Open Problems when Mapping Automotive Security Levels to System Requirements

Open Problems when Mapping Automotive Security Levels to System Requirements

Thomas Rosenstatter and Tomas Olovsson
Department of Computer Science and Engineering, Chalmers University of Technology, Gothenburg, Sweden
{*thomas.rosenstatter, tomas.olovsson*}*@chalmers.se*

Keywords: Vehicular Security, System Security, Requirements Engineering, Security Classification.

Abstract: Securing the vehicle has become an important matter in the automotive industry. The communication of vehicles increases tremendously, they communicate with each other and to the infrastructure, they will be remotely diagnosed and provide the users with third-party applications. Given these areas of application, it is evident that a security standard for the automotive domain that considers security from the beginning of the development phase to the operational and maintenance phases is needed. Proposed security models in the automotive domain describe how to derive different security levels that indicate the demand on security, but do not further provide methods that map these levels to predefined system requirements nor security mechanisms. We continue at this point and describe open problems that need to be addressed in a prospective security framework for the automotive domain. Based on a study of several safety and security standards from other areas as well as suggested automotive security models, we propose an appropriate representation of security levels which is similar to, and will work in parallel with traditional safety, and a method to perform the mapping to a set of predefined system requirements, design rules and security mechanisms.

1 INTRODUCTION

New technologies and functionalities are constantly introduced to vehicles. Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication enables vehicles to share information with each other and send warnings, e. g., about roadworks and traffic jams. Remote diagnostics is performed by vehicle manufacturers and licensed repair shops, and platforms for third-party applications in vehicles are also provided. As a consequence of this ongoing transition, a security standard is crucial in order to secure vehicles against modifications, hacks, and espionage.

The exposure of serious vulnerabilities underlines the need for security in the automotive domain. The attack surface of modern vehicles was analysed by [Checkoway et al., 2011] and they demonstrated vulnerabilities in the Tire-Pressure Monitoring System, media-player, OBD-II port, and Bluetooth. Furthermore, [Miller and Valasek, 2014] provide a survey of attack surfaces of several vehicle models and [Yan, 2015] presents vulnerabilities in connected vehicles using different attack vectors.

A systematic approach dealing with the aforementioned security threats is necessary, and in addition, an automotive security standard is needed to harmonise the hardware and software security requirements between the vehicle manufacturers and the suppliers. This becomes evident when vehicle manufacturers get more dependent on their suppliers since the complexity of third-party modules is increasing and the modules are required to be reliable and secure. A security framework which also contains a mapping to system requirements and design rules containing guidelines describing how these demands can be fulfilled, increases the efficiency during the development and testing due to the fixed structure and guidance, as well.

The need for such a security standard has also been identified by the industry, which initiated the ISO/SAE AWI 21434 *Road Vehicles – Cybersecurity engineering*. This work item is ongoing and currently under development. Proposed security models, such as EVITA [Henniger et al., 2009] and HEAVENS [Islam et al., 2016], describe methods from identifying threats to classifying them into security levels. Both models focus on the identification of risks and threats, and how to classify them. HEAVENS describes methods to derive application specific requirements, but does not perform a mapping to predefined requirements nor security mechanisms that are required for each security level. EVITA on the other hand lists the

Rosenstatter, T. and Olovsson, T.
Open Problems when Mapping Automotive Security Levels to System Requirements.
In *Proceedings of the 4th International Conference on Vehicle Technology and Intelligent Transport Systems (VEHITS 2018)*, pages 251-260
ISBN: 978-989-758-293-6

results of their risk analysis in [Ruddle et al., 2009], but does not provide a mapping to generic security requirements based on the security level.

Information security is concerned with confidentiality, integrity and availability, which will be later extended according to STRIDE [ISO 15408, 2009, Microsoft Corporation, 2005]. We define security levels similar to [Islam et al., 2016]. Security levels represent the necessity and extent for security measures in a specific function or module. The factors taken into account when deriving the security levels depend on the underlying security model that considers the severity of potential attacks, required expertise to perform the attack, or the impact for the involved parties in case of the attack. We split security requirements in two groups, system requirements and application specific requirements. System requirements are generic security requirements that need to be fulfilled for a certain security level and describe design rules or security functions. Application specific requirements are the result of a threat analysis and include individual requirements that are not covered by system requirements. Security mechanisms are methods to fulfil a requirement, for instance the choice of encryption algorithms to provide confidentiality of information, or use of access control lists to restrict the data flow in the in-vehicle network.

In this paper, we survey proposed security models and acclaimed standards in the area of safety and security, we investigate how these standards or models classify safety and security, and how they perform the transition to system requirements.

Our contributions in this paper are the following:

- A study on safety and security standards, along with proposed security models for the automotive domain.
- Propose methods for how to move forward from unique requirements of individual systems and identified security levels to a set of mandatory system requirements, design rules and security mechanisms and
- show that such requirements should be based on the security level of the function to be implemented.
- We show the benefits with having such a framework in place when dealing with third-party developed functionality.
- We show the challenges and complexity of defining such a framework.

