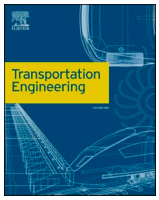
Transportation Engineering 14 (2023) 100205

Contents lists available at ScienceDirect

Transportation Engineering

journal homepage: www.sciencedirect.com/journal/transportation-engineering



Analyses on standards and regulations for connected and automated vehicles: Identifying the certifications roadmap

Meriem Benyahya *, Anastasija Collen, Niels Alexander Nijdam

Centre Universitaire d'Informatique, Geneva School of Economics and Management, University of Geneva, Route de Drize 7, Carouge, 1227, Geneva, Switzerland

ARTICLE INFO

Keywords:
Connected and automated vehicles
Cybersecurity
Data privacy
Standards
ISO/SAE 21434
UNECE R155
UNECE R156
ISO/PAS 5112

ABSTRACT

Protecting Connected and Automated Vehicle (CAV) from cyber attacks and data breaches is a major challenge facing the deployment of driverless vehicles. The CAV is a complex interconnected system consisting of sensors, Artificial Intelligence (AI) processors and external units to assure the automated driving without human interaction. Such complexity increases the attack surfaces and makes the CAV highly vulnerable to cyber assaults. It also entangles security audits and certifications procedures. Our work lays out a novel approach towards CAV's certification focused on cybersecurity and data privacy aspects. Stipulated by the analysis on existing standards' limitations, we propose a Standards Coverage Map (SCM) outlining the CAV's entire ecosystem and linking organisational and technical aspects to the latest standards and regulations from the cyber perspective.

1. Introduction

The CAV embedding cutting edge sensors, advanced Electronic Control Unit (ECU), trailblazing AI components, and connection to everything, has the potential to beneficially change the transport dimensions in the future. Six levels, varying from L0 (no automation) to L5 (fully automated), were predefined by the Society of Automotive Engineering (SAE) through the SAE J3016 and the ISO/SAE 22736 standards as depicted in Table 1. Every level is differentiated by the reference to the automation of the Dynamic Driving Task (DDT), reflecting the human as well as the Automated Driving System (ADS) engagement, and the Operational Design Domain (ODD) describing the driving conditions and delimitation[1].

To assure the CAV's highly autonomous navigation of SAE L4 and L5, the vehicle intelligently compiles inputs from both ITS internal (including cameras, Differential Global Positioning Systems (GPS), Radio Detection and Ranging (RADAR), Light Detection and Ranging (LIDAR), Tyre Pressure Monitor Systems (TPMS), odometric, and ultrasound sensors) and endless external connections to the infrastructure (Vehicle-to-Infrastructure (V2I)), to other vehicles (Vehicle-to-Vehicle (V2V)), to cloud (Vehicle-to-Cloud (V2C)), to grid (Vehicle-to-Grid (V2G)) and to everything (Vehicle-to-Everything (V2X)) [2], as depicted in Fig. 1. Such connectivity is built through multiple channels like Dedicated Short-Range Communication (DSRC) and cellular (LTE/5G) leading to the spontaneous creation of Vehicular Ad-hoc Network (VANET) [3]. However, such high automation and ubiquitous connectivity imposes the CAV to inherit cybersecurity and data privacy challenges and opens up caveats for audit and certification concerns.

Physical audits have been the unique method for safety certification of conventional vehicles [6]. Though, with the emerging technologies like CAV, the physical testing is not feasible and adapted procedures are needed [7]. Additionally, safety is not the unique concern as the CAV' stakeholders are highly aware of the new cybersecurity risks. Several researchers reported multiple attacks over CAV varying from getting control over decision making units [8], imperiling the vehicle's sensors [9] to location tracking revealing the passengers and vehicle identities [10]. Safety and cybersecurity are closely related as demonstrated by cybersecurity researchers [11], where a simple spoofing or a jamming attack can blind the vehicle from existent obstacles [12]. Nevertheless, while the safety requirements are standardised, the processes and methods for vehicular cybersecurity are generic. This is underlined by standardisation and regulatory bodies who consider the automotive cybersecurity state of the art as immature [13].

Cybersecurity and data privacy audit assesses the entire information security management to provide evidence on how the system is protected from threats and data leakages. Such process is conducted through verification plans within real world scenarios. Those plans can also be called certifications if the evaluation is conducted upon a single or multiple standards by external authorised organisations [14]. To that end, certifications' processes tie together organisational and technical

* Corresponding author.
E-mail address: meriem.benyahya@unige.ch (M. Benyahya).

https://doi.org/10.1016/j.treng.2023.100205
Received 24 April 2023; Received in revised form 9 September 2023; Accepted 28 September 2023
Available online 5 October 2023

Table 1
SAE automation levels by SAE J3016 and ISO/SAE 22736 [1,4,5].

Properties	L0	L1	L2	L3	L4	L5
Driving automation	No	Driver assistance	Partial	Conditional	High	Full
ODD	N/A	Domain specific	Domain specific	Domain specific	Domain specific	Unlimited
DDT fallback	Driver	Driver	Driver	Fallback ready-user	ADS or fallback ready-user	ADS
Connectivity	Not required	Not required	Not required	Recommended	Recommended	Extended V2X

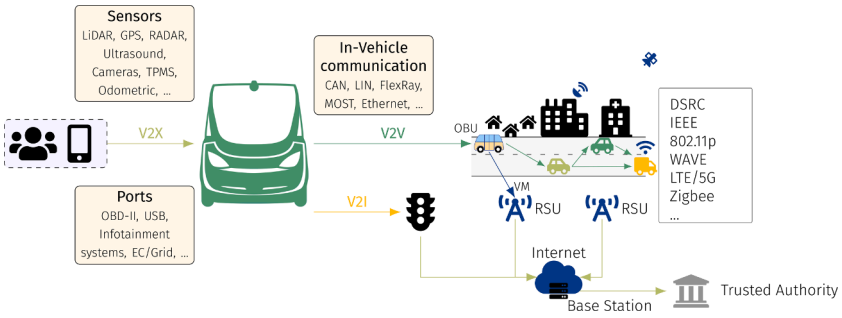


Fig. 1. CAV's environment and attack surfaces.

procedures, including the audit, to assure that the assessed risks have been controlled.

