# SAHARA: A Security-Aware Hazard and Risk Analysis Method

Georg Macher*‖, Harald Sporer*, Reinhard Berlach*, Eric Armengaud‖ and Christian Kreiner*

*Institute for Technical Informatics, Graz University of Technology, AUSTRIA
Email: {georg.macher, sporer, reinhard.berlach, christian.kreiner}@tugraz.at

‖AVL List GmbH, Graz, AUSTRIA
Email: {georg.macher, eric.armengaud}@avl.com

***Abstract*—Safety and Security are two seemingly contradictory system features, which have challenged researchers for decades. Traditionally, these two features have been treated separately, but due to the increasing knowledge about their mutual impacts, similarities, and interdisciplinary values,they have become more important. Because systems (such as Car2x in the automotive industry) are increasingly interlaced, it is no longer acceptable to assume that safety systems are immune to security risks. Future automotive systems will require appropriate systematic approaches that will support security-aware safety development. Therefore, this paper presents a combined approach of the automotive HARA (hazard analysis and risk assessment) approach with the security domain STRIDE approach, and outlines the impacts of security issues on safety concepts at system level. We present an approach to classify the probability of security threats, which can be used to determine the appropriate number of countermeasures that need to be considered. Furthermore, we analyze the impact of these security threats on the safety analysis of automotive systems. This paper additionally describes how such a method has been developed based on the HARA approach, and how the safety-critical contributions of successful security attacks can be quantified and processed.**

***Keywords*—ISO 26262, HARA, STRIDE, automotive, safety, security.**

## I. Introduction

The complexity of embedded systems in the automotive industry has grown significantly in recent years. Current luxury cars implement more than 90 electronic control units (ECU), which utilize nearly 1 Gigabyte of embedded software code [1]. By 2018, expert predict that 30% of the overall vehicle costs will be due to vehicle electronics [2]. This prediction is also strongly supported by the ongoing trend of replacing traditional mechanical systems with modern embedded systems. This enables the deployment of more advanced control strategies, thus providing additional benefits for both the customer and environment, such as reduced fuel consumption and better drivability. At the same time, the higher degree of integration and safety- and security-critical nature of the control application presents new challenges. Traditionally, safety and security features have been managed separately, because safety-critical systems have been assumed to be immune from security risks. Nevertheless, because automotive systems (such as Car2x) are increasingly interlaced this assumption is no longer valid. Future automotive systems will require appropriate systematic approaches to support security-aware safety development. Safety standards such as ISO 26262 [3] for road vehicles have been established to provide guidance during the development of safety-critical systems. Although safety might be interpreted as contradictory to security, a considerable overlap among safety and security methods exists. The contribution of this paper is to present a framework for the security-aware identification of safety hazards. SAHARA (Security-Aware Hazard Analysis and Risk Assessment) is an expansion of the inductive analysis method hazard analysis and risk assessment (HARA), and encompasses threats of the STRIDE Threat Model [5]. This approach enables the quantification of the probability of the occurrence and impacts of security issues on safety concepts (safety goals).

The document is organized as follows: In Section II, a description of the proposed SAHARA approach is provided. Section III includes an assessment of the contribution of our approach in relation to those of other related works dealing with (automotive) safety and security related topics. An application for the approach in an automotive battery management system (BMS) use-case scenario is presented in Section IV. Concluding remarks are found in Section V.

## II. Proposed Approach

Safety and security were previously managed independently from one another due to the different application arease and technical solutions. However, due to increasing impact of the Internet of Things (IoT) on aspects of the automotive domain, it is no longer acceptable to assume that safety systems are immune to security risks. In the foreseeable future, automotive engineers will require appropriate, systematic approaches and interdisciplinary knowledge of both safety and security to support the development of security-aware safety methods. Currently, the automotive domain mainly focuses on the safety-critical nature of automotive embedded systems, and therefore, has several advanced methods and processes in place (e.g., hazard analysis and risk assessment (HARA), fault tree analysis (FTA), and failure mode and effects analysis (FMEA)). In addition, an industry-wide standard for assessing the functional safety of road vehicles, covering the whole product lifecycle (ISO26262 [3]) has been established. To the contrary, several approaches to exposing security design flaws exist in other industrial sectors, but have not yet been applied within the automotive industry. STRIDE, an acronym

