Towards a Framework for Alignment between Automotive Safety and Security Standards

Christoph Schmittner and Zhendong Ma

Department of Digital Safety & Security
AIT Austrian Institute of Technology
Donau-City-Straße 1, 1220 Vienna, Austria
{christoph.schmittner.fl,zhendong.ma}@ait.ac.at
http://www.ait.ac.at/departments/digital-safety-security/

Abstract. Modern automotive systems increasingly rely on software and network connectivity for new functions and features. Security of the software and communications of the on-board system of systems becomes a critical concern for the safety of new generation vehicles. Besides methods and tools, safety and security of automotive systems requires frameworks of standards for holistic process and assurance. As a part of our ongoing work, this paper investigates the possibility of a combined safety and security approach to standards in the automotive domain. We examine existing approaches in the railway and avionics domain with similar challenges and identify specific requirements for the automotive domain. We evaluate ISO 15408 as a potential candidate for a combined safety and security approach for complementing automotive safety standard ISO 26262, and discuss their points of alignment.

Keywords: safety, security, standard, ISO 26262, ISO 15408, Common Criteria, Automotive, ASIL, EAL

1 Introduction

State of the art automotive systems are becoming increasingly software dependent and interconnected. It is estimated that around 90% of new features are enabled by programmable systems and connectivity, which transforms automotive from mechanical devices to complex cyber-physical systems where multiple networks interconnect up to 100 Electronic Control Units (ECU) within a vehicle [1]. Communications enable vehicles to interact with each other (V2V) and with the outside environment (V2I) for new functions and increase driver safety and comfort. The benefits are obvious, from applications such as remote tracking, unlocking the doors, remote diagnosis, over the air updates (OTA), to automated e-call in case of emergency.

The complexity of in-vehicle system of systems (SoS) and the inter-connectivity are growing. While the number of ECU's is increased only by a factor of 1.45 over the last five years, the total size of application software is increased by a factor of 4.5 during the same period [1]. A survey showed that in the next years

connectivity will be a distinguishing feature for automotive systems. Consumers expect connectivity with their private devices and with the outside environment [18]. This will add additional complexity to the automotive system of systems, where currently up to 4 kilometer of wiring are used to connect up to 10 different types of on-board networks with multiple forms of outside connectivity [15]. Such connectivity enables new application classes for automotive systems, which includes eco/green/mobility, convenience, crash avoidance, safety awareness and emergency applications [17].

At such a scale of complexity and connectivity, serious security concerns arise in the automotive domain. Recent events and analysis demonstrated that the current ad-hoc approach towards security engineering in the automotive domain delivers sub-optimal results. A recent survey by the U.S. Senate showed that most car manufactures did not follow a structured and systematic approach towards security engineering [20]. While all responding car manufactures stated that their vehicles offer one or more wireless connections, only one of them was able to provide information on threats and vulnerabilities. Experimental analysis of systems like the wireless tire pressure monitoring system (TPMS) [13], the external automotive attack surfaces [3], surveys of potential security threats [21] and telematics unit [7] all support the conclusion in the survey. Furthermore, the capability and processes to address vulnerability and conduct security testing are also underdeveloped.

Being safety-critical, the automotive domain has a set of established safety standards, which are used to design safety-critical components and systems and ensure that all safety risks are reduced to a tolerable level. However, security for safety-critical systems is a relatively new challenge. As safety can no longer guaranteed if security fails, the question is how to take security into consideration in the existing safety standards. For adding security to safety in the automotive domain, it is worthwhile to look at similar issues in railway and avionics. As shown by a recent study [2] in the railway domain, where similar security challenges arise [19], solving them is not restricted to identifying a need for security and safety and defining new methods. Systematic approaches that address safety and security equally are needed. In the railway domain, the ISO 15408 (Information technology - Security techniques - Evaluation criteria for IT security (Common Criteria)) [12] and the IEC 62443 (Industrial communication networks - Network and system security - Security for industrial automation and control systems) [9] have the potential to address security. The author of the study [2] proposed to use IEC 62443 as a suitable addition to established safety standards. It was also proposed to add the requirements for security level 1 to the EN 5012x standards series. The avionics domain takes a different approach and started to develop its own security standards. The generic safety standard IEC 61508 [10] was extended with security related requirements in the second edition and there is ongoing activity to extend this in the third edition.