Under the auspices of Standard Development Organisation (SDO), efforts were made to shield the CAV's environment. The International Organisation for Standardisation (ISO) and SAE claim to provide a complete cybersecurity management for the driverless landscape [15]. The United Nations Economic Commission for Europe (UNECE) published acts to unify the automotive standards by requiring the Cybersecurity Management System (CSMS) and Software Update Management System (SUMS) certifications for the SAE L3 onward. The General Data Protection Regulation (GDPR) is the fundamental privacy data law in Europe. The European Telecommunication Standards Institute (ETSI), International Telecommunication Union (ITU), 5G Automotive Association (5GAA) and Automotive Open System Architecture (AUTOSAR) institutions provide advice for securing vehicular communication [16].

Despite the notable publications by the SDO, the evolving attack feasibility and the SAE's levels introduce a new dimension of complexity, which blurs the certification process and creates uncertainty. The existing and Work In Progress (WIP) standards are applicable commonly to vehicles of SAE L3 where the risks are incomparable and have to be tackled differently from those of L4 and L5. Depending on the SAE level, the driver or the ADS has to take over or relinquish the DDT in case of a fallback led by a system failure or a cyber attack [5]. In the instance of a blinding attack targeting the perception sensors of an L3 or an L4, a fallback ready-user (remote or in-vehicle driver) can drive the vehicle into a stable and safe condition (also called Minimal Risk Condition (MRC) [1]). Projecting an equivalent scenario over an L5 CAV, the ADS per se must achieve the MRC independently from any type of human intervention. As reflected in Table 1, several features support distinguishing the properties of each SAE level including the ODD limitation, how the MRC can be conducted, and the connectivity multiplicity. However, by combining the three highest SAE levels, the SDO consider cyber threats and their related risks to be governed equally despite their properties' dissimilarity.

Furthermore, the multiple regulations are overlapping and end up by pointing to the CSMS and SUMS certifications or to high level standards which are broad enough to not to cope with the particularities of the CAV's cyber and privacy risks [17]. Thus, an SCM would guide cybersecurity and data privacy assessment and monitoring on the CAV landscape. Our work identifies the promising standards and links them to sub-components which need to be audited. Our added value and main contributions are summarised as follows:

- Investigation into the gaps and faults of existing standards, regulations and certification schemes, which aim to fulfil the vehicular cybersecurity and data protection expectations within CAV' of SAE L4 and L5.
- Development of an SCM combining technical and organisational requirements where attack surfaces are mapped to standards and regulations to serve as the foundation of a future cybersecurity and data privacy certification model.

These aimed contributions create ample opportunity to gear up the following Research Question (RQ). First, we analyse *what are the limitations of the CAV' cybersecurity and data privacy related standards and regulations, by building a structural representation of the standards suitability* in Section 3 (RQ1). Secondly, we evaluate *weather a combination of existing standards and regulations offer the foundation to build a future cybersecurity and data protection certification framework* (RQ2).

The paper is structured as follows: Section 2 makes a comparison of the present work with recent efforts. Section 3 delivers a review of crucial standards and regulations. Section 4 outlines the CAV' SCM and ITS development methodology. Finally, Section 5 offers future work orientation while Section 6 summarises our findings and provides concluding remarks.

2. Related work

A plethora of studies on building safety certification models for CAV' environment exists, while the reviews on cybersecurity and data privacy certification models remain barely evoked. Furthermore, we observe a scarcity of multi-standards frameworks defining how to thoroughly certify the CAV's system-wide layers. There is also a remarkable lack on reviews pointing out data privacy certification as it is believed that the GDPR compliance is all what is required for assuring an optimal data protection. We highlight researchers' efforts aiming to construct holistic cybersecurity and data privacy assessments of the CAV's environment based on existing and emerging standards and regulations.

Through multiple publications and in collaboration with other authors, Schmittner has been tracking the progress of the ISO/SAE 21434 development and implemented an automotive cybersecurity risk management solution compliant to that standard. Schmittner and Macher [18] provided an initial overview of the first automotive initiatives on elaborating CAV's safety and cybersecurity standards. They presented a preview of the ISO/SAE 21434 structure that was still a WIP at that time

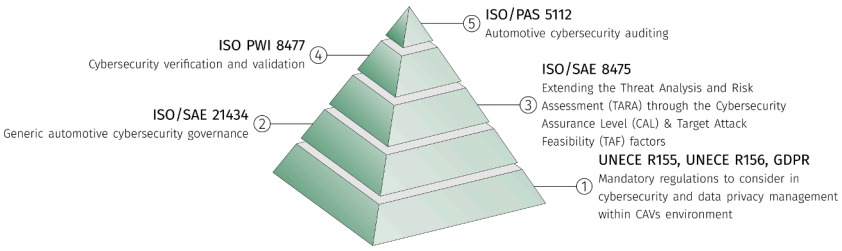


Fig. 2. Key regulations and standards co-relation.

in addition to all the other under development standards by SAE, ITU and UNECE. Subsequently, Schoitsch and Schmittner [15] provided an updated review on the ongoing SDO efforts with a focus on ISO and UNECE. In a risk management-based approach, Schmittner et al. [13] discussed an asset based automotive cybersecurity risk management approach stemming from ISO/SAE 21434. Furthermore, Vogt et al. [19] presented the interaction between safety and security through the ISO 26262 and ISO/SAE 21434 respectively. To that end, those approaches outlined succinct risk assessment methodologies without reflecting other SDO's standards.

Similarly, Marksteiner et al. [20] proposed a standardised testing process of automotive cybersecurity based on ISO/SAE 21434 and the latest regulations R155 (CSMS) and R156 (SUMS) from the UNECE. In another work, Marksteiner and Bronfman [7] highlighted the limitations of the standard for not specifying the testing procedure. To that end, the authors designed a black box security testing as a compliment to that standard. Their analysis showcased improvement avenues that are applicable to any type of vehicle where ADS or V2X are implemented without directly considering the full automation property.

Mateo Sanguino et al. [21] provided a literature review on cybersecurity certifications and audits based standards. The authors identified the steps toward cybersecurity certification in addition to a listing of audit techniques and certifying bodies. As with the rapid development of automotive standards, ISO/SAE 21434 and ISO/PAS 5112 were not reported by the time of the research work elaboration. Kim and Shrestha [16] pointed out the standardisation and regulation challenges with regard to the complex CAV environment. The authors classified the legal and standardisation requirements impacting the CAV into three groups: automotive industry, DSRC wireless based and 5G V2X communication regulations. Per each group, the authors identified the relevant regulations and standardisation bodies initiatives. However, the review combines both safety and cybersecurity and is focused mostly on V2X standards. Sui and Muehl [22] adopted a similar approach by providing a high level overview of the mainstream standards related to V2X. Khalid Khan et al. [23] delineated a conceptual cybersecurity assessment model anticipating, in a cause-effect manner, the possible system behaviour upon the deployed CAV's cybersecurity mechanisms. The authors developed a model that was distinct from any standard or regulatory obligation as their analysis showcased that existent policies do not keep pace with the rapidly evolving cybersecurity risks.