978-3-9815370-4-8/DATE15/©2015 EDAA

for six security threat categories, is a threat modeling approach [5] that uses a technique called threat modeling to review system designs in a methodical way. This allows the identification of the type of threat to which the system is vulnerable. The first category includes *spoofing threats* attempt to successfully masquerade as another person or program in order to gain illegitimate advantages. The second includes *tampering attacks* that maliciously modify data or data orders. *Repudiation threats*, which fall into the third category, target systems that are unable to trace prohibited operations and counteract illegal operations. the fourth category comprises *information disclosure threats* that involve the exposure of sensitive information. *Denial of service attacks* (D.o.S), which simply deny valid services, and threats such as babbling idiot faults belong in the fifth category. Finally, *elevation of privilege threats* aim to access, compromise or destroy data that should be available only to privileged user or programs.

Each of these threat classes potentially has a safety impact (leads to new hazards) when applied to safety-critical applications. The threat model does not make a given design 100% secure, but enables the system designer to learn from mistakes and avoid repeating them. Therefore, this approach can be seen as a method by which the security of a system can be assessed equivalent to HARA attempt for safety.

| | | Threat Level 'T' | | | |
|---|---|---|---|---|---|
| **Required Resources 'R'** | **Required Know-How 'K'** | 0 | 1 | 2 | 3 |
| 0 | 0 | 0 | 3 | 4 | 4 |
| | 1 | 0 | 2 | 3 | 4 |
| | 2 | 0 | 1 | 2 | 3 |
| 1 | 0 | 0 | 2 | 3 | 4 |
| | 1 | 0 | 1 | 2 | 3 |
| | 2 | 0 | 0 | 1 | 2 |
| 2 | 0 | 0 | 1 | 2 | 3 |
| | 1 | 0 | 0 | 1 | 2 |
| | 2 | 0 | 0 | 0 | 1 |
| 3 | 0 | 0 | 0 | 1 | 2 |
| | 1 | 0 | 0 | 0 | 1 |
| | 2 | 0 | 0 | 0 | 1 |

Fig. 1. SecL Determination Matrix - ascertains the security level from R, K, and T values

### A. Problem Statement

The focus of this approach is placed on the early development phase - the so-called concept phase - of safety-critical embedded automotive systems, which is also addressed by ISO 26262 part 3 [3]. Safety-related or safety-critical automotive systems can potentially contribute to, or cause hazards for humans or the environment. During the concept phase, it is of utmost importance to identify ways in which the system might dangerously fail and to begin formulating safety constraints. For this reason, the automotive safety standard states that the system under development (SuD) must be analyzed using the HARA approach. The intention of such a HARA is to identify and categorize hazards and formulate high level safety requirements (safety goals) in order to avoid unreasonable risks. This approach focuses on the sources of problems that could occure due to malfunction or foreseeable user misuse. However, problems caused by malicious attacks (security issues) are not addressed by HARA within the ISO 26262 standard, although such attacks may also preempt safety strategies. In parallel, the STRIDE threat model provides a way to methodically review system designs and highlight security design flaws, but does not support the categorization of security hazards or methodically formulate security requirements in such a way as to avoid identified risks.

TABLE I. REQUIRED RESOURCE 'R' CLASSIFICATION - DETERMINATION OF THE 'R' VALUE FOR REQUIRED RESOURCES TO EXERT A THREAT

| Level | Required Resource | Example |
|---|---|---|
| 0 | no additional tool or everyday commodity | randomly using the user interface, strip fuse, key, coin, |
| 1 | standard tool | screwdriver, multi-meter, multi-tool |
| 2 | simple tool | corrugated-head screwdriver, CAN sniffer, oscilloscope |
| 3 | advanced tools | debugger, flashing tools, bus communication simulators |

### B. Approach

A key outcome of the HARA approach is the definition of the automotive safety integrity levels (ASILs). The assigned ASIL determines the criticality level of the SuD and defines requirements and measures that must be applied for the remainder of the development lifecycle. For the purpose of determining the SuDs ASIL, potential hazards must be identified that endanger the system. Afterwards, these hazards are quantified according the severity of potential harm (S), probability of exposure (E), and controllability of the resulting hazardous event (C). The final step involves a formulation of high level safety requirements known as safety goals (for more detailed information see [3] part 3 Annex B).