2 BACKGROUND AND RELATED WORK

The difference between safety and security is that safety is about handling malfunctioning behaviour that is caused by random errors. Security threats are caused by an attacker who intentionally wants to modify the system, harm involved people, or gather information. It may be also the case that the owner, who has physical access and unlimited time, slips in the role of an attacker in order to perform unauthorised modifications on the vehicle. The skills of attackers may vary from limited to advanced depending on his knowledge, purpose, and equipment. For these reasons, security involves complex countermeasures. An attacker who has successfully exploited a vulnerability of one vehicle is able to apply the same method to all vehicles of that specific model or even to all vehicles of that manufacturer or supplier depending on the kind of vulnerability [SAE J3061, 2016].

The large attack surface in vehicular security is another difference to safety. Performing Hazard Analysis and Risk Assessment (HARA) on functional safety requires a narrower focus compared to assessing the security of a system. The security assessment of a system requires one to cope with a larger attack surface. For instance, a vehicle that is able to communicate with its infrastructure and cooperate with other vehicles can not only be attacked locally, it can be attacked through this communication channel as well. Moreover, vehicles have Internet access which additionally increases the attack surface. Having a built-in mobile communication unit also enables attacks via SMS and other phone services. In addition to the wireless communication, Checkoway et al. showed other attack vectors, such as an attack through the media-player [ENISA, 2016, Checkoway et al., 2011].

Looking at the different areas shows that safety has been adapted to the specific needs for this area. [ISO 26262, 2011] is the standard for functional safety of road vehicles, [RTCA DO-178, 2011] and [RCTA DO-254, 2000] (software and hardware) are customised for the aeronautics domain, and the railway domain is described in CENELEC EN 50126, CENELEC EN 50128, and CENELEC EN 50128. [Blanquart et al., 2012] perform a comparison of the criticality categories across safety standards in different domains, including the aforementioned standards and the corresponding safety standards for nuclear facilities and space systems. They highlight how these domains differ from each other in terms of structure and guidance throughout the development process.

Security standards exist in many areas, such as programming, industrial automation, and system and

device security. The [SEI CERT C, 2016] Coding Standard, for instance, defines rules for specific programming languages, in this case for C, and uses a classification in levels to indicate the impact of not addressing a certain rule. SEI CERT C shows how certain programming traits have to be implemented in order to be reliable, secure and safe. By following these rules, undefined behaviour that may lead to vulnerabilities will to a large extent be eliminated. The standard ranks each rule with an example and its priority and level. A combination of severity, likelihood and remediation costs results in such a level ranging from 1 to 3. The priorities are directly mapped to the levels.

[NIST SP 800-53r4, 2013] is catalogue of security controls and assessment procedures for information systems. The security controls are split in 18 families, such as Access Control, Incident Response, and Identification and Authentication. Consequently, each family comprises security controls mapped to priority and impact levels (*low*, *medium*, *high*). Security controls are nested, the lowest priority level has to be implemented first and controls with higher priority have to be implemented in addition to the controls with a lower priority level.

Security models for the automotive domain have been proposed by various researchers. [Burton et al., 2012] suggest a method that extends ISO 26262 with security analysis. A combined safety and security development lifecycle is presented by Schmittner et al. in [Schmittner and Ma, 2014, Schmittner et al., 2015]. Burton et al. and Schmittner et al. both focus on the differences between safety and security and how to combine them, but they do not discuss how predefined system requirements or design rules for security can be defined. Common Criteria [ISO 15408, 2009] is a standard for evaluating security properties of systems and devices. The similarities of ISO 26262 and Common Criteria are discussed in [Schmittner and Ma, 2014]. The authors describe the relationship between the Automotive Safety Integrity Levels (ASILs) from ISO 26262 and the Evaluation Assurance Levels (EALs) from Common Criteria according to the strictness and degree of formalism. The SAHARA method presented by [Macher et al., 2015] combines the existing HARA known from ISO 26262 with a security assessing method considering the needed resources and know-how. Macher et al. do not describe a method to derive system requirements based on the resulting security level. The EVITA [Henniger et al., 2009] and HEAVENS [Islam et al., 2016] models describe the procedure on how to derive security levels and how these can be used for requirement engineering, however, they do not perform a mapping to system requirements as we propose.

