vehicles

Article

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 [2]

[1] RISE—Research Institutes of Sweden, 504 62 Borås, Sweden; fredrik.warg@ri.se (F.W.); anders.thorsen@ri.se (A.T.)
[2] Telia Company, 169 94 Solna, Sweden; mats.bergman@teliacompany.com
[*] 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 machine 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 ensures 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 by 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 of this paper are: (1) outlining a method for deriving assessment templates for use in future ADS assessments; (2) demonstrating the method by analysing 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 functional scenarios linked to the ODD and KETs.

Keywords: safety assessment; operational design domain; automated driving; communication; connectivity; positioning; cybersecurity

check for updates

Citation: Skoglund, M.; Warg, F.; Thorsén, A.; Bergman, M. Enhancing Safety Assessment of Automated Driving Systems with Key Enabling Technology Assessment Templates. *Vehicles* **2023**, *5*, 1818–1843. https://doi.org/10.3390/vehicles5040098

Academic Editors: Deogratias Eustace, Bhaven Naik, Heng Wei, Parth Bhavsar and Chen Lyu

Received: 30 August 2023
Revised: 10 November 2023
Accepted: 6 December 2023
Published: 13 December 2023

1. Introduction

The introduction of Automated Driving Systems (ADSs) has created a shift in the approach to safety assurance in the automotive industry. Contrasting with 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 a 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, as seen in Figure 1.

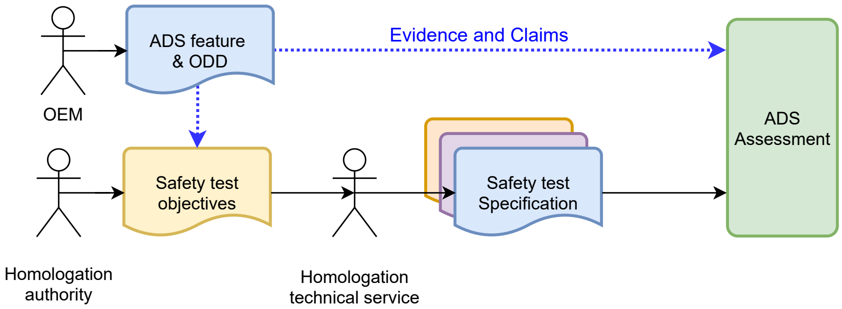

Figure 1. In the type-approval process, key entities include the OEM, Homologation Authority, and Homologation Technical Service Provider.

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 the safety, environmental impact, and legal requirements. They review documentation, conduct tests, and issue type-approval certificates. The Homologation Technical Service Provider is an independent organisation authorised by the Homologation Authority. They perform testing, evaluation, and certification services. Following standardised procedures, they assess the product performance, safety, and environmental characteristics that support the type-approval process.

An ADS assessment scheme must consider complex sensors, algorithms, and the vehicle's decision-making process to operate in automated mode. To meet the challenge of assessing an ADS, the United Nations Economic Commission for Europe (UNECE) World Forum for the Harmonisation of Vehicle Regulations (WP.29) drafted a "New Assessment and Test Method" (NATM) that may become part of the future type approval for ADSs.

The procedural goal of NATM is to conduct an empirical, objective, practical, and repeatable independent safety assessment of any ADS while maintaining technology neutrality. The assessment is based on high-level safety requirements [3] aiming to determine whether the vehicle can operate safely within its operational design domain (ODD) by examining scenarios linked to road users' behaviour, environmental conditions, and driver behaviour. A consensus exists that to evaluate an ADS implementation reliably, there is a need to employ a combination of methods to validate the capabilities; hence, NATM's multimethodologies (pillars) approach includes a scenarios catalogue that combines accelerated (simulation) testing, the test track, real-world testing, audit/assessment procedures, and in-service monitoring and reporting.

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 availability of safety-assessment frameworks, standards, and guidelines, there remains a need for detailed practical guidance in conducting safety assessments for ADSs. This necessity arises from the current work's general nature, which often lacks the specificity required to address the challenges posed by the complex operational contexts of ADSs. This is especially true for the assessment tasks envisioned by a technical service provider, which are 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 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 ADSs' 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 evaluation using a single template is currently unattainable.

To address this challenge, our contribution is threefold. First, we introduce a novel method for constructing specialised subsets of assessment templates tailored to ADSs and their specific reliance on KETs. We employ an approach that involves gathering requirements through stakeholder data collection and use cases. From these requirement groups, we derive relevant attributes that serve as the foundation for our assessment templates. In this context, requirement attributes are precisely defined as properties of a requirement that capture essential information that is well-suited for evaluation. Secondly, we put our proposed method into action by exploring requirements associated with two ubiquitous enabling technologies in ADSs: positioning and communication. Furthermore, we address the quality attribute of cybersecurity in the context of its intersection with safety considerations. This analysis results in creating specialised templates that offer a more focused and targeted approach. These templates provide forward-thinking, practical guidance tailored to assessing ADSs, ensuring an effective and thorough evaluation process. Third, we demonstrate the effectiveness of the assessment templates through a use case involving a remotely assisted truck. This practical application showcases the template content of attributes and assessable performance indicators in test scenarios.

Our threefold contribution introduces a method for developing specialised assessment templates tailored for ADSs. To the best of our knowledge, no existing approach investigates technology-aware assessment criteria to enhance safety assessments in this manner. Finally, we demonstrate the practical utility of these templates through a real-world use case, collectively advancing the field of ADS safety assessments. The KET-specific assessment templates significantly facilitate structured, technology-aware evaluations of ADS safety and performance. They establish a knowledge-driven, consistent, and repeatable assessment framework. However, it is important to note that the assessment template approach has limitations, primarily relying on predefined scenarios. As such, it is designed to complement data-driven methodologies that incorporate real-world data for a more comprehensive assessment. Additionally, these templates should be subject to continuous updates and refinements to align with ongoing technology developments.

This paper is organised 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 utilised 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, uses 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 recognised as a taxonomy and definition reference for Automated Driving Systems (ADSs) [1]. ADS features are categorised under SAE automation levels three to five. 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, nonfunctional, and technical requirements are crucial considerations throughout the development, type approval, and consumer testing of ADSs. The assessment of ADS features is significantly influenced by the concept of the operational design domain (ODD) [5,6]. The 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 set by the British Standards Institution (BSI) [7], the International Organization for Standardization (ISO) [8], and the Association for the Standardization of Automation and Measuring Systems (ASAM) OpenODD [9].

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. Another important aspect is the use of scenario-based testing [10–12]. Scenario-based testing aims to identify and test scenarios that are safety critical for the ADS feature in scope to ensure automated vehicles' safe operation [13].

The 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. 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 [14]. These approaches all enable the assessment of the system's safety and performance in various contexts. However, ensuring that autonomous systems meet the requirements and can operate safely in diverse environments requires a holistic approach.

Several efforts are made to develop standardised testing methodologies for ADSs, and some focus on assessments [15]. Examples of standardised testing are the National Highway Traffic Safety Administration (NHTSA) Framework for Automated Driving System Testable Cases and Scenarios (ref. [16]) and the New Assessment/Test Method for Automated Driving (NATM) [17] proposed by the United Nations Economic Commission for Europe (UNECE). We primarily concentrate on NATM due to its significance in the European context.

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, represents a prevalent practice within numerous assessment initiatives [10,15,17], with a sequential flow of activities in scenario-based evaluations of ADS, starting with a scenario catalogue. The efficacy and efficiency of the assessment process are heavily contingent upon the data in the scenario catalogue. Safety-performance indicators (SPIs) are tools for monitoring the validity of safety claims throughout the design, simulation, testing, and deployment stages [15]. The effective use of SPIs lies in their ability to prompt timely improvements by linking specific metrics to safety claims, ensuring a direct connection between the observed data and overall safety objectives.