Threat modeling using STRIDE [5] can be seen as a security pendant to HARA. The key goal of this threat modeling approach is to analyze each system component for its susceptibility to threats and, subsequently, mitigate all threats to these components in order to increase system security.

The first step of the SAHARA approach, combining security and safety analyses, is to quantify the STRIDE security threads of the SuD in an analog manner as is performed for safety hazards as part of the HARA approach. Threats are quantified with reference to the ASIL analysis, according to the resources (R) and know-how (K) that are required to pose the threat and the threats criticality (T).

Table I classifies the **required resources - 'R'** to threaten the SuDs security and gives some examples of tools that are required to successfully pose the security threat. Level 0 covers threats that do not require any tools or everyday commodities, and wich are available even in situations of unpreparedness.

TABLE II. REQUIRED KNOW-HOW 'K' CLASSIFICATION - DETERMINATION OF THE 'K' VALUE FOR REQUIRED KNOW-HOW TO POSE A THREAT

| Level | Required Know-How | Example |
|---|---|---|
| 0 | no prior knowledge (black-box approach) | average driver, unknown internals |
| 1 | technical knowledge (gray-box approach) | electrician, mechanic, basic understanding of internals |
| 2 | domain knowledge (white-box approach) | person with technical training and focused interests, internals disclosed |

TABLE III. THREAT CRITICALITY 'T' CLASSIFICATION - DETERMINATION OF THE 'T' VALUE OF THREAT CRITICALITY

| Level | Threat Criticality | Example |
|---|---|---|
| 0 | no security impact | no security relevant impact |
| 1 | moderate security relevance | annoying manipulation, partial reduced availability of service |
| 2 | high security relevance | damage of goods, invoice manipulation, non-availability of service, privacy intrusion |
| 3 | high security and possible safety relevance | maximum security impact and life-threatening abuse possible |

Level 1 tools can be found in any average household, while the availability of level 2 tools is more limited (such as special workshops). Tools assigned to level 3 are advanced tools to which accessibility is highly limited and not wide-spread.

Table II classifies the **required know-how - 'K'**. Here, level 0 requires no prior knowledge (the equivalent of the black-box approach). Level 1 addresses people with technical skills and a basic understanding of internals, and represents gray-box approaches. Finally, level 2 represents white-box approaches; it addresses people with focused interests and comprehensive domain knowledge.

An overview of the **criticality of a security threat - 'T'** is given in Table III. Level 0, in this case, indicates security impact that is irrelevant, such as when raw data can be visualized, but its meaning not determined. The threat impact of level 1 threats is limited to annoyances, such as reduction in availability of services, but does not imply any damage to products or manipulation of data or services; such threats and financial threats are found in level 2. Level 3 threats imply the invasion of privacy or result in impacts on human life (quality of life), as well as cover possible impacts on safety features.

These three factors determine the resulting security level (SecL). The SecL determination matrix is based on the ASIL determination approach and is illustrated in Figure 1. The quantification of required know-how and tools, instead of any estimation of likelihood (e.g., of success or failure rate of attacks) was chosen due to the fact that such a classification of these factors is more commonly performed in the automotive industry and because it will remain the same over the whole life-time of the SuD. In addition, the quantification of these two factors is related to the estimation of the likelihood that an attack will be carried out. The quantification of the impact of the threats, on the one hand, determines whether the threat is safety-related (threat level 3) or not (all other levels). This information is the trigger to hand over the threat for further analysis from the safety point of view. On the other hand, this quantification allows the determination of the limits of resources spent to protect the SuD from a specific threat (risk management in the case of security threats). Following this quantification, these threats may be then appropriately mitigated or prevented by appropriate design changes and the implementation of countermeasures.

