Towards a Comprehensive Automotive Cybersecurity Reference Architecture

Christoph Schmittner, Martin Latzenhofer,
Shaaban Abdelkader Magdy, Arndt Bonitz, Markus Hofer
Center for Digital Safety & Security
Austrian Institute of Technology
Vienna, Austria
Email: {christoph.schmittner | martin.latzenhofer |
abdelkader.shaaban | arndt.bonitz | markus.hofer}@ait.ac.at

Abstract— **While interconnectivity, complexity, and software-dependency are prerequisites for automated driving, they also increase cybersecurity risks for the whole transportation system. Information and communication technology infrastructure is becoming a second layer for critical transportation infrastructure. In the ongoing Austrian research project CySiVuS, we identified stakeholders which are involved, the services offered and consumed, as well as the risks to a cooperative intelligent transport system (C-ITS) in a structured manner. We collected and categorized different use cases and developed a specific service matrix for C-ITS. Based on an adapted security risk management process we conducted an exemplary security risk management process, using threat modelling. This serves as a fundamental preliminary step towards a comprehensive automotive cybersecurity reference architecture, which is the main objective of the CySiVuS project. Only if all components in the information and communication technology (ICT) infrastructure provide their services in a sufficient quality in accordance with the required security and safety demands, society can rely on an interconnected automotive system.**

Keywords- automotive cybersecurity; cooperative intelligent transport system; service matrix; reference architecture; risk management.

I. INTRODUCTION

In complex and multi-modal environments, smart urban mobility in form of automated driving requires new approaches, which interconnect vehicles with other road users and the road infrastructure. The paper contribution is extended from the authors' previous work [1], which refers to the Austrian national security research project “Cybersecurity for Traffic infrastructure and road operators” (CySiVuS), which aims to tackle cybersecurity and privacy as the key challenges for cooperative traffic infrastructures and automated driving of interconnected cars. The project shifts the perspective from OEMs to traffic infrastructure providers and road service operators. The existing and future road traffic system, together with the associated digital infrastructure is analyzed, and different automatic driving scenarios are collected. Various attack vectors based on different aspects of the whole automotive system require enhanced and further matured cybersecurity standards specific for the automotive domain. Based on these outcomes, the objective is to work out a comprehensive automotive cyber security reference architecture. As a step towards this goal, we identified use cases, their involved services and structured the services based on stakeholder offering and consuming services. Here, all interdisciplinary interests and objectives of stakeholders have been addressed and existing technologies and new technological innovations have been integrated. This article provides an overview of the project’s approach and highlights the urgent need for a complete reference architecture for a (cyber) secure automotive traffic infrastructure.

Main benefits of connected vehicles are a reduction of accidents by communicating road conditions, hazards, and critical situations, as well as increasing traffic efficiency through techniques like platooning or real-time traffic monitoring and control [4]. Reliable connectivity is the mandatory prerequisite for processing various states of the automated vehicle and accelerating further development. Positioning and localization, the creation of complete situational awareness, the reduction of accidents and the increase of comfort and efficiency depend on cooperative and automated driving. Current approaches towards stand-alone vehicles are sufficient for driving on highway or country roads, but these vehicles are not yet ready for urban environments. In our position paper, the idea of a comprehensive automotive cybersecurity reference architecture was postulated [1]. In this paper we included a more detailed consideration of security aspects and additional uses cases, collected from different sources. This leads to a more substantial understanding of how a cooperative intelligent transport system (C-ITS), its components and its respective stakeholders interact with each other. A preliminary step to develop the reference architecture was to establish a service matrix showing the interdependencies of services. Especially in urban environments, it is necessary to integrate automated driving vehicles into a holistic, intelligent transportation system to take advantage of all the potential benefit [2]. Therefore, this paper will specify the infrastructure and connectivity related aspects of automated driving.

Recent projects on a European level [3] identified cybersecurity as a key challenge and risk for future transportation systems. Like physical security and protection for transportation infrastructure, cybersecurity of ICT infrastructure for connected and automated vehicles cannot be left exclusively to the private sector, as their interests and objectives differ, as well as their scopes is restricted to their specific domain. Extensive mobility needs the cooperation of all stakeholders, i.e., automotive original equipment manufacturers (OEMs), infrastructure providers and road service operators, transport facilitators, end users, physical and ICT infrastructure providers, and authorities. All these actors with their different perspectives, as well as all the components together with their interrelationships are considered as one comprehensive infrastructure system. This system relies on extensive and reliable communication between these elements on different tiers. The communication should not be eavesdropped, compromised or manipulated. This makes cybersecurity a critical requirement for a connected automated transportation system, which is vital for the physical transportation infrastructure and a modern society.

This paper is divided into seven sections. After this introduction in Section II, we first give a brief overview of the state of the art of a road transport system. Here we argue that there is no sustainable structured reference architecture that supports a broad perspective on automotive cybersecurity. Risks should be identified, assessed and addressed through an extensive risk management approach. In order to establish a clear reference architecture, we suggest a tailored risk management process as discussed in Section III. Additionally, concrete use cases provide information about the implicit structure of a C-ITS. Consequently, we discuss typical use case scenarios and form use case categories with the potential affecting the security of these automotive services from the infrastructure perspective in Section IV. Based on these specific use cases, we define the structure of a proposed C-ITS service matrix in Section V. We introduce the core aspects and high-level guidelines in Section VI. The final Section VII provides conclusions and outlooks for the near future.

II. State of the Art

For automated vehicles, the Society of Automotive Engineers (SAE) J3016 [5] defines five levels, which give a framework to classify automated vehicles. Currently available mass-market systems reach up to level three. Examples of level three are highway automation and parking assistance systems. The best-known example is Tesla's autopilot and parking assistance system [6]. Higher levels, moving towards high driving automation or even complete automation, are already in a real-world test stage [7], but not yet publicly available. While systems up to level three can rely on in-vehicle sensors and generate the world model on-demand based on local sensor data, higher levels of automation need a pre-mapping to create a world model in which the vehicle is placed via sensor data [8]. This implies that such vehicles require external input to have the latest information and react on permanent or temporary modification of the road infrastructure. This is especially important in urban environments where other localization approaches, relying on Global Navigation Satellite System (GNSS) or road infrastructure (road markings or roadway detection) are more challenging [8].