Guidelines for cybersecurity with respect to the automotive domain are [SAE J3061, 2016] and [ENISA, 2016]. Both guidelines provide good practice examples and recommendations, whereas ENISA limits the scope by excluding autonomous vehicles and V2V communication in their guideline. Another difference is that J3061 sets the focus on the necessary processes and their implementation, while ENISA describes the typical architecture of smart vehicles and possible threats and attacks. J3061 lists Threat, Vulnerabilities, and implementation Risks Analysis (TVRA), which is a threat and risk assessment method developed by ETSI in TS 102 165-1 [ETSI, TS, 2011]. According to J3061, this model is not suited for control and data networks of vehicles, as it was developed specifically for telecommunications networks. These two guidelines for cybersecurity address important subjects, but do not discuss methods for mapping to system requirements nor mechanisms.

3 THE COMPLEXITY IN AUTOMOTIVE SECURITY

Lifetime. The automotive domain differs in many ways from other areas. A vehicle has a lifetime of about 150.000 to 300.000 km [Hawkins et al., 2012]. During this time, the vehicle has to be safe, secure, firmware needs to be updated, the owner may change, and vehicle parts or modules need to be replaced. Discovering a security vulnerability in the vehicle requires a fast reaction and update distribution to the vehicles. Once a severe security problem has been identified, over-the-air updates provide efficient means for distribution as they are much faster than a recall of a certain vehicle model or vehicles with a specific component from a supplier. In addition, over-the-air updates are needed because security requirements 20 years from now are likely to be different from what is designed today, since the expected lifetime from design of security functionality to the expected end of the vehicle lifetime can be as much as 20 – 25 years.

Interplay between safety and security. The safety of the passengers has to be retained in all situations. Fault detection mechanisms have to be designed in such a way that they cannot be exploited by an attacker. For example, the use of redundant modules for increased safety, may open up for attacks where both modules believe the other one is active while it is the attacker who sends the messages.

Compliance to standards. One specific challenge for heavy duty vehicles is the required compliance to

[SAE J1939, 2013]. This standard specifies the exact content of frames that have to be transmitted within the in-vehicle network. To comply, the frames may not be changed and thus encryption mechanisms may not be used. This restriction limits the set of suitable security mechanisms.

Compliance between manufacturers and suppliers. The suppliers will provide modules with more functionalities and may also need to maintain the security of their products. Manufacturers integrate software, and hardware modules from third-party developers and in-house developed modules into a vehicle and thus need to ensure the security and safety of all modules individually and combined. A well-defined framework with strict system requirements for security functions and mechanisms to be used, would simplify the requirement specifications and communications between these two parties.

Maintenance. Authorised workshops need to be able to diagnose the vehicle and replace modules in case of a failure. For this reason, they need to, for instance, be able to handle the change of security keys in an offline and online environment. Authorised devices may also need to be revoked in case of theft.

Alignment with ISO 26262. The harmonisation/alignment with the functional safety standard for road vehicles [ISO 26262, 2011] is important when introducing a new framework for automotive security. ISO 26262 has a high acceptance in the automotive domain and would, for this reason, significantly reduce the time required for introducing such a security framework, because of the already known processes. The question is to which extent it should be harmonised. Strong harmonisation has the advantage of easier integration due to known processes, but it may not be ideal for security due to the fundamental differences to safety.

Guidance. The necessary level of guidance has to be defined. Providing a strict guidance for each requirement may not be feasible or optimal for certain cases. The developers may, for certain security requirements, find other countermeasures that are more suitable. On the other hand, sparse guidance leads to overhead when evaluating security of third-party components and individual solutions may not correspond to best practices.

We address these problems by investigating how standards and other security models handle guidance and propose a method able to cope with the problems listed above.

4 STANDARDS AND MODELS

In this section, we describe standards, models, and approaches that influence the design of safety and security by assigning levels according to a defined scheme. They are all well-known and accepted in their domain or applicable for the automotive area. The insights into how these standards allocate safety or security levels and how they perform the mapping to requirements are further used for our suggested framework. The related standards and models being described in detail are [ISO 26262, 2011], [RTCA DO-178, 2011], EVITA [Henniger et al., 2009], HEAVENS [Islam et al., 2016], Trust Assurance Levels [Kiening et al., 2013], and [IEC 62443, 2013].

First, we describe the purpose of the standards and models followed by a discussion on the number of levels their analysis results in. Next, we discuss the impact of the levels in the design and development of the system and investigate how the standards or models address the relation between requirements and allocated levels. Do they provide strict information about the requirements necessary for each level or is the mapping between the allocated levels and the requirements without guidance?

4.1 Safety Standards

ISO 26262 applies HARA for a system without safety measures by taking the severity, exposure, and the controllability into account. A hazard is defined by ISO 26262 as malfunctioning behaviour that potentially causes harm. After identifying the levels for each class, such as severity and controllability, they are mapped according to a predefined matrix to the ASIL levels. The ASIL levels comprise *QM*, *A*, *B*, *C*, and *D*, where *QM* corresponds to *Quality Management*, i.e., a non-safety relevant event which does not require any further safety consideration in the design and development of the system. Events classified as ASIL D, the highest level, require the highest demand regarding risk reduction. In case a system failure causes several hazards, the highest occurring ASIL rating has to be applied [ISO 26262, 2011].

