A Proposal for a Comprehensive Automotive Cybersecurity Reference Architecture

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

***Abstract*— Interconnection, complexity and software-dependency are prerequisites for automated driving and increase cybersecurity risks for the whole transportation system. Hence, information and communication technology infrastructure becomes a second layer for critical transportation infrastructure. In a recently started research project, we identify involved stakeholders and risks in a structured manner to integrate the diverging interests and objectives of authorities, road infrastructure providers and transport facilitators, which cannot even exclusively leave to the original equipment manufacturers. Based on the emerging risk scenarios, we develop a comprehensive architectural reference framework. Only if all components in the Information and Communication Technology (ICT) infrastructure provide their services in a sufficient quality according to ensured security requirements, society can rely on the reliable automotive system.**

Keywords- automotive cybersecurity; road traffic infrastructure; reference architecture; risk management; ICT

I. INTRODUCTION

Automated driving in complex and multi-modal environments for smart urban mobility requires approaches, which interconnect vehicles with other road users and infrastructure. Main benefits of connected vehicles are a reduction of accidents due to the communication of road hazards and critical situations, as well as an increase of traffic efficiency through platooning and real-time traffic monitoring and control. Reliable connectivity is the mandatory prerequisite for processing various states of the automated vehicle and accelerating further development. Positioning, a creation of complete situational awareness, reduction of accidents and increasing 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 not ready for urban environments. In addition, 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 benefits [1]. Therefore, this paper will focus on the infrastructure and connectivity related aspects of automated driving.

Recent projects on an European level [2] 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 restricted scopes. Extensive mobility needs the cooperation of all stakeholders, i.e., automotive Original Equipment Manufacturers (OEM), infrastructure providers and road service operators, transport facilitators, end user, physical and ICT infrastructure providers, and authorities. All these actors with their different perspectives, all the components together with their relationships are considered to of a comprehensive infrastructure system requiring intense and reliable communication among these elements on different tiers not to be eavesdropped, compromised or manipulated. This makes cybersecurity a mandatory success factor for a securely and safely connected automated transportation system, which is vital for the physical transportation infrastructure and a modern society. Society can therefore rely on safe, trustworthy automotive system.

Our contribution 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 moves the perspective from the OEMs to traffic infrastructure providers and road service operators. The existing and future road traffic system, together with the concerning digital infrastructure is analyzed, and different autonomous driving scenarios are collected. Significant aspects require enhanced and further matured cybersecurity standards. Based on these conditions, the objective is to work out a comprehensive automotive cyber security reference architecture. It addresses all interdisciplinary interests and objectives of stakeholders and integrates existing and other technological innovations, that will be developed in the near future. This article provides a brief overview of the project’s approach and highlights the urgent need for a complete reference architecture for a (cyber) secure automotive traffic infrastructure.

This paper is divided into six sections. After this introduction, we will first give a short overview of the state of the art. Section II argues that there is no sustainable structured reference architecture that supports a broad perspective on automotive cybersecurity. This is underlined by some general scenarios from a practical point of view, which we obtained from a tailored risk management process discussed in Section III. Risks should be identified, assessed and addressed through an extensive risk management approach. Based on practical

 ISBN: 978-1-61208-643-9

use cases, we motivate the proposal of a future transportation system in Section IV. We discuss typical use case scenarios affecting the security of these automotive services from the infrastructure perspective. It is the objective of a recently started research project to develop this comprehensive automotive cybersecurity reference architecture in much more detail, the core aspects of which we introduce in Section V. The final Section VI provides conclusions and outlooks for the near future.

II. STATE OF THE ART

For automated vehicles, the Society of Automotive Engineers (SAE) J3061 [3] defines five levels, which give a framework to classify automated vehicles. Currently, mass-market available 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 [4]. Even higher levels, moving towards high driving automation or even complete automation, are already in a real-world test stage [5], 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 the previous mapping to generate a world model in which the vehicle is placed via sensor data [6]. This implies that such vehicles require external input to have the latest information and react on permanent or temporary modification in the road system. This is especially important in urban environments where other localisation approaches, relying on Global Navigation Satellite System (GNSS) or road infrastructure (road markings or roadway detection) are more challenging [6].