In the United States, the National Highway Traffic Safety Administration (NHTSA) [9] currently prepares regulations, which require connectivity for active safety features in all new vehicles sold in the US starting from 2020. Such features commonly referred as cooperative active safety, require a high level of trust on outside information and communication. Safety reasons were the primary motivation for OEMs to establish information communication initiated by the vehicle. Security issues – which are following a different paradigm than safety-related ones – are a rather new challenge, currently addressed by the different stakeholders from different viewpoints and with different maturities. Recent hacks show that the majority of their systems lack sufficient security protection [10], [11]. Naturally, OEMs and manufacturers tend to restrict their security focus on the vehicle itself and do not follow a holistic approach, analyzing the whole infrastructure system in which their cars are only elements. Despite first approaches, like the H.R.701 – Security and Privacy in Your (SPY) Car Study Act of 2017 [12], cybersecurity issues of the vehicle are still primarily handled by the vehicle manufacturer, not considering other stakeholders and their security measures. Especially when moving towards connected, intelligent and automated transportation systems, the road traffic infrastructure needs to be looked at in its entirety. As for the legal situation briefly summarized, new regulations are being developed, but they are not timely enough and significantly fragmented. In an automated driving scenario, ICT infrastructure becomes a second layer of critical transportation infrastructure. Hence, the European "Directive on Security of Network and Information Systems", which is also known as the NIS Directive [13] and is enforced since the end of May 2018, applies to the road authorities responsible for traffic control and the operators of intelligent transport systems (ITS). The consequences for the OEMs are not yet clear, even while the car and its communication system are a key component in the superior ITS. There is also an ongoing effort to develop a regulation for considering cybersecurity and cybersecurity processes in modern vehicles through the type approval process [14]. The European directive seeks to ensure a high level of network and information security by improving the common security level of the provider of critical services and digital contents. We expect that the transport sector will become such a critical infrastructure due to the increasing interoperability, connectivity aspects, communication requirements, ICT in general, and privacy issues. Hence, there is an urgent need for full categorization and structured development.

Autonomous and automated vehicles require detailed data about the environment to generate a situational awareness in real time and to ensure their safe movement. It is further evident that automated driving scenarios are not restricted to the vehicles as a stand-alone system. Instead, the vehicles must interact in real-time with the other vehicles and with the infrastructure to assess the current situation. Thus, interoperability is the first key requisite for efficient traffic management, co-operative functions and coordinative autonomy [15]. Furthermore, this implies that the integrity of all data is a prerequisite for autonomous inter-connected driving.

Connectivity between vehicles and other traffic elements is currently still under development, even while standards such as 802.11p already exist [16]. While almost all new premium cars offer connectivity via Global System for Mobile Communication (GSM) or newer standards like long-term evolution (LTE) to a backend system of the manufacturer [17], the main motivation is to reduce costly recalls due to software adaptions and updates [18], as well as to be compliant with the European eCall initiative. Since April 2018, all new vehicles sold in Europe are obliged to be able to automatically call the nearest emergency center in the case of a crash and submit position and crash-related information [3]. Applications like intelligent coordination are already tested and evaluated in real-world scenarios [19]. In such scenarios, vehicles and infrastructure need to communicate within a defined time frame and exchange information like traffic status, travel times, road conditions and road works warnings. There are higher requirements on the connectivity for the next level of cooperation and connectivity. Although there are ITS architecture and connectivity scenarios defined by European Telecommunications Standards Institute (ETSI) [20] available, it is unclear whether vehicles will possess multiple communication systems for each service provider or if the communication will be handled via a central data hub [21]. Different approaches to the future communication infrastructure are presented and discussed in a report of the C-ITS platform [6]. One conclusion is that, in order to support interoperability, stay cost-efficient, reduce the number of attack surfaces and support future applications, the connectivity should follow some sort of coordinated model, considering not only the vehicle, but the complete infrastructure and service value chain [1].

Especially in the field of cybersecurity, multiple indicators show that the current state of the art cannot adequately protect the new and vital role ICT will play in transportation. Automotive cybersecurity is slowly rising to this aspect [22] triggered by research and governmental pressure [17], [23], [24], [25]. Technical developments and industrial awareness of new challenges are followed by the development of first guidelines for tackling the issues [26]. On a higher level, the ITS infrastructure security is also a known issue which is addressed [27]. There is still ongoing discussion who will control and provide the communication infrastructure [3]. Since all mobility and the complete road transportation sector will depend on the ICT system, it is of utmost importance to clarify responsibilities and to achieve a dependable balance between private and public control.

As an additional security property, the protection of personally identifiable information is also an important aspect. A recent survey of the German consumer organization “Stiftung Warentest” showed that almost all connectivity solutions offered by automotive OEMs have weaknesses in protecting privacy [28]. Personal information is exchanged without encryption, and the excessive amounts of information is collected and transmitted, partially without informing the user and without explicit consent. One important discussion is here not only the protection, but also consent to data collection. There are first efforts to develop processes for addressing these issues.

III. Risk Managment

There is currently no domain-specific risk management framework available for the automotive domain [1]. First approaches [26] are promising, but initial evaluations show certain challenges in the application [29]. A guidebook [26] was published at the beginning of 2012, and after being available for half a year again set to “work in progress” status. The International Organization for Standardization (ISO) and SAE founded a common working group developing a standard for the cybersecurity engineering of road vehicles [30], but the publication is currently envisioned for 2020. There is an ongoing effort of the UNECE WP29 - UN Task Force on Cyber security and OTA issues (CS/OTA) to define a minimum required cybersecurity management system (CSMS), which includes a risk-based approach [14]. Due to the focus of the UNECE on type approval, there is a missing consideration of dynamic effects. Recent work focused on dynamic risk assessments in the IoT domain [49] and showed that traditional methods are often challenged by the dynamic nature regarding change times and system boundaries, focus to much on assets and not on the overall system context and did not consider assets as potential attack vectors. In the absence of applicable domain-specific frameworks, we propose to tailor ISO 31000 [31] for the application in the automotive domain. To set up the context, define the stakeholder and the application environment, an appropriate management framework has to be established first. A second main part of the risk management standard proposes the steps depicted in Figure 1.

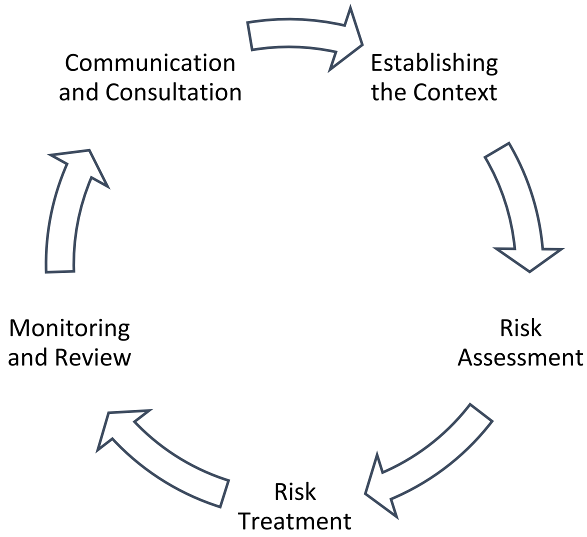

Figure 1: Risk management standard activities

We start by presenting the framework with suggestions on how it can be tailored towards the area of application. The proposed tailoring will be partially carried out on a higher level.

A. *Establishing the Context*

The previously given state of the art overview shows that currently there is no specific regulatory or legal framework for road traffic. Discussions are currently underway for a legal and regulatory framework for road transport, but no clear consensus has yet emerged. The automotive and transportation domain is an important part of ensuring and enabling our modern lifestyle, and therefore it should be avoided that a cybersecurity attack entails the consequences as described in Table I. We consider the following objectives necessary:

TABLE I. CONSEQUENCES OF CYBERSECURITY ATTACKS

Safety	Causes immediate damage to environment or human lives.
Privacy	Causes the loss of control over personal information.
Finance	Causes financial damage.
Operation	Negatively impacts the operation and traffic flow.