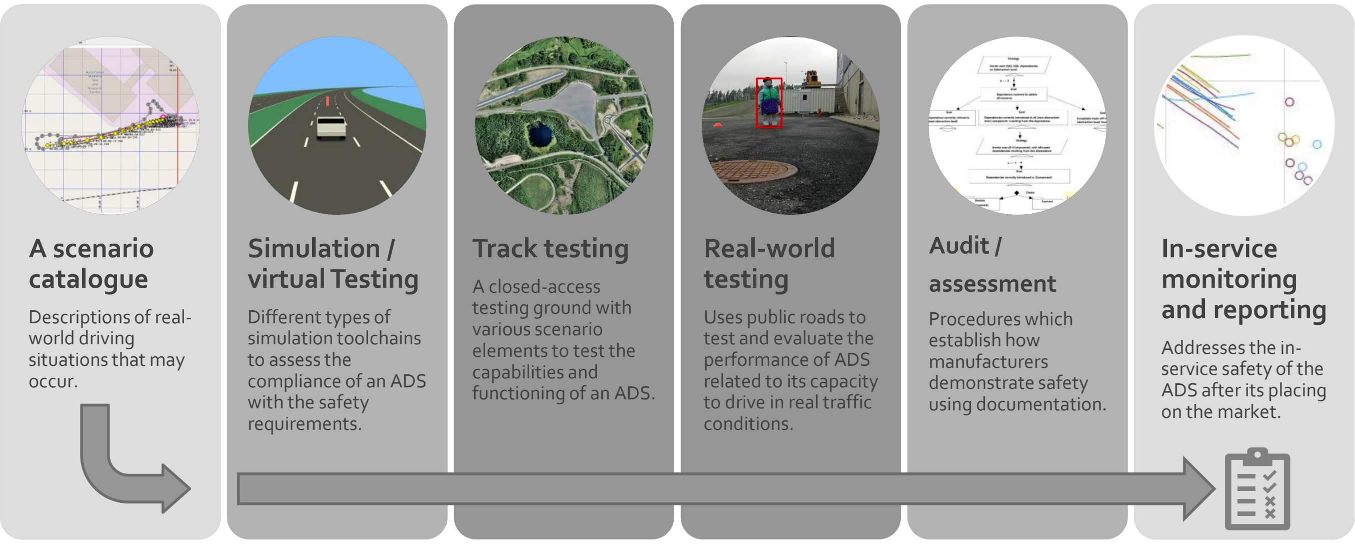
A scenario catalogue
Descriptions of real-world driving situations that may occur.
Simulation / virtual Testing
Different types of simulation toolchains to assess the compliance of an ADS with the safety requirements.
Track testing
A closed-access testing ground with various scenario elements to test the capabilities and functioning of an ADS.
Real-world testing
Uses public roads to test and evaluate the performance of ADS related to its capacity to drive in real traffic conditions.
Audit / assessment
Procedures which establish how manufacturers demonstrate safety using documentation.
In-service monitoring and reporting
Addresses the in-service safety of the ADS after its placing on the market.

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

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 [18] for different Automated Driving Systems. Since NATM is technology-neutral, 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. The authors argue that the method of using the assessment templates proposed in this paper can help mitigate these limitations. An assessment template can add general scenarios to the scenario catalogue 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

Safety-performance indicators are important in a safety-assessment process. Striking a balance between test representativeness and reliable performance indicators is essential. These indicators encompass many factors that require evaluation, which should strongly reflect the overall vehicle's safety performance. Our thesis asserts that analysing KETs is fundamental to develop practical guidance to evaluate the soundness and comprehensiveness of the ODD and functional scenarios to test 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.

Safety-performance indicators cover various critical aspects and can be categorised as follows:

1. Indicators of system reliability include assessing the system's failure rate, response time, redundancy, and more.
2. Indicators of safety by design, evaluating hazard identification, safety-critical scenarios, cybersecurity, and safety-feature activation.
3. Indicators of design soundness and coverage of the ODD.
4. Indicators of human–machine interaction, assessing driver engagement, monitoring, and user interface design.
5. Indicators of verification and validation, analysing test coverage, scenario replication, and validation.

6. Indicators of regulatory compliance, confirming adherence to legal and ethical standards.
7. Indicators of user perception, evaluating user feedback to understand perceived safety and acceptance.

It is important to note that each vehicle-level performance indicator must be further broken down into indicators relevant to the KET under assessment. For instance, if we are assessing the communication technology of the autonomous system, specific indicators related to communication reliability, latency, and data security should be considered. These KET-specific indicators must then be aggregated into a system-level indicator to provide an overarching assessment of the autonomous vehicle's safety performance. This comprehensive approach ensures that the KETs, integral to the vehicle's functionality, are thoroughly evaluated within the broader safety framework.

Analysing all major KETs is essential in providing complete guidance to evaluate any use case of automated vehicle systems. We believe this approach should be prioritised regardless of the technologies being analysed. The process of deriving assessment templates can be summarised 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 analyse various use cases to understand technology reliance and testing needs. Assess the reliance of each requirement on KETs.
2. Allocate requirements based on technology reliance: Determine which requirements directly or indirectly depend on specific KETs. Allocate and associate the requirements with the corresponding KET.
3. Derive attributes for the KET category: Derive attributes that capture the essential characteristics of each category. These attributes should primarily reflect safety considerations, 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 KET-specific contributions to 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 functional scenarios that cover diverse KET-related operational conditions and situations that will be added to the scenario database. The derived test scenarios, when executed, should exercise the system's capabilities and evaluate its performance against the criteria that set the standards and indicators that provide the means and methods for measurement.

A panel of experts was used, refining the collected requirements into attributes for each KET, as illustrated in Figure 3. However, this approach comes with certain limitations. Subjectivity is a limitation, as attribute selection relies on expert opinions, potentially leading to definitions and perceived importance variations. Furthermore, a limited representation of diverse stakeholders may result in the inadvertent oversight of requirements. Additionally, the absence of standardisation can give rise to inconsistent attribute definitions, complicating meaningful comparisons.

Nevertheless, it is worth noting that building a requirement landscape for each KET is additive, with each contribution enriching the overall understanding. These limitations become less significant when a substantial input volume is collected and aggregated to a limited number of attributes, on which consensus can be reached.

When evaluating requirements against multiple quality attributes, it is imperative to acknowledge that these attributes can inherently conflict. Consequently, addressing these conflicts requires careful consideration to establish definitive assessment criteria. One approach to managing such tradeoff conflicts is the Analytic Hierarchy Process (AHP) [19], a valuable decision-making technique. In our specific case, no real conflict was detected, and the requirement-selection process sufficiently facilitated the identification of suitable requirements.

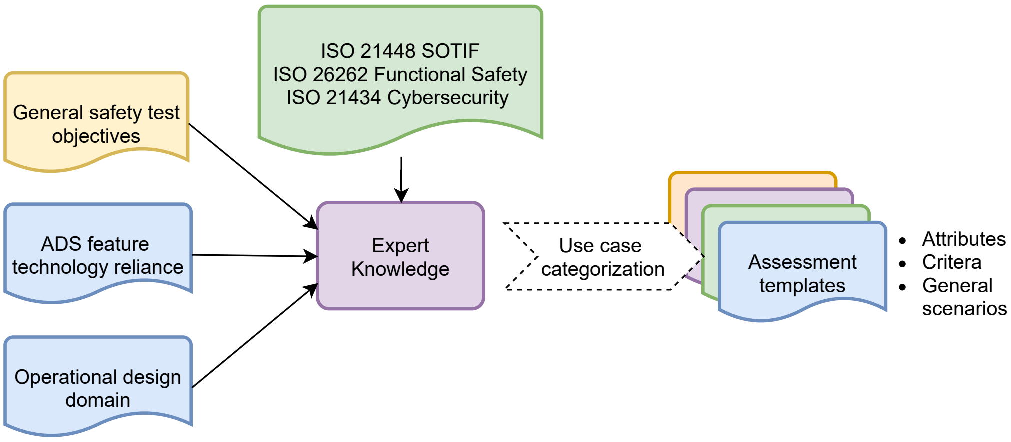

Figure 3. Schematic of assessment-templates-creation process.

Ultimately, the practical value of this approach is demonstrated in Section 5, where the viability and benefits of the method are exemplified.

Following this process, stakeholders can systematically collect requirements, identify technology dependencies, and derive requirement attributes per KET and safety-performance indicators. This structured approach systematically addresses safety considerations, leading to a more thorough and uniform evaluation of an 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 [20] project. Our main focus lies in elaborating on the attributes and assessment templates, which represent an extension of this work. At the same time, we touch upon the rudimentary aspects of requirement collection and allocating categories. 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 assessments. This approach underscores the importance of encompassing a relevant array of KETs when evaluating automated-vehicle ODDs and in scenario-based testing.

4.1. Collection Requirements

The initial phase, marked as 1 in Figure 4, involves the comprehensive collection of requirements. In our previous study [21], conducted within the HEADSTART project, a rigorous effort was made to amass functional and technical requirements pertaining to the three Key Enabling Technologies (KETs). These technologies are key for ensuring automated vehicles' proper functioning and safety, hence the term. The requirements for the KETs were identified through a three-step process. Firstly, we delved into ongoing activities within standardisation organisations and other relevant interest groups. This provided valuable insights into evolving standards and industry expectations. Subsequently, we conducted surveys, questionnaires, and interviews involving stakeholders like OEMs, Tier 1 suppliers, and regulatory bodies. This direct engagement was instrumental in understanding their distinct needs and perspectives. Lastly, we integrated requirements and insights from other pertinent research projects to enrich our analysis. This comprehensive approach ensured the collection of various requirements and needs related to the KETs.

