future internet

MDPI

Review

On the Modeling of Automotive Security: A Survey of Methods and Perspectives

Jingjing Hao [1,2,*] and Guangsheng Han [2]

[1] School of Mechanical Engineering, Tianjin University, Tianjin University Beiyangyuan Campus, No. 135 Yaguan Road, Jinnan District, Tianjin 300350, China
[2] CATARC(Tianjin) Automotive Engineering Research Institute, No. 68, Xianfeng EastRoad, Dongli District, Tianjin 300300, China; hanguangsheng@catarc.ac.cn
* Correspondence: haojingjing@catarc.ac.cn; Tel.: +86-022-84379777-8229

Received: 11 October 2020; Accepted: 10 November 2020; Published: 16 November 2020

Abstract: As the intelligent car-networking represents the new direction of the future vehicular development, automotive security plays an increasingly important role in the whole car industry chain. On condition that the accompanying problems of security are proofed, vehicles will provide more convenience while ensuring safety. Security models can be utilized as tools to rationalize the security of the automotive system and represent it in a structured manner. It is essential to improve the knowledge about security models by comparing them besides proposing new methods. This paper aims to give a comprehensive introduction to the topic of security models for the Intelligent Transport System (ITS). A survey of the current methodologies for security modeling is conducted and a classification scheme is subsequently proposed. Furthermore, the existing framework and methods to build automotive security models are broadly examined according to the features of automotive electronic system. A number of fundamental aspects are defined to compare the presented methods in order to comprehend the automotive security modeling in depth.

Keywords: automotive cybersecurity; security modeling; automotive threat modeling; automotive security engineering; risk assessment

1. Introduction

With the rapid development of the high technologies, such as Mobile Internet, Big Data, Artificial Intelligence and Cloud Computing, the automobile has gradually become a new-type of intelligent travel carrier [1,2]. There are more and more communication demands and scenarios between automobiles and the external. Due to interconnection and intelligence, the automobile is transformed from a closed system to open. Nevertheless, it also provides more connecting controllers and sensors for the attackers to be exploited, especially when the access to Internet is activated. Compromising the security of the automobile results in not only financial loss and a privacy breach, but also malicious control and a threat to safety. A demonstrative attack was conducted to remotely disable the car's brakes on a highway [3]. Recently, researchers and white hat hackers explored and manifested a number of the vulnerabilities of automobiles as shown in [4–8]. In the beginning, automotive security mainly concerned the locking systems and immobilizers because of the usage of keyless entry systems [9]. Many studies have demonstrated the possibility to access the system without permission [10–14]. With the increasing connectivity of vehicles, the external communication can be seen as new attack surfaces in modern vehicles. For example, there are various services that could affect cybersecurity, such as communicating via telematics system, connecting to OBD (on-board diagnostics) port, or reflashing ECUs (Electronic Control Unit) by OTA (Over-The-Air). The feasibility to attack vehicles by exploiting the potential weakness in these services are examined in [15].

Additionally, the manipulations from wireless connection are also used to perform attacks [16–19]. Since the autonomous vehicles on levels 2 and above need to be equipped with dozens of sensors for collecting data from the environment [20], they are vulnerable to a variety of possible security attacks [21,22]. The cameras on vehicles can be blinded [23] and the LiDAR system can be deceived with fake echoes [24]. Reference [25] listed the automotive security incidents from 2010 to 2019. Reference [26] surveyed the theoretical and practical attacks with different approaches and [27] provided a comprehensive taxonomy so that the information derived from attacks can be used for vehicular development and testing.

It is significant to attach great importance to the security of intelligent connected automobiles since the security threats are increasing substantially. Moreover, it is necessary to implement well-grounded security practices for ITS. Managing the security on different levels is a basic requirement for security activity. Therein, the elemental step is to assess and prioritize the risks with security analysis techniques. In order to improve the security of the system, we need firstly to understand what threat and risk the system will confront. The interaction and information that influence the system should be processed and analyzed primarily. It is necessary to utilize systematic approaches to identify the vulnerabilities and the latent threats. Based on that, the security objectives can be settled and the countermeasures to mitigate the risk impacts can be derived.

A security model can be built to explore all the correlated factors in an organized manner [28]. Instead of simply brainstorming and informal group discussions of the possible intentions of the adversaries, security models are exploited systematically to investigate the vulnerabilities to ensure high coverage. It is particularly important for cyber-physical systems like automobiles since it has direct physical effects on the environment instead of virtual ones [29]. Security models are developed to describe the security characteristics of systems formally and to explain the reasons for the security-related behaviors of systems accurately [30]. Since threat modeling allows to prioritize recovery strategies and decision-making regarding threats and risks, it should be started at the early stages of the design and evolved through the life cycle of the application [31,32].

There are a number of researches studying the methodologies to obtain security models. As suggested in [33], it is important to improve the knowledge about security models by comparing them besides proposing new methods. It is constructive to propose a taxonomy for the existing security models rather than enumerating the methods exhaustively. The aim of this paper is to introduce a classification scheme for describing the security modeling methods and provide a survey and a comparison about the automotive security models. Moreover, it is helpful to evaluate the automotive security models and link them to the methods from the other fields. After reviewing the previous work on security models, three main contributions are made:

1. Classifies the methods for security models into quantitative and qualitative categorizes.
2. Identifies the existing framework and methods to build security models for automobiles and provides a comprehensive overview of them.
3. Compares the available automotive security models for the design phase of automotive products, which are originally planned from security perspectives. The characteristics of each methodology are summarized. Based on the rational assessment, it gives a reference for automotive engineers to understand the methods then to choose the appropriate ones to initiate security evaluations.

The remainder of this paper is as follows: In Section 2, the security modeling methods are reviewed and classified from a different point of view. After that, the automotive security models are surveyed and compared with several fundamental aspects in Section 3. Finally, the discussion and concluding remarks are given in Sections 4 and 5. The structure of this article is illustrated in Figure 1.

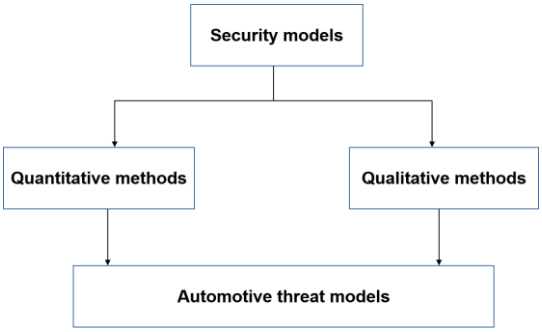

Figure 1. The structure of this article.

2. Taxonomy of Security Models

Because of widespread use of the interconnection, security becomes one of the main concerns in the industrial domain, which includes automobiles. Unlike safety, the security of a system is defined in the dimensions of intents and external influence in [34]. Generally, security is the ability to defend the confidentiality and integrity of the system by implementing protections to prevent unauthorized access [35–37]. In the automotive context, the security means all functions and interfaces of road vehicles and the automotive ecosystem are protected against cybersecurity threats. Since security is related to uncertainties like malicious events and environmental interactions, security models can be used as a tool to rationalize the security of the system and represent it in a structured manner [38].

Security models are developed to describe the security characteristics of systems formally. They are used to explain the reasons for the security-related behaviors of systems accurately [39]. There are various security models according to different purpose, for instance: the access control model, the integrity model and the threat model. In this paper, we only focus on the threat model to identify the potential threats and risks that could affect the system. It is significant for system security engineering to derive the security requirements and protection mechanisms based on the threat model [40]. Hence, the threat models are commonly used in automotive security. There are several developed threat modeling methods for software systems as illustrated in [41]. We review and categorize these approaches, which stimulate the automotive threat modeling development.