Per the analysis from the existing studies, we differentiate from the aforementioned works by: (i) Focusing on CAV's cybersecurity and data privacy regulations and standardisation and not safety or physical security certification; (ii) Providing an up to date review on the ongoing efforts from the SDO on the automotive cybersecurity and data privacy standardisation and regulation; and (iii) Mapping the identified standards to procedural and technical layers of the CAV's ecosystem through the SCM.

3. Key standards and regulations efforts

3.1. Active SDO in vehicular cybersecurity and data privacy landscape

With the CAV emergence, the development of multiple standards and regulations have been witnessed by numerous working groups from the global SDO. The SAE was the first standardisation body to issue a vehicular cybersecurity standard through the SAE J3016 [1]. From ISO, the ISO/TC22, ISO/TC204 and ISO/IEC JT1 are the key active committees on vehicular cybersecurity, Intelligence Transport System (ITS) concerns and privacy assessments accordingly. As described in details in Appendix A Table A.1, the first committee focuses on standardising the CAV' safety and cybersecurity risk management systems mainly through the ISO/SAE 21434 (where they joined their efforts with the SAE) and ISO/PAS 5112. The second committee provides the basic taxonomy of terms related to automated driving systems and associated security guidelines of the V2X communication through standards such as ISO/TS 21177 and ISO/TR 21286-3. Furthermore, the ISO/IEC JT1 aims to standardise security and privacy evaluations processes and procedures through the ISO/IEC PWI 5888 and ISO/IEC 29134. UNECE has a devoted task force working towards global vehicular cybersecurity regulations. Through the new regulations R155 and R156, the UNECE World Forum for Harmonisation of Vehicle Regulations (WP29) made the CSMS and SUMS certification mandatory in Europe for all new vehicles' types starting from June 2022 and for all vehicles starting from 2024 [7]. Still from the United Nation board, the ITU working groups developed series of security recommendations related to connected vehicles, on the one hand, X.1371 to X.1376 [24,25] which outline security threats definition, security guidelines for V2X, specification of secure software update procedure for ITS's devices and guidelines for intrusion and misbehaviour detection. On the other hand, the ITU has a dedicated Focus Group-AI for Autonomous and Assisted Driving (FGAI4AD) that is more focused on ethical and legal matters with regard to the vehicle SAE level. Moreover, the ETSI proposed several standards related to security, privacy and establishment of standardised architecture for connected vehicles. However, these guidelines are not specifying or targeting a specific CAV' automation level.

The working group 7 from the 5GAA is another global organisation who published multiple technical guidelines aiming to unify security and privacy requirements for the cooperative V2X [26,27]. In collaborations with ETSI, ISO and SAE, the 5GAA is promoting standards supporting 5G connectivity and ITS implementation within the V2X communication [16]. Before that, the 3rd Generation Partnership Project (3GPP) provided the first V2X foundations, but they were limited to the Long-Term Evolution (LTE) connectivity [28]. Furthermore, the automotive industry has also pushed to standardise security approaches over on-board systems through their collaboration on AUTOSAR standards. AUTOSAR recommendation series tend to secure in-vehicle communication networks and ECU, protect data confidentially and implement cryptography. From the data protection perspective, the GDPR remains the main law to comply with for data protection in any context including the vehicular environment. Nonetheless, the law provides the basic obligations to consider by the CAV stakeholder without guaranteeing an optimal protection from data privacy risks.

3.2. Key regulations and standards for cybersecurity and data privacy assessments

In this section, a review of the crucial regulations and standards is

provided. Their gaps and limitations are also highlighted. We constrain our analysis to explore only the standards and regulations that have been promoted and cross-referred by the key SDO. Additionally, as presented in Section 2, they have been the main focus of multiple researchers as they are perceived to assure a flawless protection from cyber threats and data privacy violation. Fig. 2 wraps those standards and regulations in a pyramid structure presentation view, where each slab represents a more narrowed and granular recommendations from the automotive cybersecurity assessment perspective. The pyramid base consists of generic, yet compulsory regulations. The second slab is represented by ISO/SAE 21434, the generic cybersecurity risk management framework that is pointed out by the UNECE R155 and UNECE R156. The third slab epitomises the ISO/SAE 8475 which complements the outcome from the previous layer. The fourth level checks the conformity of those outcomes through ISO/SAE PWI 8477. Finally, the pyramid summit is represented by ISO/PAS 5112 which encapsulates all previous outputs yielding to the CAV' procedural audit.

UNECE R155 [29] is the prominent regulation making the CSMS certification mandatory at the vehicle type approval stage. The CSMS certification aims to provide a trustworthy proof of efficient threat governance, including risk monitoring, assessment and mitigation. While the UNECE R155 regulation requires the manufacturer to have a cybersecurity management system in place counter-measuring the predefined risks annexed to the regulation; the risk of unknown attacks, also annotated hereinafter as residual risks, occurrence remain high with the CAV ecosystem [23]. Additionally, the regulation is limited to vehicles of SAE L3 onward. In other words, the UNECE R155 considers vehicles of L3, L4 and L5 to be proportionately qualified to respond to limited cyber threats, which backfires the CSMS efficiency.

UNECE R156 [30] comes along with UNECE R155 to ensure that the manufacturer put in place appropriate safety and security processes for conducting software updates. The regulation mandates an assessment that has to be carried out, exclusively, by approval authorities, who issue a SUMS certification upon the software update processes' conformity at type approval stage. According to the regulation, the SUMS has to be renewed every three years or after major software updates occurring even before the end of the three years cycle. Albeit the recently published ISO 24089 has brought out several requirements related to software update processes, technical specifications per se are still lacking as the SUMS is limited to assessing the self-documented measures developed by the manufacturer.