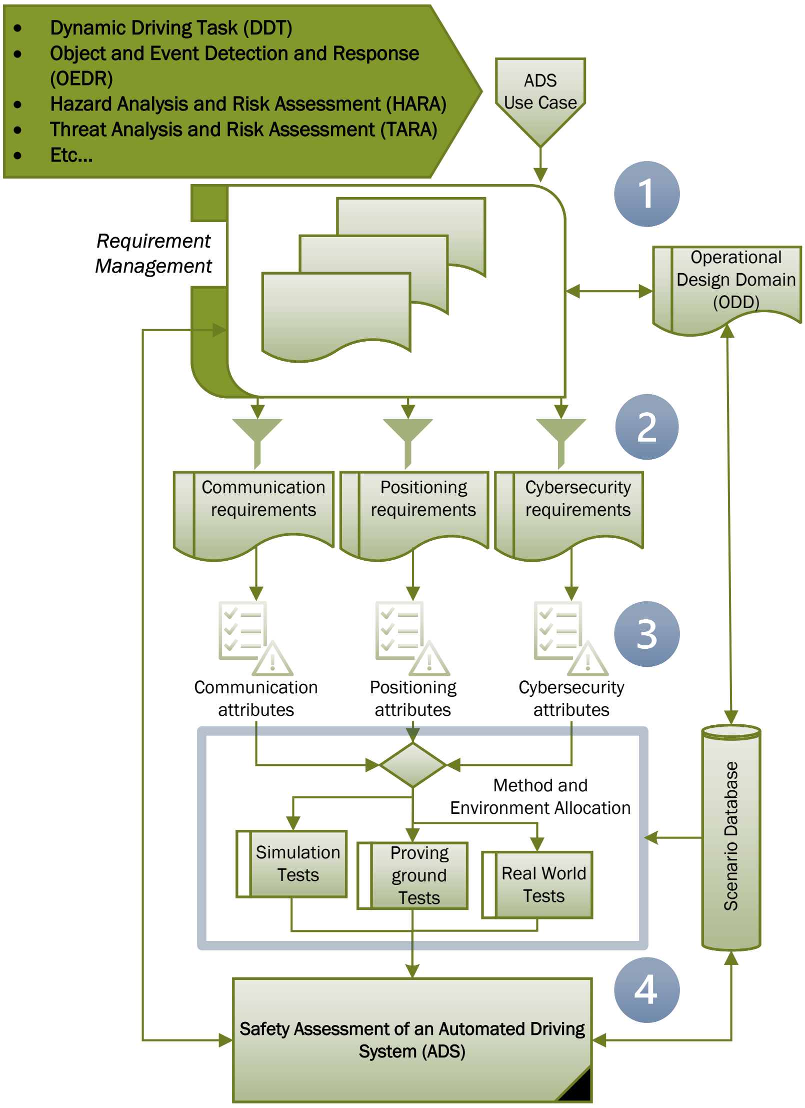
Dynamic Driving Task (DDT)
Object and Event Detection and Response (OEDR)
Hazard Analysis and Risk Assessment (HARA)
Threat Analysis and Risk Assessment (TARA)
Etc...
ADS Use Case
1
Requirement Management
Operational Design Domain (ODD)
2
Communication requirements
Positioning requirements
Cybersecurity requirements
3
Communication attributes
Positioning attributes
Cybersecurity attributes
Method and Environment Allocation
Simulation Tests
Proving ground Tests
Real World Tests
Scenario Database
4
Safety Assessment of an Automated Driving System (ADS)

Figure 4. Method to derive assessment attributes for KETs.

The data-collection efforts were conducted closely with stakeholders, including participants and affiliates of the HEADSTART project, spanning industry, research institutes, and policymakers. The data collection of stakeholder considerations revealed diverse requirements, ranging from high-level strategic needs to intricate technical specifications. The high-level strategic needs, such as the functional requirements, illuminate the specific functions that KETs are tasked with within automated systems. These functions encompass tasks like sensor-data processing, real-time data communication, and implementing cybersecurity measures. Technical requirements delve into intricate technical details, encompassing communication protocols, data-transmission rates, encryption methods, and network architecture. These details provide insights into the technical aspects that underpin KETs. Furthermore, performance attributes closely tied to these technical requirements support the evaluation of the effectiveness of KETs. These attributes cover essential factors like latency, data throughput, reliability, and redundancy, collectively contributing to the assessment of KETs' performance and their significance in ensuring the safety of automated vehicles.

Moreover, we considered the requirements for testing and validation procedures. It covers identifying relevant test scenarios simulating real-world conditions and requirements for the testing environment to ensure accurate assessments, categorising it as development, consumer-oriented, or type-approval testing. Here, the only interest is the latter and how the two prior categories can support type approval. An insight gained is that future requirement collection efforts would benefit from the regulatory-compliance perspective. This analysis revealed numerous requirements tailored to the KETs, often intricately linked to particular use cases. One notable challenge was that some of these requirements were based on desired functionalities and needs that might not be readily available with today's technology. Given the ongoing development in all three KETs, adaptation may be needed to align the requirements with the capabilities of contemporary technology. These identified requirements and constraints pertinent to the KETs have been documented and disseminated in various publications [21–23]. These publications provide a comprehensive guideline framework for developing harmonised testing and validation procedures, a key component of the HEADSTART method's overarching objectives [24].

The use cases analysed in the project, e.g., highway pilot and highway truck platooning, are used to explore various aspects of critical enabling technologies. Understanding the variation in the reliance on these underlying technologies in developing a practical assessment procedure is important. By understanding the specific requirements and challenges associated with each use case, an 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. Allocation Requirements Based on Technology Reliance

As indicated in Step Two in Figure 4, the method integrates the gathered and categorised requirements, aiming to include 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 test scenarios.

4.2.1. V2X Communication

Communication and associated requirements can be crucial in ADSs. 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, optimising collective behaviour regarding throughput, fuel consumption, emissions, and safety [25]. In the automotive industry, there are two main types of V2X communication technologies: WLAN-based, which utilises 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 organisations 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. A 5G-based predictability system was evaluated to forecast the service quality [26], proposing an enhanced scheme for vehicle-to-network communication optimisation. This method effectively alleviates base station congestion while preserving key quality attributes like delay time and throughput, showcasing efficient network management even in high-demand scenarios.

4.2.2. Positioning

Positioning is a capability required for high levels of automation. 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. The accuracy, precision, refresh rate, and integrity are subattributes associated with these aspects.

Global Navigation Satellite System (GNSS)-based positioning and High-Definition (HD) maps can be utilised 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. In the realm of GNSS technologies, ongoing standardisation efforts are spearheaded by organisations like ETSI, with test-equipment vendors actively enhancing GNSS testing capabilities. Furthermore, the interrelation of cybersecurity with GNSS positioning in Intelligent Transportation Systems (ITSs) is detailed in EN 16803-1 [27]. The European COST Action SaPPART [28] established standardised methodologies, enhancing integrity metrics, PVT error models, and positioning solutions for future ITSs. This involved validating positioning terminals and analysing GNSS receivers under the guidance of EN 16803-1.

4.2.3. Cybersecurity

In the realm of defining cybersecurity requirements, it becomes paramount to factor in potential threats. Notably, the NIST FIPS 199 [29] delineates three fundamental facets of cybersecurity, often referred to as CIA:

- Confidentiality: this dimension revolves around safeguarding authorised information access and disclosure restrictions, an endeavour encompassing the protection of personal privacy and proprietary data.
- Integrity: integrity focuses on thwarting improper information modification or destruction, thus ensuring information nonrepudiation and authenticity.
- Availability: the cornerstone of this facet is ensuring the timely and reliable access to and use of information.

Crucially, the technical and functional requirements identified emphasise that the latter two aspects are intrinsically linked to safety considerations. This underscores the importance of adhering to cybersecurity best practices throughout the product-development journey. Cybersecurity is a vital quality attribute, wielding substantial influence over the safety of ADS applications. Diverging from safety considerations, cybersecurity maintains a constant state of evolution, marked by the continuous development of new techniques and capabilities by potential attackers. Consequently, addressing cybersecurity concerns becomes an enduring requirement throughout the lifecycle of an ADS.

It is noteworthy that cybersecurity requirements deviate from those of communication and positioning. Cybersecurity is a vital quality attribute that permeates both domains. In vehicle-to-everything (V2X) communication, establishing a chain of trust through verified signatures and certificates proves indispensable. Rigorous state-of-the-art cybersecurity testing should be diligently executed across all aspects. Many best practices and design principles for cybersecurity in vehicular systems exist. These are outlined in standards such as SAE J3061 [30], NIST FIPS 2004 [29], and ISO/SAE 21434. Additionally, various studies and discussions delve into security and privacy in Connected vehicle-to-everything (C-V2X) communications [25,31,32]. Both the SAE and ISO [33] collaborate extensively in standardisation activities relevant to vehicle cybersecurity. Cybersecurity's intricacies stem from the perpetual evolution of techniques and the ever-present threats that can imperil safety.