In the automotive domain, ISO 26262 [11] is the established safety standard. It is currently in revision. The focus is on the addition and identification of safety-cybersecurity interface points, points in the safety lifecycle for informa-

tion exchange or combined activities and work products[1] with security. As a part of our ongoing work on safety and security co-engineering for the automotive domain, this paper investigates how to extend existing safety standards to address security concerns. Given the complexity of the problem, we envision a standard framework with several standards cover the whole area of safety and security. Our main contributions in this paper include:

- we identify requirements for suitable security standards for automotive safety, review and compare automotive safety standard ISO 26262 and security standard ISO 15408,
- we identify important work products and approaches in both standards for points of alignment,
- we propose an alignment of Automotive Safety Integrity Level (ASIL) and Evaluation Assurance Level (EAL), and discuss its feasibility.

In the following, Section 2 briefly discusses related work; Section 3 and 4 review the ISO 26262 and ISO 15408 standard, respectively; Section 5 presents our comparison and a proposal for alignment; Section 6 concludes the paper with a discussion of potential challenges and further steps.

2 Related work

Automotive industry has a long history of following and implementing stringent safety requirements. With the rapid development and integration of ICT components, the need for a tighter coupling of safety and security for connected safety-critical systems becomes necessary. The issue has attracted attentions in recent years. Macher *et al.* [16] developed a security extended hazard analysis and risk assessment methodology for the automotive domain and reported that they were able to identify 34% more hazardous situations in industrial use cases. Multiple studies demonstrated the different possibilities of interactions between safety and security [6, 8, 22]. A survey of safety and security for the industrial domain [14] listed 37 methods for co-engineering.

Furthermore, specific challenges for the safety engineering in the automotive domain have been identified in [5]. A domain independent approach towards a combined safety and security lifecycle is proposed in [4].

3 ISO 26262

ISO 26262 is a domain specific instantiation of IEC 61508, the generic safety standard [10]. It follows a risk based approach and is mainly based around safety integrity levels, safety goals and safety concepts.

Figure 1 gives an overview of the safety lifecycle defined in ISO 26262. Development of a new item starts in the concept phase with the item definition,

[1] A work product is the result of an activity related to a requirement.

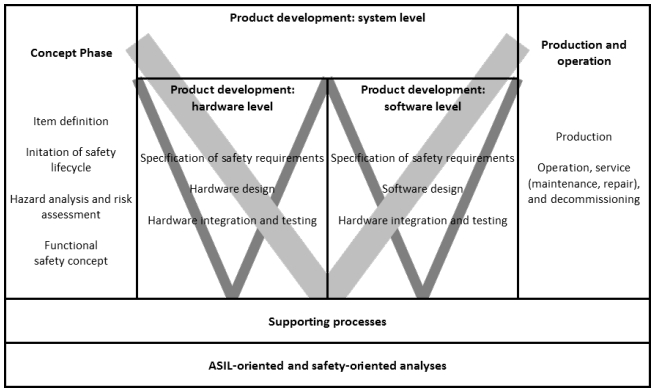

Fig. 1. Safety Lifecycle according to ISO 26262

initiation of the safety lifecycle, hazard analysis and risk assessment and definition of the functional safety concept. During hazard analysis and risk assessment, potential hazards are identified and the risks are investigated. The risk rating depends on the driving situation in which a hazard occurs, the potential controllability of the situation and the severity of the caused harm. Depending on the risks, safety goals are defined. An automotive safety integrity level (ASIL) is assigned to each safety goal. ASIL ranges from D for the most stringent level of safety measures to A for the most lenient level of safety measures. For systems with lower risks, quality management activities are sufficient.

Based on the safety goals, functional safety requirements are derived and assigned to preliminary architectural elements. The functional safety concept is compromised of all functional safety requirements and describes the functionality to achieve the safety goal.