In the United States, the National Highway Traffic Safety Administration (NHTSA) [7] currently prepares regulations, which require connectivity for active safety features for 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 urgent motivation for the 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 only by the OEMs itself. Recent hacks show that the majority of their systems lack security protection [8], [9]. Naturally, they restrict their security focus on the vehicle itself and do not follow a holistic approach, analyzing the whole infrastructure system their cars are elements. Despite first approaches, like the H.R.701 – Security and Privacy in Your (SPY) Car Study Act of 2017 [10], cybersecurity issues are still largely handled by the vehicle manufacturer simply ignoring other stakeholders. Especially when moving towards connected, intelligent and automated transportation systems, the road traffic infrastructure need to be considered in a consequently holistic way. However, briefly summarizing the legal situation in general, new regulations are evolving, but too slow promptly and substantially fragmental. In an automated driving scenario, ICT infrastructure becomes a second layer of critical transportation infrastructure. Hence, it is still in the discussion whether and how the European "Directive on Security of Network and Information Systems" also known as the NIS Directive [11] applies to the automotive sector and what the consequences for the OEMs, as well as the road infrastructure providers are in detail. This European Directive will be enforced by the end of May 2018 and 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. The transport sector is accepted to form such a critical infrastructure and due to the increasing interoperability, connectivity aspects, communication requirements, ICT in general, and privacy issues. Hence, there is an urgent need for a full categorization and orderly development.

The vehicles require detailed data about the environment to generate a broad overview of the current situation in real time and ensure their safe movement. The integrity of the data is a prerequisite for autonomous inter-connected driving. It is evident that automated driving scenarios are not restricted to the vehicles as a stand-alone system; rather the vehicles must interact in real-time with the other components among other vehicles and in particular with the infrastructure in order to assess the current situation. Thus, interoperability is the first key requisite for efficient traffic management, co-operative functions and coordinative autonomy [12].

Connectivity between vehicles and other traffic elements is currently still in development. While almost all new premium cars already offer connectivity via Global System for Mobile Communication (GSM) to a backend system of the manufacturer [13] this is currently driven by the motivation to reduce costly recalls due to software adaptions [14] and also by the European eCall initiative. Starting with 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 [2]. Applications like intelligent coordination are already tested and evaluated in real-world scenarios [15]. 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 an Intelligent Transportation System (ITS) architecture available and connectivity scenarios defined by European Telecommunications Standards Institute (ETSI) [16], it is unclear whether vehicles will possess multiple communication systems for each service provider or the communication is handled via a central data hub [17]. Different approaches of the future communication infrastructure are presented and discussed in a report of the Cooperative Intelligent Transportation System (C-ITS) platform [2]. A conclusion is that 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.

Especially in the field of cybersecurity, there are multiple signs indicating that the current state of the art cannot adequately protect the new and vital role ICT will play in

 ISBN: 978-1-61208-643-9

transportation. Automotive cybersecurity is slowly rising to this aspect [18] triggered by research and governmental pressure [13][19][20][21]. Technical developments and industrial awareness of new challenges are followed by the development of first guidelines for tackling the issues [22]. On a higher level, the ITS infrastructure security is also a known issue which is addressed [23]. There is still ongoing discussion who will control and provide the communication infrastructure [2]. Since all mobility and the complete road transportation sector will depend on the ICT system, it is of utmost important to clarify responsibilities and to achieve a dependable balance between private and public control.

One important discussion is who controls access to the data collected by the vehicle. There are first efforts to develop processes for addressing these issues [24]. A recent survey of the German consumer organization "Stiftung Warentest" showed that almost all connectivity solutions offered by automotive OEMs have weaknesses in privacy [25]. Personal information is exchanged without encryption, and the superfluous information is collected and transmitted, partially done without informing the user and his agreement.

III. RISK MANAGMENT

There is currently no domain-specific risk management framework available for the automotive domain. First approaches [22] are promising, but initial evaluations show certain challenges in the application [26]. The guidebook [22] was published at the beginning of 2016 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 (ISO/SAE 21434), but the publication is currently envisioned for 2020. In the absence of applicable domain-specific frameworks, we propose to tailor ISO 31000 [27] 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 following steps of the risk management process:

1. Establishing the Context
2. Risk Assessment
3. Risk Treatment
4. Monitoring and Review
5. Communication and Consultation

Firstly, we present the framework with suggestions on how to tailor it towards the application field. The suggested tailoring will partially be done on a higher level.