Next, a safety goal is defined for each hazardous event. The safety goals are subsequently associated with a functional safety concept, which states how the safety goal can be achieved. The next step is to formulate a technical safety concept describing how the functionality is going to be implemented by hardware and software on the system level. The software and hardware safety requirements describe the specific requirements, which will be implemented. The requirements inherit their ASIL level from their

safety goal respectively their parent requirement [ISO 26262, 2011].

ISO 26262 provides guidelines and requirements for each level on system, hardware, software, production, and operation level. In addition to the specified requirements for each ASIL level, this standard also provides three levels of recommendations, no recommendation ($\circ$), recommended ($+$), and highly recommended ($++$). The method *independent parallel redundancy* as a mechanism for error handling at the software architectural level, for instance, is recommended for ASIL C and highly recommended for ASIL D [ISO 26262, 2011].

DO-178 is the safety standard for the aeronautics domain, its categories are called Development Assurance Levels (DAL). The DALs are representing the effects of a failure condition, e. g., catastrophic or hazardous. The five DALs range from A, the most demanding level, to E, which is the equivalent to ASIL QM. A top-level function is mapped to the Function DAL (FDAL) according to a table that associates the failure condition class and the quantitative safety requirement (failures per hour) with the DAL. These top-level functions are decomposed to sub-functions, which are further decomposed to items. It may be the case that a top-level function is divided into more than one sub-function, where one of the sub-functions has a lower or the same DAL as the top-level function. DO-178 also provides guidance, but not to the same extent as ISO 26262 [Blanquart et al., 2012, RTCA DO-178, 2011, RCTA DO-254, 2000].

4.2 Security Models in the Automotive Domain

The HEAVENS and EVITA projects define models to derive security levels. [Henniger et al., 2009] describe a model developed in the EVITA project. [Islam et al., 2016] propose an ISO 26262 compliant model as part of the HEAVENS project. Both models specify how to identify threats and classify them into security levels.

Henniger et al. use attack trees based on use cases as base for the following requirements analysis. The root of the attack tree is the goal of the attack. The sub-levels contain sub-goals that can lead to the goal of the parent node.

A risk assessment is performed for each potential attack. The mapping of the three components, severity (4-component vector), probability of a successful attack, and controllability, is derived from a predefined table which leads to a security risk level. This level is not associated to a single value, it is a 4-component vector describing the security risk level for the elements of the severity vector. The levels for each element are in the range $[0,7]$, where 0 represents no risk and 6 the highest risk. Level 7 and 7+ are used for safety critical threats with controllability $C \geq 3$ and severity *high* [Henniger et al., 2009].

The authors further discuss how the security risk levels can be used to prioritise security requirements. Requirements resulting from the developed use cases and risk assessment are listed in [Ruddle et al., 2009]. Henniger et al. highlight that not only the highest rating should be considered, the number of occurrences in the attack trees has to be considered as well. A lower risk that is seen in several attack trees may have the same importance as a level 5 or higher risk that appears only once in the attack tree [Henniger et al., 2009].

The HEAVENS risk assessment model suggested by Islam et al. describes the workflow for identifying assets and threats (threat analysis), and a method describing how to perform the risk assessment. Islam et al. apply Microsoft's STRIDE model [Microsoft Corporation, 2005] to identify the asset/threat pairs.

The result of the risk assessment is the security level, which is a combination of the threat level and the impact level. The levels for the resulting security level are *QM*, *low*, *medium*, *high*, *critical*. Islam et al. highlight the parallels to ISO 26262. The functional safety requirements derived from the safety goals in ISO 26262 have the same property as the high-level security requirements originating in the asset/threat pair and their corresponding security level. Both are high-level requirements that are independent from the implementation. These requirements are consequently divided into technical security requirements on system level, which further result in hardware and software security requirements.

4.3 Trust Assurance Levels for V2X Communication

The purpose of the Trust Assurance Levels is to classify the security of Vehicle-to-Everything (V2X) communication nodes. [Kiening et al., 2013] provide the minimum requirements for each Trust Assurance Level (TAL) and discuss the benefits of certifying V2X nodes and how to perform the verification of security. The mapping of the TAL is performed according to a predefined table. This table contains the minimum requirements and a description of security implications for each level. The proposed levels are nested and range from 0 to 4. A node with TAL 0 does not have any security measures. With an increasing TAL, the core V2X communication modules and other relevant modules of the node need to be secured.

For instance, TAL 4 requires all involved modules to be protected. Moreover, the authors map the TALs to the EALs of Common Criteria [Kiening et al., 2013].

