Available online at www.sciencedirect.com
ScienceDirect
Procedia Computer Science 83 (2016) 1288 – 1294
Procedia Computer Science

The 1st Workshop on Safety & Security Assurance for Critical Infrastructures Protection (S4CIP)

Threat and Risk Assessment Methodologies in the Automotive Domain

Georg Macher[a,*], Eric Armengaud[a], Eugen Brenner[b], Christian Kreiner[b]

[a]*AVL List GmbH, Hans-List-Platz 1, 8010 Graz, Austria*
[b]*Graz University of Technology, Inffeldgasse 16, 8010 Graz, Austria*

Abstract

Safety and security are both qualities that concern the overall system. However, these disciplines are traditionally treated independently in the automotive domain. Replacement of classical mechanical systems with safety-critical embedded systems raised the awareness of the safety attribute and caused the introduction of the ISO 26262 standard. In contrast to this, security topics are traditionally seen as attacks of a mechanical nature and as only affecting single vehicles (e.g. door lock and immobilizer related). Due to the increasing interlacing of automotive systems with networks (such as Car2X), new features like autonomous driving, and online software updates, it is no longer acceptable to assume that car fleets are immune to security risks and automated remote attacks. Consequently, future automotive systems development requires appropriate systematic approaches to support cyber security and safety aware development.

Therefore, this paper examines threat and risk assessment techniques that are available for the automotive domain and presents an approach to classify cyber-security threats, which can be used to determine the appropriate number of countermeasures that need to be considered. Furthermore, we present a combined approach for safety and security analysis to be applied in early development phases, which is a pre-requisite for consistent engineering throughout the development lifecycle.

Peer-review under responsibility of the Conference Program Chairs
Keywords: ISO 26262, HARA, STRIDE, automotive systems, safety / security co-engineering.

1. Introduction

In the late 1970s self-contained embedded systems called Electronic Control Units (ECUs) were introduced into production vehicles. Since then, the complexity of embedded systems in the automotive industry has grown significantly. Embedded automotive systems are estimated account for 80 % of product innovations in the past decade and are responsible for 25% of current vehicle costs[25]. Such computer systems have been integrated into almost every aspect of a car and control throttle, transmission, brakes, passenger climate and infotainment.

Additionally, today's information society strongly supports inter-system communication (Car2X) in the automotive domain. Consequently the boundaries of application domains are disappearing even faster, which causes multiple cross-domain collaborations and interactions. This higher degree of integration and the safety- and security-criticality of the control application raises new challenges. These challenges have a major impact on product development and

* Corresponding author. Tel.: +43-316-878-2974 ; fax: +43-316-878-2974.
E-mail address: georg.macher@avl.com

Peer-review under responsibility of the Conference Program Chairs
doi:10.1016/j.procs.2016.04.268

product release as well as the brand reputation of a company. Consequently, future automotive systems development requires appropriate systematic approaches to support cyber security and safety aware development.

Therefore, safety standards such as ISO 26262 [12] for road vehicles have been established to provide guidance during the development of safety-critical systems. In contrast to this, security topics are traditionally seen as physical attacks that only affect single vehicles (e.g. door lock and immobilizer related). Due to new functionalities like autonomous driving, and online software updates, it is no longer acceptable to assume that car fleets are immune to security risks and automated remote attacks. Consequently, future automotive systems development requires appropriate systematic approaches to support cyber security and safety aware development.

To that aim, this paper examines threat and risk assessment techniques available for the automotive domain and presents an approach to classify cyber-security threats, which can be used to determine the appropriate number of countermeasures that need to be considered. Furthermore, we present a combined approach for safety and security analysis to be applied in early development phases, which is a pre-requisite for consistent engineering along the development lifecycle. Indeed, a common analysis method delivering consistent dependability targets across the different attributes is the basis of performing consistent dependability engineering during the entire product development.

This document is organized as follows: Section 2 assesses related works dealing with (automotive) safety and security related topics. Section 3 provides a description of the applied method and the contribution to an early development phase safety-hazards and security-threat analysis. An application of the approach for an automotive battery management system (BMS) use-case scenario is presented in Section 4. Concluding remarks can be found in Section 5.

2. Related Work

Safety and security engineering are very closely related disciplines and could greatly benefit from one another if adequate interactions are defined. Both disciplines focus on system-wide features and should be integrated into the development process from the initial phases and onwards. Safety engineering is already an integral part of automotive engineering and safety standards are well established in the automotive industry. Safety assessment techniques, such as failure mode and effects analysis (FMEA) [9] and fault tree analysis (FTA) [10], among others, are specified, standardized, and integrated in the automotive development process landscape. Nevertheless, security engineering practices and methods are not yet that settled in the automotive domain.