GDPR [31] is perceived as the most advanced European personal data protection framework with a global impact [16]. The GDPR sets strict obligations related to personal data processing, rights for concerned individuals, technical requirements to employ privacy preserving mitigation strategies, and Data Protection Impact Assessment (DPIA) deployment for any new technologies with privacy risks. However, within the CAV's complex environment, the application of the GDPR data processing principles remain convoluted, as the CAV's stakeholder can accumulate multiple roles making them data processors and data controllers at the same time [32]. Another limitation of the GDPR is that it excludes anonymisation as a privacy preserving technique from the legislation scope considering that it is a permanent solution. Though, with minor reverse engineering efforts, the personal data can be de-anonymised with no compliance violation to the GDPR [33]. Based on the GDPR requirements, further analysis on data privacy protection was evoked by the European Data Protection Board (EDPB) [34,35]. Although the EDPB's guidelines are referring to the processing of personal data in relation to CAV and highly recommends the DPIA execution, they inherit the GDPR's pitfalls. To that end, a successful implementation of DPIA, and even full compliance to the GDPR, does not rhyme with an absolute personal data protection for CAV, confirming the need for a combined execution of further standards from the upper levels as depicted in Fig. 2.

ISO/SAE 21434 [36] came up with high level definitions and guidelines to implement cybersecurity management principles throughout the entire life-cycle, including concept, development and post-development phases for all road vehicles. In a light-weighted approach, the standard elicited the road map on how to conduct Threat Analysis and Risk Assessment (TARA), the appropriate cybersecurity assessment for the vehicular vulnerabilities [37], which is intended to be extended in ISO/SAE 8475. Similar to TARA presentation, the standard introduced fundamental definitions for other cybersecurity actions and processes like cybersecurity verification and validation in addition to auditing that are elevated further in ISO/SAE PWI 8477 and ISO/PAS 5112 respectively. Though, the standard scope is broad enough to cover all vehicles with electrical and electronic systems that can match any SAE level. Additionally, the ISO/SAE 21434 did not evoke specific technologies to counter cybersecurity risks. Furthermore, while it is true that it offers agility on applying security concepts at different stages of the vehicle life-cycle, no detailed guidance is provided on how to implement them and using which tools.

ISO/SAE 8475 [38] evokes the Cybersecurity Assurance Level (CAL) and Targeted Attack Feasibility (TAF) factors to complement the TARA process introduced by the ISO/SAE 21434. In parallel to TARA steps, the CAL is initiated and reviewed throughout the process to reflect the assurance level and confidence on the asset protection. Conversely, the TAF represents an additional metric to the assessment reflecting the intended level of attack feasibility. Both the CAL and TAF can be used for continuous monitoring, which means even after the TARA accomplishment. Additionally, they can be updated whenever an operational change occur to the system.

ISO/SAE PWI 8477 [39] is foreseen as a complement to the ISO/SAE 21434, ISO/SAE 8475 and UNECE R155 where the TARA outcomes are verified and the residual risks are validated. On the one hand, the verification process relies on confirming the appropriateness of the risk treatment conducted within the TARA. It iteratively justifies the conformity of the implemented risk mitigation with regard the cybersecurity requirements until no further refinement is necessary. On the other hand, the validation process aims to confirm, with tolerable level of confidence, that the residual risk is acceptable. The cybersecurity validation can be executed through fuzzy or penetration testing with the intention to test the system's robustness. To that end, the ISO/SAE PWI 8477 standard can provide valuable technical inputs to conduct procedural audit as defined in ISO/PAS 5112 standard.

ISO/PAS 5112 [14] is a result of combining the outcomes and requirements from preceding levels as shown in Fig. 2. Consequently, the brand new standard provides an extension of the ISO/SAE 21434 through a mapping of the audit objectives and evidences managing the conformity to the CSMS and SUMS certifications program. The standard aims to be applicable to conduct internal or external audits as well as to train auditors competences. Albeit the ISO/PAS 5112 orients toward a successful audit program focusing on organisational cybersecurity processes, it does not provide technical requirements on achieving cybersecurity or data privacy assessments.

As an answer for RQ1, the following limitations demonstrate shortcomings of the key existing standards and regulations:

- The current approaches remain generic to different automation levels, while the highly automated vehicles of SAE L4 and L5 should be tackled properly with reference to their features including ODD, DDT fallback and connectivity as reported in Table 1.
- The standards do not consider granular evaluation per CAV's layer and sub components.
- Standards that are providing coarse verification techniques, as per ISO/SAE 8475 and ISO/SAE PWI 8477, are still WIP which make them more tailored to major changes and with the risk to influence the audit quality that can be perceived by the ISO/SAE 5112.
- The data protection within CAV's environment requires more efforts to strengthen the existing regulation and to provide more insights on conducting continuous privacy assessments.

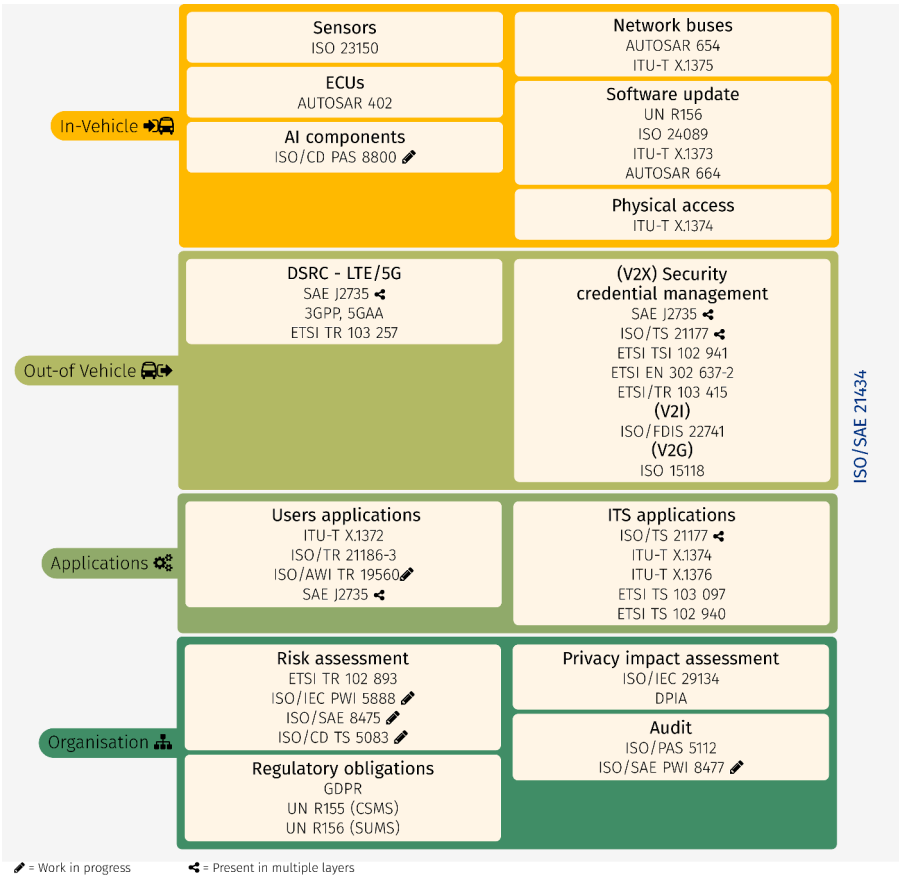


Fig. 3. CAV's ecosystem SCM.