Next step is the product development on system level. During this step the technical safety requirements are specified, the system is designed, hardware and software of the item are integrated and tested, compliance and correctness of the safety goals and their implementation is validated and the functional safety is assessed. Complementary to the functional safety concept, the technical safety concept consists of all technical safety requirements and describes how the functional safety requirements are implemented in hardware or software. The system development includes hardware and software development. During the hardware development, hardware safety requirements are specified, the hardware is designed, observation of hardware architectural metrics in regard to fault handling is assessed and potential violation of safety goals due to random hardware failures are evaluated. The hardware development is concluded with integration and testing. In a similar manner software design starts with the specification of software safety requirements, the design of the software architecture, and the design and implementation of the individual software units. It is concluded by testing of the units, software integration and integration testing and verification of the software safety requirements.

Additional parts of ISO 26262 are concerned with production and operation and safety analysis for determining the ASIL. The final evidence for the functional safety of an item is the safety case which summarizes all work products from the ISO 26262. A particularity in the ISO 26262 is the Safety Element out of Context (SEooC). A SEooC is an element for which the final item and operating environment is not known during design and development. It is therefore developed using assumptions and hypothesis. This assumptions have to be confirmed in order to safely integrate a SEooC in a item. A SEooC can be verified, the validation occurs during the item development.

4 ISO 15048, Common Criteria

Comparing with most safety standards, the ISO 15048 follows a different approach. While safety defines a system lifecycle and an engineering approach, ISO 15048 focuses on the evaluation and assurance of the system security.

The Target of Evaluation (ToE) is evaluated based on security specifications with different levels of generality. A Protection Profile (PP) is a implementation independent specification of security requirements for a class of systems. A Security Target (ST) is the implementation specific specification of security requirements for a system. Since automotive protection profiles are more of an idea for future work, we will focus on the security target definition. An ST consists of the definition of the ST, the conformance claim to any protection profiles, the definition of the security problem and the security objectives, the extended components definition, the security requirements and the TOE summary specification. Figure 2 gives an overview about the contents of an security target.

An ST is intended as a specification of the security properties of a TOE and as a definition for the scope of the evaluation. It is not intended as a detailed or complete specification for the design or implementation of a system. It is explicitly mentioned in the ISO 15408: "This means that in general an ST may be part of a complete specification."[12].

The assumptions in the security problem definition (cf. Figure 2) describe assumptions about the operating environment of a TOE. If a TOE is placed in operational situations where these assumptions are not true, the TOE may not be able to provide its security functionality. ISO 15408 differs between the Security Functional Requirements (SFR) and the Security Assurance Requirements (SAR). The SFRs are a formalized and implementation independent specification how the security objectives are achieved. The SARs describe how and to which strictness a TOE is evaluated. Evaluation assurance levels (EAL) describe seven sets of SARs with rising strictness. The TOE summary specification finally describes how a TOE implements the SFRs.

Using properly, ISO 15408 can increase software and hardware security assurance level. It provides the assurance by enforcing good and comprehensive documentation during the system design and development phase, including system specification, system internals, system tests, and development tools. It also forces a development team to take security as the main objective from the begin-