Shifting our focus to the responsibilities of type-approval assessors concerning cybersecurity, their purview primarily centres on the system level. However, this scope intentionally remains narrower than the expansive realm of cybersecurity. The primary objective revolves around conducting a comprehensive evaluation of documentation, ensuring the coverage of critical cybersecurity dimensions. These encompass cybersecurity-management systems, software-update management, cybersecurity measures, risk identification, risk-mitigation strategies, and measures enacted to ensure unwavering compliance with legislative requirements. This evaluation carries significance as it aligns with the overarching goal of uncovering potential cyberattack vulnerabilities, which could compromise the vehicle's safety. The evaluation encompasses the scrutiny of the physical testing environment, spanning proving grounds and public roads. It also entails examining the manufacturer's documentation on the virtual toolchain. Lastly, it is at the assessor's discretion to determine whether comprehensive tests of the integrated toolchain are warranted. Such tests aim to affirm the credibility of the toolchain's cybersecurity safeguards, fortifying the commitment to a robust cybersecurity framework.

4.3. Derive Attributes for KETs

The general safety objectives include potential hazards during a generalised 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 [33–35], relevant to the reliance of KETs by analysing 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 KETs 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 static and dynamic attributes.

ISO 34503 proposes dividing the operating conditions into three primary attributes: scenery, environmental conditions, and dynamic elements. Scenery refers to nonmoving 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 subattributes like accuracy, precision, and refresh rate integrity, as shown in Table 2. Cybersecurity requirements can be derived based on the categorisation proposed by Firesmith [36], as presented in Table 3.

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

Attributes	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 a message being sent by a sender and being received by the intended recipient. Indicates the responsiveness of the 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 pre-empt and plan for degraded coverage, latency, and throughput.

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

Attributes	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. Indicates the solution's responsiveness.
Confidence	Confidence reflects the ability to quantify the uncertainty in measurements. Indicates the ability to handle and pre-empt degraded services. 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 is preferable to stop risks from being realised than to 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 Firesmith's defensibility solution types [36].

Numerous vital questions still need to be addressed and recognised, 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 and also assessments of common time-base solutions for synchronised cooperative ADS.

While the attributes presented in Tables 1–3 may not cover all the gathered requirements, and in all likelihood, not all relevant concerns are addressed, they provide useful patterns and attribute families to analyse the performance of KETs and map 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 Functional Scenarios

Much effort has been spent on the development of performance indicators [37,38] and scenario databases [39,40], focusing on data-driven aspects like longitudinal control (acceleration, braking, and road speed), lateral control (lane discipline), and environment monitoring (headway, side, and 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 realise 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. Criteria set the evaluative standards, and safety-performance indicators provide the means for measuring compliance with those standards. Both are integral to the assessment process but serve different purposes: criteria guide what to measure, and indicators define how to measure it. Knowledge-driven indicators can be assigned to 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:
  - External and internal human–machine interfaces;
- Triggering conditions for minimum risk manoeuvres:
  - External and internal human–machine interfaces;
- Conditions for deactivation:
  - 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.

In scenario-based testing, two primary criteria come into play: pass/fail and metric criteria. Both of these criteria rely on objective observations of the executed scenario. Context-specific safety-performance indicators are used to establish success criteria and metrics. These indicators serve as data gatherers, facilitating evaluating and comparing the automated vehicle's expected and executed behaviour. Each KET introduces specific attributes that must be met during operation. Failure to meet these conditions often triggers a minimal risk manoeuvre (MRM) activation to return the system to a minimal risk state. Various failures, encompassing scenarios such as attacks on vehicle control, environmental monitoring, and interactions within the human–machine interface (HMI), both internally and externally, may trigger MRMs. It is imperative to assess the appropriateness of these MRM and HMI interactions [41].

Coverage pertains to the extent of the communication system's reach. It is important to determine the acceptable coverage values based on the specific safety requirements of the ADS and its ODD. Establishing and improving these values requires an iterative process and an understanding of real-world operational conditions. Latency, another critical metric, gauges the time it takes for data to travel between the sender and receiver. Ensuring low latency is essential, especially for safety-critical applications. This assessment should align with the safety requirements outlined for the ADS within its ODD. The throughput assesses the system's data-transfer capacity, often measured in terms of bandwidth. Defining acceptable throughput values necessitates thoroughly examining the ADS's safety prerequisites and ODD. Maintaining adequate throughput levels is essential, even in challenging operational conditions. Predictability evaluates the system's ability to deliver expected results consistently. Predictable communication is vital for the safe functioning of an ADS. Establishing criteria for predictability should align with safety requirements and ODD specifications. These metrics are the foundation for creating an assessment template, as depicted in Table 4. Stakeholders can systematically evaluate the communication system's performance and alignment with safety objectives by defining acceptable values for these metrics tailored to the specific ADS and its operational context.

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 manoeuvres, ensuring safety is maintained.

Table 4. Sample template for communication with attributes and basic related HMI aspects.

KET	Test Scenario	Attribute [1]	Criteria Description	Evaluation
Communication	Activation-condition scenarios	Coverage	Activation criteria for coverage	□ Pass □ Fail
Communication	Activation-condition scenarios	Latency	Activation criteria for latency	□ Pass □ Fail
Communication	Activation-condition scenarios	Throughput	Activation criteria for throughput	□ Pass □ Fail
Communication	Activation-condition scenarios	Predictability	Activation criteria for predictability	□ Pass □ Fail
Communication	Internal HMI activation scenarios	⋮	Criteria for internal HMI evaluation	□ Pass □ Fail
Communication	External HMI activation scenarios	⋮	Criteria for external HMI evaluation	□ Pass □ Fail
Communication	Internal HMI control-transition scenarios	⋮	Criteria for control-transition evaluation	□ Pass □ Fail
Communication	MRC triggering-condition scenarios	Coverage	Criteria for MRC evaluation	□ Pass □ Fail
Communication	MRC triggering-condition scenarios	Latency	Criteria for MRC evaluation	□ Pass □ Fail
Communication	MRC triggering-condition scenarios	Throughput	Criteria for MRC evaluation	□ Pass □ Fail
Communication	MRC triggering-condition scenarios	Predictability	Criteria for MRC evaluation	□ Pass □ Fail
Communication	Internal HMI of MRC triggering scenarios	⋮	Criteria for HMI MRC evaluation	□ Pass □ Fail
Communication	External HMI of MRC triggering scenarios	⋮	Criteria for HMI MRC evaluation	□ Pass □ Fail
Communication	Deactivation-condition scenario	Coverage	Criteria for deactivation evaluation	□ Pass □ Fail
Communication	Deactivation-condition scenario	Latency	Criteria for deactivation evaluation	□ Pass □ Fail
Communication	Deactivation-condition scenario	Throughput	Criteria for deactivation evaluation	□ Pass □ Fail
Communication	Deactivation-condition scenarios	Predictability	Criteria for deactivation evaluation	□ Pass □ Fail
Communication	Internal HMI deactivation scenarios	⋮	Criteria for deactivation HMI evaluation	□ Pass □ Fail
Communication	External HMI deactivation scenarios	⋮	Criteria for deactivation HMI evaluation	□ Pass □ Fail

[1] Attributes related to human–machine interfaces (HMI) are beyond the current scope.

Similarly, for positioning, evaluating the ADS's capability to determine its position and track objects in its environment may require metrics such as accuracy, precision, refresh rate, and integrity. The acceptable values for these metrics will hinge on the specific use case and the safety-critical requirements governing it.

When delving into cybersecurity aspects, metrics can encompass factors such as robustness against cyberattacks, resistance to unauthorised access, and the integrity of data transmission. Also, determining acceptable metric values is contingent upon industry best practices, relevant standards, and the criticality of the ADS's functions. In summation, as we address the requirements posed by the various KETs, the scenario catalogue expands with an array of assessment criteria for minimum risk manoeuvres, hand-over transitions, HMI (both internal and external), and driver monitoring. It is vital to review this expanding catalogue to ensure that its representation and completeness align rigorously with the demands and expectations of the system under evaluation.

5. Evaluation of the Use of Assessment Templates

Analysing 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 for 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 the functional 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.

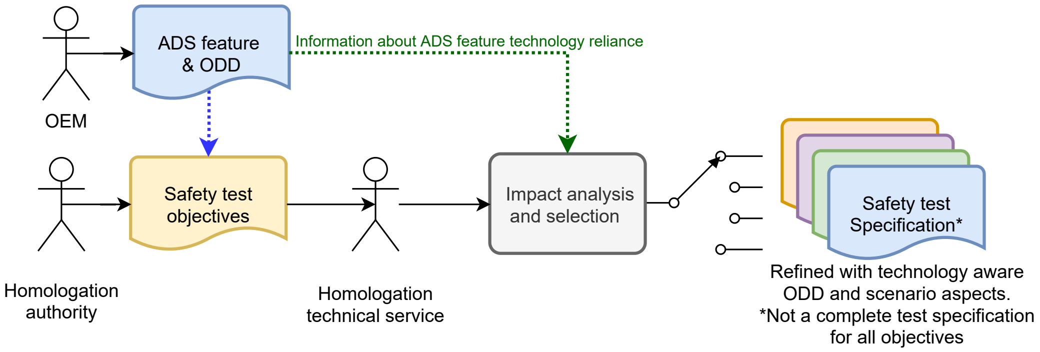
OEM
ADS feature & ODD
Information about ADS feature technology reliance
Homologation authority
Safety test objectives
Homologation technical service
Impact analysis and selection
Safety test Specification*
Refined with technology aware ODD and scenario aspects.
*Not a complete test specification for all objectives

Figure 5. Schematic of selection process of assessment templates.