4. CAV's ecosystem SCM

The present section discusses the established methodology on constructing the SCM, delineates ITS layers and outlines the confronted challenges on building such mapping.

4.1. Methodology

A suitable approach to build a robust cybersecurity and data privacy certification framework starts from a foresight analysis of the CAV's potential threats, an in-depth assimilation of the existing regulatory and standardisation bodies efforts; and a visual representation that simplifies the knotted CAV's ecosystem. We initiated our process with building a taxonomy of potential threats and mapped them to their related attack surfaces and mitigation schemes through our previous works [2,32]. This approach enabled a granular capturing of all the components requiring a cybersecurity and data privacy assessments which supported to construct our SCM. We opted for a representation reflecting the empirical attack surfaces, the intertwined standardised processes and the main facets of cybersecurity audits. Furthermore, guided by the review of the most recent standards from Section 3, we elevate our SCM further by matching the identified attack surfaces to the existing or WIP standards as drawn in Appendix A Table A.1 As a result, Fig. 3 depicts our SCM which combines the technical and organisational audit avenues applied to the CAV's ecosystem. The map is classified into four layers: in-vehicle, out-of vehicle, applications and organisation, where every layer groups the respective technical standards. As a parent node of the four layers, ISO/SAE 21434 is set as the core, yet the broad standard. The combination of both generic and technical standards on the SCM is foreseen to overcome the broadening of the ISO/SAE 21434 leading to a more thorough assessment.

4.2. The SCM layers

The in-vehicle layer incorporates the attack surfaces at the vehicle level which we classify into six sub-layers. First, 'sensors' category defines the guidance on standardising the interfaces between the different sensors and the fusion unit leading to the automation navigation decisions. Second, 'network buses' category where standards propose guidelines on detecting intrusions and authentication measures within the in-vehicle communication networks. Third, the 'ecu' standard aims to prevent from non-authorised access to the vehicular software modules. Fourth, 'software update' outlines the directives on how to conduct secure software update during the vehicle life-cycle. Fifth, 'ai components' standard provides guidance on secure usage of ai-based functions involved on the automation decision making. Finally, the 'physical access' specifies countermeasures against threats from plugged external devices.

The out-of vehicle layer relies on two main categories wrapping standards related to CAV's internet channels and V2X communications.

To secure the CAV's internet access using 'DSRC, LTE and 5G', considerable standards provided a set of secure channel models and through several use cases. Besides, the multiple V2X communications have been standardised by ISO, ETSI and SAE. The 'security credential management' standards, which sets V2X certificates security and privacy requirements, define the precise structure, format, and authentication schemes supporting the CAV's communication to peer instances. It is noteworthy to mention that other V2X communications such as 'V2I' and 'V2G' have been supported by dedicated standards while others as per the V2C is still considered under the umbrella of broad standards like SAE J2735.

The application layer consists of two sub-layers reflecting two types of applications: users and ITS. The CAV's deployment is associated to the means of several services provided to the end user and to the smart city. The 'users applications' standards focus on data access and cryptography best practices to consider while building interfaces to the CAV's hardware or software. Likewise, the 'ITS applications' standards recommend mechanisms to determine permitted actions among the peer ITS applications to achieve security properties such as authorization, integrity and confidentially. Though, it is worthy to be highlighted that standards such as SAE J2735 and ISO/TS 21177 have larger scope covering the V2X communication in general and, hence, other sub-components from the second layer too.

The organisation layer incorporates four procedural sub-layers. The 'risk assessment' reflects evaluation procedures on quantifying cybersecurity threats likelihood and impact. The 'privacy impact assessment' warps standardised processes and reports on privacy impact assessments. The 'regulatory obligations' sets the mandatory laws that the CAV's environment has to comply with which are summarised into the GDPR, UNECE R155 and R156. Finally, the 'audit' group wraps the cybersecurity verification, validation and auditing processes that are encapsulated on ISO PAS 8477 and ISO/PAS 5112.

4.3. Challenges

To build our SCM and synthesised standards in Appendix A Table A.1, several challenges were confronted where few assumptions were made. First, the identified standards' scope, even for the most technical ones, aggregate multiple attack surfaces which justifies their appearance in multiple sub-layers as shown in Fig. 3. Second, duplicated efforts were observed to protect components such as software update, V2X communication and ITS applications while other vectors remain uncovered or limited. Additionally, the SAE level definition lacks granular descriptions within multiple guidelines. Very few standards like ISO/PAS 5112 and ISO/CD TS 5083 specify the automation level to be L3 onward, while the others either target connected vehicles without automation description or invoke the presence of ADS (which provides partial automation at L2 and full automation starting from L3 [40]). To that end, standards targeting only connected vehicles are classified in Appendix A to be of SAE L1 onward, while standards covering vehicles with implemented ADS are foreseen to be an L2 onward. On the same note, a Not Applicable (NA) attribute was assigned to standards where knowledge on the connectivity maturity or ADS availability was lacking, as well as when the standards' scope is not limited to CAV.

5. Discussion & future work

The SCM presented in this paper is currently an ongoing research. To address RQ2, the SCM has been developed to reflect an efficient approach on tackling the overall cybersecurity and data privacy CAV's assessment and as a step toward building a certification framework considering risks related to L4 and L5 CAV. It is envisioned to conduct several iterations of the SCM to cope with the rapidly evolving CAV's technologies and to keep pace with the regulation and standardisation efforts. As a work in progress, we intend to build a certification framework for CAV's ecosystem that represents the road-map to audit the whole system layers. Based on sets of procedures and processes and a clear workflow, the framework aims to identify, in a step by step manner, the path to a compliant environment. The archetype would introduce a harmonised ratings reflecting the evolving attacks feasibility, priority and impact per SAE automation level. It aims to measure and quantify risks upon an established catalogue of scenarios related to cybersecurity critical situations and personal data leakage. Then, a testing environment with predefined architecture and configuration will be chosen to deploy the required assessment on a pass-fail criteria mode. In other words, the verification of our certification framework is foreseen to be tested in real world cases, specifically within the scope of SHOW [41] and ULTIMO [42] projects where vehicles of SAE L4 and L5 are deployed.

