The Design of a Divide-and-Conquer Security Framework for Autonomous Vehicles

Abdelkader Magdy Shaaban
Center for Digital Safety & Security
Austrian Institute of Technology GmbH
Giefinggasse 4, 1210 Vienna, Austria
Email: abdelkader.shaaban@ait.ac.at

Christoph Schmittner
Center for Digital Safety & Security
Austrian Institute of Technology GmbH
Giefinggasse 4, 1210 Vienna, Austria
Email: christoph.schmittner@ait.ac.at

Arndt Bonitz
Center for Digital Safety & Security
Austrian Institute of Technology GmbH
Giefinggasse 4, 1210 Vienna, Austria
Email: arndt.bonitz@ait.ac.at

***Abstract*—The vehicular security engineering process endeavors to build up a secure vehicle with a high level of security assurance. The well-identified security flaws and conforming security countermeasures help to deliver secure vehicles. This work presents a newly Divide-and-Conquer security framework which can be integrated with the early stages of the vehicular development process to emphasize the security-by-design. The framework proposes to divide the vehicle components into separate layers and sublayers, according to common security parameters. Subsequently, the framework applies a series of security management actions to define potential threats and security vulnerabilities in a vehicle; thereupon, it selects a list of security countermeasures which can mitigate the vehicular's risk. Eventually, the framework performs a security verification and validation to ensure that the vehicle has been developed according to the highest degree of protection level.**

Keywords–Threats; Vulnerabilities; Security Requirements; Risk Assessment; Ontologies; Automotive.

I. INTRODUCTION

The technology of autonomous vehicles is one of the leading innovative research topics in the automotive industry. This technology considers one of the most vivid application examples of the new Internet of Things (IoT) applications. The global automotive IoT market is expected to reach $106.32 billion by 2023 as declared by Netscribes market research [1]. Autonomous vehicles will play an essential role in lessening accident rates and improving traffic efficiency by providing information about traffic conditions, and critical situations. According to the World Bank, traffic congestion can cost developing economies up to 5%, and for developed economies 0.5-3% of their annual Gross Domestic Product (GDP). Therefore, the traffic issues cause to reduce the global economy to $1.4 trillion annually [2].

Fully or highly autonomous vehicles require the cooperation of all road transport actors, road infrastructure, and service providers. These parts influence as a comprehensive infrastructure system that requires new reliable communication approaches to enable communication between vehicles-to-vehicles and vehicles-to-infrastructure. Accordingly, reliable connectivity is the primary requirement for processing various states of the motorized vehicle and accelerating further development [3]. Modern cars can communicate with smartphones via Bluetooth for various purposes, such as hands-free calls, navigation, or multimedia applications. Additionally, new motor cars can connect to the internet to provide additional services such as unlocking and starting the car remotely [4]. These connectivity methods come at a cost; however, that launches a new set of cybersecurity attacks. Other interconnected interfaces, ports, units, or wireless sensors which are directly connected to the internal bus of the vehicle, that can lead to severe attack surfaces [2]. The connected cars and the existence of hackers are now part of life. Therefore, the security must be involved as an integral part of all vehicle development phases to be able to address security vulnerabilities in the early stages of the vehicular development process [2].

Currently, there is no specific risk management framework available for the automotive domain [3]. This contribution presents the first steps into a comprehensive risk management framework for the current and future vehicular industry. The framework proposes to integrate with the vehicular development lifecycle. Divide-and-Conquer inspires the concept of this framework. The Divide-and-Conquer works recursively by breaking down a problem into sub-problems of equivalent specifications until it becomes simple to be solved. The framework follows the same concept of the Divide-and-Conquer by dividing the vehicle into separate layers and sublayers according to common security parameters. Then, the model performs multiple actions on each layer recursively by identifying assets' potential threats, and vulnerabilities. Then, the model evaluates the risks to differentiate between hundreds or thousands of risks that needed to be addressed by the precise security countermeasures. Finally, the framework verifies and validates the selected security countermeasure and suggests additional security countermeasures which can meet the actual security needs.

The paper is structured as follows; the related work on automotive cybersecurity is discussed in section II. Section III includes the main contribution of this work. The section discusses the structured phases of the Divide-and-Conquer security framework. The framework applied to a self-automated vehicle case study as is presented in section IV. The paper concludes with a summary, conclusion, and presents our plans for future work.

II. RELATED WORK

A baseline definition regarding self-driving or partially automated vehicles has been established by SAE International, which has been founded as the Society of Automotive

 ISBN: 978-1-61208-720-7

Engineers. It defines five levels of self-driving technology [5]. By this definition, level zero until two describe varying levels of acclimatization, ranging from warnings and momentary assistance to brake/acceleration and steering support. One example of a more advanced level two vehicle is the Tesla Autopilot [6], which offers both steering support and drivetrain control, but does not yet fall into the SAE level three until five categories. Here, an operator is not considered a "driver" of a vehicle, even when placed in the drivers seat.

A basis for further automation can be extended and more verbose between vehicles, as well as vehicles and roadside infrastructure. However, full connectivity among vehicles and other roadside elements is still under development phases [3]. As described by [3], the connectivity should follow some coordinated model not only based on the vehicle itself but also with the complete infrastructure. The term Cooperative Intelligent Transport Services (C-ITS) summarises these efforts to create a fully integrated transport system. On the forefront of standardization are, as described in [7], the Intelligent Transport Systems (ITS) standards by the European Telecommunications Standards Institute (ETSI). Also worth mentioning are the Cooperative ITS standards from ISO [8]. First attempts to test the feasibility of these standards and C-ITS have been made with the European Cooperative ITS joint development project, which created the first implementation of such a system spreading across the borders of the Netherlands, Germany, and Austria.