The road vehicles functional safety norm ISO 26262 [12] and its basic norm IEC 61508 [8] both provide a first approach to integrating security requirements in their novel draft editions. IEC 61508 Ed 2.0 states that security threats should be considered during hazard analysis in the form of a security threat analysis. However, this threat analysis is not specified in more details in the standard and IEC 61508 Ed 3.0 is due to be elaborated regarding security-aware safety topics. Also ISO 26262 Ed 2.0, which is currently in progress, is likely to include recommendations for fitting security standards and appropriate security measure implementations. Nevertheless, neither the recently presented SAE cybersecurity guidebook SAE J3061 [30], nor the ISO 26262 draft specify the threat analysis methods to be applied in more detail.

In aeronautics domain ARP4754 [22] provides guidance for system level development and defines steps for the adequate refinement and implementation of requirements. Security concerns in the aeronautics industry are tackled by the Common Criteria [29,13] specification.

Other standards, such as IEC 62443 [11], or guidelines, such as SAE J3061 [30], are not applicable in practice for the automotive domain in their current state. An analysis done by SoQrates Security AK [2] indicates that the available standards are frequently fragmented or incomplete, and typically assume that their open issues are covered by other guidelines or standards. For this reason, several other researchers and research projects have also recently made efforts and publications to combine security and safety engineering approaches.

As mentioned earlier in the document, security has long been a concern in the aeronautics domain. In the avionics domain DO-178C [27], which addresses aeronautics software safety, and ARP4754 [22] provide 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), among others, are specified by ARP4761 [21] and security concerns in aeronautics industry are tackled, for example, by the Common Criteria [29,13] approach and the ED202 specification [5].

Paulitsch et. al [18] outline issues in assessing the reliability of avionics software for safety and security perspectives. The authors aim at finding indicators and collecting evidence of effectiveness of existing safety-related and security-related processes in terms of effects on aircraft security.

An overall security threat analysis of an unmanned aerial vehicle (UAV) is done by Javaid et. al [14]. This work calculates the likelihood, impact, and risk of a security threat. Nevertheless, an estimation of the likelihood of an

attack can be inappropriate due to the fact that in some cases a threat's likelihood of appearing must be assumed to be 100% for the design phase.

A threat analysis framework for critical infrastructures is proposed by Simion et. al[26]. This framework identifies and defines threat attributes and uses these attributes to characterize the threat potential. The authors consider the required resources and attacker's commitment in order to determine the threat attributes.

In other domains, such as personal computers and consumer electronics, security analysis is more common and approaches and best practices are well known. Although, embedded automotive systems and the automotive domain do have different constraints to these domains and adaptations are required.

The STRIDE threat model approach[17] developed by Microsoft Corporation can be used to expose security design flaws. This approach uses a technique called threat modeling which is based reviewing the system design in a methodical way. Threat modeling is processed in five steps: (a) the identification of security objectives, (b) a survey of the application, (c) the decomposition of the application, (d) the identification of threats, and (e) the identification of vulnerabilities. Threat models, like the STRIDE approach, may often not prove that a given design is secure, but they help to learn from mistakes and avoid repeating them.

In the automotive domain project, SeSaMo[1] (Security and Safety Modeling for Embedded Systems) the focus is on synergies and trade-offs between security and safety in concrete use-cases. The work of Gashi et al.[7] is part of this project and focuses on redundancy and diversity, and their effects on safety and security of embedded systems.

A security-informed risk assessment is mentioned in the work of Bloomfield et. al[4]. The focus of this publication is a 'security-informed safety case' and the impact of security on an existing safety case, but neither guidance for such an assessment is provided nor an assessment approach is proposed. The authors mention the requirement of such an assessment methodology and describe a risk assessment process briefly, but neither provide guidance as to how such an assessment is done, nor do they propose an approach to it.

Kath et. al[15] state model-based approaches as a promising approach to guarantee safety and security feature implementation. The authors present a model driven approach to security accreditation of service-oriented architectures in their work.

Some recent publications in the automotive domain also focus on security in automotive systems. On the one hand, the work of Schmidt et. al[23] presents a security analysis approach to identify and prioritize security issues, but solely provides an analysis approach for networked connectivity.

The work of Ward et. al[31], on the other hand, also mentions a risk assessment method for security risk in the automotive domain called threat analysis and risk assessment, based on HARA. This work identifies potential security attacks and the risk associated with these attacks. The work also describes how such a method has been developed based on the state-of-the-art HARA method.

The works of Roth et. al[20] and Steiner et. al[28] also deal with safety and security analysis, but focus on state/event fault trees for modeling of the system under development, while Schmittner et. al[24] present a failure mode and failure effect model for safety and security cause-effect analysis. This work also categorizes threats also with the help of the STRIDE threat model with the focus of an IEC60812 conforming FMEA approach.