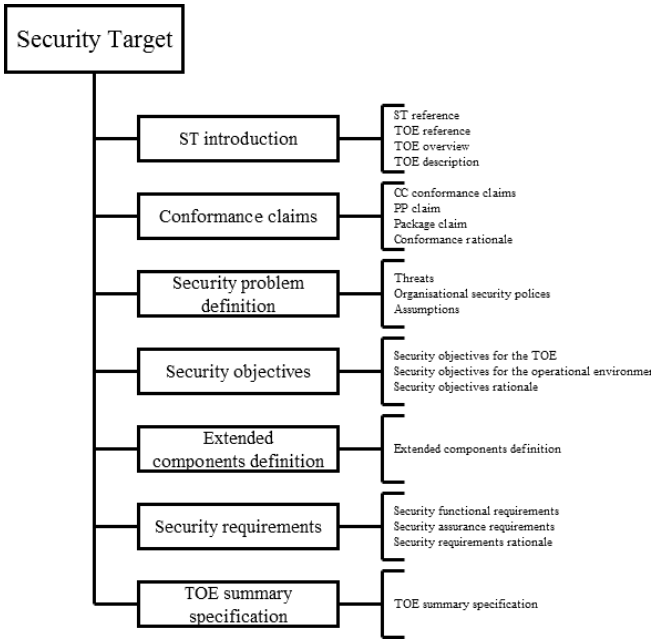

Fig. 2. Security Target contents according to ISO 15408

ning of the project. It raises awareness of the security problems throughout the system's design and development phase, in which both security and non-security team members are invovled. The specification of PP, SFRs, and SARs, defined in accordance with ISO 15408 will provide comprehensive and clear specifications on the requirements of critical parts in the automotive system. Such an intensive practice can force the project team to identify ambiguities early on and solve the identified problems accordingly.

5 Comparison and points for interaction

To complement automotive safety standard ISO 26262 and to promote a combined approach to safety and security, we identified the following requirements for the evaluation of candidate security standards:

1. There should be an overlap in required work products for safety and security argumentation. It should be possible to build a holistic assurance case which reuses and extends existing work products for safety argumentation and combine them with security related work products.
2. Assurance levels between safety and security should be translatable. Verification activities for safety and security should be on a similar level. Strictness of required documentation, design, testing and verification should be similar between pure safety goals and security motivated safety goals.

3. Approaches and concepts from the ISO 26262 should be mirrored by the security standard. ISO 26262 supports some automotive specific approaches, like the Safety Element out of Context. Such approaches and concepts should be representable by the security standard.

Based on these requirements, we investigate the feasibility of using ISO 15408 to complement ISO 26262 for safety and security.

5.1 Work products

Table 1 shows a comparison of work products from the two standards. It can be seen that for the required parts of a security target, existing work products from the ISO 26262 contain similar, or in some parts, overlapping content. However, it does not imply a complete overlap between safety and security work products. Numbers in the ISO 15408 column refer to part 1 of the standard. The reference to parts of ISO 26262 are given for each specific requirement.

Table 1. Work products from ISO 15408 and ISO 26262

ISO 15408	ISO 26262
A.4.1 ST reference and TOE reference	Part3-5: Item definition
A.4.2 TOE overview	
A.4.3 TOE description	
A.5 conformance claims	-
A.6.2 Threats	Part3-7.5.1: Hazard analysis and risk assessment
A.6.3 Organisational security policies	Part2-5: Overall safety management, Part2-5.5.1: Organization specific rules and processes for functional safety Part2-7: Safety management after release for production, Part2-7.5: Evidence of a field monitoring process
A.6.4 Assumptions	Only for Safety element out of Context
A7.2.1 Security objectives for the TOE	Part3.7.5.2: Safety Goals
A7.2.2 Security objectives for the operational environment	-
A7.3. Relation between security objectives and the security problem definition	Part3-7.5.3: Verification review of hazard analysis and risk assessment and safety goals
A.8 Extended components definition	-
A.9.1 Security functional requirements	Part3-8.5.1: Functional safety concept
A.9.2 Security assurance requirements	Part2-6: Safety management during development of the item, Part2-6.5.5: Confirmation plan Part6-11:Verification of software safety requirements Part6-11.5.1: Software verification plan
A.9.3 Security requirements rationale	
A.10 TOE summary specification	Part2-6.5.3: Safety Case

The table lists safety work products from ISO 26262 that are best suited to be extended with their security specific counterpart from ISO 15408. It will define a holistic assurance case, which integrates required parts for the safety case with the mandatory parts for a security target. For example, the item definition of ISO 26262 contains mission, functional and non-functional requirements, dependencies between the item and its outside and already known safety requirements from familiar items. In addition, the boundaries, interfaces, elements, distribution of functions, operating scenarios and requirements from and on other items are described. The item description already contains most required parts of the

TOE reference, TOE overview and TOE description. It needs to be extend with an overview of the included security features and the functionality of the item.

While the conformance claim has no direct counterpart in ISO 26262, the next row demonstrates how a safety work product may be extended. The goal of the hazard analysis and risk assessment is to identify and evaluate all hazards for an item and to formulate the safety goals to achieve the necessary risk reduction. The intention of ISO 15408 is similar, in which a list of all undesired actions from a threat agent may have negatively influence on one or more properties. Extending the hazard analysis and risk assessment with a list of potential threat scenarios that negatively influence the safety of the item can be used for safety and security argumentation.