The diversity in communication protocols and heterogeneity of components in vehicles that creates new security threats can exploit vulnerabilities to attack vehicle [9]. The work [10] presents several security vulnerabilities, threats, and suggest a variety of security standards for existing and future vehicular systems. However, these points are suitable for particular security conditions in vehicular systems due to the entirely different attacker motivations, attacker skills, and various potential damages [11]. To cope with that, security objectives have to be defined. The first three objectives are Confidentiality (C), Integrity (I) and Availability (A) [12].

III. The Architecture Model of Divide-and-Conquer Security Framework

The lack of existing security framework in the vehicular sector motivates the ISO and the SAE organizations to propose a novel cybersecurity engineering standard for road vehicles [3]. The standard is still undergoing, and the first version is purposed to be published in 2020 [13].

This contribution looks forward to introducing a new security framework for the automotive domain. That work is a part of the Austrian national security research project "Cybersecurity for Traffic Infrastructure and Road Operators" (CySiVuS) [14]. The framework strives to ensure vehicle development life-cycle:

- Identify the potential threats which threatened the vehicle.
- Define security vulnerabilities that can be exploited by potential threats.
- Evaluate the risks of all detected threats and defined vulnerabilities.
- Address the unaccepted risks with suitable security countermeasures.
- Verify and validate the selected security countermeasures to ensure, they meet the actual security protection level.

The security protection level measures of trust that the Industrial Automation Control Systems (IACS) is free from vulnerabilities. ISA/IEC 62443-3-3 specifies security levels that enable a component to mitigate threats for given security protection level [15]:

- SL 1: Prevent the unauthorized disclosure of information via eavesdropping or accidental exposure.
- SL 2: Prevent the unauthorized disclosure of information to an entity actively searching for it using simple means with low resources, general skills, and low motivation.
- SL 3: Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with moderate resources and moderate motivation.
- SL 4: Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with extensive resources and high motivation.

Figure 2 depicts the architectural plan of the Divide-and-Conquer security framework. The framework consists of five main phases (i.e., Security Layers, Risk Analysis, Risk Assessment, Risk Treatment, and Security Assurance). These phases are iterative processes and could be started at any separate stages in the process life-cycle, as shown in Figure 1. The following subsections canvass the task of each phase.

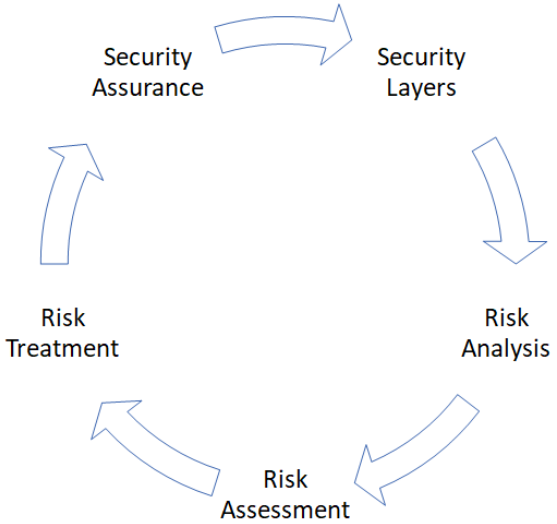

Figure 1. Divide-and-Conquer security framework lifecycle

A. Security Layers

The framework organizes the vehicle into four separate layers. Each layer contains components with common criteria such as type of components, security aspects, security