Threat modeling is a group of planned activities for identifying and assessing application threats and vulnerabilities [28] as shown in Figure 2. We propose a classification scheme to categorize the methods of threat modeling into the qualitative models, which are mainly in descriptive form, and the quantitative models like stochastic models.

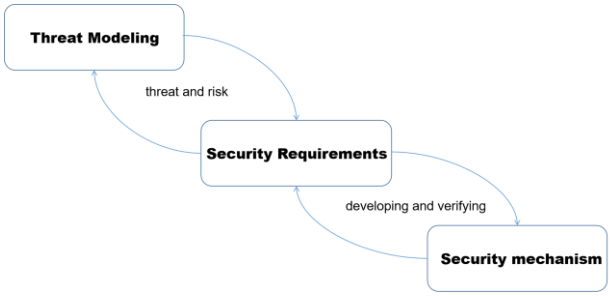

Figure 2. The process of system security engineering [28].

2.1. Qualitative Security Methods

Qualitative methods aim to analytically discover and state the security threats. Different from informal group discussions of the potential threats, qualitative security models can be used as a tool to investigate the vulnerabilities systematically. The models can be built either from the developers' perspective or the attackers'.

One of the classical qualitative approaches is the STRIDE model proposed by Microsoft. It is a structured approach for identifying the threats according to the purposes of the attacks. STRIDE model was originally applied in a software system. STRIDE represents the acronym of potential threats: spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege [42]. Firstly, the evaluated system is described with a data flow diagram (DFD). The entities and the data flow of the system are labeled in the DFD as security-related elements. Then the elements are examined to check if their security attributes of confidentiality, integrity and availability are violated. Based on the examination, the threats are identified with associated terms from the potential types of threats. The advantage of the STRIDE model is that the possible attacks are generalized into limited kinds of threats instead of every specific attack. Moreover, it emphasizes the completeness and repeatability of identifying the threats and is applicable for non-security-experts [43]. Myagmar et al. applied STRIDE model in [28] to derive security requirements for complex systems like networked systems. Three case studies of software applications and computer systems are presented in the paper to show the threat modeling process. There are many similar methods derived from STRIDE. For example, a method named LINDDUN is used for data security to assess privacy [44]. It stands for linkability, identifiability, non-repudiation, detectability, disclosure of information, unawareness, and non-compliance [45,46].

Qualitative methods can be used to visualize threats from the attackers' counterpart. It allows to figure out what activities the attackers will perform, the way they carry out the attacks, and how they make decisions [47,48]. Persona non Grata (PnG) is a method to model the threats by analyzing the motivations and skills of human attackers from an unintended use point of view [49]. It helps the developers to realize the vulnerabilities and compromise spots from the other side [50]. Refs. [51,52] respectively considered the security problems in the attackers' perspective and from the viewpoint of the misuse cases. While the former one proposed a persona methodology to understand the complex ways attackers might work, the latter one specified a sequences of actions to be avoided to prevent various threats.

2.2. Quantitative Security Methods

While qualitative models identify the threats in a descriptive language, quantitative methods are used to derive numerically description for security properties. Rather than assessing the executed security policies at the management level [53], the quantitative models referred to in this paper concern the operational aspects of security. It aims to measure the level of threats of implemented systems during operation. Verendel in [33] surveyed numbers of different quantitative methods to evaluate if security can be represented quantitatively. The quantitative methods are reviewed with a taxonomy including the parameters such as perspectives, targets, assumptions, and validation. The conclusion pointed out that quantified security is a weak hypothesis and can be hardly validated for most cases. However, quantification modeling is still a fundamental topic since it is worthwhile for risk assessment and management. Thus, there are numerous research efforts to explore quantitative methods on threat modeling.

The Common Vulnerability Scoring System (CVSS) is a numerical method that provides a scoring system to evaluate vulnerabilities and their severity [54]. It is composed of three metric groups: Base, Temporal, and Environmental, with a set of elements, which reflect threats in each [55]. A CVSS score is computed with a provided formula combining all possible metrics, which can be obtained from a vulnerability look-up table. There is an online calculator available for the computation of the score. The CVSS was developed for software vulnerabilities and now it has been adapted for cyber-physical platforms.

Attack trees are graphical representations to show possible attacks with a tree structure. The root of the tree is the attackers' goal. The means to achieve the goal are denoted by the leaf nodes of the tree and they are connected by logical gates "AND" and "OR" [56]. Attack trees describe the different routes to exploit the vulnerabilities of the system to reach a desired state [57]. They provide a

quantitative basis to calculate the attack potential [58]. Furthermore, attack trees can be used for the designers to decide which actions should be prevented. Thus, there are some exploratory extensions like attack-defense trees or the integration of countermeasures in the attack tree [34]. A quantitative model of attack tree is presented in [59] to present the intrusion process. The quantitative analysis of attacker behavior was performed by identifying the probability of different attack phases according to the empirical data collected from intrusion experiments.

In addition, there are some stochastic methods to quantify security. In [60], a method is proposed to build the security model with existing tools for reliability. It suggests viewing the threat of a system as a system failure. A Markov model is used to quantify the vulnerabilities with the probability of potential attacks. The dynamic state transition is considered with the specified detecting probabilities to estimate the security such as availability of an embedded system. An automotive system, namely a cooperative adaptive cruise control system, is used to illustrate the analysis. The security attributes of an intrusion tolerant system are assessed quantitatively in [61]. The general probability distribution functions are identified to describe the attacker behavior and the system's response. The probability of security failure is computed to demonstrate the violation impacts of different security attributes.

When the systems become more complex, the interdependences among their components are denser. Thus, the methods of the threat modeling are needed to be evolved. A hybrid method made of three types of threat modeling methods is proposed in [62]. The attack trees are built according to the threat categories of STRIDE. Then the attack likelihood of the tree components are calculated with CVSS method. The method is validated with a case study of railway communications network.

The qualitative and quantitative threat modeling methods reviewed above offer a valuable foundation for automotive security modeling. The combination of these methods becomes a common tendency in applications like automotive system and they inspired the development of the automotive security model.

3. Automotive Security Models

As the intelligent car-networking represents the new generation of the vehicular trend, security plays a more and more important role in automotive industry. Unlike IT security, the security of the automotive system can have an effect on the physical environment directly. Therefore, several research projects for security in transport systems were funded and conducted over the last decade. The projects like PRESERVE (preparing secure vehicle-to-X Communication systems), EVITA (E-safety vehicle intrusion protected applications) and OVERSEE (open vehicular secure platform) were launched to study how to ensure the security of the intelligent transport system by European Commission. The objectives of PRESERVE is to design a scalable security subsystem for the communication of ITS. It aimed to secure the V2X (vehicle to everything) communication and protect the data being abused by malicious attackers. The performance and the cost are also considered for the product deployment in close-to-market implementation [63]. EVITA focused on the trustworthy intra-vehicular communication in order to protect the sensitive data, which are transferred inside a vehicle [64]. The goal of EVITA is to design a secure automotive on-board architecture. The security requirements are specified after analyzing the relevant use cases and the threat scenarios. EVITA proposed hardware security modules as trust anchors for automotive controllers to fulfill the security requirements. To meet the demand of information and communication management for vehicular applications, OVERSEE targeted to realize an open vehicular IT platform [65]. Based on the architecture of the platform, the applications are deployed in a secure and dependable way to avoid interfering with the functionality and safety of the vehicle.