4.4 Cyber Security Standard - IEC 62443

[IEC 62443, 2013] is a group of security standards for Industrial Automation and Control Systems. Part 3 describes the system security requirements and security levels. The security levels range from 0 to 4 and are further split into Target Security Levels (SL-T), Achieved SLs (SL-A), and Capability SLs (SL-C). A security level of 0 corresponds to no specific requirements for security and level 4 implies the highest demand on security. SL-T is derived from a consequence analysis on a particular system, called zone, and describes the desired security level. During the iterative design phase SL-A and SL-T are compared with each other after every cycle. Components and systems need to provide the SL-C that indicates its capability in regards to the defined security levels. In case that SL-C does not meet the required SL-T, compensating countermeasures have to be implemented [IEC 62443, 2013].

The high-level requirements are named Foundational Requirements (FRs) and consist of seven elements, e. g., system integrity, data confidentiality, and use control. These FRs are consequently broken down into System Requirements (SRs) and Requirement Enhancements (REs). The security level for a specific zone or component does not consist of a single value, it is a 7-component vector describing the security level for each FR. A table in IEC 62443 maps the SRs and REs to the security level of each FR [IEC 62443, 2013].

Equation 1 shows the composition of the Security Levels (SLs) in IEC 62443. Each component listed in this vector refers to a FR. An example shown in IEC 62443-3-3 is the SL-T of a basic process control system zone. It is specified that this zone requires a SL of 3 for the FRs *Restricted data flow* and *Resource availability*. In contrast, measures to provide *Data confidentiality* are not required, as the SL is 0.

Table 1 provides an overview of the reviewed standards and models. It highlights the differences between safety and security. Functional safety standards have five different levels whereas the automotive security models, such as EVITA and HEAVENS, use a more complex representation of security or risk levels. IEC 62443, developed for the security of industrial automation and control systems, classifies security as a 7-component vector with a range of five levels for each element and differs compared to ISO 26262 with respect to how it relates the SLs to requirements.

$$SL = \begin{bmatrix} \text{Identification \& authentication ctrl.} \\ \text{Use control} \\ \text{System integrity} \\ \text{Data confidentiality} \\ \text{Restricted data flow} \\ \text{Timely response to events} \\ \text{Resource availability} \end{bmatrix} = \begin{bmatrix} 2 \\ 2 \\ 0 \\ 1 \\ 3 \\ 1 \\ 3 \end{bmatrix} \quad (1)$$

5 PROPOSED SECURITY LEVELS AND MAPPING

Our previous discussion about the problems of implementing security in vehicular systems followed by a survey of standards and models, are the base for the following suggestion for the number and representation of security levels, and the mapping to system requirements, design rules and security mechanisms. Investigating how established standards and proposed security models define a classification in form of Security Levels (SLs) is important for suggesting an automotive security framework. Additionally, we discuss how to evaluate or even certify the security compliance of a module, and how well our proposed framework is aligned with ISO 26262. We want to highlight that the suggested solutions are a proposal based on the review of several standards and models from safety or other security domains and should provide a recommendation to future research.

5.1 Number of Security Levels

The decision on the number of SLs and the mapping to system requirements strongly depends on the underlying model for risk/threat assessment. Models differ in their composition and weights for parameters, such as expertise to perform the attack, opportunity, and impact level.

Both functional safety standards, ISO 26262 and DO-178, use five levels to classify safety, but security models propose different solutions. The TALs with the focus on V2X communication security use five levels. Two automotive security models propose a more complex classification of security or risk levels. EVITA focusses on the risk of security relevant attacks by representing the risk as a 4-component vector and HEAVENS associates the SLs with a specific asset/threat pair.

Following the HEAVENS approach by using its classification of SLs leads to one level in the range of 0 to 4 for each threat/asset pair, meaning that the

Table 1: Overview of the reviewed Standards in respect to their classification approach.

	ISO 26262	DO-178	IEC 62443	TAL	EVITA	HEAVENS
Field of Application	Safety	Safety	Security	Security	Security	Security
# Security Levels	5	5	5	5	8	5
Representation / vector size	1	1	7	1	4	1[a]
Predefined System Requirements	(✓)[b]	–	✓	✓	–	–

[a] HEAVENS associates each threat/asset pair with a SL.
[b] ISO 26262 provides recommendations for specific methods depending on the SL.

threat violating confidentiality of an individual asset ranges between these levels. Continuing with defining high-level requirements and technical security requirements for each threat/asset pair would only result in more overhead. Instead, we recommend the use of system requirements, which describe the necessary security measures for each type of threat and security attribute and thus provide the developer already with necessary requirements that need to be fulfilled depending on the SL.

The classification of SLs needs to provide sufficient categories to have a distinct separation of the required security measures. Having a wide range of SLs may lead to an overly detailed guidance, which may be inefficient due to the high granularity of requirements and the difficulty to distinguish between the SLs.