6. Conclusion

It is true that there is no standard to identify what constitutes or motivates a cyber assault, though the CAV' standards need to be specific and improved to effectively protect from malicious attacks harming the CAV' users security, privacy and, hence, safety. The attacks will not remain frozen in time, hence, standards, regulations and adequate risk management models have to continuously evolve to ensure an optimal protection. Our research goal was threefold: present an up to date review of the SDO efforts, highlight the key standards and regulations with a review of their current limitations and provide the technical and procedural audit avenues through the SCM. Per our findings, topic on how to ensure the CAV cybersecurity and data privacy certification is still not comprehensively addressed. The existing approaches remain theoretical, broad and not holistic to cover all the sophisticated sub-components of the complex CAV' environment. Bearing that in mind, we proposed the SCM which wraps potential attack surfaces, the most recent SDO efforts, and both generic and specific guidelines into a graphical view.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgment

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under grant agreement No 875530, Horizon Europe research and innovation programme under grant agreement No 101077587 and from the Swiss State Secretariat for Education, Research and Innovation (SERI). We would also like to thank Teri Lenard for the valuable insights on the manuscript and proofreading.

Appendix A. Standards

Table A.1
CAV's cybersecurity and privacy standards baseline.

Organisation	Standard ID	Year	Scope	SAE[a]	Description
ISO/TC22	ISO/SAE 21434 [36]	2021	CAV	●●●●●●	Cybersecurity engineering
	ISO/PAS 5112 [14]	2022	CAV	○○○●●●●	Guidelines for auditing cybersecurity engineering
	ISO 23150 [43]	2021	CAV	○○●●●●●	Data communication between sensors and data fusion unit for automated driving functions
	ISO 15118 [44]	2019	CAV	○●●●●●●	Vehicle to grid communication interface
	ISO/CD PAS 8800 [45]	WIP	CAV	○○○●●●●	Safety and artificial intelligence
	ISO 24089 [46]	2023	CAV	○●●●●●●	Software update engineering
	ISO/SAE 8475 [38]	WIP	CAV	○●●●●●●	Cybersecurity Assurance Levels and Target Attack Feasibility
	ISO/SAE PWI 8477 [39]	WIP	CAV	○●●●●●	Cybersecurity verification and validation
	ISO/CD TS 5083 [47]	WIP	CAV	○○○●●○	Safety for automated driving systems- Design, verification and validation
ISO/TC204	ISO/SAE PAS 22736 [4]	2021	CAV	●●●●●●	Taxonomy and definitions for terms related to driving automation systems for On-Road Motor Vehicle (RMV)
	ISO/AWI TR 19560 [48]	WIP	CAV	○○○●●○	Information interface framework between ADS and user
	ISO/TS 21177 [49]	2019	ITS	○●●●●●	ITS station security services for secure session setup and authentication between trusted devices
	ISO/TR 21186-3 [50]	2021	ITS	○●●●●●	Guidelines on the usage of standards - Part 3: Security
	ISO/FDIS 22741 [51]	2022	ITS	NA	Roadside modules AP-DATEX (application profile data exchange) data interface
ISO/IEC JT1	ISO/IEC 29134 [52]	2017	IT	NA	Guidelines for privacy impact assessment
	ISO/IEC PWI 5888 [53]	WIP	CAV	○○○●●●●	Cybersecurity and privacy protection - Security requirements and evaluation activities for CAV
UNECE WP29	R155 [29]	2021	CAV	○○●●●●	Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system
	R156 [30]	2021	CAV	●●●●●●	Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system
ITU	X.1371 [24]	2020	ITS	○●●●●●	Security threats to connected vehicles
	X.1372 [54]	2020	ITS	○●●●	Security guidelines for V2X

(*continued on next page*)

Table A.1 (*continued*)

Organisation	Standard ID	Year	Scope	SAE[a]	Description
	X.1373 [55]	2017	ITS	○●●●●●	Secure software update capability for ITS communication devices
	X.1374 [56]	2020	ITS	○●●●●●	Security requirements for external interfaces and devices with vehicle access capability
	X.1375 [57]	2020	ITS	○●●●●●	Guidelines for an intrusion detection system for in-vehicle networks
	X.1376 [25]	2021	ITS	○●●●●●	Security-related misbehaviour detection mechanism using big data for connected vehicles
	FG-AI4AD-2 [58]	2021	ITS	○○○●●●	Automated driving safety data protocol- Ethical and legal considerations of continual monitoring
ETSI	ETSI TR 102 893 [59]	2017	ITS	○●●●●●	Threat, vulnerability and risk analysis
	ETSI TS 102 731 [60]	2010	ITS	○●●●●●	Security Services and Architecture
	ETSI TS 102 940 [61]	2019	ITS	○●●●●●	ITS communications security architecture and security management
	ETSI TS 102 941 [62]	2021	ITS	○●●●●●	Trust and Privacy Management
	ETSI TS 103 097 [63]	2020	ITS	○●●●●●	Security header and certificate formats
	ETSI TS 103 415 [64]	2018	ITS	○●●●●●	Pre-standardisation study on pseudonym change management
	ETSI TS 103 257-1 [65]	2019	ITS	○●●●●●	Channel Models for the 5,9 GHz frequency band
	ETSI EN 302 637-2 [66]	2014	ITS	○●●●●●	Specification of cooperative awareness basic service
SAE	J2735 [67]	2020	V2X	○●●●●●	V2X communications message set dictionary
	J3216 [68]	2021	CAV	●●●●●●	Taxonomy and definitions for terms related to cooperative driving automation for RMV
	J3016 [1]	2016	CAV	○○●●●●	Taxonomy and definitions for terms related to driving automation systems for RMV
AUTOSAR	402 [69]	2014	In-Vehicle	●●●●●●	Specification of crypto service manager
	654 [70]	2017	In-Vehicle	●●●●●●	Specification of secure onboard communication
	664 [71]	2016	In-Vehicle	●●●●●●	Overview of functional safety measures

[a] The ● refers to the indicated SAE level(s).

References

[1] SAE International, SAE J3016 Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles. Technical Report, SAE International, 2021.

[2] M. Benyahya, A. Collen, S. Kechagia, N.A. Nijdam, Automated city shuttles: mapping the key challenges in cybersecurity, privacy and standards to future developments, Comput. Secur. 122 (2022) 102904, https://doi.org/10.1016/j.cose.2022.102904.