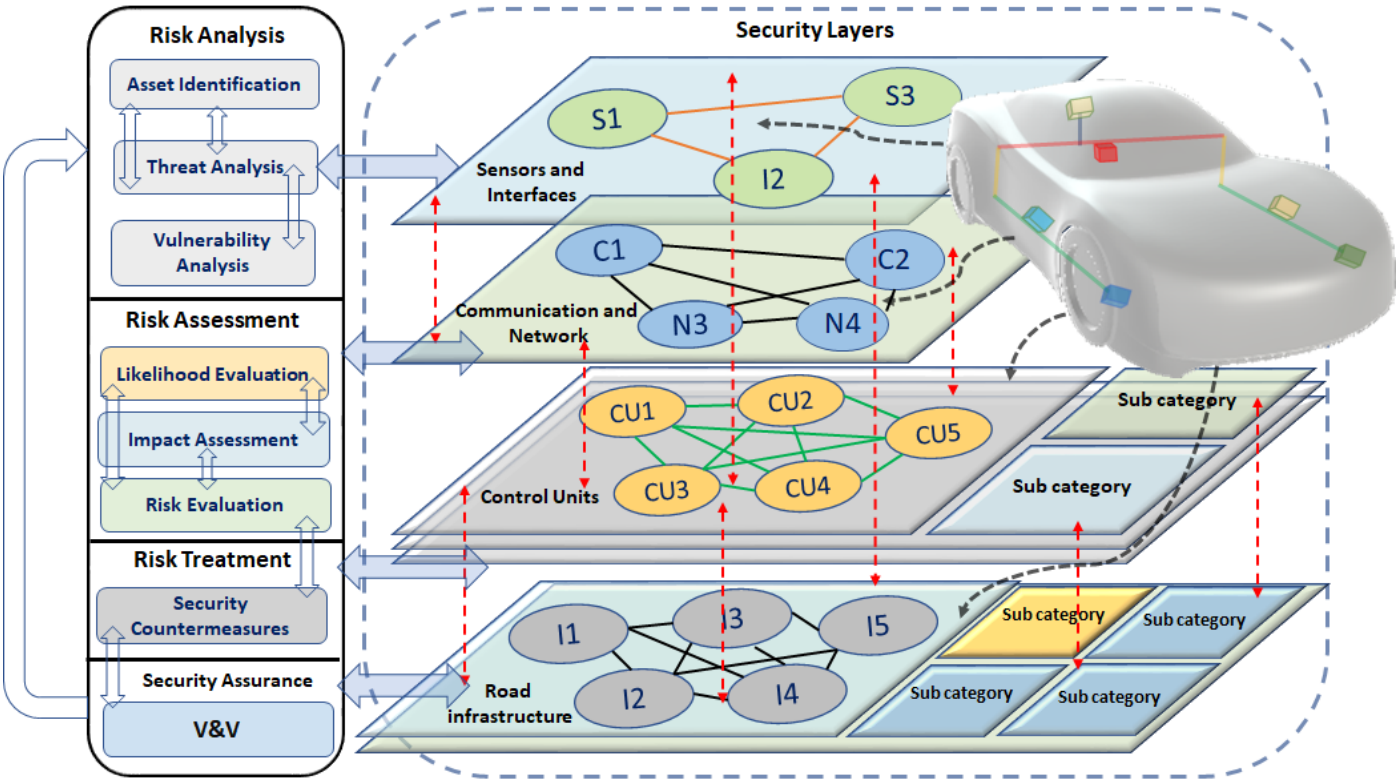

Figure 2. Vehicular security framework architecture model

protection levels, etc. This work proposes to classify the components according to the types of components such as Sensors, Control Units, Actuators, etc. Additionally, some components need more security concerns; consequently, it is proposed to accommodate these components into sublayers according to a specific security protection level.

a) Layer One: Sensors and Interfaces: this layer contains all sensors, ports, and communication interfaces which communicate internal vehicle components together or with the external environment. Some components can be stacked into equivalent sublayers, according to a specific security protection level. For example, internal interfaces which are connected directly with internal units in the vehicle do not need a highly-level of security protection; where external communication interfaces which communicate the vehicle with the external world that require a higher level of security to keep the vehicle secure.

b) Layer Two: Communication and Network: this layer encompasses all communication devices, which allow the internal vehicular units to communicate together within the vehicular boundary. Moreover, the external networking units are organized as highly protected sublayers, which needs more protection concerns.

c) Layer Three: Control Units: this layer has different types of electronic control units (ECUs) in a vehicle. Several ECU units have a list of security parameters (i.e., Tamper Protection, Authentication, Secure Boot, ASIL Rating, etc.) which are used to define the security mechanism for each ECU component. Furthermore, the model uses these parameters to classify the vehicular ECUs according to specific protection level need to be achieved for each unit.

d) Layer Four: Road Infrastructure: as mentioned previously, fully automated vehicles need assistance from the road infrastructure, such as Road Side Units (RSUs), Communication Infrastructure, Traffic Controls, or Intelligent Transportation Systems (ITS) [16]. This layer accommodates all components related to the traffic infrastructure and classifies them into sublayers according to the degree of protection level.

B. Risk Analysis

The risk analysis is an activity that aims to define the relationships between threats and the vulnerabilities which are threatened the vehicle. These relationships establish a set of classes and subclasses to decompose threats scenario into possible attack paths [17]. This activity consists of three main stages as Asset Identification, Threats Analysis, and Vulnerability Analysis.

1) Asset Identification: an asset in a vehicle considered as data, device, component, or either a physical or a logical object. The assets identification process concerns with the following tasks [18]:

- Create an asset record.
- Identify asset information.
- Define the topological structure of interconnected assets.

2) Threat Analysis: in the vehicular domain, the threat analysis is an activity that identifies the potential negative actions that affect the security mechanism in vehicles. The threat analysis process can be divided into the following essential steps:

 ISBN: 978-1-61208-720-7

1) Model the vehicle with all security related assumptions and necessary information.
2) Model potential adversaries with there capabilities, actions, tactics, techniques, and procedures.
3) Apply the threat model to the system model to identify potential threats.
4) Evaluate all identified threats and decide on the risk treatment.
5) Update the system model with the security countermeasures.
6) Repeat step 3 in order to identify missed or new threats.

In the course of our research, we developed the Threat Management Tool (ThreatGet) [19]. ThreatGet identifies and understands potential threats in the automotive domain. It helps to:

- Identify threats.
- Detect security vulnerabilities.
- Evaluate the risks of the identified security issues.

ThreatGet has a threat catalog contains the most common potential threats in the vehicular domain. The threat catalog is managed by ThreatGet to ensure a wide range of potential threats is considered. The following source documents were used to develop the threat catalog:

- Threat Modelling for Automotive Security Analysis [20].
- Connected Cars - Threats, Vulnerabilities and Their Impact [12].
- Threat Landscape and Good Practice Guide for Internet Infrastructure [21].
- A survey of Remote Automotive Attack Surfaces [22].

The tool classifies the potential threats into six main groups according to the STRIDE model (i.e., Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service (DoS), and Elevation of Privilege) [23].

3) Vulnerability Analysis: the vehicle vulnerability analysis process concerns with exploring, defining, identifying, and prioritizing vulnerabilities or security weaknesses in vehicles. The researcher in the Austrian Institute of technology developed a vulnerability analysis tool is called Failure Modes, Vulnerability, and Effect Analysis (FMVEA) [24]. FMVEA is based on the Failure Mode and Effect Analysis (FMEA) [25] and extends the standard approach with security-related threat modes [26].