Moreover, some standardization activities are carried out to address and enforce the security aspects for automotive industry [66]. Some security standards for vehicles have been developed such as SAE J3061 [67] and ISO 20078 [68]. Some are still under development like ISO/SAE 21434 [69], whose progress is reported in [70]. In August of 2020, the UNECE WP.29 (the UN Economic Commission for Europe and the World Forum for Harmonization of Vehicle Regulations) released an exposure draft

of uniform provisions. If it is passed, the member countries will be regulated to implement automotive cybersecurity practices and the cybersecurity management systems from January of 2021 [71].

The standards and the framework projects provide groundwork for in-depth study. They allow for supports for the applications in the field of automotive security. For the development of modern vehicles, rigorous security engineering is required as well as safety engineering [72]. An overview on how to apply security testing technologies to automotive engineering is conducted in [73]. Five techniques that are commonly used for automotive engineering are identified and classified according to the applications of different vehicle lifecycle phases and architecture layers. This paper addressed the need to develop testing methods to combine safety aspects for future work. As the security is brought up later than safety in automotive development, how to integrate them into the existing lifecycle is discussed in [74]. The SAE J3061 suggests some interaction points between safety and security engineering during development processes [75]. In [76], a process to integrate the properties of safety and security through automotive system development is proposed and illustrated with the use case of an electronic steering column lock system. Dürrwang et al. adapted the safety hazards analysis method with security guide-words in [77]. It is used to identify the threats and security requirements during the safety analysis. In addition, there are several researches performed to adapt the safety models with security characteristics for system analysis, such as the model of Failure Mode, Vulnerabilities and Effects Analysis (FMVEA) [78], and the model of Combined Harm Assessment of Safety and Security for Information Systems (CHASSIS) [79]. Unlike [80], this paper focuses on the perspectives of automotive security engineering—only the threat models originally designed for automotive security with independent inputs and outputs are considered. Thus, the adapted safety models are out of the scope of the discussion.

3.1. Security Modeling Methods for Automotive Industry

Since the outputs of threat models identify the potential attacks and the corresponding mitigation, modeling and assessing the security risks are demanded at the first stage of the design [81]. Several automotive security modeling methods are proposed for automotive engineering [82]. The J3061 Appendix A specifies some methods and techniques including the approach that originated from the framework project such as EVITA [64] and standards such as European Telecommunications Standards Institute (ETSI) Threat Vulnerability, and implementation Risk Analysis (TVRA) standard [83]. In this section, we review the security risk analysis approaches, which are widely used by automotive industrial organizations and compare them from different aspects. It aims to provide hints for automotive engineer to better understand the security models.

The literature survey of the references on automotive security modeling was conducted and five representative methods for the subject were found. The modeling methods are introduced and their characteristics analyzed in the following section.

3.1.1. EVITA

A security process is described in EVITA project and a security model proposed to analyze the risks of a vehicular IT security system in [84]. The threats are investigated and modeled from the dark-side scenarios. The security requirements are derived based on a set of use cases. Since the risk is determined by the probability of a successful attack and the damage effects caused by the attack, the proposed method took both of these two factors into account. It calculated the attack potential by using the Common Methodology for Information Technology Security Evaluation (CEM) [85]. The CEM method is used for the Common Criteria for Information Technology Security Evaluation (CC) [86]. The likelihood of mounting a successful attack depends on the parameters such as: the available information and the access to the target, the expertise and the tools of the attacks, and the elapsed time the attack takes. The attack paths to achieve attack objectives can be identified with attack trees. Moreover, the paper presented a method to compute the damage potential including four factors as: safety, finance, privacy, and operational performance for the automotive security domain. Among them,

safety is a leading factor to determine the severity. The safety damage potential is valued according to automotive functional safety in [87]. In [88], the authors summarized a risk matrix based on the EVITA method. The risk matrix is designed by taking the example from the railway safety engineering to indicate the risk acceptance values, from negligible to unacceptable [89]. The paper also pointed out that the security threats and attack paths are identified from high-level security objectives, which are derived from the security questionnaires. This risk assessment approach can provide the automotive developers and the manufacturers with a systematic method to balance between costs and security risks and to make justifiable decisions effectively. The presented approach has been applied by some automotive manufacturers and been proven by a few projects. An automotive testing and evaluation methodology is proposed and validated for the case study of automotive Bluetooth interface [90]. The testing is carried out based on the EVITA threat model and the attack trees after the analysis. The main elements and process of the EVITA methodology are summarized and illustrated in Figure 3.

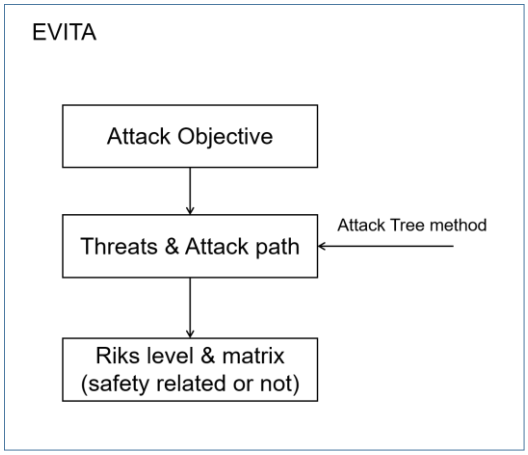

Figure 3. The main elements and process of EVITA method.

3.1.2. HEAVENS

A Swedish project HEAVENS, acronym for "healing vulnerabilities to enhance software security and safety" is funded by VINNOVA to study the methods and tools for security evaluation of automotive electrical and/or electronic systems (E/E) systems [91]. It outlined a modeling framework to analyze threats, assess risks and estimate security levels. In the end, security requirements and security measures can be derived. One of the deliverable of the projects is about automotive security models. It mentioned several security models from other fields and discussed the distinctions of their work from others in [92]. The security attributes are extended from the classic CIA (confidentiality, integrity and availability) triad to eight security attributes for the objectives applied to vehicles. The STRIDE method is used for threat analysis. The assets of the evaluated system are identified and the corresponding threats are analyzed to characterize the relations between threats and vulnerabilities. Similar to the method of EVITA, the threat levels, which reflect the likelihood of the threat, are computed based on the same parameters used in Common Criteria [85]. The impact of the threats is quantified by considering the expected loss of the objectives, which are safety, finance, operation, and privacy & legislation. Then the security level is derived based on the threat level and the impact level to guide the management of the risks for each asset/threat pair. The process of the security model also parallels to automotive safety design [93]. Unlike the EVITA approach to identify all possible attacks from dark scenarios, the HEAVENS approach focuses more on the effects of possible attacks being labeling by a limited number of threat categories. Moreover, the impact of legislation is taken into account in the HEAVENS approach with specific guidelines as well as for the other three objectives from the related standards and regulations in [94–96]. The general process of HEAVENS methodology is described in Figure 4.