A. Establishing the Context

The previous state of the art overviews shows that there is currently no specific regulatory or legal framework for road traffic. This means we can only apply generic rules and base the context on the environment and values of the society for road traffic. There are ongoing discussions about which regulations should be applied to the road traffic domain, but no clear consensus emerged so far. The automotive and transportation domain is an important part of ensuring and enabling our modern lifestyle and we, therefore, consider following objectives as necessary. It should be avoided, that a cybersecurity attack

- causes immediate damage to environment or human lives (safety);
- causes the loss of control over personal information (privacy);
- causes financial damage (finance); and
- negatively impacts the operation and traffic flow (operation).

We propose two restrictions to these objectives. Firstly, we restrict the risk management to direct and immediate consequences. This 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. Secondly, we assess the impact rating on users and society higher than the impact on the organization. That means that safety impacts and rate financial impacts for users or society are higher prioritized than for 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 ISO/IEC 31010 presents examples for risk assessment techniques, none of them is tailored for cybersecurity in the road traffic domain. There exist multiple proposals to extend established safety risk assessment methods towards cybersecurity [28], [29] or to tailor cybersecurity methods for the automotive domain [30], [31]. It should be remarked that there is no silver bullet to risk assessment implementation and any selected methodology needs to be justified. Depending on the abstraction level, different methods are favored. We propose threat modelling [33] for the analysis of risks. For risk evaluation purposes, we propose four impact levels, divided into four categories, as shown in Table I. This is an abstraction of the categories proposed by SAE J3061 [22] and EVITA [34]. Both use similar categories, but with more levels per category.

TABLE I. IMPACT LEVELS

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

A critical factor for risk evaluation in cybersecurity is the evaluation of likelihood. While for transportation domains it is discussed only to consider the impact of risk evaluation [35], this could move the focus on very unlikely risks. Details

 ISBN: 978-1-61208-643-9

of the likelihood assessment are presented in [26], 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 the society, which means that the benefits of the connected and automated road traffic scenario outweigh the risk. 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 is currently no clear responsibility for monitoring and review of risks. This is impeded by the hierarchical silo structure which dominates the automotive domain at the moment. OEMs have a restricted system view and are only able to identify risks on this level. Suppliers are responsible for the implementation of risks treatments for their specific contribution and can detect change requirements. There is no unambiguous allocation of the risk monitoring responsibilities. Established approaches in the automotive domain follow mainly 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.

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 the risk management transparent and comprehensible. It should be remarked that such records are sensitive and could be potentially misused by attackers.

IV. PRACTICAL USE CASE

In the CySiVuS project, we will analyze different use cases to develop the overall context requiring a comprehensive reference architecture. The first collection of use cases is based on the C-ITS Day 1 Use Case [36]. 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 RoadWorks Warning (RWW) use case. This use case describes an interaction between vehicles and cooperative roadside elements, which provides information to about short time modifications in the road infrastructure to optimize traffic flow and driving strategy. Further, we analyze the Intersection Safety (ISS) use case. This use case refers to an interaction between vehicles and cooperative roadside elements, which provides information to optimize the 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 vehicles will in the future automatically act based on the received information in the future. 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 detect the information with the vehicle sensors to consider it in their planning.

Figure 1 depicts the introduced three use cases. The RoadSide 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

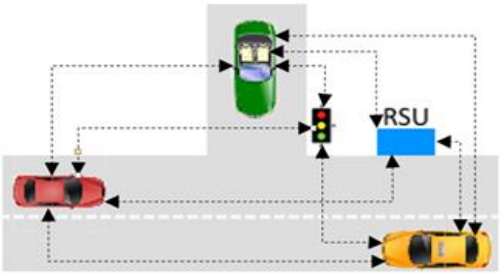

Figure 1. Use cases

system. We exercise the risk management approach based on the RWW use case. We apply threat modeling [31] for the risk assessment step.

Figure 2 visualizes the dataflow model for the interaction between vehicle A, B and the roadside units. Without any mitigation measures, twelve threats were identified. We focus in the following on the interaction type and the following threat, seen in Table II.