C. Risk Assessment

Risk assessment is an activity for evaluating the degree of risks. This activity is based on the parameters of impact and likelihood, which are used to evaluate the specific risk level. This phase takes place after it collects all details about vehicular components, threats, and vulnerabilities which are identified and detected by the previous phase (Risk Analysis). The next subsections discuss the likelihood, impact, and risk evaluation briefly.

1) Likelihood Evaluation: the evaluation of likelihood considers the significant factor for the risk evaluation process. The likelihood assessment is explained in details in [27]. However, this work proposes four different aspects of the likelihood [3]:

- Assumed attacker capabilities.
- Ease of gaining information about the vehicle.
- Reachability and accessibility of vehicular data.
- Tailor-made equipment to attack vehicles.

Table I shows the parameters of the likelihood evaluation. The attacker capabilities are classified according to the skills of the hacker. The data reachability and availability are the main parameters of this evaluation process, which define how easy it is for an attacker to get data. The attacker could use tailor-made devices to attack vehicles; the last row in this Table shows the likelihood values of these outcomes to occur. These parameters are explained in [3].

2) Impact Assessment: the impact assessment process is an activity that aims to evaluate risk when potential threats and security vulnerabilities are defined. In the automotive domain, it is important to ensure that different types of impacts do not damage the vehicle or cause other accident scenarios:

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

Table II discusses the impact levels of these four acceident scenarios. The parameter values of these impact levels are discussed in [3].

- Firstly, the direct consequences (i.e., the operational impact would also impact emergency services and could, cause damage to human lives).
- Secondly, assesses the impact evaluation on users and society higher than the impact on the manufacturer. That means the rates of the safety impacts and the financial impacts for users or society are higher prioritized than for organizations. That is because the community trusts the transportation system.

3) Risk Evaluation: this phase uses the estimated parameters of likelihood and impact, as described previously. Then, it performs a risk assessment methodology to calculate the exact risk level. This work applies the well-known risk assessment formula as described in (1).

$$Risk = Threat * Vulnerability * Consequence \quad (1)$$

where:

$Threat * Vulnerability$ = Likelihood
$Consequence$ = Impact

The formula evaluates the risk level of each detected threats based on the parameters of Table I (likelihood)

TABLE I. PROPOSED LIKELIHOOD PARAMETERS

Parameters	Values			
Capabilities	Amateur (4)	Mechanic, Repair shop, etc. (3)	Hacker, Automotive expert, etc. (2)	Expert etc. (1)
Availability	Public (4)	Information for Maintenance Availability (3)	information for maintenance availability (2)	information for ECUs' company availability (1)
Reachability	Untrusted Network (4)	Private Network (3)	Part time Accessible (2)	Physical Access (1)
Financial	Standard Devices (4)	Specialize Devices (3)	Tailor-Made Device (2)	Multiple Tailor-made devices (1)

TABLE II. IMPACT LEVELS [3]

Impact Levels	User/Society	Manufacturer
Safety	1	-
Operational	3	4
Privacy	2	3
Financial	3	4

and Table II (impact). The results are plotted on a risk scale, is called "Risk Curve," as depicted in Figure 3. This work expects that the Tolerable Value (TV) is equal to two. That means all values (risk evaluation results) above this threshold (TV), need to be addressed by suitable security countermeasure(s) to mitigate risk.

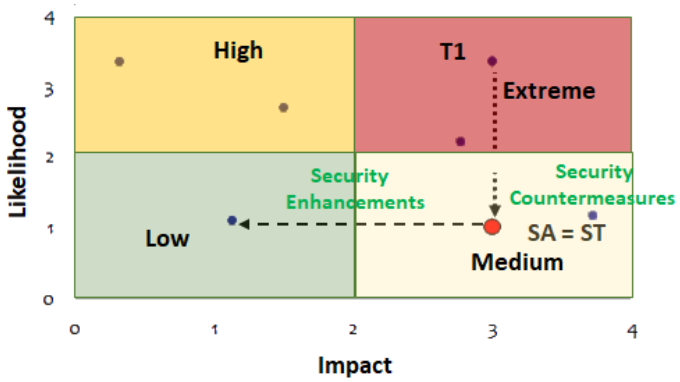

Figure 3. Risk mitigation curve

For example, the point T1 on the Risk Curve is considered as a threat, and its severity is Extreme. Therefore, security countermeasure(s) apply to mitigate that risk into an acceptable security level and to reach the Security Target (ST). Once the security countermeasures are applied, T1 moves into a new level of risk; this state is called Security Achieved (SA), which implies the current state of the security level. The process repeated until the SA=ST otherwise, other security countermeasures, have to be applied to decrease the risk further to a satisfactory security level. In this case, these security countermeasures are called Security Enhancement (SE)

D. Risk Treatment

Selecting the security countermeasures process is considered a significant challenge in the system development process. This phase plays an important role to address potential threats and security vulnerabilities to keep the risk always low. In the course of our research; we developed a Model-based Security Requirement Management Tool (MORETO) for managing a vast number of different security requirements. MORETO reuses different features driven by concepts and knowledge of system modeling.

The tool plays a vital role in this work for generating a list of security countermeasure for a large number of different components. MORETO receives the data generated from the previous phases, such as risk evaluation of the detected threats and vulnerabilities. Then, it generates security countermeasures according to the specific security target which needs to be achieved. MORETO is an Enterprise Architect (EA) plugin for managing the IEC 62443 security standard [28].