5.1. ADS Feature and ODD Under Evaluation

The evaluation centres on a highly automated freight vehicle in a dedicated urban area (Figure 6). The vehicle aims for SAE level 4 automation [1], indicating it can perform all driving tasks under certain conditions without human intervention. Additionally, the vehicle is equipped with remote-assistance functionality, allowing for human oversight and intervention remotely, which is essential for addressing scenarios beyond the capabilities of the automated system or during transitions between automated and manual control. 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 Figure 5, the input is the safety objectives, function description, and intended ODD. The ADS features describe the system utilised, 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 [42]), emphasising including a traffic safety analysis and an independent risk assessment in all exemption applications. These safety objectives ensure that the evaluation process addresses and fulfils 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.

A potential site for conducting the ADS feature trials has been identified in the urban traffic environment in 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 hour. VRUs are expected to walk and cycle throughout the area.

- Road conditions: public urban roads going straight, at intersections, and at turns.
- Geographical area: Lindholmen, Sweden. Exact geographic site determined with Geofence.
- Environmental conditions: daylight, good visibility, no or light rain, and 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.

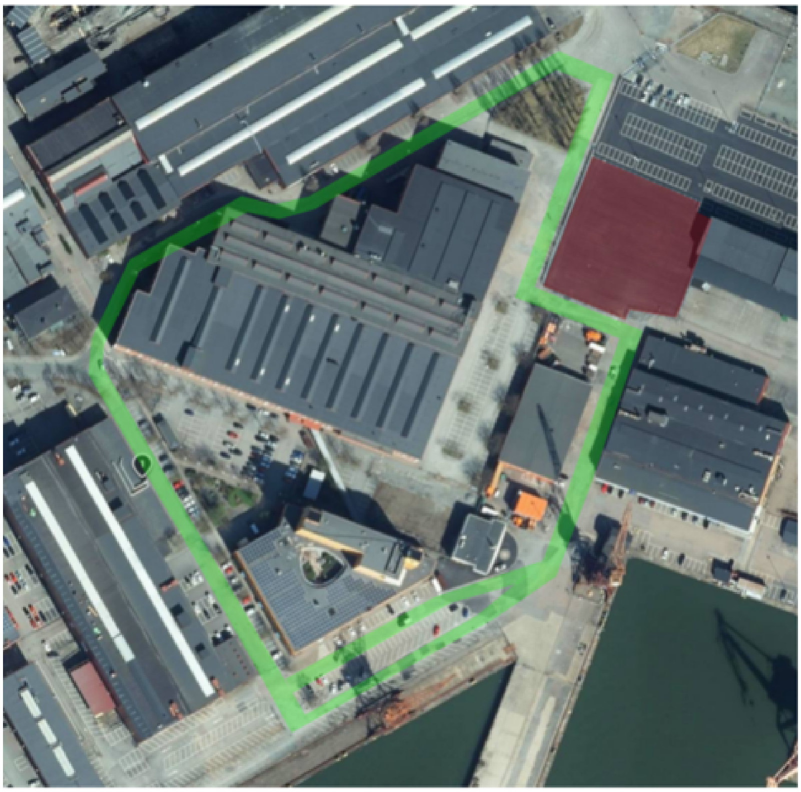

Figure 6. Potential ODD at Lindholmen. The geofenced route is denoted by green.

To ensure that 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 utilising a GNSS is a safety and cybersecurity mechanism used to mitigate vehicle-operating risks beyond the defined ODD. While geofencing is partially rooted in threat analysis, additional cybersecurity assessments currently fall beyond the scope of this study. Maintaining precise positioning within the ODD often supports the fulfilment of critical system safety and security requirements. This investigation primarily centres 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

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

Integrating 5G communication into the ODD expands the evaluation of operational conditions. The ODD's boundaries are extended by incorporating 5G communication attributes to encompass connectivity considerations. This evaluation covers 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 [43].

The control loop for a remotely assisted automated vehicle operates as a continuous process where the vehicle's sensors gather environmental and status data, which are transmitted to a remote operator. The operator issues control commands back to the vehicle. The vehicle then executes these commands, completing the loop. The real-time demands within this 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 manoeuvres. The guarantee of this minimum throughput holds utmost importance throughout the entire ODD. Maintaining high service availability is critical to pre-empting potential service congestion and counteracting inadequate coverage, especially in adverse weather conditions, emphasising the need for predictability. This comprehensive coverage requirement must be consistently met within the ODD in alignment with the communication-assessment template specified in Table 4.

Furthermore, the Quality of Service (QoS) for bandwidth reservation involves allocating specific portions of the network capacity to certain applications or services to ensure consistent performance levels, especially for data throughput and latency. This ensures that essential services receive the bandwidth unaffected by network 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.

The assessment of GNSS-based geofence considerations follows a similar approach. It employs the prototype template in Table 2. This assessment emphasises the need for accurate absolute positioning, which GNSS systems are tasked to provide. The evaluation criteria stipulate that the geofence system should maintain accuracy within a meter, a benchmark achievable by implementing real-time kinematic (RTK) solutions. The assessment process also involves evaluating the confidence level in the positioning measurements, including analysing how the system quantifies and manages the inherent uncertainty. In the context of geofencing, the precision of positioning is paramount. The assessment, therefore, involves verifying that RTK-based positioning consistently meets the system's accuracy requirements. Additionally, the assessment includes examining the refresh rate at which the system updates its position measurements, with a rate exceeding 1 Hz being the general target for the geofencing application to ensure timeliness. 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. Incorporating a second observer for plausibility checks and using dual-frequency receivers are evaluated to determine how they contribute to the overall integrity of the geofence system. The accuracy and reliability of GNSS-based geofence solutions can be assessed by evaluating these criteria.

In applying the cybersecurity attributes delineated in Section 4.3, the emphasis is placed on preventative measures. Specifically, the objective is to fortify the vehicle against unauthorised control by employing authenticated and encrypted communication protocols.

Detection mechanisms are essential to identify malicious activity during remote assistance, and in the case of failure or an attack, a fail-safe reaction strategy should be employed. This transition ensures the safe operation with reduced functionality and may involve over-the-air updates for security patches.

To evaluate the presence and appropriateness of cybersecurity measures, although not a direct component of the ODD, including cybersecurity criteria improves the evaluation process. The enhancement entails a direct association between threat agents, their underlying motives, and potential attack surfaces within the ODD. This refined linkage provides more precise guidance for implementing measures against prospective attacks. By integrating cybersecurity measures, the assessment plan comprehensively evaluates the system's safety and resilience, aligning with future type-approval requirements.

The attributes derived in Section 5 have enhanced assessment planning and analyses of use cases. They emphasise the importance of maintaining 5G communication coverage with a QoS bandwidth priority to ensure a consistent bandwidth, whether due to natural factors or malicious actions. Further assessments of these attributes' suitability for proving ground testing are pending. Utilising the prototype-assessment templates in collaboration with specific functional scenarios—such as minimal risk manoeuvres, activation, and deactivation—facilitates the evaluation of 19 distinct test scenarios.

These indicators are especially relevant to 5G communication and geofencing conditions. They have been categorised into different domains, including activation conditions, minimal risk manoeuvres, and external and internal HMI considerations. The distribution of these conditions within each category is not uniform; for instance, at least four conditions are explicitly pertinent to 5G communication, while six conditions are geared towards geofence considerations.

5.3. Test Scenario Execution for 5G Communication

An evaluation of the cellular coverage at the test site is conducted 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 a balanced symmetric bandwidth and low latency for the control channel requires consistent capacity to attain robust connectivity. Comprehending the capabilities and limitations of the test site is instrumental for effective planning and preparation for operational deployment. This understanding is achieved by identifying areas necessitating enhancement or optimisation and verifying that essential infrastructure and connectivity prerequisites are satisfied to successfully demonstrate the ADS feature.

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 the available uplink capacity, which is likely to be the limiting factor in a remote-assistance and monitoring scenario.

The assessment predominantly focused on measuring the Reference Signal Received Power (RSRP). The RSRP is a reliable indicator for predicting the radio uplink capacity since it gauges the cell's proximity from a radio standpoint. Uplink radio interference is mainly due to other handsets moving within the cell, making it more dynamic and more challenging to predict 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 prioritising high bandwidth, this approach considers the absolute latency and latency variation (jitter).

In the experimental procedure, the tester held a measurement terminal during the initial lap of the site under assessment, as shown in Figure 6; the corresponding speed profile is illustrated in Figure 7. For laps 2 to 5, the handheld device was positioned between the front seats of a car circulating the track. The first two laps were executed with a target bitrate of 20 Mbit/s, while the bitrate for the subsequent laps was elevated to 50 Mbit/s.