For connected automotive vehicles and their corresponding 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

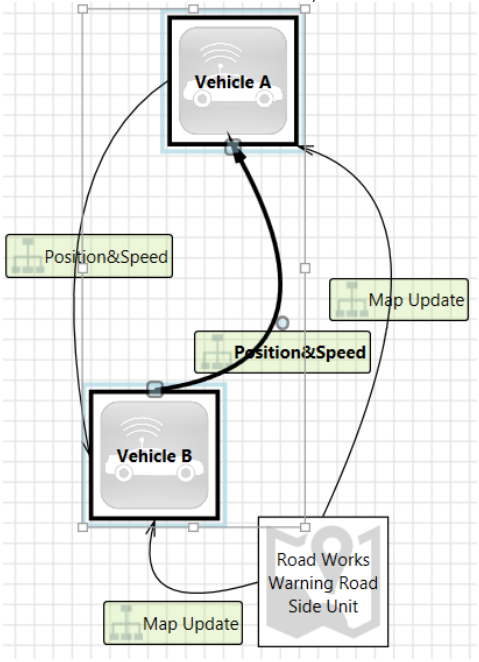

Figure 2. Data flow model for threat assessment

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 [37], [38]. The adapted Table III summarizes, the considerations above. 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.

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

Category	**Spoofing**
Description	Spoofing vehicle A in order to send malicious updates
Justification	<no mitigation provided>
Attack method	Impersonate the car (clone sim or similar) and then craft the malicious update

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

Category	**Spoofing**
Description	Spoofing vehicle A in order to send malicious updates
Justification	~~<no mitigation provided>~~ *Distance bounding avoids remote attacks and requires physical access to the environment in order to conduct the attack*
Attack method	Impersonate the car (clone sim or similar) and then craft the malicious update

V. REFERENCE ARCHITECTURE

An automotive reference architecture for security analysis was presented in [9]. 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 division is vital.

As a first approach, we divide the ITS into five clusters of elements as shown in Figure 3. 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 (WiFi) or GSM, which can be applied for V2V or Vehicle to Infrastructure (V2I) communication.

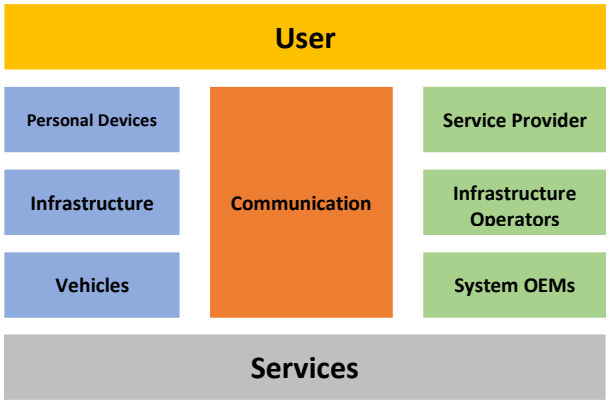

Figure 3. Clustering of elements in the transportation system

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 [2] and [17], 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

 ISBN: 978-1-61208-643-9

infrastructure and vehicle, conducted by system OEM and infrastructure providers, which is shown in Figure 4.

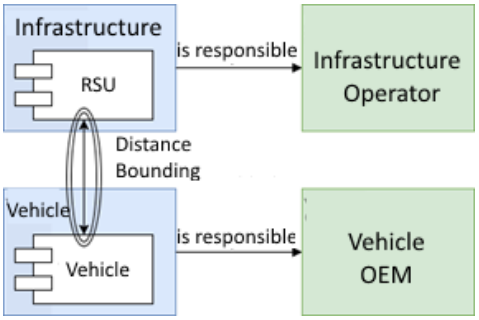

Figure 4. Application of the structural model

A possible solution approach is a structured multi-tiered reference architecture. However, a consistent risk management method is a critical success factor that this consistent architecture can be developed along all perspective layers. Our approach is to take the widely accepted risk management standard ISO 31000 [27] as a basis and tailor it to the automotive requirements. 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

VI. Conclusion and Outlook

To conclude our contribution, the technological and legal state of the art of automated driving for smart urban mobility is still not yet sufficient to cope with the complex requirements of such an environment. We identified four current challenges in a comprehensive traffic road system. 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 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 in a flow.