E. Security Assurance

In the vehicular domain, the Security Assurance (SA) is a method of guarantee vehicles operate at a high level of security protection. For that purpose, the authors introduced a newly ontology security testing algorithm (OnSecta). OnSecta generates an ontological representation of all detected threats, vulnerabilities, and selected security countermeasures. The algorithm performs a series of inference rules to verify that the selected security countermeasures are handled the detected security flaws. Then, OnSecta validates these countermeasures to a specific security protection level. The algorithm manages numerous security countermeasures which are stored in an ontological structure. OnSecta uses the stored data to select additional security countermeasures when the selected ones have not met the needed security level.

IV. CASE STUDY: SELF-AUTOMATED VEHICLE

Automotive driving is an essential aspect of future transportation. Develop a fully automated vehicle, of the mobility system for people and goods, is demanded. According to the growth of the vehicular industry, new security issues arise. The cybersecurity is considered an integral part of the vehicular development process. A secure vehicle can be designed and developed if security issues are well-identified, and security countermeasures are correctly defined. This case study shows, how our contribution can be conducted in the early stages of the vehicular development lifecycle to ensure security-by-design.

Figure 4 depicts a self-driving scenario. It shows two vehicles A and B communicate together throughout a V2X gateway. The vehicles receive traffic updates from multiple

 ISBN: 978-1-61208-720-7

road units over the V2X gateway. The vehicles A and B contain multiple sensors, actuators, electronic control units, internal gateways, various communication protocols, and various communication interfaces. The red links represent the highest risks points in this example, which communicate vehicles with external environments.

All these components are divided into four layers (i.e., Sensors and Interfaces, Communication and Network, Control Units, and Road Infrastructure) according to the Divide-and-Conquer security framework as described in Section III-A. The framework defines the security issues in this example by applying risk analysis methodology as described in Section (III-B). It is essential to evaluate the detected security issues to determine the exact risk, as explained in Section (III-C). Furthermore, it determines the security countermeasure to address the detected security flaws, as discussed in Section (III-D). Finally, the security framework verifies and validates the reached security level to ensure that the SA = ST as considered in Section (III-E). The following subsections explain how the framework applies a series of security methodologies to achieve an acceptable level of security protection and to deliver a secure vehicle.

A. Risk Analysis

This phase applies ThreatGet on that example, and without changs in the security parameters of components, the tool detects over 300 potential threats. Currently, modern vehicles have an average of 60 to 100 sensors, and communication interfaces on board [29]; plus, around 150 Automotive ECUs [30]. Therefore, the number of potential threats in fully automated vehicles is expected to be thousands.

ThreatGet classifies the detected threats according to the STRIDE model. Table III reviews the classes and the numbers of the identified potential threats.

TABLE III. THE CLASS AND NUMBERS OF THE DETECTED POTENTIAL THREATS ACCORDING TO SREIDE MODEL

Threat Types	Numbers
Denial of Service	44
Elevation of Privilege	43
Information Disclosure	88
Repudiation	21
Spoofing	80
Tampering	50

Afterward, the FMVEA tool applied to this example to perform vulnerabilities analysis. The FMVEA defines the vehicles and the road infrastructure as environments. The environment is a container that has components as depicts in Figure 5.

The FMVEA defines security vulnerabilities based on a set of rules to define the structural behavior of components in a given model. In this example, these rules need to be defined first. In this example, the following rules are applied to detect security vulnerabilities:

a) Secure Remote Access Point:

Rule: RemoteAccessPoint.attributes(Authentication = false).hasAncestor(vehicle)

Description: If the remote access point of a vehicle is not secured by Authentication this Access Point could be exploited as weakness in a vehicle.

b) External Gateway Update Frequency and Security:

Rule: Connection.from(InfrastructureGateway) .to(VtoXGateway).attributes(UpdateFrequency>10s, Encryption=false)

Description: External Gateway must communicate in a safe manner over an encrypted connection.

Figure 6 illustrates the detected security vulnerabilities by FMVEA. The red color represents the venerable components in this example,

B. Risk Assessment

This phase evaluates risks based on parameter values of the likelihood and impact level, as explained in Table I and Table II respectively. The assessed risk is classified as one of the primary four risk levels (i.e., extreme, high, medium, or low). The evaluation process focuses only on the highly valued components from the attacker viewpoint, which need a high level of security protection. Figure 7 shows the results of the risks evaluation process of that example.

C. Risk Treatmeant

The MORETO tool plays a vital role in this work to cover the detected security gaps with suitable security countermeasures to mitigate the unacceptable risks. MORETO automatically selects security countermeasures according to the detected threats and vulnerabilities for each affected unit separately, as shown in Figure 8. The figure displays the elected security countermeasures of the V2X Gateway based on the IEC 62443-4-2 security series [31].

D. Security Assurance

The last step is to validate and verify the selected security countermeasures, which are selected by MORETO to coved security flaws in this example. OnSecta is applied to verify and validate the security protection level. It defines the ontological representation of threats, vulnerabilities, and countermeasures, as shown in Figure 9. Then, it applies various reasoning rules to validate and verify the selected security countermeasures and suggests further ones to meet the actual security level.