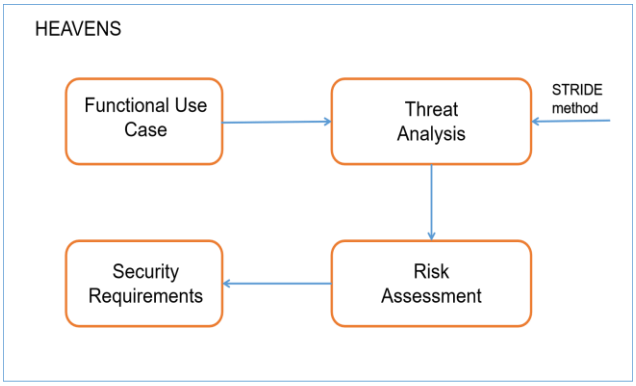

Figure 4. The general process of HEAVENS method.

3.1.3. SINA

A methodology named Security In Networked Automotive (SINA) is presented in [97] to analyze and identify security issues for connected vehicle systems. The car2X scenarios are distinguished according to the communication participants in order to classify the different security threats for chosen problems. Similar to the method of STRIDE, SINA also applied the data flow diagrams to analyze the target system. The potential threats are described with a keyword-based threat classes. Beyond that, SINA defined an entity named communication zone as boundaries in the communication networks and the threats are categorized into seven classes. Besides the threats like tampering, denial of services, and information disclosure listed in STRIDE, SINA employed other specific threat types like "creation of additional data on a communication channel", "modification of transient information as it is exchanged in a data flow", "eavesdropping on a communication channel", and "blocking of a data flow". A model based approach is used to enumerate the threats based on the DFDs. In order to improve the coverage, attack trees are built for the most severe threats to reveal the risks. The method is designed in alignment with an automotive safety development process so that the potential security threats can be identified at the design phase. The risks of the probable effects are evaluated according to the safety severity. Other impacts like privacy and finance are not considered in SINA. The general process of SINA methodology is shown in Figure 5.

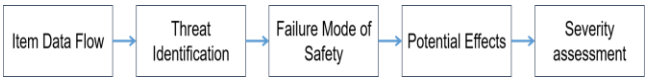

Figure 5. The diagram of SINA method.

3.1.4. SAHARA

A security-aware hazard and risk analysis method (SAHARA) is proposed to combine automotive security and safety analysis for earlier development phases [98]. The threats are classified with STRIDE method on the basis of the hazard analysis and risk assessment (HARA) for safety analysis. Then the impact of the threats is quantified based on three parameters, the resources (R), the knowledge (K) and the threat's criticality (T). A security level is defined based on these factors, as illustrated in Figure 6. Instead of estimating the likelihood of the threats, SAHARA focused on the high criticality of the threats, which would violate the safety goals. If the safety goal is breached, the threats need to be handed over to the safety analysis again. With this step, the completeness of safety analysis can be improved. In the later work presented in [99], they extended their threat and risk analysis from one single car to the whole car fleets. Moreover, the remote attacks are considered. They proposed a new threat classification approach to quantify the threats with five parameters, which are damage potential, reproducibility, exploitability, affected users, and discoverability. A risk priority number is derived by adding the impact factors for each threat. This method has been applied to the use case of automotive battery management.

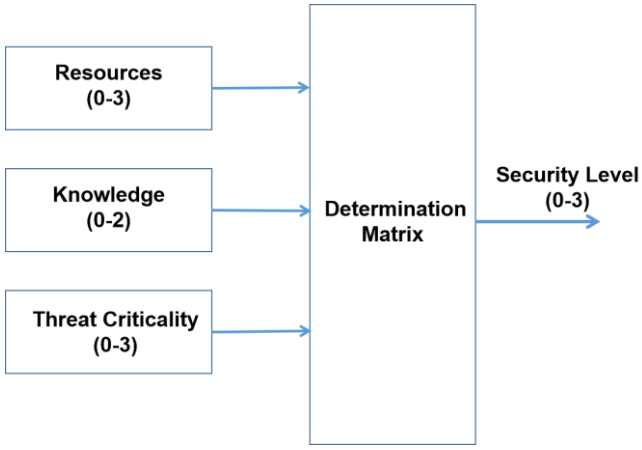

Figure 6. The criteria to derive security level in SHARA method.

3.1.5. TVRA

The European Telecommunications Standards Institute (ETSI) proposed a threat, vulnerability and risk analysis (TVRA) methodology for their standards developers to deal with security issues originally in the telecommunications industry. Then ETSI adapts this method for ITS based on European V2V communication platform [82]. The target of the TVRA method evaluation is used to identify the threats and risks of the communications and services of vehicle-to-vehicle and vehicle-to-roadside network infrastructure in the ITS. The security objectives are evaluated by specifying the CIAAA attributes, namely confidentiality, integrity, availability, authenticity and accountability. The TVRA is a systematic method to identify the assets of the system and the threats the system may be subject to. The classifications of threats are defined as interception, manipulation, denial of service, and repudiation of sending and receiving [100]. The potential of the threats is evaluated based on the parameters like knowledge, time, expertise, opportunity, and equipment. The intensity level of an attack is scaled with three levels from 1 to 3. Then the likelihood and the impact of a risk can be quantified and the security requirements are derived.

3.2. Comparisons of the Automotive Security Modeling Methods

After reviewing the methods, the considerations and variables of these methods are analyzed and compared in order to utilize them appropriately. There are a number of aspects to differentiate the above methods for understanding. First, even though all these methods are designed for the automotive field, each method is studied in its specific application context. Second, the different security attributes are considered as the objectives in the different methods. Third, automotive security modeling methods are inspired by traditional IT security modeling methods so they use the quantitative and qualitative methods for references. Fourth, safety is the principle factor for vehicles and many automotive security modeling methods are designed to align with safety process. Finally, unlike the traditional security modeling methods, risk analysis is a significant part of the method, and the impact elements are considered for the different purposes. In order to clarify these aspects, a comparison is made with respect to the reviewed methods and the results are showed in Table 1.

- Application context: The five modeling methods for automotive security reviewed in the last section are exploited for different usage scope. Some methods targeted on the systems on the vehicle and others took the V2X scenarios into account. For example, the method of the TVRA is designed to evaluate the communications and services of network infrastructure in the ITS.
- Security attributes: The security attributes are the protected targets of the valuable asset. Ordinarily, security is composed of the attributes of confidentiality, integrity and availability. The attributes and security objectives in the context of the automotive systems are extended by adding authenticity, accountability, authorization, privacy, non-repudiation, and freshness. The explanation of the

attributes can be referred to in [83,92]. Each method specifies different security attributes as objectives.

- Reference methods: Since automotive security is developed based on the traditional IT security modeling methods, the approaches to build a threat model used either the quantitative or the qualitative methods. Most of the methods have been reviewed in Section 2.
- Safety related: The safety has always been regarded as a critical engineering concern for the automotive industry. Unlike IT security, the safety process is essential for automotive design.
- Risk impacts: Risk assessment is employed to rank the threat with impact level parameters. It aids to analyze the potential impacts of threats on the stakeholders like user, dealer or manufacturer of the vehicles. The impact factors can be considered such as the safety of the car occupants and road users, the direct and indirect financial cost for the stakeholders, the operational incidents, and the violation of privacy and regulations. These factors assist to derive the security objectives.
- Inputs and outputs: These factors can be used to better understand the models especially from the engineering point of view. The perspectives of analysis are different from the methods, and thus, the required and start point are different. Since the objectives of each method are various, the outcomes are diverse accordingly.

Table 1. Comparison of the automotive security models.