We propose two restrictions to these statements. First, we restrict the risk management to direct and immediate consequences. It means that we do not consider second-level consequences, e.g., an operational impact would also impact emergency services and could therefore cause damage to human lives. Our focus lies on the direct consequences. Second, we assess the impact rating on users and society higher than the impact on the organization. That means that safety impacts and financial impacts for users or society are prioritized compared with risks for individual organizations. Society needs to trust and rely on the transportation system, which is supported by ensuring their needs and protection first.

B. *Risk Assessment*

Risk assessment includes identification, analysis and evaluation of risks. While [32] presents examples of risk assessment techniques, none of them are tailored for cybersecurity in the road traffic domain. Multiple proposals exist to extend established safety risk assessment methods towards cybersecurity [33], [34] or to tailor cybersecurity methods for the automotive domain [35], [36]. It should be remarked that there is no general risk assessment implementation, each selected methodology needs to be justified. Depending on the abstraction level, different methods are favored. We propose threat modelling [37] for the analysis of risks. For risk evaluation purposes, we choose four impact levels, divided into four categories, as shown in Table II. This covers most forms of potential impact of attacks. This is an abstraction of the categories proposed by SAE J3061 [26] and EVITA [38]. Both use similar categories.

TABLE II. IMPACT LEVELS

	User / Society	**Service provider / organization**
Safety	1	-
Operational	3	4
Privacy	2	3
Financial	3	4

A critical factor for risk evaluation in cybersecurity is the consideration of likelihood. For example, the railway domain is discussing to consider the potential impact as only input for risk evaluation [39]. This can lead to unlikely risks being given higher priority. Details of the likelihood assessment we are using are presented in [29], but in short, we propose to evaluate the likelihood based on the following four parameters:

- Assumed attacker capabilities
- Ease of gaining information about the systems
- Reachability and accessibility of the system
- Required equipment for an attack

C. *Risk Treatment*

Risk treatment is based on an assessment whether the risk is tolerable for a specific stakeholder. CySiVuS focuses on the society as the most relevant stakeholder, which means that benefits of connected and automated road traffic scenarios should outweigh the risks, especially to human lives. Unless this is the case, we need to either modify the risk by implementing specific technical or organizational measures or avoid the risk altogether by deciding not to implement the scenario. Each risk treatment needs to be followed by an assessment of the effectiveness of the treatment, e.g., if the remaining risk is tolerable and can be accepted. Risk treatment assessment also includes the evaluation if the chosen measures influence other risks or scenarios.

D. *Monitoring and Review*

There are currently no clear responsibilities defined for monitoring and reviewing of risks. This is impeded by the hierarchical silo structure which currently dominates the automotive domain. OEMs only have a restricted system view and are only able to identify risks on their level. Suppliers are responsible for the implementation of risk treatment activities, in fact mitigation measures, for their specific components and identification of change requirements. There is no unambiguous allocation of risk monitoring responsibilities. Established approaches in the automotive domain mainly follow an incident based approach, i.e., reactive behaviour. For cybersecurity challenges, active monitoring and reaction are necessary. We propose to assign a reporting responsibility and develop a cyber incident response plan. In addition to that, risk treatments need to be coordinated between all stakeholders.

E. *Communication and Consultation*

As a continuous and parallel step along the risk assessment, treatment and monitoring, the complete management process needs to be recorded, documented and communicated to the stakeholders. This includes capturing the decisions, results and most importantly the justification for decisions and actions. Only this step makes risk management transparent and comprehensible. It should be remarked that such records are sensitive and could be potentially misused by attackers.

IV. USE CASES

In the CySiVuS project, we identified and collected various use cases for typical situations that a C-ITS has to cope with. The scoping of the use cases supports the identification of stakeholder, roles, components, communication types and data flows, interfaces, as well as all critical services. Thus, they form a starting point for further structuring the system and prepare a preliminary step to develop a comprehensive reference architecture. In the following we introduce the use case collection.

A. *C-ITS Day 1 Use Cases*

The first collection of use cases is based on the Cooperative Intelligent Transport System C-ITS Day 1 Use Case [40]. Day 1 refers to the first set of uses cases implemented and evaluated in the European Corridor – Austrian Testbed for Cooperative Systems (Eco-AT) project. One typical use case is the Road Works Warning (RWW) use case. This use case describes an interaction between vehicles and cooperative roadside elements, which provide information about short time modifications in the road infrastructure to optimize traffic flow and driving strategy. In Eco-AT the transmitted data will only be used as information for the vehicle driver. We will consider the next step and assume that in the future vehicles will automatically act based on the received information. In addition, we will also set up a third Vehicle to Vehicle (V2V) use case, e.g., a vehicle is broadcasting information about position and speed to enable other vehicles, which cannot obtain the information by their built-in sensors to adapt their trajectories according to the current situation.

Figure 2 depicts the introduced use cases. The Road Side Unit (RSU) sends information to all vehicles about a temporal change in the road shape. Vehicles A and B coordinate how B, which is not visible to A, enters the main road and all vehicles receive information from the traffic light system.

B. *CySiVuS Use Cases*

Examples of additional typical use cases in an ITS are listed in the following subsections. We categorized them in five different categories.

1) Normal cases: The term normal refers to the most frequently encountered applications of an ITS or an automated vehicle. The typical generic forms in a transport system by using the road infrastructure and its technical equipments are:

- *Transport of people and goods* from place A to place B. Some concrete use cases for transport of people are trips from home to work, to places for leisure activities, to fulfill daily needs, of service providers and time-critical blue-light emergency drives. Examples for transport of goods are home deliveries of daily goods, special transport of chemicals, heavy- or money-transports and time-critical transports like blood and organs. Another type of normal transport use cases are maintenance drives for snow removal, road cleaning or driving school trips.

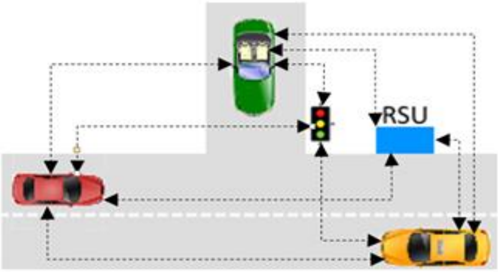

Figure 2: Use cases

- *Departing predefined routes* (e.g., sightseeing) in a specific order or driving as a leisure activity for fun.

2) Emergency cases: Emergency cases are cases in which the ITS needs to react on some unforseen event in order to esnure safety of human life and avaialability of the transportation service.

- The *function of vehicle components is suddenly no longer available* (e.g., steering, brake, EMP). It requires reporting to other vehicles, roadside units, original equipment manufacturer (OEM) backend, etc. It is necessary to transfer the vehicle to a safe location or condition and to call for support, e.g., the ambulance or service personnel.
- *The driver is not able to interact* (e.g., impaired, unconscious, or dead);
- *Occurrence of an unexpected event* (e.g., mudslide, avalanche) requires a report to the RSU. It is necessary to transfer the vehicle to a safe location or condition and to call for support, e.g., the ambulance or service personnel.
- *Unauthorized active or passive intervention of third parties* (e.g., hacking, targeted scattering of misleading information) leads to a broadcast information to other vehicles, the RSUs, OEM backend disabling all the network functionalities of the concerned vehicle.
- *Authorized active or passive interference of third parties* (e.g., targeted manipulation of the control unit from outside) requires verifying the authorization, broadcasting information to other vehicles, the RSUs, OEM backend when appropriate, applying the action needed, transmitting the location data and to transfer the vehicle to a safe location or condition.
- *Automatic acquisition of civil vehicles for emergency transports* requires to transfer the vehicle to a safe

location or condition, to verify the authorization and the execution of the action.