Since security needs to address many different aspects or attributes, such as the authenticity of messages and their origin, system integrity, and data confidentiality, it is reasonable to use a vector defining the SL for each component representing one of these areas. The SL of each component is in the range of 0 to 4. Such an approach is described in IEC 62443 and seems to be appropriate for the automotive domain as well, as the representation as a single value may lead to imbalanced security measures. For certain modules or subsystems, it might be necessary to provide data confidentiality, whereas data integrity might be of greatest importance for many other subsystems, hence, it is benefiting to distinguish between such attributes and assign them SLs individually. In addition, a vector representation eases the communication between the parties, as a vector already combines the demanded level of security for each attribute.

Furthermore, we suggest to distinguish between target, achieved and capability SL, as described in IEC 61442. Modules provided by suppliers, or in-house developed modules should be classified according to their security capability (SL-C). This may lead to a more efficient reuse of developed modules, as they are clearly marked with the SL they are capable of. This approach also simplifies the design of the system, since modules and systems can be labelled with their target SL (SL-T) that states the necessary system requirements and design rules.

Describing security as a vector instead of a single value is different to ISO 26262, nevertheless, we believe that it is unavoidable to present security as a structure describing several attributes. As an example, $SL(auth.) = 1$ may require a verification of the new firmware when performing an upgrade, whereas $SL(auth.) = 3$ may require a firmware verification at every start-up and $SL(auth.) = 4$ may additionally require the authenticity of messages sent and received within this particular subsystem. IEC 62443 and other security models also use a vector or other similar approaches and thus support our choice.

5.2 Mapping to Security Requirements and Mechanisms

There are different ways to map SLs to system requirements and security mechanisms. One option is to perform a binary mapping of the SLs, e. g., a system requirement has to or does not have to be fulfilled. An alternative is the introduction of recommendations in combination to the binary mapping, which is a closer approach to ISO 26262. The presentation of the requirements for certain SLs, is another important aspect.

ISO 26262 lists the requirements and recommendations in separate documents, e. g., description for system, hardware and software level. IEC 62443 on the other hand provides a compact overview of the required security measures. The System Requirements (SRs) and Requirement Enhancements (REs) of a Foundational Requirement (FR) are mapped to the SLs. The demands for fulfilling a SL of a FR is reflected in the required SRs and REs. For lower levels, it is sufficient to only fulfil a few requirements, but in order to provide the highest SL, one must fulfil all SRs and REs. This way, it is ensured that also modules or subsystems with lower SLs provide basic methods to

Table 2: Binary Mapping of Security Levels to System Requirements and Requirement Enhancements.

FR 1	0	1	2	3	4
	none	*low*	*medium*	*high*	*critical*
SR 1		•	•	•	•
SR 2			•	•	•
RE 2.1				•	•
RE 2.2					•
SR 3			•	•	•
...					

ensure a specific security attribute. Table 2 illustrates the structure of this approach. It shows which SRs and REs of FR 1 are required for each SL. For instance, SL 1 requires only SR 1, whereas SL 2 requires SR 1, SR 2, and SR 3. Higher levels demand also the RE 2.1 respectively RE 2.1 and RE 2.2.

The FRs and their associated SRs and REs shown in Table 2 still need to be defined. One approach is to use the FRs of IEC 62443 (see Equation 1) as a base and adjust the SRs and REs by incorporating automotive specific requirements which are described in Section 3, e. g., the possibility to exchange vehicle parts in an offline environment (offline distribution of cryptographic keys) and offline diagnostics in a workshop (see Section 3). Another approach we propose is to combine the structure of IEC 62443 with HEAVENS – the FRs are the security attributes, which are mapped to Microsoft's STRIDE model [Islam et al., 2016, Microsoft Corporation, 2005]. This leads to a 6-component vector for each asset, as shown in Equation 2. This example shows the security demands for each element, e. g., the demands for integrity are *high*, whereas there are no demands on confidentiality. Additionally, SRs and REs for each FR have to be defined and mapped to the SLs.

With this approach, it is possible to incorporate design rules in the SRs as well. Plausible design rules may be the physical isolation of critical networks, multi-factor authentication of diagnostic devices or other modules with a critical SL, or the composition of modules with different SLs in one control unit.

$$SL = \begin{bmatrix} \text{Authenticity} \\ \text{Integrity} \\ \text{Non-repudiation} \\ \text{Confidentiality} \\ \text{Availability} \\ \text{Authorisation} \end{bmatrix} = \begin{bmatrix} 2 \\ 3 \\ 1 \\ 0 \\ 2 \\ 1 \end{bmatrix} \tag{2}$$

A mapping to specific security mechanisms can be performed through recommendations. The challenge when introducing such a mapping is its dynamics. The mapping changes over time as cryptographic algorithms may be considered as broken or existing hardware may have sufficient processing capabilities to solve the cryptographic problem on which the mechanism is built upon. Such recommendations support the developers in choosing mechanisms that satisfy a certain SL. They can be represented as a list of requirements associated with certain mechanisms. This method requires an individual identifier or a version number for each mapping to a security mechanism in order to provide a seamless documentation of how the SRs have been addressed.