In the case of safety-related security threats, such threats will be analyzed and the resulting hazards evaluated according to their criticality, exposure, and severity. This security analysis helps to improve the completeness of the HARA situation analysis by implying factors of reasonably foreseeable misuse (security treats) in a more structured way.

## III. RELATED WORK

Safety and security of control systems are challenging research areas that are characterized by continuous development and steadily increasing importance. For this reason, many researchers and industrial experts have recently made efforts to combine security and safety.

Although only safety standards, such as the road vehicles functional safety norm ISO 26262 [3] and its basic norm IEC 61508, exist in the automotive industry, several safety and security norms and guidelines have been established in aeronautics industry. In addition to DO-178C [10], which addresses aeronautics software safety, ARP4754 [7] provides guidance for system level development and defines steps for the adequate refinement and implementation of requirements. Safety assessment techniques, such as failure mode and effects analysis (FMEA) and functional hazard assessment (FHA) anmong others, are specified by ARP4761 [6]. Security concerns in aeronautics industry are tackled e.g., by the Common Criteria [12] [4] approach and ED202 specification.

Some recent publications in the automotive domain also focus on security in automotive systems. The work of Schmidt et. al [8] presents a security analysis approach to identify and prioritize security issues, but only provides an analytical approach for networked connectivity. Alternatively, the work of Ward et. al [13] additionally mentions a method to assess security risks in the automotive domain, which is called threat analysis and risk assessment, and is based on the HARA. In contrast to these approaches, our approach combines hazard and threat analysis in order to identify threats that can contribute to the safety-concept or lead to violations of safety goals. The works of Schmittner et. al [9] and Steiner et. al [11] also deal with safety and security analysis, but focus on state/event fault trees or a failure mode and failure effect model to perform safety and security cause-effect analysis.

## IV. APPLICATION OF THE APPROACH

This section describes the application of the SAHARA approach to an automotive battery management system (BMS).

Battery management systems are control systems inside of high-voltage battery systems used to power electric or hybrid vehicles.

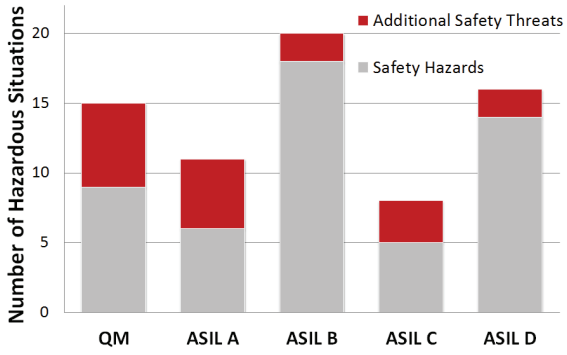


Fig. 2. Analysis of the SAHARA Approach for the BMS Use-Case - representation of safety hazards (identified using the common HARA approach) and additional hazards resulting from security threats (newly identified using the SAHARA approach)

The BMS is a safety-related system that is intended for installation in series production passenger cars and therefore within the scope of ISO 26262. Within the scope of this work, the focus was set on hazard analysis and risk assessment (HARA) in order to elaborate on a functional safety concept that had been developed using the SAHARA approach.

The SAHARA of the BMS use-case covered 52 hazardous situations, quantified the respective ASIL and assigned safety goals that were fully in line with the ISO 26262 standard. Additionally, 37 security threats were identified using the STRIDE approach and were quantified with their respective SecL. 18 of those security threats were classified as having possible impacts on safety concepts and were, therefore, further analyzed for their impacts on the safety of the SuD. Figure 2 presents the number of hazardous situations which were analyzed and quantified with ASILs, and highlights the additional safety hazards that were derived from the security threats. For this specific example, the SAHARA approach identified 34% more hazardous situations than the traditional HARA approach. SAHARA thus represents a systematic approach that can be taken to combine safety and security development, and takes into consideration the harmonization of safety and security methods.