3) Comfort cases: There are different perspectives of comfort features. These features are not really necessary for the fundamental task to transport persons or goods from A to B, but they make the process more convenient. This could be beneficial for the driver or passengers, for the OEM or manufacturer, the road or infrastructure operator or for other stakeholders. Some examples are driver assistance systems, intelligent route planning, entertainment routes, multimodal transport services, additional bookable driving performance or features, etc.

4) Road safety and other special cases: These cases concern the road operator and aim to ensure the usability of road sections. Here cases like the distribution of information about dangerous zones or special situations, e.g., due to weather conditions, road works, atypical lane guidance, unusual behavior of other road users, outage of infrastructure elements, maintenance works, and traffic controls are collected.

5) Traffic management cases: There are some situations for the road operator to interfere in the traffic flow to enforce speed limits, release service lanes as additional lanes, service announcements with alternative routes, telematic systems for road work areas.

V. Service Matrix

Based on the proposed risk management process described in Section III and the collection of use cases discussed in the previous Section IV, we set up a service matrix, where we clarify the inherent dependencies between the services provided by different stakeholders. Firstly, we introduce the different stakeholders, assign the specific components to their responsibility to finally document which stakeholder provides essential services within a C-ITS for the other stakeholders.

A. C-ITS Stakeholder

The various stakeholders, shown in Figure 3, were deducted from the use cases discussed in Section IV. Each stakeholder has their own view on the C-ITS, with different requirements, usage patterns or interests.

- Vehicle users are direct users of the transportation system, and usually those who are transported in the vehicle itself.
- Vehicle manufacturers (i.e., OEMs) and maintenance providers.
- Infrastructure and road operators are typically responsible for the construction and maintenance of roads, road networks, bridges and tunnels and other infrastructure elements.
- Authorities, for example, police, the ministry of transport or delegated organizations, are responsible for ensuring the proper functioning of the transport system.
- Third-party service providers summarize all entities that provide services, for example, fuel stations, mobility clubs, insurance companies or telecommunication providers.
- Society comprises all persons living, working and residing in a given area.

B. C-ITS Infrastructure Components

This section identifies the components and their structural connections. The following formulates the road transport system, seen in Figure 4 below.

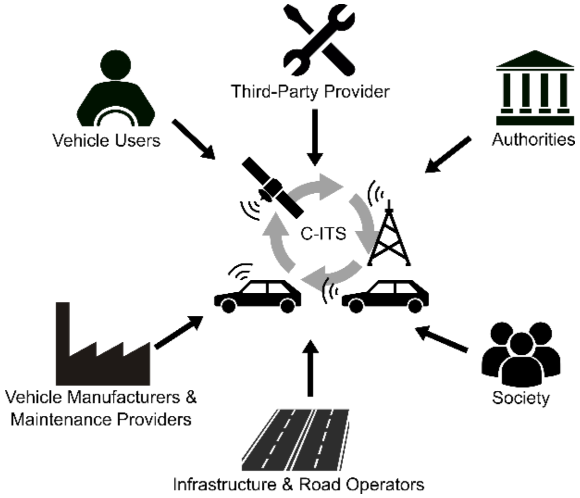

Figure 3: Stakeholder of a C-ITS

1) Communication in the Vehicle. There are various communication requirements in the vehicle between Electronic Control Units (ECU), sensors, and actuators. Different communication busses help to structure the data flow.

- Classically, the Controller Area Network bus (CAN) is used for communication between control units [46]. The CAN protocol was defined in 1986. In 1991 the first vehicle with CAN was available on the market [47]. The CAN bus was developed as a standard vehicle protocol that minimizes cabling effort and enables prioritization of communication. The big amounts of data such as generated by sensors or camera systems can be a big challenge for a CAN network.
- A Local Interconnect Network (LIN) [48] was developed to a network which an increasing number of sensors in the vehicle with the control units. Most of the sensors have requirements with fewer capabilities than the CAN network. Therefore, the CAN network can be useful for simple networks.