Finally, we discuss some previous works and propose core considerations on a comprehensive automotive reference architecture. We identify five element clusters required to interact with each other. 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 task in the upcoming period is to cope with the complexity and streamline the extremely different current and future developments on the various perspective levels.

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] Q. Xu, K. Hedrick, R. Sengupta, and J. VanderWerf, “Effects of vehicle-vehicle/roadside-vehicle communication on adaptive cruise controlled highway systems,” in *Vehicular Technology Conference, 2002. Proceedings. VTC 2002-Fall. 2002 IEEE 56th*, 2002, vol. 2, pp. 1249–1253 [Online]. Available: http://ieeexplore.ieee.org/ xpls/abs_all.jsp?arnumber=1040805. [Accessed: 27-Oct-2014]

[2] C-ITS Platform, “Working Group 6 - Access to in-vehicle resources and data,” 2015.

[3] SAE, “J3016 Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles.” 2016.

[4] M. Dikmen and C. M. Burns, “Autonomous Driving in the Real World: Experiences with Tesla Autopilot and Summon,” 2016, pp. 225–228 [Online]. Available: http://dl.acm.org/citation.cfm?doid=3003715.3005465. [Accessed: 27-Sep-2017]

[5] 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.

[6] 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*, pp. 1–1, 2017.

[7] United States Department of Transportation, “NHTSA | National Highway Traffic Safety Administration,” 2017. [Online]. Available: https://www.nhtsa.gov/. [Accessed: 28-Sep-2017]

[8] A. Greenberg, “The Jeep Hackers Are Back to Prove Car Hacking Can Get Much Worse | WIRED,” 08-Jan-2016. [Online]. Available: https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/. [Accessed: 29-Sep-2017]

[9] J. Brückmann, T. Madl, and H.-J. Hof, “An Analysis of Automotive Security Based on a Reference Model for Automotive Cyber Systems,” presented at the SECURWARE 2017: The Eleventh International Conference on Emerging Security Information, Systems and Technologies, Rome, 2017, pp. 136–141.

[10] Library of Congress, “H.R.701 - 115th Congress (2017-2018): SPY Car Study Act of 2017,” *Congress.gov*, 31-Jan-2017. [Online]. Available: https://www.congress.gov/bill/115th-congress/house-bill/701. [Accessed: 28-Sep-2017]

 ISBN: 978-1-61208-643-9

[11] 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: 22-Aug-2017]

[12] J. Harding *et al.*, "Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application." National Highway Traffic Safety Administration, Washington DC, Aug-2014 [Online]. Available: https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/readiness-of-v2v-technology-for-application-812014.pdf. [Accessed: 02-Oct-2017]

[13] C. Miller and C. Valasek, "A Survey of Remote Automotive Attack Surfaces," White Paper, 2014.

[14] H. A. Odat and S. Ganesan, "Firmware over the air for automotive, Fotamotive," in *Electro/Information Technology (EIT), 2014 IEEE International Conference on*, 2014, pp. 130–139 [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6871751. [Accessed: 17-Dec-2014]

[15] Autobahnen- und Schnellstraßen-Finanzierungs-Aktiengesellschaft (ASFINAG, in English: "Autobahn and high way financing stock corporation") Maut Service GmbH, "ECo-AT The Austrian contribution to the Cooperative ITS Corridor," 2017. [Online]. Available: http://eco-at.info/. [Accessed: 24-Jan-2017]

[16] European Telecommunications Standards Institute, "Intelligent Transport Systems (ITS); Cooperative ITS (C-ITS); Release 1." 2013.

[17] B. Datler, M. Harrer, M. Jandrisits, and S. Ruehrup, "A Road Operator's View on Cloud-based ITS – Requirements and Cooperation Models," presented at the 23rd ITS World Congress, Melbourne, Australia, 2016.

[18] L. Apvrille *et al.*, "Secure automotive on-board electronics network architecture," in *FISITA 2010 world automotive congress, Budapest, Hungary*, 2010, vol. 8 [Online]. Available: http://www.eurecom.fr/fr/publication/3132/download/rs-publi-3132.pdf. [Accessed: 29-Jan-2017]

[19] D. Spaar, "Car, open yourself! Vulnerabilities in BMW's ConnectedDrive," c't, no. 5, pp. 86–90, 2015.