V. SUMMARY, CONCLUSION, & FUTURE WORK

The paper has introduced a novel comprehensive security framework for autonomous vehicles. The framework aims to be a part of the early stages of the vehicular developments phases to detect security flaws and address these issues with proper security countermeasures. It divides the vehicle into four layers according to the types of components. Each layer contains other sublayers which accommodate components that need a high level of protection. Afterward, the model uses the ThreatGet and FMVEA to define the potential threats and the vulnerabilities in a vehicle. Then, the framework calculates the likelihood and determines the impact levels of the identified security issues. The risk treatment phase selects security countermeasures to mitigate the overall risk. Finally, the OnSecta algorithm verifies the security countermeasures to ensure that all detected threats and vulnerabilities have been handled; additionally, validates the security countermeasures

 ISBN: 978-1-61208-720-7

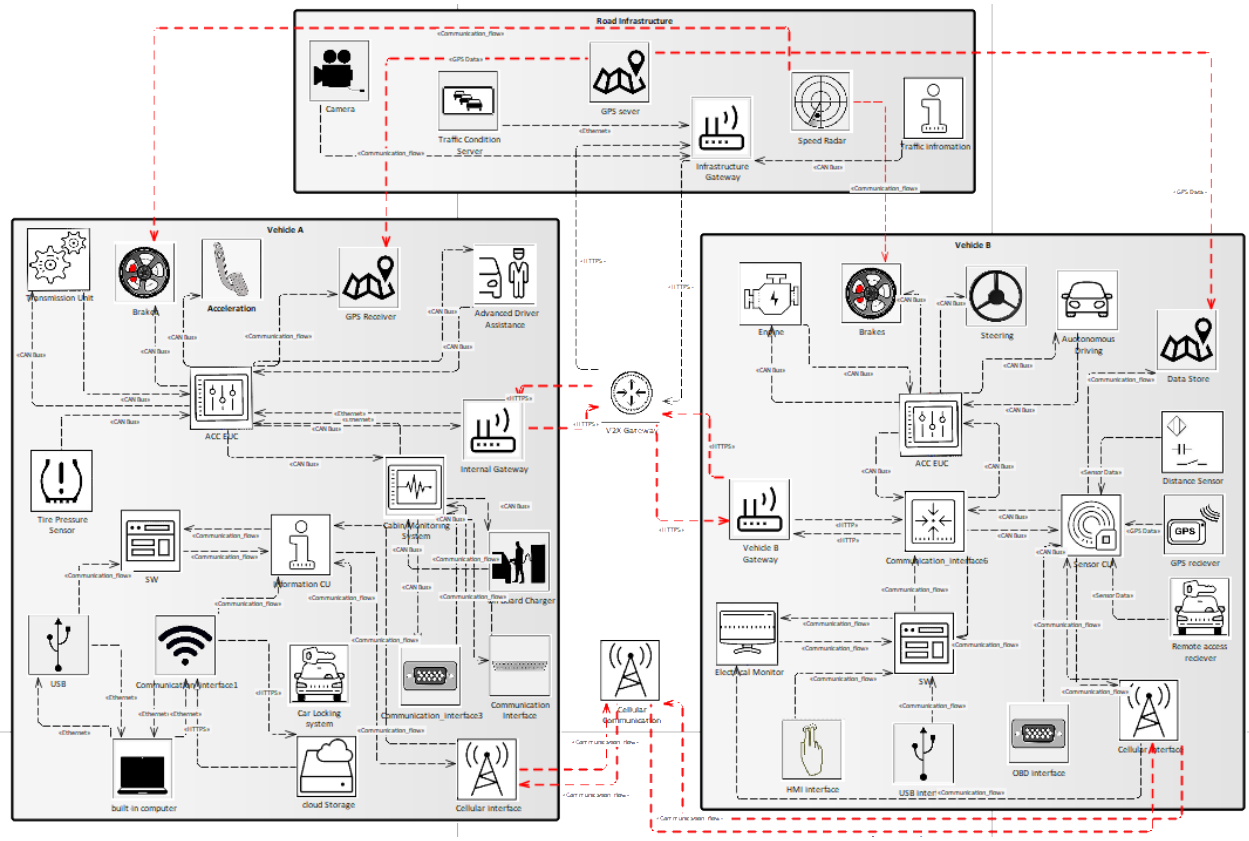

Figure 4. Dataflow between vehicles A, B, and infrastructure units

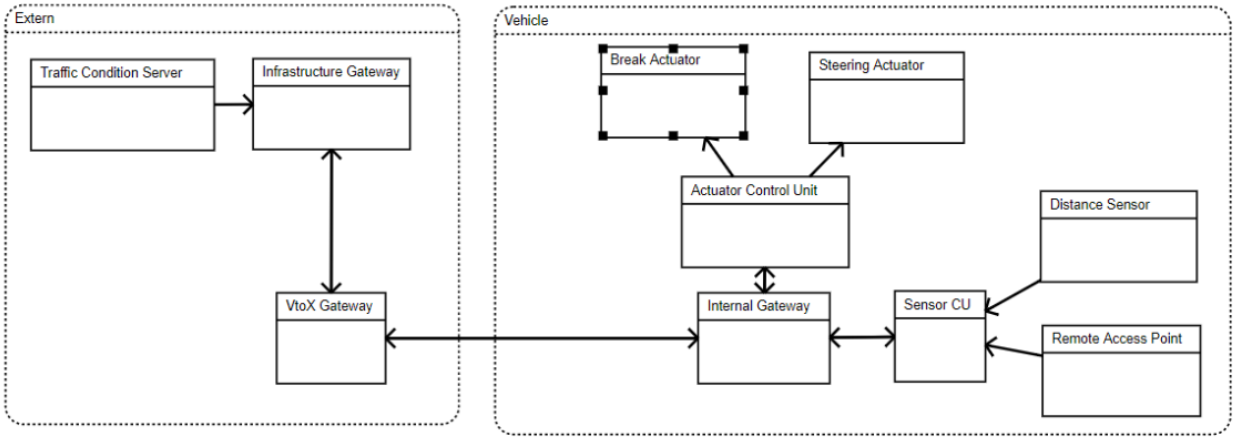

Figure 5. Automotive vehicle example model using FMVEA

to meet the actual security level needed. Future work will include the following points:

- Improve the threat database of ThreatGet.
- Integrate additional security countermeasures with MORETO's database like as ISO 27000 for information security management systems.
- Improve the risk evaluation methodology to be suitable for complex models.
- Enhance the OnSecta building blocks to manage more characteristics and relationships of threats, vulnerabilities, and security countermeasures.