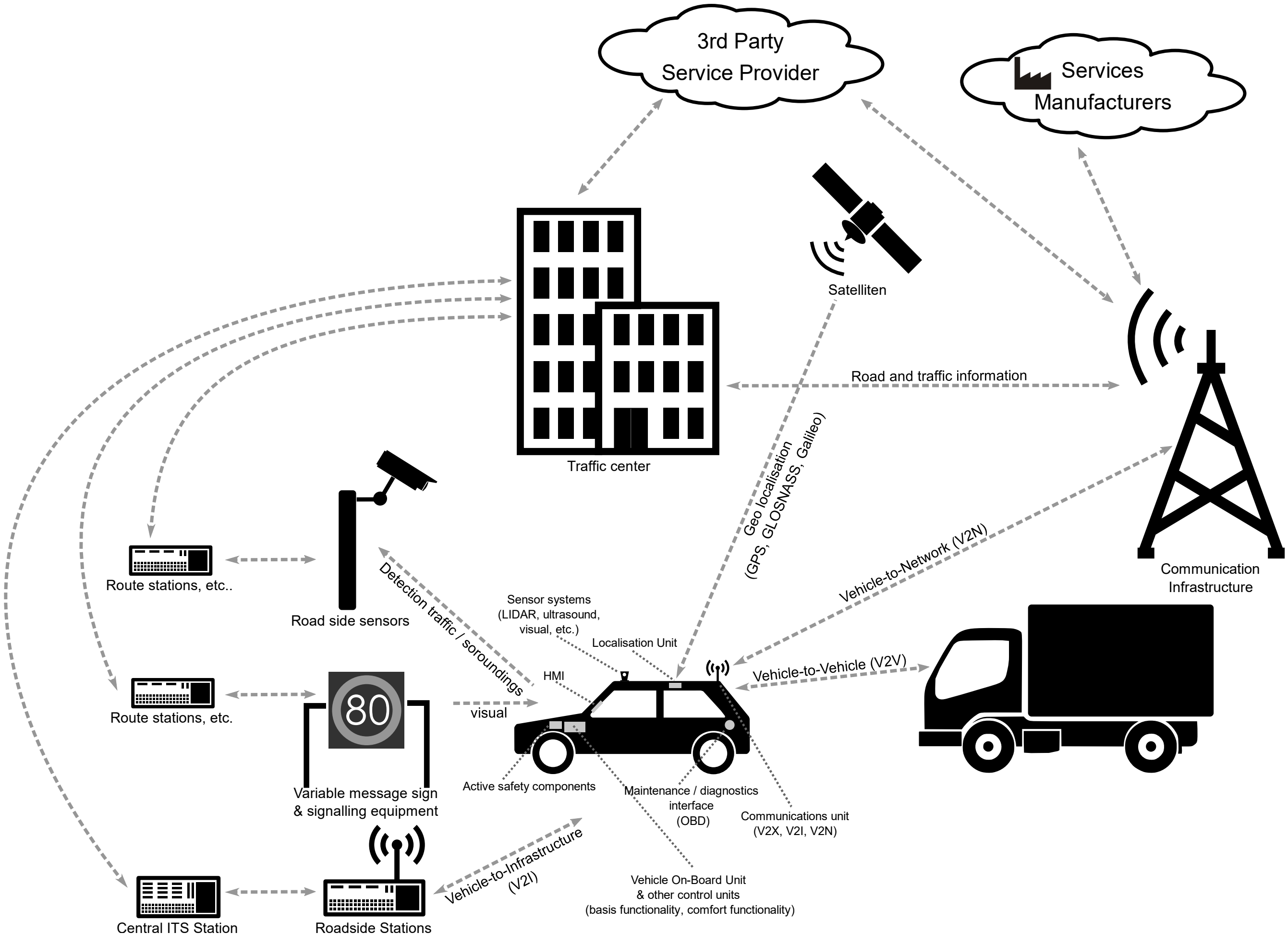

Figure 4: C-ITS Overview

- The Media Oriented Systems Transport (MOST) bus was developed to enable the communication of media content in the vehicle. It can be used, to transmit video content to monitors in the vehicle.

2) Vehicle Interfaces: There are different types of interfaces, which allow the transfer of data to and from the vehicle:

- On-board diagnostics (OBD) and increasingly USB interfaces require a physical connection. ODB is designed for Machine-to-Machine (M2M) communication between the diagnostic system and the vehicle system, while USB is a way for the user to exchange data with the vehicle.
- WLAN, Bluetooth, and WLAN-based V2X protocols provide medium-range wireless communication. Normally, no additional infrastructure is required, and the devices communicate directly with each other. The interfaces are intended for communication between systems.
- The last group consists of interfaces for long-distance communication, such as radio receivers or mobile (cellular) radio transceivers. The radio receiver is the only unidirectional interface.

3) Road Infrastructure Interfaces: The road infrastructure has the following general communication interfaces in order to provide data exchange with RSUs.

- Interfaces to internal sensors and actuators, e.g., to traffic detectors or traffic control technology such as variable-message signs
- Interfaces to vehicles moving on the road infrastructure such as radio interfaces from roadside units to vehicles
- Interfaces to third-party providers, e.g., DATEX II Web Service

4) Backend infrastructure and services. This category compromises all non-road specific background services, i.e., the backend systems of the car manufacturer or navigation service providers. Depending on the service, the vehicle ECU might either be directly connected via a cellular radio modem to a background service (for example for accessing manufacturer updates) or use a modem integrated to a dedicated device, i.e., a navigation unit.

C. C-ITS Service Matrix

The types of services that can be implemented for automated driving applications are diverse. To gain a better overview and understanding, the identified services of the entire road traffic system should be visualized so that not only the actual basic components, but also their inherent connections can be easily grasped. The service matrix introduced in this section is one possibility which helps to get a good overview of the complexity by showing which services are offered by which stakeholders and which stakeholders in turn used them. This means, the possible services should be considered from different stakeholder perspectives, i.e., vehicle (user), infrastructure and road operators, vehicle manufacturers (OEM) and maintenance providers, third party service providers, authorities, and the society as a whole.

The following service matrix in Figure 5 shows the evaluation being carried out by the project team as a type of expert evaluation. It shows how the importance of services provided by a certain entity for the user of the service, i.e., the extent to which the service user is impaired by the discontinuation of the service in the safe execution of his tasks and his responsibilities.

The first step of generating this matrix was to find and define exemplary services for each combination of two of the stakeholders. For example, services being provided by infrastructure and road operators to vehicle users are numerous, including but not limited to traffic flow information, construction site warnings, traffic status information, and route information. Less strong, for example, is the connection between infrastructure and road operators and third-party service providers, the only relevant services here are traffic radio, and in some cases information for the modification of infrastructure.

The final service matrix was derived from this intermediate matrix with all services found and then rated for criticality by the experts in the project consortium. The scale used for rating goes from 0 (irrelevant), over 1 (little impact) and 2 (impairment) up to 3 (critical). As an example, the services provided by an infrastructure and road operator is crucial to a vehicle user, but not to OEMs or maintenance providers. A general observation revealed by the service matrix is that most of the stakeholder rely on services provided by others. This means that a C-ITS is a highly interdependent overall system and requires a well-structured reference architecture to be understandable by key players forming a C-ITS like authorities, decision makers as well as the industry.

Service Customer ➔ Service Providers 🡣	Vehicle user	Infrastructure and Road Ops	OEM, Maintenance Provider	Third Party Service Provider	Society	Authorities
Vehicle user	2	2	2	1	0	2
Infrastructure and Road Ops	3	1	0	1	1	2
OEM, Maintenance Provider	3	1	0	2	0	2
Third Party Service Provider	0	1	1	2	1	1
Society	2	1	2	1	2	1
Authorities	3	2	2	1	2	2

Figure 5. Service provider/service user matrix

D. Security analysis example

We identify security threats based on the data flow between vehicle A, B, and roadside units in Figure 2. We use the threat analysis tool [36] developed by Austrian Institute of Technology. The threat tool uses several source materials to ensure a range of threats is considered. The following source documents were used to develop the threats database:

- Threat Modeling for Automotive Security Analysis [36]
- Connected cars Threats, vulnerabilities and their impact [41]
- The ENISA Threat Landscape 2015, Top Threats [42].

Figure 6 depicts the data flow between vehicle A, B, and RSUs. Based on the given input to the tool, and without any security mitigation measures, 55 threats were identified.

The threat tool classifies the detected potential threats into six main classes according to the STRIDE model [43], i.e., Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service (DoS), and Elevation of privilege. Table III summarizes the numbers of the detected threats regarding the STRIDE model.

TABLE III. DETECTED THREATS ACCORDING TO STRIDE CLASSIFICATION

Type	Numbers
Denial of Service	7
Elevation of Privilege	7
Information Disclosure	15
Repudiation	5
Spoofing	14
Tampering	7

The tool performs a risk assessment process to classify the risk of the identified threats as an extreme, high, medium, or low risks. Figure 7 shows statistical percentages of risks in the