Factors Methods	Application Context	Security Attributes	Reference Methods	Safety-Related	Risk Impact	Inputs & Outputs
EVITA	Vehicular IT systems	Authenticity, Integrity, Authorization, Freshness, Non-repudiation, Privacy, Confidentiality, Availability	Attack tree	YES	Safety, Finance, Privacy, Operation	Input: system use cases and assets Output: attack scenarios, risk levels and security requirements
HEAVENS	Automotive electrical and/or electronic systems	Confidentiality, Availability, Integrity, Authenticity, Authorization, Non-repudiation, Privacy, Freshness	STRIDE	YES	Safety, Finance, Privacy & legislation, Operation	Input: functional use cases Output: risk matrix with threat level and impact level, high-level security requirements
SINA	Connected vehicle systems	Authenticity, Availability, Integrity, Confidentiality, Authorization	STRIDE (with different threat types), Attack tree	YES	Safety	Input: system use cases Output: the list of threats, failure mode, potential effects and severity
SAHARA	Automotive embedded systems	Confidentiality, Availability, Integrity	STRIDE	YES	Safety	Input: the outcomes of safety analysis Output: threat level and security level
TVRA	Communications and services in ITS	confidentiality, integrity, availability, authenticity, accountability	TVRA for Telecommunications	NO	Availability of the network, Customer confidence	Input: ITS target of evaluation Output: risk determination and possible countermeasures

4. Discussion

Security analysis is a fundamental activity in the security engineering process. The purpose of security analysis is to identify threats and assess potential risks, and then to manage the risks with countermeasures. Security models are built up to expound the security characteristics of systems. There are various security models from different domains, other than surveys there are few taxonomies to categorize the existing models. According to different conditions and usages, some systems only

need to enumerate the threats, which may be encountered with given types of threats. Thus, descriptive models, for example STRIDE, are sufficient to discover and analyze the security threats. For other applications, vulnerabilities must be evaluated in a quantitative form to testify its security rating. Numerical or stochastic models such as CVSS are needed to present the security properties.

To overcome the security problems in automotive system development, security models as essential methods are needed to be explored urgently. There are several security models designed or adapted for the automotive industry as introduced in the standard of SAE J3061. However, how to differentiate the existing automotive security models and apply them in a proper and efficient manner are unclear and confused. Hence, the common methods that have been used for vehicles have been reviewed and compared with six fundamental aspects, which are most interested in automotive electronic and electrical (EE) design.

The security models are chosen depending on the different analysis objects. SINA is used for the V2X system of vehicles. The communication between the vehicle and the backend can be analyzed with TVRA method. The automotive electrical and/or electronic systems includes the IT system and the embedded systems. Thus, HEAVENS can be applied to a larger scope than EVITA and SAHARA. STRIDE is utilized by three of the mentioned methods to list the potential threats for the further analysis. The attack paths of dark scenarios are sorted out with attack trees in EVITA. This reflects one of the major differences of EVITA from the other methods, that is, EVITA starts the analysis from the attacker's point of view, while other methods are from the designer's point of view.

Moreover, the qualitative and quantitative methods from traditional IT security are referenced in the automotive security models. Qualitative methods are used as systematic tools to investigate and state the security threats in a descriptive language. Three of the listed automotive security models have used STRIDE method to identify the threats. Since STRIDE is well-structured and well applied in IT security, it helps engineers to frame the threats and limit the kinds of threats. The importance of the threat models is to identify the protected goals and the security requirements for the further design in the security process, other than enumerating all the threats. Thus, the qualitative methods are preferred for the automotive security models at this stage. Quantitative modeling methods are used to derive numerical description for security properties. In the method of EVITA, the method of attack tree is used to analyze the potential attacks from the dark scenarios and to calculate the probability of the attack. This also reflects a common fact in the field of security. It is difficult to characterize security in quantitative terms due to the subjective nature of security. Experts' opinions and descriptive forms are often needed. The method of SINA used STRIDE model firstly to derive the threats then used attack trees to determine a minimal set of attacks. Generally, the probabilistic approaches are not well developed and seldom applied in automotive security. Besides the inherent difficulties of assessing the security, the automotive security focuses more on the risk level, which will determine the following actions.

In addition, different security properties are considered for different targets. One of the important objectives of security is to guard the safety functions for vehicles. If the safety is a primary requirement, the above methods except TVRA considered it in the security modeling. To implement the threat modelling for automotive security, the introduction of use cases is required for most methods. For the method of SAHARA, the outcomes of safety analysis are needed as well. The other methods referred safety as an impact factor. They are all designed from the security perspective. Different from the traditional security models, the methods used for automotive security include threat or severity levels for risk determination. These numerical parameters are defined by considering the impact factors, which are typical for the automotive industry. They are different from the quantitative security methods introduced in chapter 2. However, there is still no unified criteria to standardize the risk level to guide the industry. To develop a security assurance level for automobiles is one of the industry's biggest demands currently.

5. Conclusions and Outlook

Security modeling is required within virtually all security design cycles especially for automotive design. The systematic approaches to model threats and rank security risks can be used as the inputs to architectural design for secure systems. To better understand the problem of automobile security, it is necessary to analyze the threat and assess the risk at the beginning of the design. By knowing in-depth the security threats and risks faced by the intelligent connected vehicle, it is conducive to fundamentally cope with the security problems. Moreover, the upcoming automotive security standard underlines the importance for threat modeling and it requires the designers to utilize the suitable methods for modeling. Based on the survey and comparison, the rational choice of proper method can be made for security evaluation in automotive security engineering. Afterwards, the appropriate methods will be derived and applied for the corresponding protected systems and scenarios. Furthermore, the security models for different phases in the lifecycle of automobiles can be investigated. Since the integration and coordination of safety and security in automotive domain are still in exploration, the models combining these two properties deserve further discussions.

Author Contributions: Conceptualization, J.H. and G.H.; methodology, J.H.; investigation and formal analysis, J.H.; resources, J.H. and G.H.; writing—original draft preparation, J.H.; writing—review and editing, J.H. and G.H.; visualization, J.H. and G.H.; supervision, G.H.; project administration, G.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Li, K.; Dai, Y.; Li, S.; Bian, M. State-of-the-art and technical trends of intelligent and connected vehicles. *Automot. Saf. Energy* **2017**, *8*, 1–14. [CrossRef]
2. Pelkmans, L.; Hultén, S.; Cowan, R.; Azkarate, G.; Christidis, A. *Trends in Vehicle and Fuel Technologies: Review of Past Trends*; European Science and Technology Observatory: Seville, Spain, 2003.
3. Greenback, A. The Jeep Hackers Are Back to Prove Car Hacking Can Get much Worse. Available online: https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/ (accessed on 8 January 2016).
4. Anderson, R. Electronic safety and security-new challenges for the car industry. In Proceedings of the 1st Workshop on Embedded Security in Cars (ESCAR), Bochum, Germany, 18–19 November 2003.
5. Miller, C.; Valasek, C. A Survey of Remote Automotive Attack Surfaces. Available online: https://ioactive.com/wp-content/uploads/2018/05/IOActive_Remote_Attack_Surfaces.pdf (accessed on 1 July 2014).
6. Miller, C.; Valasek, C. Remote Exploitation of an Unaltered Passenger Vehicle. Available online: https://ioactive.com/pdfs/IOActive_Remote_Car_Hacking.pdf (accessed on 10 August 2015).
7. Koscher, K.; Czeskis, A.; Roesner, F.; Patel, S.; Kohno, T.; Checkoway, S.; McCoy, D.; Kantor, B.; Anderson, D.; Shacham, H.; et al. Experimental security analysis of a modern automobile. In Proceedings of the IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 16–19 May 2010; pp. 447–462. [CrossRef]
8. Checkoway, S.; McCoy, D.; Kantor, B.; Anderson, D.; Shacham, H.; Savage, S.; Koscher, K.; Czeskis, A.; Roesner, F.; Kohno, T. Comprehensive experimental analyses of automotive attack surfaces. In Proceedings of the 20th USENIX Conference on Security, San Francisco, CA, USA, 8–12 August 2011.
9. King, J.D. Passive Remote Keyless Entry System. U.S. Patent US623,633,3B1, 22 May 2001.
10. Francillon, A.; Danev, B.; Capkun, S. Relay attacks on passive keyless entry and start systems in modern cars. In Proceedings of the Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, 6–9 February 2011. [CrossRef]
11. Verdult, R.; Garcia, F.D.; Balasch, J. Gone in 360 seconds: Hijacking with Hitag2. In Proceedings of the 21st 5USENIX6 Security Symposium (5USENIX6 Security 12), Bellevue, WA, USA, 8–10 August 2012; pp. 237–252.
12. Verdult, R.; Garcia, F.D.; Ege, B. Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer. In Proceedings of the USENIX Security Symposium, Washington, DC, USA, 14–16 August 2013; pp. 703–718.