[20] J. Petit and S. E. Shladover, "Potential Cyberattacks on Automated Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–11, 2014.

[21] C. Miller and C. Valasek, "Remote Exploitation of an Unaltered Passenger Vehicle," Black Hat 2015, Aug. 2015.

[22] Society of Automotive Engineers, *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems (work in progress)*. 2017.

[23] ECo-AT, "ECo-AT SWP3.4 Security, Release 3.6." 2016 [Online]. Available: http://www.eco-at.info/system-spezifikationen.html

[24] International Organization for Standardization, "ISO/DIS 20077-1 Road Vehicles - Extended vehicle (ExVe) methodology - Part 1: General information," 2016. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_ics/. [Accessed: 27-Jan-2017]

[25] Stiftung Warentest, "Connected Cars: Apps of the automobile manufacturer are data sniffers" ["Connected Cars: Die Apps der Autohersteller sind Datenschnüffler"], 26-Sep-2017 [Online]. Available: https://www.test.de/Connected-Cars-Die-Apps-der-Autohersteller-sind-Datenschnueffler-5231839-5231843/

[26] 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*, vol. 9923, A. Skavhaug, J. Guiochet, E. Schoitsch, and F. Bitsch, Eds. Cham: Springer International Publishing, 2016, pp. 157–170 [Online]. Available: http://link.springer.com/10.1007/978-3-319-45480-1_13. [Accessed: 28-Sep-2017]

[27] International Organization for Standardization, Ed., *ISO 31000:2009 Risk management - Principles and guidelines*. ISO, Geneva, Switzerland, 2009.

[28] G. Macher, Harald Sporer, Reinhard Berlach, Eric Armengaud, and Christian Kreiner, "SAHARA: A Security-Aware Hazard and Risk Analysis Method," in *Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition*, 2015, pp. 621–624.

[29] C. Schmittner, T. Gruber, P. Puschner, and E. Schoitsch, "Security application of failure mode and effect analysis (FMEA)," in *Computer Safety, Reliability, and Security*, Springer, 2014, pp. 310–325 [Online]. Available: http://link.springer.com/chapter/10.1007/ 978-3-319-10506-2_21. [Accessed: 04-Nov-2014]

[30] C. Schmittner, Z. Ma, E. Schoitsch, and T. Gruber, "A Case Study of FMVEA and CHASSIS as Safety and Security Co-Analysis Method for Automotive Cyber-Physical Systems," 2015, pp. 69–80 [Online]. Available: http://dl.acm.org/citation.cfm?doid=2732198. 2732204. [Accessed: 29-Sep-2017]

[31] M. Zhendong and C. Schmittner, "Threat Modeling for Automotive Security Analysis," presented at the SecTech 2016, Jeju, 2016.

[32] G. Sindre and A. L. Opdahl, "Eliciting security requirements with misuse cases," *Requirements Engineering*, vol. 10, no. 1, pp. 34–44, Jan. 2005.

[33] Frank Swiderski and Window Snyder, *Threat Modeling*. Microsoft Press Redmond, 2004.

[34] Fraunhofer Institute for Secure Information Technology, "EVITA Project Summary," Deliverable D0, 2013 [Online]. Available: http://www.evita-project.org/Publications/EVITAD0.pdf. [Accessed: 31-Oct-2014]

[35] J. Braband, "Towards an IT Security Framework for Railway Automation," presented at the Embedded Real Time Software and Systems, Toulouse, 2014 [Online]. Available: http://www.erts2014.org/site/0r4uxe94/fichier/erts2014_7c3.pdf. [Accessed: 22-Oct-2014]

[36] Federal Ministry of Transport, Innovation and Technology, "C-ITS Strategy Austria" ["C-ITS Strategy Austria."], Bmvit, 2016.

[37] K. B. Rasmussen and S. Capkun, "Realization of RF Distance Bounding.," in *USENIX Security Symposium*, 2010, pp. 389–402.

[38] 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*, 2008, pp. 194–202.

 ISBN: 978-1-61208-643-9