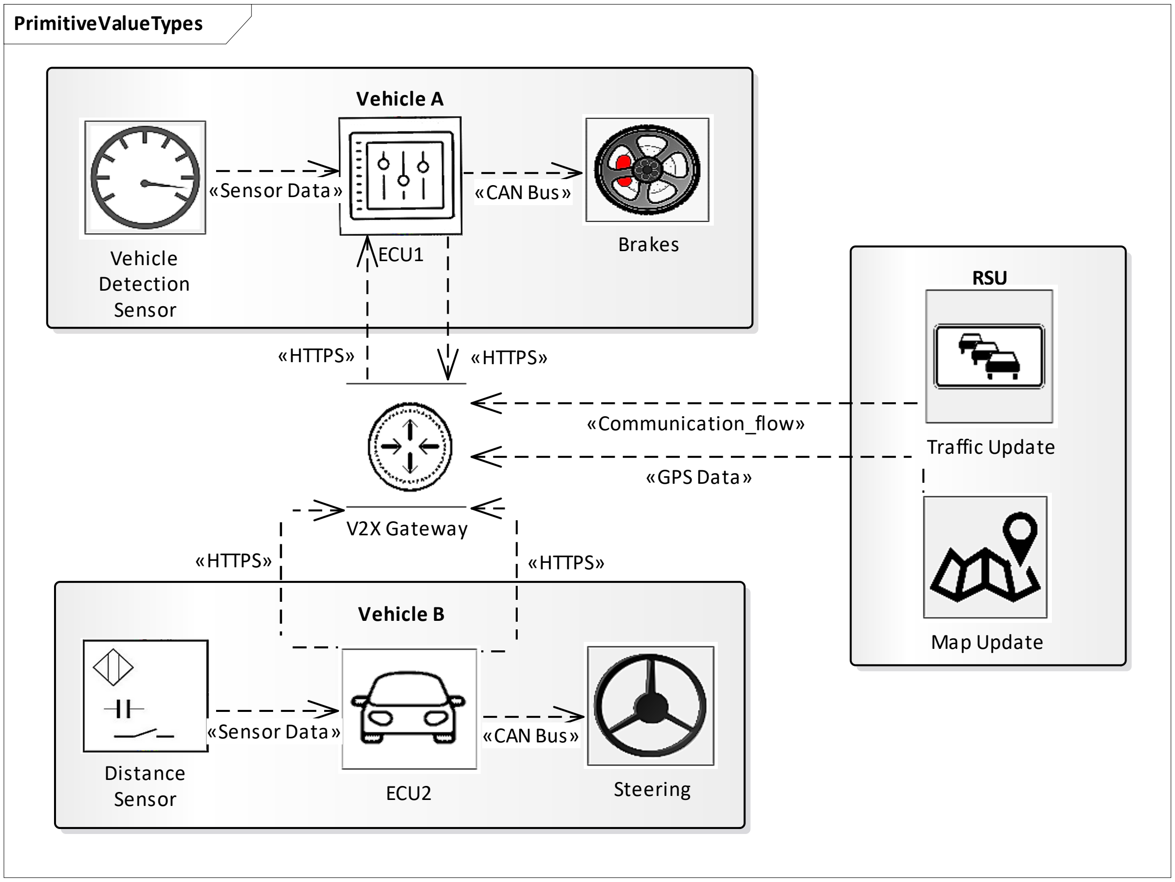

Figure 6: Data flow model for threat assessment

identified threats. From the observed risk statistic, we see that the highest number of risks are medium risks.

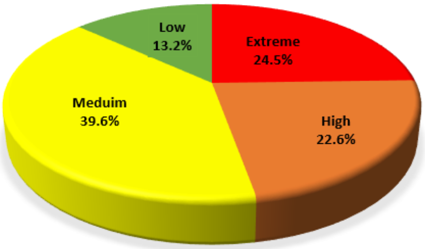

Figure 7: Statistical percentage of risks

We focus in the following on the interaction type and the corresponding threat, seen in Table IV.

TABLE IV. DELIVER MALICIOUS UPDATES TO VEHICLE B [PRIORITY: HIGH]

Category	**Spoofing**
Description	Deliver Malicious Updates to Vehicle B
Justification	<no mitigation provided>
Attack method	Spoofing vehicle A in order to send malicious updates.

For connected automotive vehicles and their corresponding brakes control and steering algorithms, the correct and especially secure reception of safety and kinematic related messages is of utmost importance. A manipulated sending unit from some distance away could communicate status information, e.g., nonexistent barriers, road works or vehicle positions ahead leading to slow down or even stop of the traffic culminating to accidents. To prevent such a threat, we propose distance-bounding protocols that allow a safe decision if the communication partner is within a certain radius, defined as bubble [44], [45].

The adapted Table V summarizes the considerations detailed above.

TABLE V. DELIVER MALICIOUS UPDATES TO VEHICLE B [PRIORITY: LOW]

Category	**Spoofing**
Description	Deliver Malicious Updates to vehicle B
Justification	~~<no mitigation provided>~~ *Distance bounding avoids remote attacks and requires physical access to the environment in order to conduct the attack*
Attack method	Spoofing vehicle A in order to send malicious updates.

This capability requires the introduction of a bidirectional communication link between Verifier (V) and Proofer (P) and a fast processing of the challenge sent from V to P. This reduces the evaluated attack likelihood by enforcing physical access to conduct such attacks and reduces the risk to a tolerable level.

VI. Reference Architecture

An automotive reference architecture for security analysis was presented in [11]. While it includes the elements of communication between backend and vehicle, it does not consider all relevant scenarios for C-ITS like V2V communication. Furthermore, it only defines the technical elements and does not differentiate between environments, stakeholder, objects in the architecture a division. However, this pure technical approach is not sufficient and to apply the reference architecture in practice, this separation is vital.

As a first approach, we divide the ITS into five clusters of elements as shown in Figure 8. On the physical side (blue, left side), we have vehicles, infrastructure and personal devices. The provider's side (green, right side) contains elements which are maintained and operated by infrastructure operators and road service providers offering mobility services (grey, lower side) available to the users (yellow, upper side). All elements are interconnected by a communication system (orange, in the middle). It should be highlighted that these blocks can overlap, e.g., infrastructure providers can also provide services; and blocks can contain multiple diverse sub-blocks, e.g., communication collects a multitude of techniques like wireless networking (WLAN) or GSM, which can be applied for V2V or Vehicle to Infrastructure (V2I) communication.

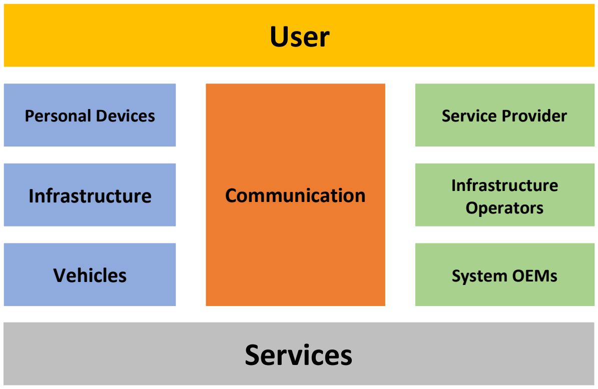

Figure 9: Clustering of elements in the transportation system

Moreover, the approach described above offers a relatively high-level view on the system, which is, to a certain degree, architecture independent. As it is discussed in [6] and [21], it is still in discussion how the connectivity architecture will finally look like, but all discussed architectural variants fit in the presented structural model. Such a structural model helps to identify the involved parties, allows assigning risk mitigations to technical elements and assigns the responsibility of implementing and maintaining these risk mitigations to involved parties. To be practically applicable, the identified risk mitigation measure is implemented in infrastructure and vehicle, conducted by system OEM and infrastructure providers, which is shown in Figure 9.