13. Eisenbarth, T.; Kasper, T.; Moradi, A.; Paar, C.; Salmasizadeh, M.; Shalmani, M.T.M. On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoq Code Hopping Scheme. In *Advances in Cryptology-CRYPTO 2008*; Wagner, D., Ed.; Springer: Berlin/Heidelberg, Germany, 2008; Volume 5157, pp. 203–220. [CrossRef]
14. Courtois, N.T.; Bard, G.V.; Wagner, D. Algebraic and Slide Attacks on KeeLoq. In *Fast Software Encryption*; Nyberg, K., Ed.; Springer: Berlin/Heidelberg, Germany, 2008; Volume 5086, pp. 97–115. [CrossRef]
15. Hoppe, T.; Kiltz, S.; Dittmann, J. Security Threats to Automotive CAN Networks-Practical Examples and Selected Short-Term Countermeasures. In *Computer Safety, Reliability, and Security*; Harrison, M.D., Sujan, M.A., Eds.; Springer: Berlin/Heidelberg, Germany; New York, NY, USA, 2008; Volume 5219, pp. 235–248. [CrossRef]
16. Woo, S.; Jo, H.J.; Lee, D.H. A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN. *IEEE Trans. Intell. Transp. Syst.* **2014**, *16*, 993–1006. [CrossRef]
17. Foster, I.D.; Prudhomme, A.; Koscher, K.; Savage, S. Fast and Vulnerable: A Story of Telematic Failures. In Proceedings of the Workshop on Offensive Technologies (WOOT), Washington, DC, USA, 10–11 August 2015.
18. Mahaffey, K. Hacking a Tesla Model S: What We Found and What We Learned. Available online: https://blog.lookout.com/hacking-a-tesla (accessed on 5 August 2015).
19. Spill, D.; Bittau, A. BlueSniff: Eve Meets Alice and Bluetooth. In Proceedings of the first USENIX workshop on Offensive Technologies (WOOT 07), Berkeley, CA, USA, 6–10 August 2007; pp. 1–10.
20. Ground Vehicle Standard J3016_201806. *Taxonomy and Definitions for Terms Related to on-Road Motor Vehicle Automated Driving Systems*; SAE International: Warrendale, PA, USA, 2018.
21. Sommer, F.; Durrwang, J. IEEM-HsKA/AAD: Automotive Attack Database (AAD). Available online: https://github.com/IEEM-HsKA/AAD (accessed on 16 April 2019).
22. Eykholt, K.; Evtimov, I.; Fernandes, E.; Li, B.; Rahmati, A.; Xiao, C.; Prakash, A.; Kohno, T.; Song, D. Robust Physical-World Attacks on Deep Learning Models. Available online: http://arxiv.org/pdf/1707.08945v5 (accessed on 10 April 2018).
23. Petit, J.; Stottelaar, B.; Feiri, M.; Kargl, F. Remote attacks on automated vehicles sensors: Experiments on camera and lidar. In Proceedings of the Black Hat Europe 2015, Amsterdam, The Netherlands, 10 November 2015.
24. Sitawarin, C.; Bhagoji, A.N.; Mosenia, A.; Chiang, M.; Mittal, P. DARTS: Deceiving Autonomous Cars with Toxic Signs. Available online: http://arxiv.org/pdf/1802.06430v3 (accessed on 31 May 2018).
25. Upstream Security Ltd. Smart Mobility Cyber Attacks Repository. Available online: https://www.upstream.auto/research/automotivecybersecurity/ (accessed on 13 August 2020).
26. Ring, M.; Dürrwang, J.; Sommer, F.; Kriesten, R. Survey on vehicular attacks—Building a vulnerability database. In Proceedings of the 2015 IEEE International Conference on Vehicular Electronics and Safety (ICVES), Yokohama, Japan, 5–7 November 2015; pp. 208–212. [CrossRef]
27. Sommer, F.; Dürrwang, J.; Kriesten, R. Survey and Classification of Automotive Security Attacks. *Information* **2019**, *10*, 148. [CrossRef]
28. Myagmar, S.; Lee, A.J.; Yurcik, W. Threat modeling as a basis for security requirements. In Proceedings of the IEEE Symposium on Requirements Engineering for Information Security (SREIS), Paris, France, 29 August 2005.
29. Lee, E.A. Cyber Physical Systems: Design Challenges. In Proceedings of the 11th IEEE Symposium onObject/Component/Service-Oriented Real-Time Distributed Computing (ISORC), Orlando, FL, USA, 5–7 May 2008; pp. 363–369. [CrossRef]
30. Dykstra, J. *Essential Cybersecurity Science—Build, Test, and Evaluate Secure Systems*, 1st ed.; O'Reilly: Sebastopol, CA, USA, 2015.
31. Fabian, B.; Gurses, S.; Heisel, M.; Santen, T.; Schmidt, H. A comparison of security requirements engineering methods. *Requir. Eng.* **2010**, *15*, 7–40. [CrossRef]
32. Ma, Z.; Schmittner, C. Threat modeling for automotive security analysis. *Adv. Sci. Technol. Lett.* **2016**, *139*, 333–339. [CrossRef]
33. Verendel, V. Quantified security is a weak hypothesis: A Critical Survey of Results and Assumptions. In Proceedings of the 2009 Workshop on New Security Paradigms Workshop, Oxford, UK, 8–11 September 2009; pp. 37–49.
34. Pietre-Cambacedes, L.; Bouissou, M. Cross-fertilization between safety and security engineering. *Reliab. Eng. Syst. Saf.* **2013**, *110*, 110–126. [CrossRef]