5.2 Assurance levels

ISO 15408 follows a strict assignment of measures to levels, while ISO 26262 has levels of highly recommend, recommend and methods without recommendation. The different EAL can be summarized as:

- EAL1: functionally tested
- EAL2: structurally tested
- EAL3: methodically tested and checked
- EAL4: methodically designed, tested and reviewed
- EAL5: semi-formally designed and tested
- EAL6: semi-formally verified design and tested
- EAL7: formally verified design and tested.

Since EAL and security in general relates mostly to software design, implementation and testing, we based our structuring of the ASIL mostly on the ASIL dependent requirements for this part of the complete system engineering. However, at the moment, there is no absolute direct translation and mapping. For example, formal methods are only recommend for the highest ASIL, while semi-formal methods are highly recommend for ASIL D and C.

Based on a examination of the ISO 26262 requirements, a translation between EAL and ASIL, based on their strictness and degree of formalism is proposed as following.

- ASIL A: EAL3
- ASIL B: EAL4
- ASIL C: EAL5
- ASIL D: EAL6

Similar to the conversion from SIL to ASIL, where the highest SIL is more critical than the highest ASIL, in a summarized translation, EAL7 would be out of reach. A more elaborate approach might be to build a specific set of SAR tailored according to the requirements from ISO 26262. ISO 15408 allows such an approach with the EALX+ specification. It describes a set of requirement which exceeds EALX in strictness in some parts but does not reach the next EAL. This would allow a more accurate translation.

5.3 Automotive domain specific concepts

Compared to the generic safety standard IEC 61508, the automotive domain has defined a few domain-specific concepts in ISO 26262. As described in [2], it becomes challenging to add security to safety if attack probabilities are to be considered. Probability estimation in ISO 26262 is based on the concept of "how frequently and for how long individuals find themselves in a situation where the aforementioned hazardous event can occur." In ISO 26262, this is defined to be a measure of the probability of the driving scenario taking place in which the hazardous event can occur (E = exposure) [11]. As shown in[16], the risk rating for ISO 26262 is therefore well suited for an integration of security threats. One can simply redefine exposure as probability that a driving scenario takes place in which a cyber attack is possible and therefor causes a hazardous event. The determined ASIL for security motivated safety goals can then be translated to an EAL for the corresponding security objective.

An important concept in the ISO 26262 is the SEooC. It enables supplier to develop components for different OEMs and to carry out safety engineering based on the assumed usage and operational environment of the component. ISO 15408 supports a similar concept with the dependency on the operational environment for security. The final assessment depends in both cases on the operational environment.

6 Conclusion

Automotive systems become increasingly software-intensive and interconnected. This makes security a burning issue and attracts many attentions in recent years. Cooperation between safety and security standards is urgently needed in the automotive domain. As a part of our on-going work on safety and security co-engineering, we investigate the possibility of a framework of standards that addresses safety and security in automotive domain in a holistic and cooperative way. We investigate domains with similar safety-critical requirements and evaluate ISO 15408 and ISO 26262 to find points that have the potential for combinations.

As a work-in-progress, out next step is to conduct more in-depth analyzes of existing automotive safety and security standards. Specifically, we will address the challenge of how to align and harmonize assurance levels on safety and security in different standards.

Acknowledgment

This research has received funding from the EU ARTEMIS Joint Undertaking under grant agreements no. 621429 (EMC^2) and from the FFG (Austrian Research Promotion Agency) on behalf of BMVIT, The Federal Ministry of Transport, Innovation and Technology.