## V. Conclusion

Automotive embedded systems are safety-critical and, therefore, require appropriate risk identification and management throughout the development cycle. Moreover, these computing platforms are increasingly connected to their environment (e.g., on-board diagnosis, GPS, Car-2-Car or Car-2-infrastructure). In this context, safety-related functionalities rely on the trustworthiness of information gathered from the environment. Because security threats might have an impact on the safety of the system, automotive embedded systems cannot be considered immune to security attacks. Therefore, joint considerations of security and safety are necessary. This paper presents a combined approach, merging of the automotive HARA (hazard analysis and risk assessment) with the security domain STRIDE, proposing the security-aware hazard analysis and risk assessment (SAHARA) approach. The SAHARA approach is fully in line with the requirements of a HARA analysis according to the automotive safety standard, ISO 26262 [3], for road vehicles. SAHARA represents a systematic approach that addresses the need to synchronize the development of safety and security methods.

## Acknowledgments

This work is partially supported by the INCOBAT and the MEMCONS projects.

The research leading up to these results was funded by the European Unions Seventh Framework Programme (FP7/2007-2013) under the grant agreement n 608988 and through financial support from the Austrian Federal Ministry for Transport, Innovation and Technology (BMVIT), the Austrian Federal Ministry of Economy, Family and Youth (BMWFJ), the Austrian Research Promotion Agency (FFG), the Province of Styria, and the Styrian Business Promotion Agency (SFG) through the "COMET K2 - Competence Centers for Excellent Technologies Programme".

The authors thank Sara Crockett for assistance with language editing and proofreading.

Furthermore, we would like to express our thanks to our supporting project partners, AVL List GmbH, Virtual Vehicle Research Center, and Graz University of Technology.

## References

[1] C. Ebert and C. Jones. Embedded Software: Facts, Figures, and Future. *IEEE Computer Society*, 0018-9162/09:42–52, 2009.

[2] R. Hilbrich, J. Reinier van Kampenhout, and H.-J. Goltz. Modellbasierte Generierung statischer Schedules fuer sicherheitskritische, eingebettete Systeme mit Multicore-Prozessoren und harten Echtzeitanforderungen. *Informatik aktuell*, pages 29 – 38, 2012.

[3] ISO - International Organization for Standardization. ISO 26262 Road vehicles Functional Safety Part 1-10, 2011.

[4] ISO - International Organization for Standardization. ISO/IEC 15408. In H. C. A. van Tilborg and S. Jajodia, editors, *Encyclopedia of Cryptography and Security (2nd Ed.)*. Springer, 2011.

[5] Microsoft Corporation. The stride threat model, 2005.

[6] SAE International. Guidelines and Mehtods for Conductiong the Safety Assessment Process on Civil Airborne Systems and Equipment, 1996.

[7] SAE International. Guidelines for Development of Civil Aircraft and Systems, 2010.

[8] K. Schmidt, P. Troeger, H. Kroll, and T. Buenger. Adapted Development Process for Security in Networked Automotive Systems. *SAE 2014 World Congress & Exhibition Proceedings*, (SAE 2014-01-0334):516 – 526, 2014.

[9] C. Schmittner, T. Gruber, P. Puschner, and E. Schoitsch. Security Application of Failure Mode and Effect Analysis (FMEA). In A. Bondavalli and F. Di Giandomenico, editors, *Computer Safety, Reliability, and Security*, volume 8666 of *Lecture Notes in Computer Science*, pages 310–325. Springer International Publishing, 2014.

[10] Special Committee 205 of RTCA. DO-178C Software Considerations in Airborne Systems and Equipment Certification, 2011.

[11] M. Steiner and P. Liggesmeyer. Combination of Safety and Security Analysis - Finding Security Problems That Threaten The Safety of a System. In *SAFECOMP 2013 - Workshop DECS (ERCIM/EWICS Workshop on Dependable Embedded and Cyber-physical Systems) of the 32nd International Conference on Computer Safety, Reliability and Security*, 2013.

[12] The Common Criteria Recognition Agreement Members. Common Criteria for Information Technology Security Evaluation. http://www.commoncriteriaportal.org/, 2014.

[13] D. Ward, I. Ibara, and A. Ruddle. Threat Analysis and Risk Assessment in Automotive Cyber Security. *SAE 2013 World Congress & Exhibition Proceedings*, pages 507–513, 2013.