[3] M. Lee, T. Atkison, VANET applications: past, present, and future, Veh. Commun. 1 (2020) 100310.

[4] ISO, ISO - ISO/SAE PAS 22736:2021 - Taxonomy and Definitions for Terms Related to Driving Automation Systems for on-Road Motor Vehicles. Technical Report, ISO, 2021.

[5] M. Girdhar, Y. You, T.J. Song, S. Ghosh, J. Hong, Post-accident cyberattack event analysis for connected and automated vehicles, IEEE Access 10 (2022) 83176–83194, https://doi.org/10.1109/ACCESS.2022.3196346.

[6] M.C. Galassi, A. Lagrange, P. Guido, R. Mele, B. Ciuffo, O. Piron, W. Malfait, European Commission. Joint Research Centre, ERA - JRC Workshop on Safety Certification and Approval of Automated Driving Functions: Analogies and Exchange of Best Practices Between Railway and Automotive Transport Sectors. Technical Report, European Commision, Joint Research Centre, 2021.

[7] S. Marksteiner, S. Bronfman, Using cyber digital twins for automated automotive cybersecurity testing, in: IEEE (Ed.), 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 2021, pp. 123–128, https://doi.org/10.1109/EuroSPW54576.2021.00020.

[8] C. Miller, C. Valasek, Remote exploitation of an unaltered passenger vehicle, Defcon 23 2015 (2015) 1–91.

[9] C. Yan, W. Xu, J. Liu, Can you trust autonomous vehicles: contactless attacks against sensors of self-driving vehicle, DEFCON 24 (8) (2016) 109.

[10] P. Asuquo, H. Cruickshank, J. Morley, C.P. Ogah, A. Lei, W. Hathal, S. Bao, Z. Sun, Security and privacy in location-based services for vehicular and mobile communications: an overview, challenges, and countermeasures, IEEE Internet Things J. 5 (6) (2018) 4778–4802.

[11] M. Benyahya, P. Bergerat, A. Collen, N.A. Nijdam, Symbiotic analysis of security assessment and penetration tests guiding real L4 automated city shuttles, Telecom 4 (1) (2023) 198–218, https://doi.org/10.3390/telecom4010012.

[12] S. Malik, W. Sun, Analysis and simulation of cyber attacks against connected and autonomous vehicles. 2020 International Conference on Connected and Autonomous Driving, Institute of Electrical and Electronics Engineers Inc, 2020, pp. 62–70.

[13] C. Schmittner, B. Schrammel, S. Konig, Asset driven ISO/SAE 21434 compliant automotive cybersecurity analysis with ThreatGet, in: Springer Nature Switzerland AG (Ed.), European Conference on Software Process Improvement EuroSpi2021 vol. 1442, Springer Nature Switzerland AG, Cham, 2021, pp. 548–563.

[14] ISO, ISO/PAS 5112 - Guidelines for Auditing Cybersecurity Engineering. Technical Report, ISO, 2022.

[15] E. Schoitsch, C. Schmittner, Ongoing cybersecurity and safety standardization activities related to highly automated/autonomous vehicles. Intelligent System Solutions for Auto Mobility and Beyond, Springer, Cham, 2020, pp. 72–86.

[16] S. Kim, R. Shrestha, Automotive Cyber Security, Springer Singapore, Singapore, 2020, https://doi.org/10.1007/978-981-15-8053-6.

[17] G. Macher, C. Schmittner, O. Veledar, E. Brenner, ISO/SAE DIS 21434 automotive cybersecurity standard - In a Nutshell. Computer Safety, Reliability, and Security, Springer, Cham, 2020, pp. 123–135.

[18] C. Schmittner, G. Macher, Automotive cybersecurity standards - relation and overview. Lecture Notes in Computer Science vol. 11699 LNCS, Springer, Cham, 2019, pp. 153–165.

[19] T. Vogt, E. Spahovic, T. Doms, R. Seyer, H. Weiskirchner, K. Pollhammer, T. Raab, S. Rühup, M. Latzenhofer, C. Schmittner, M. Hofer, A. Bonitz, C. Kloibhofer, S. Chlup, A comprehensive risk management approach to information security in intelligent transport systems, SAE Int. J. Transp. Cybersecur. Privacy 4 (1) (2021), https://doi.org/10.4271/11-04-01-0003.11–04

[20] S. Marksteiner, N. Marko, A. Smulders, S. Karagiannis, F. Stahl, H. Hamazaryan, R. Schlick, S. Kraxberger, A. Vasenev, A process to facilitate automated automotive cybersecurity testing. 2021 IEEE 93rd Vehicular Technology Conference vol. 2021-April, IEEE Inc, 2021, pp. 1–7.

[21] T.d.J. Mateo Sanguino, J.M. Lozano Domínguez, P. de Carvalho Baptista, Chapter four - cybersecurity certification and auditing of automotive industry, in: D. Milakis, N. Thomopoulos, B. van Wee (Eds.), Policy Implications of Autonomous Vehicles, Advances in Transport Policy and Planning, vol. 5, Academic Press, 2020, pp. 95–124, https://doi.org/10.1016/bs.atpp.2020.01.002.

[22] A. Sui, G. Muehl, Security for autonomous vehicle networks. ICEICT 2020 - IEEE 3rd International Conference on Electronic Information and Communication Technology, Institute of Electrical and Electronics Engineers Inc., 2020, pp. 67–69.

[23] S. Khalid Khan, N. Shiwakoti, P. Stasinopoulos, A conceptual system dynamics model for cybersecurity assessment of connected and autonomous vehicles, Accid. Anal. Prev. 165 (2022), https://doi.org/10.1016/j.aap.2021.106515.

[24] ITU-T, X. 1371 Security Threats to Connected Vehicles. Technical Report, ITU-T, 2020.

[25] ITU-T, X.1376 Security-Related Misbehaviour Detection Mechanism using big Data for Connected Vehicles. Technical Report, ITU-T, 2021.

[26] 5GAA, 5GAA Efficient Security Provisioning System White Paper. Technical Report, 5GAA, 2020.

[27] 5GAA, Privacy by Design Aspects of C-V2X. Technical Report, 5GAA, 2020.

[28] G. Velez, A. Martín, G. Pastor, E. Mutafungwa, 5G beyond 3GPP release 15 for connected automated mobility in cross-border contexts, Sensors (Switzerland) 20 (22) (2020) 1–19, https://doi.org/10.3390/s20226622.

[29] UNECE, R155. Technical Report, UNECE, 2020.