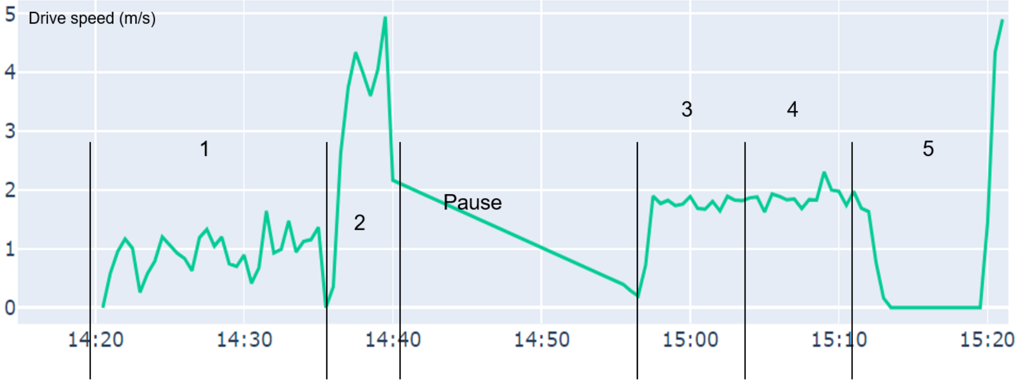

Figure 7. Data were collected over a total of 5 laps at the route at Lindholmen.

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

An adaptive UDP stream, emulating adaptive video, was used to measure the 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. The RT BW serves as a performance indicator for the throughput, as depicted in Figure 10, and the related scenarios are portrayed in Figure 11.

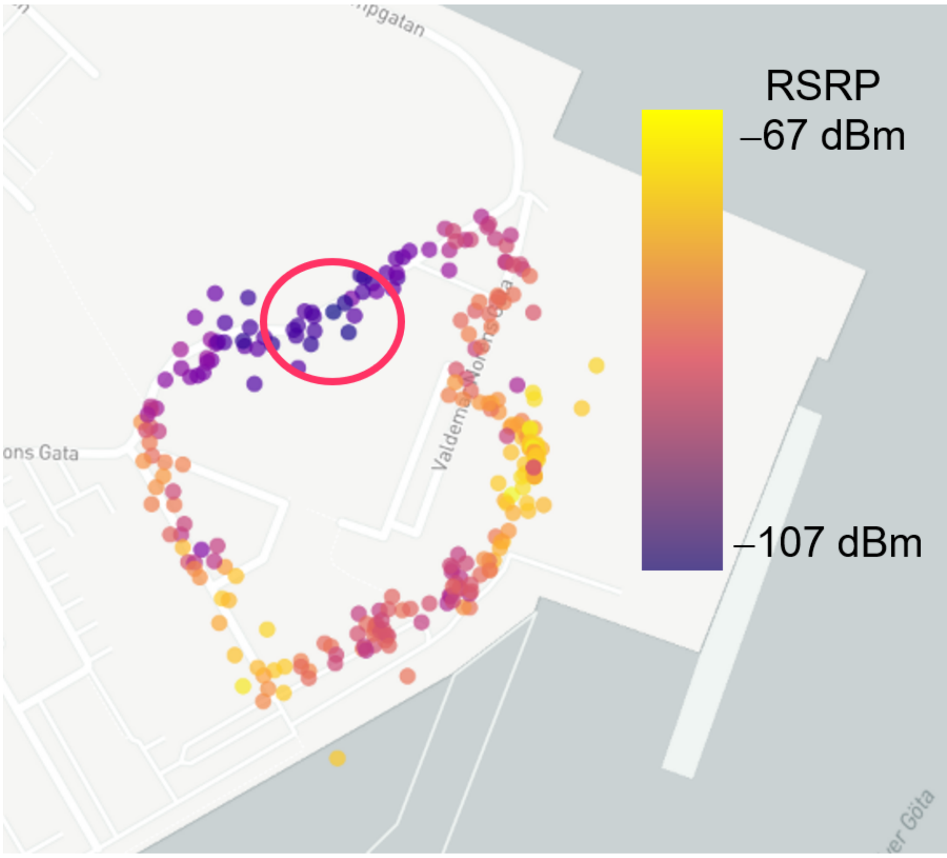

Figure 8. Reference Signal Received Power (RSRP) primary cells. Points of interest are circled in red.

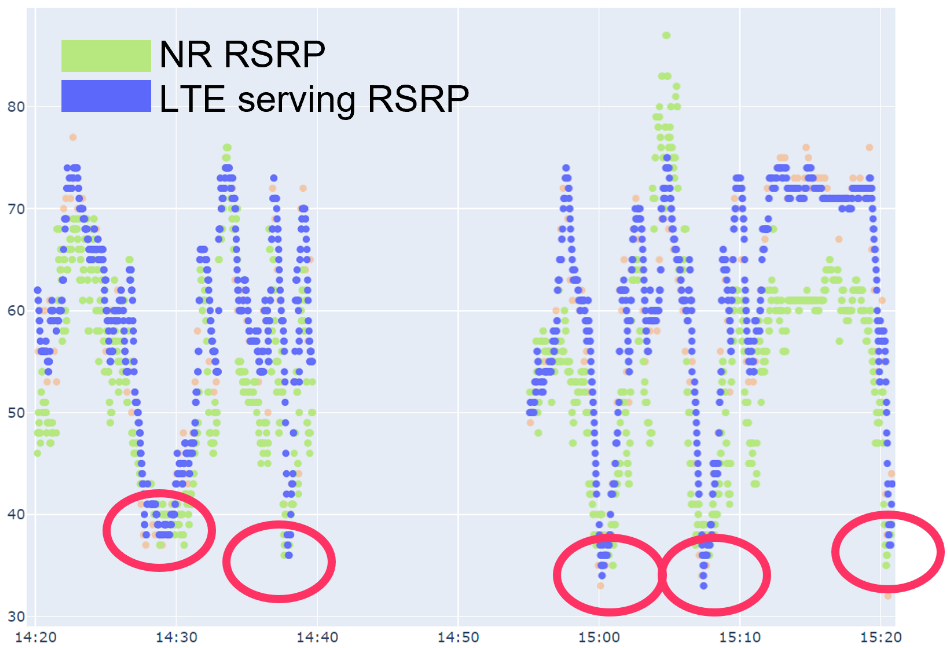

Figure 9. NR and LTE Reference Signal Received Power (RSRP) over time. Points of interest are circled in red.

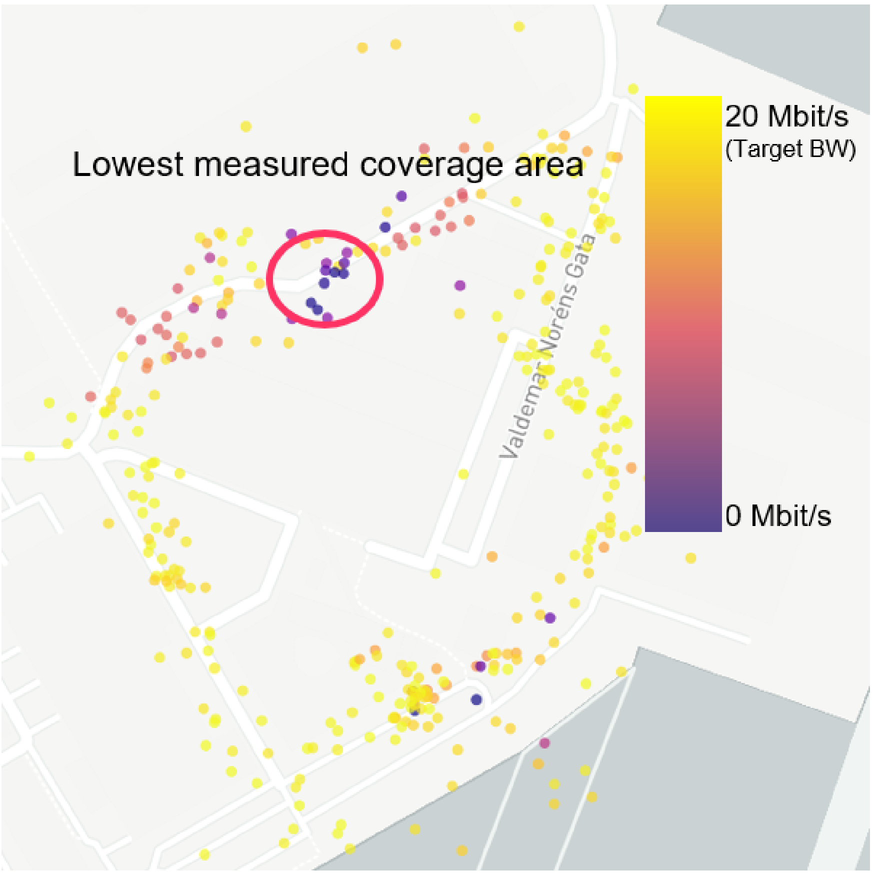

Figure 10. Measured bandwidth in the demonstration area. Points of interest are circled in red.