References

1. Abelein, U., Lochner, H., Hahn, D., Straube, S.: Complexity, quality and robustness-the challenges of tomorrow's automotive electronics. In: Design, Automation & Test in Europe Conference & Exhibition (DATE), 2012. pp. 870–871. IEEE (2012), http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6176573
2. Braband, J.: Towards an IT Security Framework for Railway Automation. Toulouse (Feb 2014), http://www.erts2014.org/site/0r4uxe94/fichier/erts2014_7c3.pdf
3. 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 (2011)
4. Christoph Schmittner, Zhendong Ma, Erwin Schoitsch: Combined Safety and Security Development Lifecylce. Cambridge (2015)
5. Christoph Schmittner, Zhendong Ma, Thomas Gruber: Standardization Challenges for Safety and Security of Connected, Automated and Intelligent Vehicles. Wien (Nov 2014)
6. David Peter Eames, Jonathan Moffet: The Integration of Safety and Security Requirements. In: Lecture Notes in Computer Science, Computer Safety, Reliability and Security. vol. 1698, pp. 468 – 480. Springer, Toulouse (1999)
7. Dieter Spaar: Auto, ø"ffne dich! Sicherheitsl"cken bei BMWs ConnectedDrive. c't (5), 86 – 90 (2015), http://heise.de/-2536384
8. Dong-bo Pan, Feng Liu: Influence between Safety and Security. In: ICIEA 2007. pp. 1323 – 1325 (2007)
9. International Electrotechnical Commission: IEC 62443, Industrial communication networks - Network and system security - Security for industrial automation and control systems
10. International Electrotechnical Commission: IEC 61508: Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems (2010)
11. International Organization for Standardization: ISO 26262 Road vehicles - Functional safety (2011)
12. International Standardization Organization: ISO 15408, Information technology - Security techniques - Evaluation criteria for IT security (Common Criteria)
13. Ishtiaq Roufa, R.M., Mustafaa, H., Travis Taylora, S.O., Xua, W., Gruteserb, M., Trappeb, W., Seskarb, I.: Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study. In: 19th USENIX Security Symposium, Washington DC. pp. 11–13 (2010), https://www.usenix.org/legacy/event/sec10/tech/full_papers/Rouf.pdf
14. Kriaa, S., Pietre-Cambacedes, L., Bouissou, M., Halgand, Y.: A survey of approaches combining safety and security for industrial control Systems. Reliability Engineering & System Safety (Mar 2015), http://linkinghub.elsevier.com/retrieve/pii/S0951832015000538
15. Leen, G., Heffernan, D.: Expanding automotive electronic systems. Computer 35(1), 88–93 (2002), http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=976923
16. Macher, G., Harald Sporer, Reinhard Berlach, Eric Armengaud, Christian Kreiner: SAHARA: A Security-Aware Hazard and Risk Analysis Method. In: Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition. pp. 621–624 (2015)

17. Onishi, H., Mlinarsky, F.: Wireless technology assessment for automotive applications. In: Proc. ITS World Congress (2012), http://www.octorange.com/English/Collaterals/Whitepapers/octoScope_WP_WirelessAutomotive_20120421.pdf
18. Ralf Kalmbach, Wolfgang Bernhart, Philipp Grosse Kleimann, Marcus Hoffmann: Automotive Landscape 2025 - Opportunities and challenges ahead. Tech. rep., Roland Berger, Strategy Consultants (Mar 2011)
19. Smith, J., Russell, S., Looi, M.: Security as a safety issue in rail communications. In: Proceedings of the 8th Australian workshop on Safety critical systems and software-Volume 33. pp. 79–88. Australian Computer Society, Inc. (2003), http://dl.acm.org/citation.cfm?id=1082058
20. Staff of Senator Edward J. Markey: Tracking & Hacking Security & Privacy Gaps Put American Drivers at Risk. Tech. rep. (2015)
21. Studnia, I., Nicomette, V., Alata, E., Deswarte, Y., Kaniche, M., Laarouchi, Y.: Survey on security threats and protection mechanisms in embedded automotive networks. In: Dependable Systems and Networks Workshop (DSN-W), 2013 43rd Annual IEEE/IFIP Conference on. pp. 1–12. IEEE (2013), http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6615528
22. Sun, M., Mohan, S., Sha, L., Gunter, C.: Addressing safety and security contradictions in cyber-physical systems. In: Proceedings of the 1st Workshop on Future Directions in Cyber-Physical Systems Security (CPSSW09) (2009), http://cimic3.rutgers.edu/positionPapers/cpssecurity09_MuSun.pdf