35. Ross, S.T. Computer security: A practical definition. In *Unix System Security Tools*; Mcgraw-Hill: New York, NY, USA, 1999; pp. 15–26.
36. Tomas, O. A Structured Approach to Computer Security. Technical Report No. 122. 1992. Available online: https://research.chalmers.se/en/publication/166411 (accessed on 11 November 2020).
37. *Simson Garfinkel and Gene Spafford, Practical UNIX & Internet Security*, 2nd ed.; O'Reilly: Sebastopol, CA, USA, 1996.
38. Zalewski, J.; Drager, S.; McKeever, W.; Kornecki, A.J. Threat modeling for security assessment in cyberphysical systems. In Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop (CSIIRW 13), Oak Ridge, TN, USA, 8–10 January 2013; Volume 10, pp. 1–4. [CrossRef]
39. Jonsson, E. Towards an integrated conceptual model of security and dependability. In Proceedings of the 1st IEEE International Conference on Availability, Reliability and Security, Vienna, Austria, 20–22 April 2006; pp. 646–653. [CrossRef]
40. Felderer, M.; Katt, B.; Kalb, P.; Jurjens, J.; Ochoa, M.; Paci, F.; Tran, L.M.S.; Tun, T.T.; Yskout, K.; Scandariato, R.; et al. Evolution of security engineering artifacts: A state of the art survey. *Int. J. Secur. Softw. Eng.* **2014**, *5*, 48–98. [CrossRef]
41. Shevchenko, N.; Chick, T.A.; O'Riordan, P.; Scanlon, T.P.; Woody, C. *Threat Modeling: A Summary of Available Methods*; SEI Carnegie Mellon University: Pittsburgh, PA, USA, 2018. [CrossRef]
42. Swiderski, F.; Snyder, W. *Threat Modeling (Microsoft Professional)*; Microsoft Press: California, CA, USA, 2004; pp. 238–246.
43. Shostack, A. Experiences threat modeling at Microsoft. In Proceedings of the Modeling Security Workshop, Lancaster, UK, 4–5 October 2008.
44. Deng, M.; Wuyst, K.; Scandariato, R.; Preneel, B.; Joosen, W. A privacy threat analysis framework supporting the elicitation and fulfillment of privacy requirements. *Requir. Eng.* **2011**, *16*, 3–32. [CrossRef]
45. LINDDUN. Privacy Threat Modeling. Available online: https://distrinet.cs.kuleuven.be/software/linddun/index.php (accessed on 26 March 2020).
46. Wuyts, K.; Joosen, W. *Linddun Privacy Threat Modeling: A Tutorial*; linddun: Leuven, Belgium, 2015.
47. Cooper, S.; Nickell, C.; Piotrowski, V.; Oldfield, B.; Abdallah, A.; Bishop, M.; Caelli, B.; Dark, M.; Hawthorne, E.K.; Hoffman, L.; et al. An exploration of the current state of information assurance education. *ACM SIGCSE Bull.* **2009**, *41*, 109–125. [CrossRef]
48. Ponikwar, C.; Hof, H.J.; Wischhof, L. Towards a High-Level Security Model for Decision Making in Autonomous Driving. In Proceedings of the ACM Chapters Computer Science in Cars Symposium (CSCS), Munich, Germany, 6 July 2017; pp. 1–4.
49. Cleland-Huang, J. How well do you know your personae non gratae? *IEEE Softw.* **2014**, *31*, 28–31. [CrossRef]
50. Mead, N.; Shull, F.; Vennuru, K.; Villadsen, O. *A Hybrid Threat Modeling Method*; Carnegie Mellon University: Pittsburgh, PA, USA, 2018.
51. Tariq, A.M.; Brynielsson, J.; Artman, H. Framing the Attacker in Organized Cybercrime. In Proceedings of the European Intelligence and Security Informatics Conference (EISIC), Odense, Denmark, 22–24 August 2012; pp. 30–37. [CrossRef]
52. Sindre, G.; Opdahl, A.L. Eliciting security requirements with misuse cases. *Requir. Eng.* **2005**, *10*, 34–44. [CrossRef]
53. Zalewski, J.; Drager, S.; McKeever, W.; Kornecki, A.J. Can we measure security and how? *ACM Int. Conf. Proc. Ser.* **2013**, *1*, 1–4. [CrossRef]
54. Common Vulnerability Scoring System v3.1: Specification Document. Available online: https://www.first.org/cvss/v3.1/specification-document (accessed on 5 October 2020).
55. Common Vulnerability Scoring System v3.1: User Guide. Available online: https://www.first.org/cvss/v3.1/user-guide (accessed on 5 October 2020).
56. Schneier, B. Attack trees: Modeling security threats. *Dr. Dobbs J.* **1999**, *12*, 9–21.
57. Sheyner, O.; Haines, J.; Jha, S.; Lippmann, R.; Wing, J. Automated generation and analysis of attack graphs. In Proceedings of the IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 12–15 May 2002; pp. 273–284.
58. Moore, A.P.; Ellison, R.J.; Linger, R.C. *Attack Modeling for Information Security and Survivability (CMU/SEI-2001-TN-001)*; Carnegie Mellon University: Pittsburgh, PA, USA, 2001. [CrossRef]

59. Jonsson, E.; Olovsson, T. A quantitative model of the security intrusion process based on attacker behavior. *IEEE Trans. Softw. Eng.* **1997**, *23*, 235–245. [CrossRef]
60. Kornecki, A.; Zalewski, J.; Stevenson, W.F. Availability assessment of embedded systems with security vulnerabilities. In Proceedings of the 34th Annual IEEE software Engineering Workshop, Limerick, Ireland, 20–21 June 2011; pp. 42–47. [CrossRef]
61. Madan, B.B.; Gogeva-Popstojanova, K.; Vaidyanathan, K.; Trivedi, K.S. Modeling and quantification of security attributes of software systems. In Proceedings of the International Conference on Dependable Systems and Networks, Bethesda, MD, USA, 23–26 June 2002; pp. 505–514. [CrossRef]
62. Potteiger, B.; Martins, G.; Koutsoukos, X. Software and attack centric integrated threat modeling for quantitative risk assessment. In Proceedings of the Symposium and Bootcamp on the Science of Security, Pittsburgh, PA, USA, 19–21 April 2016; pp. 99–108. [CrossRef]
63. PRESERVE Project. Preparing Secure V2X Communication Systems (PRESERVE). Available online: http://www.preserveproject.eu/ (accessed on 5 October 2020).
64. EVITA Project. E-safety Vehicle Intrusion Protected Applications (EVITA). Available online: http://www.evitaproject.org/ (accessed on 5 October 2020).
65. OVERSEE Project. Open Vehicular Secure Platform (OVERSEE). Available online: https://www.oversee-project.com/ (accessed on 5 October 2020).
66. Ur-Rehman, O.; Zivic, N.; Ruland, C. An Overview of Automotive Security Standards. Available online: http://docs.mipro-proceedings.com/iss/03_iss_5618.pdf (accessed on 5 October 2020).
67. SAE J3061. *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems*; SAE International: Warrendale, PA, USA, 2016.
68. ISO/TR 20078-4. *Road Vehicles—Extended Vehicle (ExVe) 'Web Services'*; ISO/TC 22/SC 31 Data Communication; Technical Committee: Geneva, Switzerland, 2019.
69. ISO/SAE DIS 21434. *Road Vehicles—Cybersecurity Engineering*; ISO/TC 22/SC 32 Electrical and Electronic Components and General System Aspects; Technical Committee: Geneva, Switzerland, 2020.
70. Schmittner, C.; Ma, Z. Status of the Development of ISO/SAE 21434. In Proceedings of the 25th European Conference, EuroSPI 2018, Bilbao, Spain, 5–7 September 2018. [CrossRef]
71. Burkacky, O.; Deichmann, J.; Klein, B.; Pototzky, K.; Scherf, G. *Cybersecurity in Automotive, Mastering the Challenge*; McKinsey & Company: New York, NY, USA, 2020.
72. Schmittner, C.; Ma, Z. Towards a framework for alignment between automotive safety and security standards. In Proceedings of the 34th International Conference on Computer Safety, Reliability, and Security, Delft, The Netherlands, 23–25 September 2015; pp. 133–143. [CrossRef]
73. Pekaric, I.; Sauerwein, C.; Felderer, M. Applying Security Testing Techniques to Automotive Engineering. In Proceedings of the ARES'19: 14th International Conference on Availability, Reliability and Security, Canterbury, UK, 26–29 August 2019; pp. 1–10. [CrossRef]
74. Schoitsch, E.; Schmittner, C.; Ma, Z.; Gruber, T. The need for safety and cybersecurity co-engineering and standardization for highly automated automotive vehicles. In *Advanced Microsystems for Automotive Applications 2015*; Schulze, T., Müller, B., Meyer, G., Eds.; Springer: Berlin/Heidelberg, Germany, 2016; pp. 251–261. [CrossRef]
75. Schmittner, C.; Ma, Z.; Reyes, C.; Dillinger, O.; Puschner, P. Using SAE J3061 for Automotive Security Requirement Engineering. In Proceedings of the 35th International Conference on Computer Safety, Reliability, and Security, Trondheim, Norway, 20–23 September 2016. [CrossRef]
76. Macher, G.; Messnarz, R.; Armengaud, E.; Riel, A.; Brenner, E.; Kreiner, C. Integrated Safety and Security Development in the Automotive Domain. In Proceedings of the SAE International WCX™ 17: SAE World Congress Experience, Detroit, MI, USA, 4–6 April 2017. [CrossRef]
77. Dürrwang, J.; Beckers, K.; Kriesten, R. A Lightweight Threat Analysis Approach Intertwining Safety and Security for the Automotive Domain. In Proceedings of the SAFECOMP 2017: 36th International Conference on Computer Safety, Reliability, and Security, Trento, Italy, 12–15 September 2017; pp. 305–319. [CrossRef]
78. Schmittner, C.; Gruber, T.; Puschner, P.; Schoitsch, E. Security Application of Failure Mode and Effect Analysis (FMEA). In Proceedings of the SAFECOMP 2014: 33rd International Conference on Computer Safety, Reliability, and Security, Florence, Italy, 10–12 September 2014; Volume 8666, pp. 310–325. [CrossRef]