ACKNOWLEDGMENT

The research project "Cybersicherheit für Verkehrsinfrastruktur- und Straßenbetreiber" (CySiVuS, in English: "Cybersecurity 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

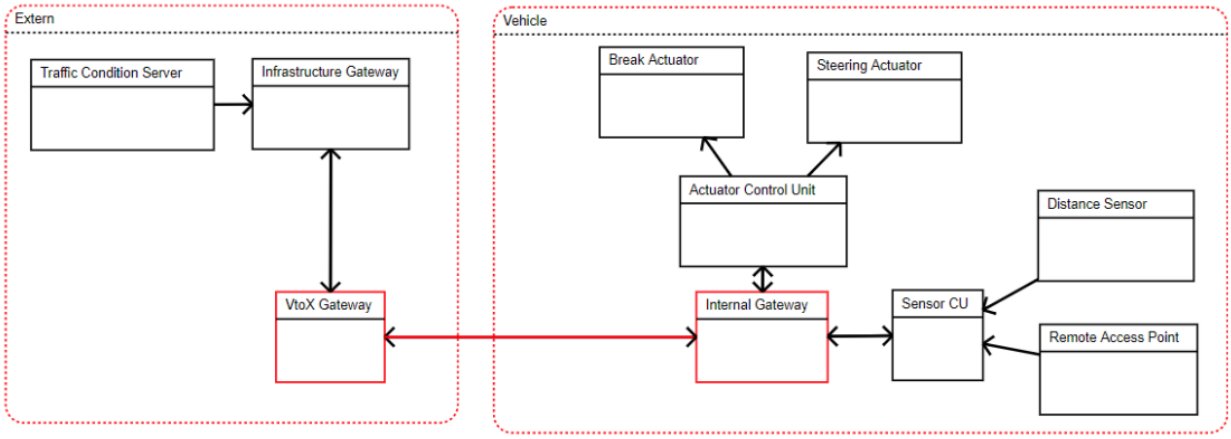

Figure 6. Affected elements and connections regarding rule the applied rules

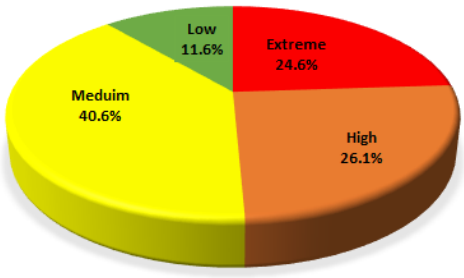

Figure 7. Statistical percentage of risk levels

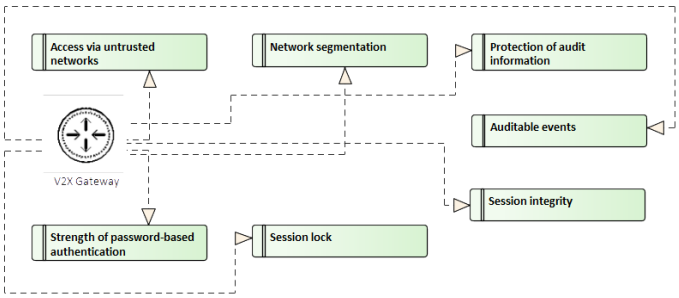

Figure 8. List of IEC 62443-4-2 security requirements of the V2X Gateway

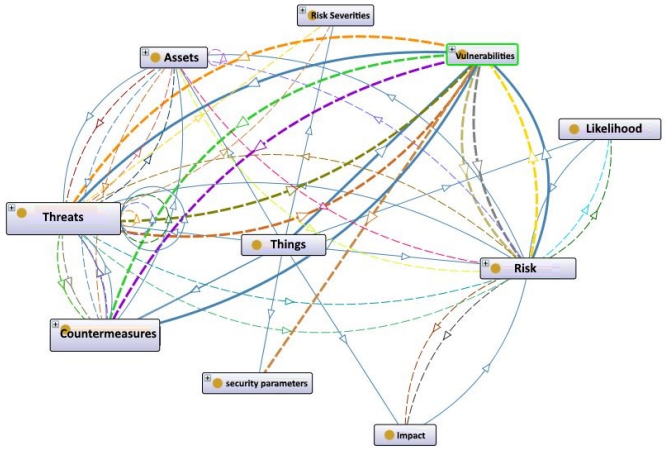

Figure 9. The ontological representation of threats, vulnerabilities, and security requirements

and Technology (BMVIT) and Austrian Research Promotion Agency (FFG) 2017).

REFERENCES

[1] Netscribe Blog, "Applications of IoT in the automotive industry | netscribes blog." [Online]. Available: https://www.netscribes.com/the-present-and-future-role-of-automotive-iot/ [accessed on: 2019-05-19].

[2] Carrie Cox and Andrew Hart, "How autonomous vehicles could relieve or worsen traffic congestion," Here Technologies, Tech. Rep., 2017.

[3] C. Schmittner, M. Latzenhofer, A. M. Shaaban, 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, 2018.

[4] A. Birni and T. van Roermund, "A multi-layer vehicle security framework," BU Automotive, NXP Semiconductors, Automotive Security, 2016.