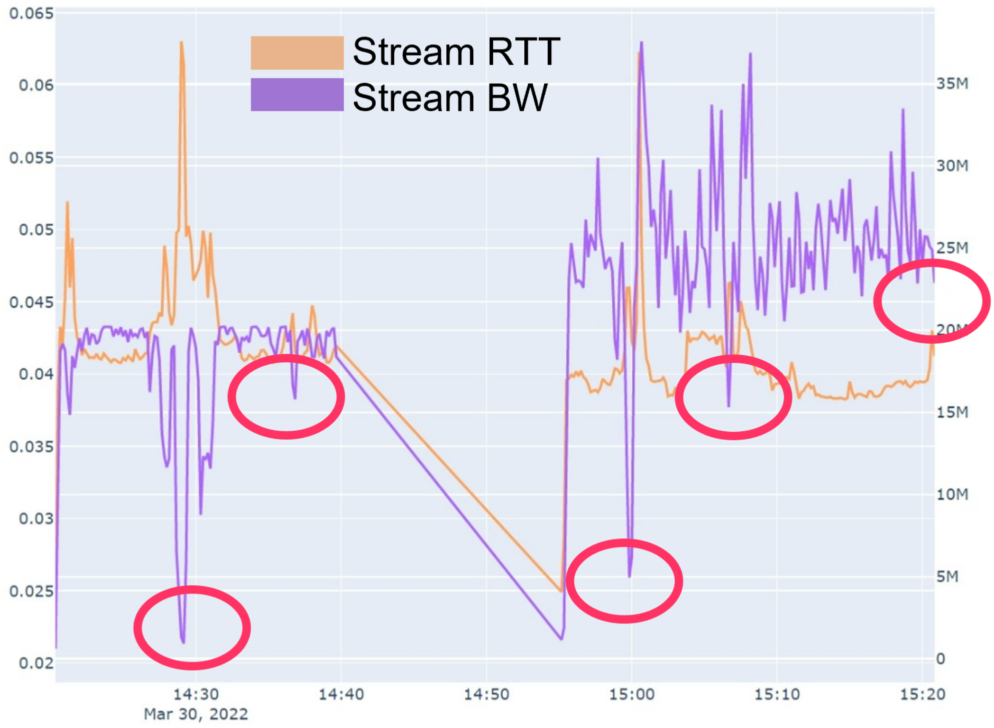

Figure 11. Stream round trip time (RTT) and stream bandwidth (BW) over time. Points of interest are circled in red.

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

The measurement tool employs Ericsson's SCReAM algorithm [44], a mobile-optimised congestion-control algorithm. SCReAM dynamically adjusts the bandwidth based on various metrics, including the round trip time (RTT). As depicted in Figure 11, SCReAM responds by reducing the bandwidth when the RTT increases, effectively minimising the latency. Therefore, the RT BW refers to the data delivered within a reasonably bounded RTT delay. Both the bandwidth and throughput serve as indicators of the network performance. While the bandwidth indicates the available or predicted network capacity, the throughput represents the transmitted data. Given the susceptibility of the intended networks to congestion, mainly as they are not private, the throughput is a more pertinent measurement in this context.

Accurately predicting handover issues between cellular network cells is vital for coverage testing. Assessment criteria such as the signal strength, quality, and latency are used to identify potential challenges during the handover procedure, as shown between cell one and cell two in Figure 12. Through scenario simulations and a network-performance analysis, operators can improve handover algorithms and configurations to maintain connectivity. Conducting a specialised ODD assessment is necessary to validate and assess the results.

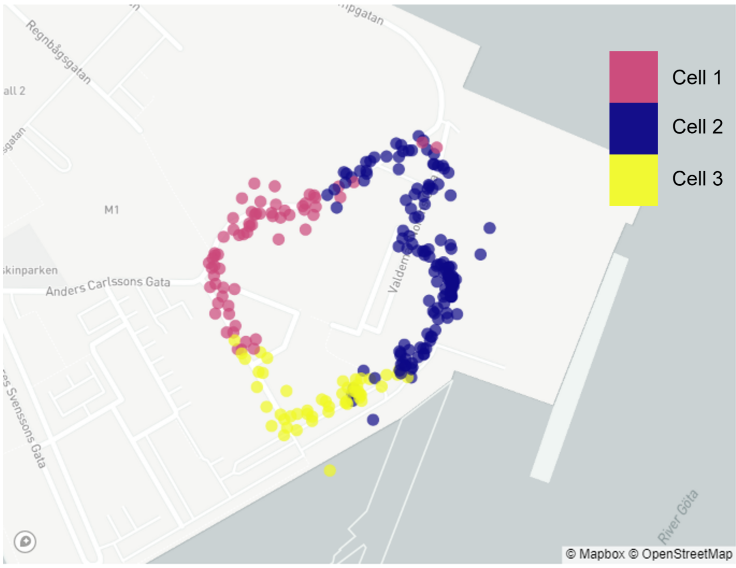

Figure 12. Three cells are involved in the coverage.

Using an assessment template, as shown in Table 4, improves the efficiency of the site assessments for ADSs. This template, which links predefined performance indicators with test scenarios, provides a structured framework that reduces the effort required. It establishes a starting point for developing a more-detailed and customised assessment strategy, as Table 5 exemplifies. The advantage of this approach lies in its focus on test scenarios closely connected to KET and ODD dependencies, especially concerning connectivity and positioning. These scenarios form a pertinent baseline suite to test whether the conditions for activating and maintaining the ADS features throughout the ODD are met. Compared to approaches without such templates, this method offers a more organised and comprehensive way to conduct tests. It ensures that pertinent scenarios and performance indicators are considered, which is crucial to accurately assess an ADS's capabilities and limitations.

Table 5. Excerpt of application of assessment template for 5G communication at Lindholmen.

KET	Test Scenario	Attribute	Criteria Description	Evaluation
⋮	⋮	⋮	⋮	⋮
5G communication	Activation-condition scenario	Coverage	Coverage is present in the whole Lindholmen ODD. Coverage is achieved by several cells. Handover must not affect throughput.	□ Pass ☑ Fail
5G communication	Activation-condition scenario	Latency	Here, latency is assessed to be subsumed by 5G coverage and validated by video-performance tests.	□ Pass ☑ Fail
5G communication	Activation-condition scenario	Throughput	Target bandwidth: 20 Mbit/s. Unsafe below 1 MBit/s or 15 frames per second.	□ Pass ☑ Fail
5G communication	Activation-condition scenario	Predictability	Deployment-site test measurements and Quality of Service (QoS).	☑ Pass □ Fail
⋮	⋮	⋮	⋮	⋮

Using KET-assessment templates makes the assessment process a systematic exercise in evaluating the ADS's functionality and performance within the defined ODD. The perceived efficiency gain can be attributed to:

1. Structured testing: ensures the comprehensive coverage of essential test scenarios and indicators, reducing the risk of missing critical evaluation aspects.

2. Consistency and comparability: provides a uniform framework for assessing different ADSs, enabling consistent and fair comparisons.
3. Time efficiency: saves time by offering KET-relevant indicators with a predefined set of criteria and scenarios, speeding up the assessment process.
4. Customise framework: allows adjustments to fit specific ADS features or testing environments, maintaining relevance across various assessments.

In summary, the KET-assessment templates aid in a more-efficient and complete evaluation process, aligning the assessment with the specific requirements of the tested ADS. This contributes to better-informed decision making and safer Automated Driving Systems.

6. Conclusions

In conclusion, while notable strides have been taken in safety-assessment strategies for automated vehicles, certain limitations linked to practical assessment endeavours 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. The 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 bottom-up analysis with 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 and address the limitation posed by relying on predefined scenarios. One notable weakness of KET-related predefined test scenarios is their reliance on historical information, which may not adequately account for the expected novelties in KETs. As such, our method is designed to complement data-driven approaches that incorporate real-world data to create a more-comprehensive assessment. To overcome the potential limitations imposed by rigid, predefined templates, it is necessary to continuously develop, update, and refine the templates to remain aligned with ongoing technology developments—a challenge encountered in all checklist-based approaches. We highly recommend combining knowledge-driven and data-driven approaches in future safety-assurance-framework endeavours. This harmonious blend can enrich the assessment framework by capitalising on existing knowledge and real-world data. Its relevance is especially pronounced in situations where substantial real-world data are scarce. To facilitate the seamless integration of these approaches, we propose adopting a policy that underscores the importance of integrating prior knowledge into the assessment processes and any scenario databases. Such a policy can be a stepping stone for accommodating evolving challenges and fostering a comprehensive safety-assurance approach.

Therefore, developing technology-aware assessment criteria for attributes derived from enabling technologies is important. These criteria should complement the overarching high-level requirements and encompass the fundamental behavioural facets of the automated function within the defined ODD. This involves appraising the functionality of sensors and communication devices, adherence to protocols and standards, and the 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: Conceptualisation and methodology, M.S.; validation measurements, M.B.; investigation, M.S., A.T. and F.W.; writing—original draft preparation, M.S., A.T. and F.W.; writing—review and editing, M.S., A.T. and F.W.; supervision, F.W. All authors have read and agreed to the published version of the manuscript.