A possible solution approach is a structured multi-tiered reference architecture. However, a consistent risk management methodology is a critical success factor for developing a unified architecture across all perspectives. Our approach is to take the widely accepted risk management standard ISO 31000 [31] as a basis and tailor it to the automotive requirements.

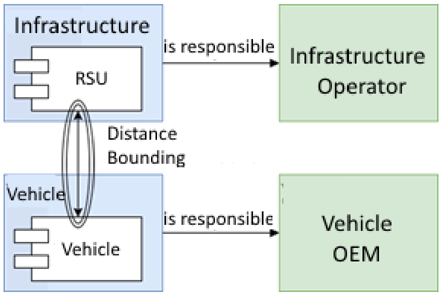

Figure 8: Application of the structural model

We discuss the five main steps of the risk management process when we apply it to a road traffic system. It is crucial to restrict the proposed approach to direct risks only and to weight the impacts differently depending on the consequences. The risk management analysis steps are

essential to finding an appropriate mixture of applicable methods to form a reliable methodology for the assessment. Additionally, the evaluation of the likelihood and the handling of uncertainty needs to be solved. Risk treatment in a complex and interconnected environment must consider different actors.

VII. Conclusion and Outlook

In this paper we analyze the technological and legal state of the art of automated driving for smart urban mobility. We conclude that the current state of the art is not yet sufficient with the complex requirements of such an environment. We identified four current challenges to a comprehensive traffic road system: The interoperability of the components among the vehicles as well as the infrastructure elements, connectivity and communication tasks especially for interacting and cooperation of the different components, ICT in general and cybersecurity issues to address security threats, and privacy finally aspects which subsume protection requirements of personal data of the vehicle drivers. There are efforts to form a compliant legal and technological framework, but all these considerations are not yet completed. By considering a tailored risk management process and collecting and categorizing different use cases, we initially identified stakeholders and components. Based on this, we developed a C-ITS service matrix to visualize the service usage between the five stakeholder groups and to reveal their interdependencies among each other. This is a potential starting point for future cyber security investigations.

Considering the challenges for cybersecurity risk management in dynamic environments like Internet of Things we already consider some of the challenges [49], [50]. By following a model-based approach we are able to automatically re-asses the system and our risk evaluation already considers assets as potential attack vectors. The model-based approach is challenged by systems with unclear boundaries or composition, e.g., new risks due to a change in system composition are difficult to measure.

The primary task of the CySiVuS research project is to develop a wide-ranging model on all necessary perspective levels, which the rough approach introduced in this article could be a starting point. By conducting the risk management process and developing the reference architecture, we show the multidimensional nature of a road traffic system. The main upcoming challenges are a concrete in-depth-analysis of risk assessment by applying adapted risk management methods. The next step is to develop a comprehensive automotive reference architecture based on the considerations introduced in the previous section. The main objective is to determine an appropriate layered visualization taking the different stakeholders, components, services into account.

Acknowledgment

The research project "Cybersicherheit für Verkehrsinfrastruktur- und Straßenbetreiber" (CySiVuS, in English: „Cyber security for transport infrastructure and road operators") (Project-Nr. 865081) is supported and partially funded by the Austrian National Security Research Program KIRAS (Federal Ministry for Transport, Innovation and Technology (BMVIT) and Austrian Research Promotion Agency (FFG) 2017).

References

[1] C. Schmittner, M. Latzenhofer, S. Abdelkader, and M. Hofer, "A Proposal for a Comprehensive Automotive Cybersecurity Reference Architecture," in *VEHICULAR 2018, The Seventh International Conference on Advances in Vehicular Systems, Technologies and Applications*, Venice, 2018, pp. 30–36

[2] Q. Xu, K. Hedrick, R. Sengupta, and J. VanderWerf, "Effects of vehicle-vehicle/roadside-vehicle communication on adaptive cruise controlled highway systems," in *Proceedings IEEE 56th Vehicular Technology Conference*, Vancouver, BC, Canada, 2002, vol. 2, pp. 1249–1253

[3] C-ITS Platform, "Working Group 6 Access to in-vehicle resources and data," Dec. 2015.

[4] European Telecommunications Standards Institute (ETSI), "ETSI TR 102 638 V1.1.1; Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions." Jun-2009 [Online]. Available: https://www.etsi.org/deliver/etsi_tr/102600_102699/102638/01.01.01_60/tr_102638v010101p.pdf [Accessed: 28-05-2019]

[5] SAE, "J3016 Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles," *2016*.

[6] M. Dikmen and C. M. Burns, "Autonomous Driving in the Real World: Experiences with Tesla Autopilot and Summon," in Proceedings of the 8th International Conference on Automotive User Interfaces and Interactive Vehicular Applications, 2016, pp. 225–228

[7] M. Aeberhard *et al.*, "Experience, Results and Lessons Learned from Automated Driving on Germany's Highways," *IEEE Intelligent Transportation Systems Magazine*, vol. 7, no. 1, pp. 42–57, 2015.

[8] G. Bresson, Z. Alsayed, L. Yu, and S. Glaser, "Simultaneous Localization and Mapping: A Survey of Current Trends in Autonomous Driving," *IEEE Transactions on Intelligent Vehicles*, vol. 2, no. 3, pp. 194–220, Sep. 2017.

[9] NHTSA, "NHTSA | National Highway Traffic Safety Administration." [Online]. Available: https://www.nhtsa.gov/ [28-05-2019]

[10] A. Greenberg, "The Jeep Hackers Are Back to Prove Car Hacking Can Get Much Worse.", Wired, 08.01.16 [Online]. Available: https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/ [Accessed: 28-05-2019]

[11] J. Brückmann, T. Madl, and H. J. Hof, "An Analysis of Automotive Security Based on a Reference Model for Automotive Cyber Systems," *SECURWARE 2017 : The Eleventh International Conference on Emerging Security Information, Systems and Technologies* [Online]. Available: https://www.researchgate.net/publication/319932479_An_Analysis_of_Automotive_Security_Based_on_a_Reference_Model_for_Automotive_Cyber_Systems [Accessed: 28-05-2019]

[12] Library Congress, "H.R.701 - 115th Congress (2017-2018): SPY Car Study Act of 2017." [Online]. Available: https://www.congress.gov/bill/115th-congress/house-bill/701/text [Accessed: 28-05-2019]

[13] European Union, *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*, vol. L194. 2016 [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:194:FULL&from=EN [Accessed: 28-05-2019]

[14] Secretary of the UN Task Force on Cyber Security and Over-the-Air issues, "Draft Recommendation on Cyber Security of the Task Force on CyberSecurity and Over-the-air issues of UNECE WP.29 GRVA (Informal Document)." 20-Sep-2018 [Online]. Available: https://www.unece.org/fileadmin/DAM/trans/doc/2018/wp29grva/GRVA-01-17.pdf [Accessed: 28-05-2019]

[15] NHTSA, "Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application," National Highway Traffic Safety Administration, US Department of Transportation.