[5] P. WARRENDALE, "SAE international releases updated visual chart for its "Levels of Driving Automation" standard for self-driving vehicles," 2018. [Online]. Available: https://www.sae.org/news/press-room/2018/12/sae-international-releases-updated-visual-chart-for-its-%E2%80%9Clevels-of-driving-automation%E2%80%9D-standard-for-self-driving-vehicles [accessed on: 2019-05-10].

[6] Electrek, "Tesla autopilot," 2019. [Online]. Available: https://electrek.co/guides/tesla-autopilot/ [accessed on: 2019.05.18].

[7] L. Chen and C. Englund, "Cooperative its - eu standards to accelerate cooperative mobility," in 2014 International Conference on Connected Vehicles and Expo (ICCVE). IEEE, 2014, pp. 681–686.

[8] ISO, "Iso 17427-1:2018 intelligent transport systems – cooperative its – part 1: Roles and responsibilities in the context of co-operative its architecture(s)," International Organization for Standardization, Standard, 2018.

[9] A. M. Shaaban, C. Schmittner, T. Gruber, A. B. Mohamed, G. Quirchmayr, and E. Schikuta, "Cloudwot-a reference model for knowledge-based iot solutions," in Proceedings of the 20th International Conference on Information Integration and Web-based Applications & Services. ACM, 2018, pp. 272–281.

 ISBN: 978-1-61208-720-7

[10] Wolf, Marko and Daly, PW, Security Engineering for Vehicular IT Systems, may 2009 ed. Vieweg and Teubner, 2009.

[11] M. Wolf and M. Scheibel, "A systematic approach to a qualified security risk analysis for vehicular it systems," Automotive-Safety & Security 2012, 2012.

[12] 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). IEEE, 2018, pp. 375–380.

[13] C. Schmittner, G. Griessnig, and Z. Ma, "Status of the development of isosae 21434," in European Conference on Software Process Improvement. Springer, 2018, pp. 504–513.

[14] KIRAS Security Research, "Cyber security for transport infrastructure- and road operators (cysivus)." [Online]. Available: https://www.kiras.at/en/financed-proposals/detail/d/cyber-security-for-transport-infrastructure-and-road-operators-cysivus/ [accessed on: 2019.05.02].

[15] IEC 62443-3-3, "Industrial communication networks - network and system security - part 3-3: System requirements and security levels," International Electrotechnical Commission, Tech. Rep., 2013.

[16] S. Mehar, S. M. Senouci, A. Kies, and M. M. Zoulikha, "An optimized roadside units (rsu) placement for delay-sensitive applications in vehicular networks," in 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC). IEEE, 2015, pp. 121–127.

[17] ISO-SAE 21434, "Road vehicles – cybersecurity engineering cd," 2019. [Online]. Available: https://www.iso.org/standard/70918.html [accessed on: 2019.05.16].

[18] Oracle Asset Identification, "Overview to Asset Identification," 2013. [Online]. Available: https://docs.oracle.com/cd/E26228_01/doc.93/e21539/ [accessed on: 2019.04.28].

[19] Sparx Services CE, "Threat Modeling with STRIDE," 2019. [Online]. Available: https://cybersecurity.sparxservices.eu [accessed on: 2019.05.21].

[20] Z. Ma and C. Schmittner, "Threat modeling for automotive security analysis," Advanced Science and Technology Letters, vol. 139, 2016, pp. 333–339.

[21] C. Lévy-Bencheton, L. Marinos, R. Mattioli, T. King, C. Dietzel, and J. Stumpf, "Threat landscape and good practice guide for internet infrastructure," EU Agency for Network and Information Security (ENISA), 2015.

[22] C. Miller and C. Valasek, "A survey of remote automotive attack surfaces," black hat USA, vol. 2014, 2014, p. 94.

[23] A. Shostack, "Experiences threat modeling at microsoft," vol. 413, 2008.

[24] C. Schmittner, Z. Ma, and P. Smith, "Fmvea for safety and security analysis of intelligent and cooperative vehicles," in International Conference on Computer Safety, Reliability, and Security. Springer, 2014, pp. 282–288.

[25] I. E. Commission et al., "Iec 60812: Analysis techniques for system reliability-procedure for failure mode and effects analysis (fmea)," Geneva, Switzerland: International Electrotechnical Commission, 2006, pp. 1–93.

[26] 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," in Proceedings of the 1st ACM Workshop on Cyber-Physical System Security. ACM, 2015, pp. 69–80.

[27] C. Schmittner, Z. Ma, C. Reyes, O. Dillinger, and P. Puschner, "Using sae j3061 for automotive security requirement engineering," in International Conference on Computer Safety, Reliability, and Security. Springer, 2016, pp. 157–170.

[28] A. M. Shaaban, E. Kristen, and C. Schmittner, "Application of iec 62443 for iot components," in International Conference on Computer Safety, Reliability, and Security. Springer, 2018, pp. 214–223.

[29] Automotive Sensors and Electronics Expo 2017, "Automotive sensors and electronics expo 2017," 4th Annual Conference and Exhibition, 2017. [Online]. Available: http://www.automotivesensors2017.com [accessed on: 2019.04.27].

[30] embitel, "ECU is a three letter answer for all the innovative features in your car: Know how the story unfolded," 2017. [Online]. Available: https://www.embitel.com/blog/embedded-blog/automotive-control-units-development-innovations-mechanical-to-electronics [accessed on: 2019.05.15].

[31] IEC 62443-3-2, "IEC 62443 security for industrial automation and control systems - part 3-2: Security risk assessment and system design." ISA, Security Standard Committee Draft for Vote (CDV) IEC 62443-3-2 ED1.

 ISBN: 978-1-61208-720-7