Funding: The SUNRISE project is funded by the European Union's Horizon Europe Research and Innovation Actions under grant agreement no.101069573. The views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or European Union's Horizon Europe Research and Innovation Actions. The SCAT project (2020-04205) has received funding from Vinnova, Sweden's innovation agency. The content reflects only the authors' views. Sweden's innovation agency is not responsible for any use that may be made of the information it contains.

Conflicts of Interest: Author Mats Bergman was employed by the company Telia Company. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. *J3016 APRIL2021*; 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: Warrendale, PA, USA, 2021.
2. ECE/TRANS/WP.29/2020/81. UN Regulation No 157—Uniform Provisions Concerning the Approval of Vehicles with Regards to Automated Lane Keeping Systems [2021/389]. 2021. Available online: https://op.europa.eu/s/y6kz (accessed on 1 December 2023).
3. WP.29/GRVA. Current Draft of the Guidelines and Recommendations Concerning Safety Requirements for ADS (FRAV). 2022. Available online: https://unece.org/transport/documents/2022/05/informal-documents/frav-current-draft-guidelines-and-recommendations (accessed on 1 December 2023).
4. Chan, C.Y. Advancements, Prospects, and Impacts of Automated Driving Systems. *Int. J. Transp. Sci. Technol.* **2017**, *6*, 208–216. [CrossRef]
5. Chen, C.; Zhao, Q.; Zheng, T.; Zhai, Y.; Zhu, X. 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), Guiyang, China, 17–22 July 2022; pp. 744–747. [CrossRef]
6. 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), Toulouse, France, 29–31 January 2020.
7. *PAS 1883:2020*; Operational Design Domain (ODD) Taxonomy for an Automated Driving System (ADS)—Specification. Technical Report; BSIGROUP: London, UK, 2020.
8. *ISO 34503:2023*; Road Vehicles—Test Scenarios for Automated Driving Systems—Specification for Operational Design Domain. International Organization for Standardization: Geneva, Switzerland, 2023. Available online: https://www.iso.org/standard/78952.html (accessed on 1 December 2023).
9. Association for Standardization of Automation and Measuring Systems. ASAM OpenODD. Available online: https://www.asam.net/standards/detail/openodd/ (accessed on 1 December 2023).
10. Sunrise Project. *D3.1 Report on Baseline Analysis of Existing Methodology*; Technical Report; Sunrise Project: 2023. Available online: https://ccam-sunrise-project.eu/deliverable/d3-1-report-on-baseline-analysis-of-existing-methodology/ (accessed on 1 December 2023).
11. 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, Gran Canaria, Spain, 15–18 September 2015; pp. 982–988. [CrossRef]
12. 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), Changshu, China, 26–30 June 2018; pp. 1821–1827.
13. Koopman, P.; Wagner, M. Autonomous Vehicle Safety: An Interdisciplinary Challenge. *IEEE Intell. Transp. Syst. Mag.* **2017**, *9*, 90–96. [CrossRef]
14. 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. [CrossRef]
15. Underwriters Laboratories. *UL 4600: Standard for Evaluation of Autonomous Products*; Technical Report; Underwriters Laboratories: Northbrook, IL, USA, 2020.
16. 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: Washington, DC, USA, 2018.

17. 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. Available online: https://unece.org/sites/default/files/2021-01/GRVA-09-07e.pdf (accessed on 1 December 2023).
18. 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 *Computer Safety, Reliability, and Security. SAFECOMP 2022 Workshops, Proceedings of the International Conference on Computer Safety, Reliability, and Security, Munich, Germany, 6–9 June 2022*; Lecture Notes in Computer Science; Trapp, M., Schoitsch, E., Guiochet, J., Bitsch, F., Eds.; Springer International Publishing: Cham, Switzerland, 2022; pp. 178–191. [CrossRef]
19. Zhu, L.; Aurum, A.; Gorton, I.; Jeffery, R. Tradeoff and sensitivity analysis in software architecture evaluation using analytic hierarchy process. *Softw. Qual. J.* **2005**, *13*, 357–375. [CrossRef]
20. HEADSTART Project. Available online: https://www.headstart-project.eu/ (accessed on 1 December 2023).
21. 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 ITS World Congress 2021, Hamburg, Germany, 11–15 October 2021.
22. Thorsén, A.; Skoglund, M.; Warg, F.; Jacobson, J.; Hult, R.; Wagener, N.; Ballis, A.; van de Sluis, J.; Perez, J.J.; Steccanella, A. HEADSTART D 1.3 Technical and Functional Requirements for KETs. HEADSTART Deliverable D 1.3 v2.0, HEADSTART Project. 2021. Available online: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5ddc96d9f&appId=PPGMS (accessed on 1 December 2023).
23. Skoglund, M.; Hult, R.; Jacobson, J.; Jonasson, M.; Ballis, A.; Weissensteiner, P.; Coget, J.-B.; Otaegui, O.; Wiggerich, A.; Wagener, N.; et al. HEADSTART D 1.4 Functional Requirements of Selected Use Cases. HEADSTART Deliverable D 1.4, HEADSTART Project. 2019. Available online: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5c833933d&appId=PPGMS (accessed on 1 December 2023).
24. Wagener, N. Common Methodology for Data-Driven Scenario-Based Safety Assurance in the HEADSTART Project. In Proceedings of the Virtual ITS European Congress, Virtual event, 9–10 November 2020. [CrossRef]
25. NGMN Alliance. *V2X Task Force: V2X White Paper*; Technical Report; NGMN Alliance: 2018. Available online: https://www.ngmn.org/publications/v2x-task-force-white-paper-v1-0.html (accessed on 1 December 2023).
26. Hasegawa, R.; Okamoto, E. Adaptive Transmission Suspension of V2N Uplink Communication Based on In-Advanced Quality of Service Notification. *Vehicles* **2023**, *5*, 203–222. [CrossRef]
27. *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. CEN/CENELEC: Brussels, Belgium, 2016.
28. Štern, A.; Kos, A. Positioning Performance Assessment of Geodetic, Automotive, and Smartphone GNSS Receivers in Standardized Road Scenarios. *IEEE Access* **2018**, *6*, 41410–41428. [CrossRef]
29. 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: Gaithersburg, MD, USA, 2004.
30. *SAE J3061*; Cybersecurity Guidebook for Cyber-Physical Automotive Systems. Technical Report; SAE International: Warrendale, PA, USA, 2016.
31. 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), Coimbra, Portugal, 21–24 June 2016; pp. 1–6. [CrossRef]
32. Marojevic, V. C-V2X Security Requirements and Procedures: Survey and Research Directions. *arXiv* **2018**, arXiv:1807.09338. [CrossRef]
33. *ISO/SAE 21434:2021*; Road Vehicles—Cybersecurity Engineering. Technical Report; ISO/SAE: Geneva, Switzerland, 2021.
34. *ISO 26262:2018*; Road Vehicles: Functional Safety. Technical Report; International Organization for Standardization: Geneva, Switzerland, 2018.
35. *ISO/PAS 21448:2019*; Road Vehicles—Safety of the Intended Functionality. Technical Report; International Organization for Standardization: Geneva, Switzerland, 2019.
36. Firesmith, D.G. A Taxonomy of Security-Related Requirements. In Proceedings of the Fourth International Workshop on Requirements Engineering for High-Availability Systems (RHAS'05), Kyoto, Japan, 6 September 2005; p. 11.
37. de Gelder, E.; Paardekooper, J.P. Assessment of Automated Driving Systems Using Real-Life Scenarios. In Proceedings of the 2017 IEEE Intelligent Vehicles Symposium (IV), Los Angeles, CA, USA, 11–14 June 2017; pp. 589–594.
38. 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, Detroit, MI, USA, 5–8 June 2017.
39. Nalic, D.; Mihalj, T.; Bäumler, M.; Lehmann, M.; Eichberger, A.; Bernsteiner, S. Scenario Based Testing of Automated Driving Systems: A Literature Survey. In Proceedings of the FISITA Web Congress, Virtual event, 24 November 2020; Volume 10.
40. Düser, T.; Abdellatif, H.; Gutenkunst, C.; Gnandt, C. Approaches for the Homologation of Automated Driving. *ATZelectron. Worldw.* **2019**, *14*, 48–53. [CrossRef]

41. 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), Virtual event, 27–30 September 2021; pp. 1–7. [CrossRef]
42. Transportstyrelsen. *Transportstyrelsens Föreskrifter Och Allmänna råd om Tillstånd att Bedriva Försök Med Automatiserade Fordon*; Transportstyrelsen: Norrköping, Sweden, 2022.
43. 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: Göteborg, Sweden, 2023.
44. SCReAM. 2023. Available online: https://github.com/EricssonResearch/scream/ (accessed on 1 December 2023).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.