proceedings of ITS World Congress 2021, 2021.
- Anders Thorsén.; Martin Skoglund.; Fredrik Warg.; Jan Jacobson.; Robert Hult.; Nicolas Wagener.; Athanasios Ballis.; Jacco van de Sluis.; Juan Jose Perez.; Andrea Steccanella. HEADSTART D 1.3 Technical and Functional Requirements for KETs. HEADSTART Deliverable HEADSTART D 1.3v2.0, HEADSTART project, 2021.

21. Martin Skoglund.; Robert Hult.; Jan Jacobson.; Mats Jonasson.; Athanasios Ballis.; Patrick Weissensteiner.; Jean-Baptiste Coget.; Oihana Otaegui.; Andre Wiggerich.; Nicolas Wagener.; et al. HEADSTART D 1.4 Functional Requirements of Selected Use Cases. HEADSTART Deliverable HEADSTART D 1.4, HEADSTART project, 2019. 765
22. Wagener, N. Common Methodology for Data-Driven Scenario-Based Safety Assurance in the HEADSTART Project. In Proceedings of the Virtual ITS European Congress. Zenodo, 2020. <https://doi.org/DOI:10.5281/zenodo.5358057>. 766
23. Alliance, N. V2X Task Force: V2X White Paper. Technical report, NGMN Alliance, 2018. 767
24. CEN/CENELEC. EN 16803-1:2020 - Space - Use of GNSS-based Positioning for Road Intelligent Transport Systems (ITS) - Part 1: Definitions and System Engineering Procedures for the Establishment and Assessment of Performances. Technical Report EN 16803-1:2020, CEN/CENELEC, 2016. 768
25. Radack, S. Federal Information Processing Standard (Fips) 199, Standards for Security Categorization of Federal Information and Information Systems. Technical report, National Institute of Standards and Technology, 2004. 769
26. SAE. SAE J3061 - Cybersecurity Guidebook for Cyber-Physical Automotive Systems. Technical report, SAE International, 2016. 770
27. ISO/SAE. ISO/SAE 21434:2021 -Road Vehicles — Cybersecurity Engineering. Technical report, ISO/SAE, 2021. 771
28. Lonc, B.; Cincilla, P. Cooperative ITS Security Framework: Standards and Implementations Progress in Europe. In Proceedings of the 2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2016, pp. 1–6. <https://doi.org/10.1109/WoWMoM.2016.7523576>. 772
29. Marojevic, V. C-V2X Security Requirements and Procedures: Survey and Research Directions, 2018, [arxiv:cs, eess/1807.09338]. <https://doi.org/10.48550/arXiv.1807.09338>. 773
30. ISO. ISO/TR 4804:2020 Road Vehicles — Safety and Cybersecurity for Automated Driving Systems. Technical Report, International Organization for Standardization., 2020. 774
31. ISO. ISO 26262:2018 Road Vehicles : Functional Safety. Technical report, ISO, 2018. 775
32. ISO. ISO/PAS 21448:2019 - Road Vehicles – Safety of the Intended Functionality. Technical report, International Organization for Standardization, 2019. 776
33. Firesmith, D.G. A Taxonomy of Security-Related Requirements. In Proceedings of the Proceedings of the Fourth International Workshop on Requirements Engineering for High-Availability Systems (RHAS'05); , 2005; p. 11. 777
34. de Gelder, E.; Paardekoooper, J.P. Assessment of Automated Driving Systems Using Real-Life Scenarios. In Proceedings of the 2017 IEEE Intelligent Vehicles Symposium (IV). IEEE, 2017, pp. 589–594. 778
35. Roesener, C.; Sauerbier, J.; Zlocki, A.; Fahrenkrog, F.; Wang, L.; Várhelyi, A.; de Gelder, E.; Dufils, J.; Breunig, S.; Mejuto, P.; et al. A Comprehensive Evaluation Approach for Highly Automated Driving. In Proceedings of the 25th International Technical Conference on the Enhanced Safety of Vehicles (ESV)National Highway Traffic Safety Administration, 2017. 779
36. Nalic, D.; Mihalj, T.; Bäumlér, M.; Lehmann, M.; Eichberger, A.; Bernsteiner, S. Scenario Based Testing of Automated Driving Systems: A Literature Survey. In Proceedings of the FISITA Web Congress, 2020, Vol. 10. 780
37. Düser, T.; Abdellatif, H.; Gutenkunst, C.; Gnanndt, C. Approaches for the Homologation of Automated Driving. *ATZelectronics worldwide* **2019**, *14*, 48–53. 781
38. Warg, F.; Skoglund, M.; Sassman, M. Human Interaction Safety Analysis Method for Agreements with Connected Automated Vehicles. In Proceedings of the 2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall), 2021, pp. 01–07. <https://doi.org/10.1109/VTC2021-Fall52928.2021.9625202>. 782
39. Transportstyrelsen. Transportstyrelsens föreskrifter och allmänna råd om tillstånd att bedriva försök med automatiserade fordon, 2022. 783
40. Sobiech, C.; Berglund, P.; Bergman, M.; Johansson, V.; Lundahl, J.; Nylander, T.; Skoglund, M.; Strandberg, T. Safety Case for Autonomous Trucks (SCAT). Technical report, Research Institutes of Sweden, 2023. 784
41. SCReAM. github.com/ericssonresearch/scream, 2023. 785