[16] European Telecommunications Standards Institute (ETSI), "ETSI ES 202 663 V1.1.0; Intelligent Transport Systems (ITS); European profile standard for the physical and medium access control layer of Intelligent Transport Systems operatingin the 5 GHz frequency band." Nov-2009 [Online]. Available: https://www.etsi.org/deliver/etsi_es/202600_202699/202663/01.01.00_50/es_202663v010100m.pdf [Accessed: 28-05-2019]

[17] C. Valasek and C. Miller, "A Survey of Remote Automotive Attack Surfaces," IOActive [Online]. Available: https://ioactive.com/wp-content/uploads/2018/05/IOActive_Remote_Attack_Surfaces.pdf [Accessed: 28-05-2019]

[18] H. A. Odat and S. Ganesan, "Firmware over the air for automotive, Fotamotive," in *IEEE International Conference on Electro/Information Technology*, 2014, pp. 130–139.

[19] EcoAT, “Der österreichische Beitrag zum Kooperativen ITS Korridor“ [Online]. Available: http://eco-at.info/ [Accessed: 28-05-2019]

[20] ETSI, “Automotive Intelligent Transport Systems,” *European Telecommunications Standards Institute*. [Online]. Available: https://www.etsi.org/technologies-clusters/technologies/automotive-intelligent-transport [Accessed: 28-05-2019]

[21] B. Datler, “A Road Operator’s View on Cloud-based ITS – Requirements and Cooperation Models,” *23rd ITS World Congress*, 2016

[22] E. Khayari, “SECURE AUTOMOTIVE ON-BOARD ELECTRONICS NETWORK ARCHITECTURE,” p. 9.

[23] D. Spaar, “Car, open yourself! Vulnerabilities in BMW’s ConnectedDrive,” pp. 86–90, 2015.

[24] J. Petit and S. E. Shladover, “Potential Cyberattacks on Automated Vehicles,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 546–556, Apr. 2015.

[25] D. C. Miller and C. Valasek, “Remote Exploitation of an Unaltered Passenger Vehicle,” p. 91.

[26] *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems*. SAE, 2016

[27] ECo-AT, “ECo-AT SWP3.4 Security,” ECo-AT, 2016 [Online]. Available: http://www.eco-at.info/system-spezifikationen.html [Accessed: 28-05-2019]

[28] “Connected Cars: Die Apps der Auto-hersteller sind Daten-schnüffler.” 26-Sep-2017 [Online]. Available: https://www.test.de/ Connected-Cars-Die-Apps-der-Autohersteller-sind-Datenschnueffler-5231839-5231843/ [Accessed: 28-05-2019]

[29] C. Schmittner, Z. Ma, C. Reyes, O. Dillinger, and P. Puschner, “Using SAE J3061 for Automotive Security Requirement Engineering,” in *Computer Safety, Reliability, and Security*, 2016, pp. 157–170.

[30] International Organization for Standardization, Ed., *ISO/SAE CD 21434 Road Vehicles - Cybersecurity engineering*. ISO, Geneva, Switzerland [Online]. Available: https://www.iso.org/standard/70918.html [Accessed: 28-05-2019]

[31] “ISO 31000:2009 Risk management -- Principles and guidelines,” ISO, Feb. 2018 [Online]. Available: https://www.iso.org/standard/65694.html [Accessed: 28-05-2019]

[32] International Organization for Standardization, Ed., *ISO 31010:2009 Risk management - Risk assessment techniques*. ISO, Geneva, Switzerland, 2009.

[33] G. Macher, H. Sporer, R. Berlach, E. Armengaud, and C. Kreiner, “SAHARA: A security-aware hazard and risk analysis method,” in *2015 Design, Automation Test in Europe Conference Exhibition (DATE)*, 2015, pp. 621–624.

[34] C. Schmittner, T. Gruber, P. Puschner, and E. Schoitsch, “Security Application of Failure Mode and Effect Analysis (FMEA),” in *Computer Safety, Reliability, and Security*, 2014, pp. 310–325.

[35] “A case study of FMVEA and CHASSIS as safety and security co-analysis method for automotive cyber-physical systems,” *ResearchGate*. [Online]. Available: https://www.researchgate.net/publication/282792587_A_case_study_of_FMVEA_and_CHASSIS_as_safety_and_security_co-analysis_method_for_automotive_cyber-physical_systems [Accessed: 28-05-2019]

[36] M. Zhendong, and C. Schmittner. "Threat modeling for automotive security analysis." Advanced Science and Technology Letters 139 (2016): 333-339.

[37] F. Swiderski and W. Snyder, *Threat Modeling (Microsoft Professional)*. 2004.

[38] “E-safety vehicle intrusion protected applications,” EVITA, 2008 [Online]. Available: https://www.evita-project.org/Publications/EVITAD0.pdf [Accessed: 28-05-2019]

[39] J. Braband, “Towards an IT Security Framework for Railway Automation,” presented at the Embedded Real Time Software and Systems,” *Toulouse*, Feb. 2014.

[40] “C-ITS Strategy Austria [C-ITS Strategy Austria],” Network Drivers, Promote Efficiency and Safety in Transport., Jun. 2016 [Online]. Available: https://www.bmvit.gv.at/en/service/publications/transport/downloads/citsstategy.pdf [Accessed: 28-05-2019]

[41] S. Strobl, D. Hofbauer, C. Schmittner, S. Maksuti, M. Tauber, and J. Delsing, “Connected cars — Threats, vulnerabilities and their impact,” in *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*, 2018, pp. 375–380.

[42] “ENISA Threat Landscape 2015 — ENISA.” [Online]. Available: https://www.enisa.europa.eu/publications/etl2015 [Accessed: 28-05-2019]

[43] “Uncover Security Design Flaws using The STRIDE Approach,” *MSDN Magazine*, Nov. 2006 [Online]. Available: https://adam.shostack.org/uncover.html [Accessed: 28-05-2019]

[44] K. B. Rasmussen, S. Capkun “Realization of RF Distance Bounding”. InUSENIX Security Symposium 11-08-2010 (pp. 389-402).

[45] G. P. Hancke and M. G. Kuhn, “Attacks on Time-of-flight Distance Bounding Channels,” in *Proceedings of the First ACM Conference on Wireless Network Security*, New York, NY, USA, 2008, pp. 194–202 [Online]. Available: http://doi.acm.org/10.1145/1352533.1352566 [Accessed: 28-05-2019]

[46] “History of CAN technology.” [Online]. Available: https://www.can-cia.org/can-knowledge/can/can-history/ [Accessed: 28-05-2019]

[47] “Mercedes W140: First car with CAN.” [Online]. Available: https://can-newsletter.org/engineering/applications/160322_25th-anniversary-mercedes-w140-first-car-with-can [Accessed: 28-05-2019]

[48] International Organization for Standardization, Ed., *ISO 17987-1:2016 Road vehicles; Local Interconnect Network (LIN); Part 1: General information and use case definition*. ISO, Geneva, Switzerland, 2016.

[49] J. R. C. Nurse, S. Creese, and D. De Roure, “Security Risk Assessment in Internet of Things Systems,” IT Prof., vol. 19, no. 5, pp. 20–26, 2017.

[50] J. R. C. Nurse, P. Radanliev, S. Creese, and D. De Roure, “If you can’t understand it, you can’t properly assess it! The reality of assessing security risks in Internet of Things systems,” Living in the Internet of Things: Cybersecurity of the IoT - 2018,