79. Raspotnig, C.; Karpati, P.; Katta, V. A Combined Process for Elicitation and Analysis of Safety and Security Requirements. In *Enterprise, Business-Process and Information System*; Bider, I., Halpin, T.A., Krogstie, J., Nurcan, S., Ukor, R., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; Volume 113, pp. 347–361. [CrossRef]
80. Macher, G.; Armengaud, E.; Brenner, E.; Kreiner, C. A Review of Threat Analysis and Risk Assessment Methods in the Automotive Context. In *Computer Safety, Reliability, and Security*; Skavhaug, A., Guiochet, J., Bitsch, F., Eds.; Springer: Berlin/Heidelberg, Germany, 2016; Volume 9922, pp. 130–141. [CrossRef]
81. Eichler, J.; Angermeier, D. Modular risk assessment for the development of secure automotive systems. In Proceedings of the 31st VDI/VW joint conference Automotive Security, Wolfsburg, Germany, 21–22 October 2015.
82. Alberts, C.J.; Behrens, S.G.; Pethia, R.D.; Wilson, W.R. *Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVESM) Framework, Version 1.0*; Carnegie Mellon University: Pittsburgh, PA, USA, 1999. [CrossRef]
83. European Telecommunication Standards Institute (ETSI). *Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)*; ETSI: Sophia Antipolis Cedex, France, 2017.
84. Alastair, R.; Benjamin, W.; Sajid, I.; Roudier, Y.; Michael, F.; Timo, L.; Fuchs, A.; Gurgens, S.; Henninger, O.; Roland, R.; et al. *Deliverable D2.3: Security Requirements for Automotive on-Board Networks Based on Dark-Side Scenarios (EVITA, E-Safety Vehicle Intrusion Protected Applications)*; East Valley Institute of Technology (EVIT): Mesa, AZ, USA, 2009. [CrossRef]
85. Common Methodology for Information Technology Security Evaluation (CEM v3.1). Available online: https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf (accessed on 5 October 2020).
86. *ISO/IEC 15408: Information Technology-Security Techniques-Evaluation Criteria for IT Security*; Technical Committee: Geneva, Switzerland, 2009.
87. *ISO 26262, Road Vehicles—Functional Safety*; Technical Committee: Geneva, Switzerland, 2018.
88. Wolf, M.; Scheibel, M. A systematic approach to a quantified security risk analysis for vehicular IT systems. *Automot. Saf. Secur.* **2012**, *210*, 195–210.
89. British Standard EN 501261999. *Railway Applications—The Specification and Demonstration of Reliability, Availability, Maintainability, and Safety (RAMS)*; European Committee for Eiectrotechnical Standardization: Brussels, Belgium, 1999.
90. Cheah, M.; Shaikh, S.A.; Bryans, J.; Wooderson, P. Building an automotive security assurance case using systematic security evaluations. *Comput. Secur.* **2018**, *77*, 360–379. [CrossRef]
91. Olovsson, T. HEAling Vulnerabilities to ENhance Software Security and Safety (HEAVENS) Project. Available online: https://research.chalmers.se/en/project/5809 (accessed on 5 October 2020).
92. Islam, M.; Sandberg, C.; Bokesand, A.; Olovsson, T.; Brober, H.; Kleberger, P.; Lautenbach, A.; Hansson, A.; Soderberg-Rivkin, A. *P.Kadhirvelan, S. Deliverable D2: Security Models (Version 2.0)*; Vinnova/FFI (Fordonsutveckling/Vehicle Development): Göteborg, Sweden, 2016.
93. Islam, M.; Lautenbach, A.; Sandberg, C.; Olovsson, T. A risk assessment framework for automotive embedded systems. In Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security, Xi'an, China, 31 May 2016; pp. 3–14.
94. *Federal Office for Information Security (BSI) Standard 100-4*; Version 1.0; Information Security Management System (ISMS): Bonn, Germany, 2009.
95. Automotive Industry Action Group (AIAG). *Potential Failure Mode and Effects Analysis (FMEA)*, 4th ed.; AIAG: Michigan, Mi, USA, 2008.
96. Federal Office for information security (BSI). *Privacy Impact Assessment Guideline*; BSI: Bonn, Germany, 2011.
97. Schmidt, K.; Troger, P.; Kroll, H.M.; Bunger, T.; Krueger, F.; Neuhaus, C. Adapted development process for security in networked automotive systems. *SAE Int. J. Passeng. Cars Electron. Electr. Syst.* **2014**, *7*, 516–526. [CrossRef]
98. Macher, G.; Sporer, H.; Berlach, R.; Armengaud, E.; Kreiner, C. SAHARA: A security-aware hazard and risk analysis method. In Proceedings of the Design, Automation Test in Europe Conference Exhibition (DATE), Grenoble, France, 9–13 March 2015; pp. 621–624. [CrossRef]

99. Macher, G.; Armengaud, E.; Brenner, E.; Kreiner, C. Threat and risk assessment methodologies in the automotive domain. *Procedia Comput. Sci.* **2016**, *83*, 1288–1294. [CrossRef]
100. European Telecommunication Standards Institute (ETSI). *Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN)*; Methods and Protocols, Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis; ETSI: Sophia Antipolis Cedex, France, 2011.