Table 3: Combined presentation of security and functional safety levels.

		0	1	2	3	4
		QM	*A*	*B*	*C*	*D*
Security	Authenticity			•		
	Integrity				•	
	Non-repudiation		•			
	Confidentiality	•				
	Availability			•		
	Authorisation		•			
Safety				•		

Tools for the secure implementation of software are the [SEI CERT C, 2016] Coding Standard and the [MISRA C:2012, 2013] Guideline, both give guidance and provide rules to develop software that is safe, secure, and reliable. ISO 26262, for instance, recommends the use of MISRA C. We propose to comply with such a secure coding standard for any SL greater than 0, as basic vulnerabilities inherited from programming languages or the wrong use of it can be limited this way.

We believe that a vector representation allows the combination of demands from different disciplines, such as safety. Adding the ASIL levels from ISO 26262 to the vector is beneficial when discussing and deploying the requirements for a module or subsystem, as the requirements of both areas have to be implemented in the very same module or feature. Providing a vector or table as illustrated in Table 3 is thus useful for the software architects and developers to see if required safety mechanisms interfere with security requirements or vice versa. We propose such a combined presentation of both, safety and security demands, as it is necessary in order to fulfil the necessary requirements.

5.3 Evaluation and Certification

Providing evidence about how the SL has been achieved is necessary for the vehicle manufacturers in order to rely on the security capabilities of modules offered by suppliers. Common Criteria, a standard for IT security evaluation, specifies methods and requirements for each Evaluation Assurance Level. Schmittner et al. perform in [Schmittner and Ma, 2014] a mapping of the levels defined in Common Criteria and the ASIL levels from ISO 26262. [Wooderson and Ward, 2017] describe how the assessment as in Common Criteria can be applied for cybersecurity in vehicular systems. They further discuss the benefits and disadvantages of an internal assessment and an independent certification body.

We suggest, that evidence for compliance in form of documents, such as the attack tree analysis or the threat analysis and an overview how the identified threats have been addressed, is sufficient for lower SLs. However, components requiring a SL of high (3) or critical (4) need to provide a more detailed documentation on how the security measures are taken into account.

As the SLs consist of a vector, it is possible to define the level of detail for the required documentation for each element (FR) of the vector. This way, it is ensured that no unnecessary overhead for documentation has to be performed.

6 CONCLUSION

With the increasing functionality of modern vehicles, it is essential to have a standardised security framework for vehicles that specifies the development lifecycle as well as System Requirements (SRs). A standard, such as ISO 26262 for functional safety of road vehicles, is needed so that all involved parties, e. g., manufacturer and suppliers, share the same understanding for automotive security.

We provide a study on several safety and security standards from different domains and discuss specific problems that have to be solved before a similar security standard can be introduced in the automotive domain. Based on this, we suggest a representation of Security Levels (SLs), how to map them to SRs, and discuss how the security compliance of systems and modules with a certain SL can be proven.

The number of SLs found to be suitable is five. Having five SLs not only harmonises with ISO 26262, it allows also a sufficient guidance through specifying system requirements and suitable security mechanisms. A higher number of levels leads to a stricter guidance and would only increase the complexity of the mapping to requirements. However, as shown in IEC 62443 and two automotive security models, security needs to address different attributes or categories, e. g., confidentiality and integrity. For this reason, we propose to define one SL for each category and consequently use a vector for representation. Due to the use of a vector, we also suggest to include safety as one element in order to provide a matrix that presents all safety and security demands, as safety measures may interfere with security. Furthermore, we propose the use of a capability SL (SL-C), similar to IEC 62443, to be used as a classifier for the security of third-party modules and all in-house developed modules.

Providing guidance in the process of mapping SLs to system requirements as part of a security framework has benefits, such as a common understanding of the required security for each level, and the compliance of products from suppliers. Adding recommendations for how to implement certain SRs by providing suitable mechanisms, further guides the developer. It has to be highlighted that such recommendations need to be continuously maintained and updated as security mechanisms might have to be revised due to published exploitation methods.

The evaluation and compliance of components is important for the vehicle manufacturer. During the concept and design phase it has to be known what the system or subsystems need to be capable of and what components provided by suppliers are capable of. For lower SLs, we believe that the documentation of the threat analysis and attack tree analysis together with documented proof providing information how these security requirements have been handled, is sufficient. For the SL high and critical, we propose to adapt Common Criteria according to the specific needs in the automotive domain.

In future work, the detailed security requirements and mechanisms have to be identified, evaluated for their applicability in the automotive domain, and mapped to SLs. Additionally, it is necessary to include this proposed structure in a security framework that is suitable for this domain.

ACKNOWLEDGMENT

This research was funded by the HoliSec project (2015-06894) funded by VINNOVA, the Swedish Governmental Agency for Innovation Systems.