[30] UNECE, R156. Technical Report, UNECE, 2020.

[31] The European Parliament and the Council of the European Union, Regulation (EU) 2016/679 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data. Technical Report, European Commission, 2016.

[32] M. Benyahya, S. Kechagia, A. Collen, N.A. Nijdam, The interface of privacy and data security in automated city shuttles: the GDPR analysis, Appl. Sci. 12 (9) (2022) 4413, https://doi.org/10.3390/app12094413.

[33] European Union Agency for Cybersecurity, Data Protection Engineering. Technical Report, ENISA, 2022.

[34] European Data Protection Board, Guidelines 1/2020 on Processing Personal Data in the Context of Connected Vehicles and Mobility Related Applications. Technical Report January, EDPB, 2020.

[35] European data Protection Board, Guidelines 1/2020 on Processing Personal Data in the Context of Connected Vehicles and Mobility Related Applications. Technical Report March, EDPB, 2021.

[36] ISO, ISO/SAE 21434 Road Vehicles-Cybersecurity Engineering. Technical Report, ISO/SAE, 2021.

[37] M. Benyahya, T. Lenard, A. Collen, N.A. Nijdam, A systematic review of threat analysis and risk assessment methodologies for connected and automated vehicles. Proceedings of the 18th International Conference on Availability, Reliability and Security vol. 1, ACM, New York, NY, USA, 2023, pp. 1–10, https://doi.org/10.1145/3600160.3605084.

[38] ISO, ISO/SAE AWI 8475 - Cybersecurity Assurance Levels (CAL) and Target Attack Feasibility (TAF). Technical Report, ISO, 2023.

[39] ISO, ISO/SAE PWI 8477 Road Vehicles - Cybersecurity Verification and Validation. Technical Report, ISO, 2023.

[40] P. Koopman, SAE J3016 User Guide, 2021. https://users.ece.cmu.edu/~koopman/j3016/.

[41] Show Consortium, Show project, 2022. https://show-project.eu/.

[42] European Comission, ULTIMO - Advancing Sustainable User-centric Mobility with Automated Vehicles, 2022. https://cordis.europa.eu/project/id/101077587/fr.

[43] ISO, ISO 23150:2021 Road Vehicles - Data Communication Between Sensors and Data Fusion Unit for Automated Driving Functions - Logical Interface. Technical Report, ISO, 2021.

[44] ISO, ISO 15118-20:2022 Road Vehicles - Vehicle to Grid Communication Interface. Technical Report, ISO, 2022.

[45] ISO, ISO/AWI PAS 8800 Road Vehicles - Safety and Artificial Intelligence. Technical Report, ISO, 2023.

[46] ISO, ISO 24089 - Road Vehicles - Software Update Engineering. Technical Report, ISO, 2022.

[47] ISO, ISO/AWI TS 5083 Road Vehicles - Safety for Automated Driving Systems - Design, Verification and Validation. Technical Report, ISO, 2023.

[48] ISO, ISO - ISO/AWI TR 19560 Intelligent Transport Systems - Information Interface Framework Between Automated Driving System and User. Technical Report, ISO, 2023.https://www.iso.org/standard/85901.html

[49] ISO, ISO/TS 21177:2019. Technical Report, ISO, 2019.

[50] ISO, ISO/TR 21186. Technical Report, CEN and ISO, 2021.

[51] ISO, ISO 22741-1:2022 Intelligent Transport Systems - Roadside Modules AP-DATEX Data Interface. Technical Report, ISO, 2022.

[52] ISO, ISO/IEC 29134:2017 Information Technology - Security Techniques - Guidelines for Privacy Impact Assessment. Technical Report, ISO, 2017.

[53] ISO, ISO/IEC AWI 5888 Information Security, Cybersecurity and Privacy Protection - Security Requirements and Evaluation Activities for Connected Vehicle Devices. Technical Report, ISO, 2023.

[54] ITU-T, X.1372 Security Guidelines for Vehicle-to-Everything (V2X) Communication. Technical Report, ITU-T, 2020.

[55] ITU-T, X.1373 Secure Software Update Capability for Intelligent Transportation System Communication Devices. Technical Report, ITU-T, 2017.

[56] ITU-T, X.1374 Security Requirements for External Interfaces and Devices with Vehicle Access Capability. Technical Report, ITU-T, 2020.

[57] ITU-T, X.1375 Guidelines for an Intrusion Detection System for In-Vehicle Networks. Technical Report, ITU-T, 2020.

[58] ITU-T, Focus Group on AI for Autonomous and Assisted Driving, 2023. https://www.itu.int/en/ITU-T/focusgroups/ai4ad/Pages/default.aspx.

[59] ETSI, ETSI TR 102 893 Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA). Technical Report, ETSI, 2010.

[60] ETSI, ETSI TS 102 731 v2 Intelligent Transport Systems (ITS); Security; Security Services and Architecture; Release 2. Technical Report, ETSI, 2022.

[61] ETSI, ETSI TS 102 940 V1.3.1 - Security; ITS Communications Security Architecture and Security Management. Technical Report, ETSI, 2018.

[62] ETSI, TS 102 941 - V1.3.1 - Intelligent Transport Systems (ITS); Security; Trust and Privacy Management. Technical Report, ETSI, 2019.

[63] ETSI, TS 103 097 - V1.3.1 - Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats. Technical Report, ETSI, 2017.

[64] ETSI, ETSI TR 103 415 - V1.1.1 - Intelligent Transport Systems (ITS); Security; Pre-Standardization Study on Pseudonym Change Management. Technical Report, ETSI, 2018.

[65] ETSI, ETSI TR 103 257-1 V1.1.1 Intelligent Transport Systems (ITS); Access Layer; Part 1: Channel Models for the 5,9 GHz Frequency Band. Technical Report, ETSI, 2019.

[66] ETSI, EN 302 637-2 - V1.3.1 - Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service. Technical Report, ETSI, 2014.
[67] SAE, SAE J2735 Surface Vehicle Standard. Technical Report, SAE, 2020.
[68] SAE, Surface Vehicle Information Report. Technical Report, SAE, 2021.
[69] AUTOSAR, Autosar 402 Specification of Crypto Service Manager. Technical Report, AUTOSAR, 2009.
[70] AUTOSAR, Autosar 654 Specification of Secure Onboard Communication. Technical Report, AUTOSAR, 2017.
[71] AUTOSAR, Autosar 664 Overview of Functional Safety Measures in AUTOSAR. Technical Report, Autosar, 2015.