REFERENCES

Blanquart, J.-P., Astruc, J.-M., Baufreton, P., Boulanger, J.-L., Delseny, H., Gassino, J., Ladier, G., et al. (2012). Criticality categories across safety standards in different domains. *ERTS-2012, Toulouse*, pages 1–3.

Burton, S., Likkei, J., Vembar, P., and Wolf, M. (2012). Automotive functional safety = safety + security. In *Proceedings of the First International Conference on Security of Internet of Things - SecurIT 12*. Association for Computing Machinery (ACM).

Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., et al. (2011). Comprehensive experimental analyses of automotive attack surfaces. In *USENIX Security Symposium*. San Francisco.

ENISA (2016). Cyber Security and Resilience of smart cars. Technical report, The European Union Agency for Network and Information Security (ENISA).

ETSI, TS (2011). 102 165-1: Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN). *Methods and protocols*.

Hawkins, T. R., Gausen, O. M., and Strømman, A. H. (2012). Environmental impacts of hybrid and electric vehicles—a review. *The International Journal of Life Cycle Assessment*, 17(8):997–1014.

Henniger, O., Apvrille, L., Fuchs, A., Roudier, Y., Ruddle, A., and Weylr, B. (2009). Security requirements for automotive on-board networks. In *2009 9th International Conference on Intelligent Transport Systems Telecommunications, (ITST)*. Institute of Electrical and Electronics Engineers (IEEE).

IEC 62443 (2013). IEC 62443 – Industrial communication networks - Network and system security. Standard, International Electrotechnical Comission.

Islam, M. M., Lautenbach, A., Sandberg, C., and Olovsson, T. (2016). A risk assessment framework for automotive embedded systems. In *Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security - CPSS 16*. Association for Computing Machinery (ACM).

ISO 15408 (2009). ISO/IEC 15408:2009 Information technology – Security techniques – Evaluation criteria for IT security. Standard, International Organization for Standardization (ISO).

ISO 26262 (2011). ISO 26262:2011 Road Vehicles – Functional Safety. Standard, International Organization for Standardization (ISO).

Kiening, A., Angermeier, D., Seudie, H., Stodart, T., and Wolf, M. (2013). Trust assurance levels of cybercars in V2X communication. In *Proceedings of the 2013 ACM workshop on Security, privacy & dependability for cyber vehicles - CyCAR 13*. Association for Computing Machinery (ACM).

Macher, G., Sporer, H., Berlach, R., Armengaud, E., and Kreiner, C. (2015). SAHARA: A security-aware hazard and risk analysis method. In *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2015*. EDAA.

Microsoft Corporation (2005). The stride threat model. Available at https://msdn.microsoft.com/en-us/library/ee823878.aspx.

Miller, C. and Valasek, C. (2014). A survey of remote automotive attack surfaces. *Black Hat USA*.

MISRA C:2012 (2013). *MISRA C: Guidelines for the Use of the C Language in Critical Systems 2012*. Motor Industry Research Association.

NIST SP 800-53r4 (2013). NIST Special Publication 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations. Standard, National Institute of Standards and Technology.

RCTA DO-254 (2000). Design assurance guidance for airborne electronic hardware. Standard, RTCA and EUROCAE.

RTCA DO-178 (2011). Software considerations in airborne systems and equipment certification. Standard, RTCA and EUROCAE.

Ruddle, A., Ward, D., Weyl, B., Idrees, S., Roudier, Y., Friedewald, M., Leimbach, T., et al. (2009). Deliverable D2.3: Security requirements for automotive on-board networks based on dark-side scenarios. Deliverable, E-safety vehicle intrusion protected applications (EVITA).

SAE J1939 (2013). Serial Control and Communications Heavy Duty Vehicle Network - Top Level Document. Technical report, SAE International.

SAE J3061 (2016). SAE J3061: SURFACE VEHICLE RECOMMENDED PRACTICE - Cybersecurity Guidebook for Cyber-Physical Vehicle Systems. Standard, SAE International.

Schmittner, C. and Ma, Z. (2014). Towards a framework for alignment between automotive safety and security standards. In *International Conference on Computer Safety, Reliability, and Security*, pages 133–143.

Schmittner, C., Ma, Z., and Schoitsch, E. (2015). Combined safety and security development lifecylce. In *2015 IEEE 13th International Conference on Industrial Informatics (INDIN)*. Institute of Electrical and Electronics Engineers (IEEE).

SEI CERT C (2016). Sei cert c coding standard rules for developing safe, reliable, and secure systems. book, Carnegie Mellon University.

Wooderson, P. and Ward, D. (2017). Cybersecurity testing and validation. In *SAE Technical Paper*. SAE International.

Yan, W. (2015). A two-year survey on security challenges in automotive threat landscape. In *2015 International Conference on Connected Vehicles and Expo (ICCVE)*. IEEE.