Raspotnig et. al[19] also combine safety and security methods for combined safety and security assessments of air traffic management systems. The approach of their publication relies on modeling misuse cases and misuse sequence diagrams within a UML behavior diagram.

The SAHARA concept[16] quantifies the security impact on dependable safety-related automotive system development at system level. This concept classifies the security threats of an automotive system using the STRIDE approach[17] and a special quantification scheme developed for automotive application. The basis for this security analysis is the hazard analysis and risk assessment (HARA)[12] safety analysis, which identifies and categorizes hazardous events relating to components of the system under development (SuD). This approach combines hazard and threat analysis within one approach to acknowledge threats that may contribute to the safety-concept or lead to violation of safety goals. Moreover, it also allows the systematical identification of non-safety related security threats (in contrast to[14,4,31]) based on the STRIDE approach. In contrast to[20,28,24], which require higher analysis efforts and more details of the SuD, the characterization of the attack probabilities with the SAHARA approach is less complex and more applicable for earlier development phases.

3. Safety-Aware Hazard Analysis and Risk Assessment (SAHARA) Approach

This section describes the SAHARA approach[16], and characterizes the contribution of this paper, the enhancements of the quantification scheme for remote and fleet cyber-security attacks, which will be applied in the next section in more detail. The SAHARA method combines the automotive HARA[12] with the security domain STRIDE

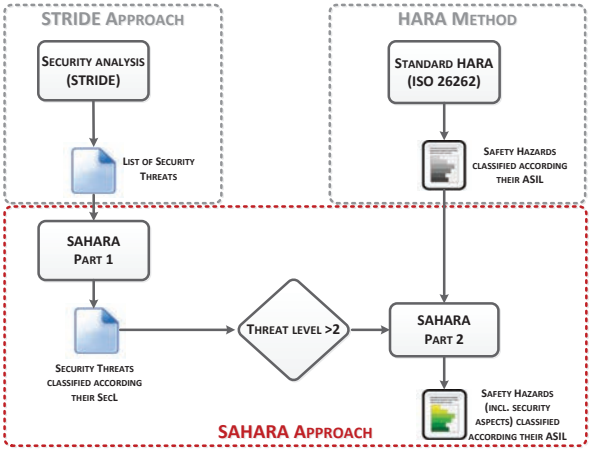

Fig. 1. Conceptual overview of the SAHARA method [16]

approach [17] to trace the impact of security issues on safety concepts at system level. STRIDE is an acronym for **S**poofing, **T**ampering, **R**epudiation, **I**nformation disclosure, **D**enial of service, and **E**levation of privileges; moreover the STRIDE threat model can be seen as the security equivalent to HARA. The key concept of this threat modeling approach is the analysis of each system component for susceptibility of threats and mitigation of all threats to each component in order to argue that a system is secure.

Figure 1 shows the conceptual overview of the SAHARA method. As can be seen in the figure, an ISO 26262 conforming HARA analysis (right part of the overview figure) can be performed in a conventional manner. Besides this, attack vectors of the system can be independently modeled using the STRIDE approach (left part of **Fig. 1**) by specialists of the security domain. The two-stage SAHARA method then combines the outcome of this security analysis with the outcomes of the safety analysis. The SAHARA method applies a key concept of the HARA approach, the definition of automotive safety integrity level (ASILs), to the STRIDE analysis outcomes. Threats are quantified similarly to ASIL quantification, according to the resources (R) and know-how (K) required to exert the threat, and the threat's criticality (T). Security threats that might lead to a violation of safety goals (T = 3) can be handed over to HARA for further safety analysis. This helps to improve completeness of safety analysis in terms of the ISO 26262 requirement of analysis of 'foreseeable misuse', in this case hazardous events initiated due to security attacks.

Table 1 contains examples of resources, know-how, and threat levels for each quantification level of K, R, and T values. The three factors define a security level (SecL), as shown in Table 2 which is used to determine the appropriate number of countermeasures needed to be considered.

Table 1. Classification Examples of Knowledge 'K', Resources 'R', and Threat 'T' Value of Security Threats

Level	Knowledge Example	Resources Example	Threat Criticality Example
0	average driver, unknown internals	no tools required	no impact
1	basic understanding of internals	standard tools, screwdriver	annoying, partial reduced service
2	internals disclose, focused interests	non-standard tools, sniffer, oscilloscope	damage of goods, invoice manipulation, privacy
3		advanced tools, simulator, flasher	life-threatening possible

Table 2. SecL Determination Matrix - Determination of the security level from R, K, and T values

Required Resources 'R'	Required Know-How 'K'	Threat Level 'T' 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

This quantification of required know-how and tools instead of any likelihood estimation (e.g. of the attack's success or fail, done by Javaid et al.[14]) is beneficial due to the fact that the classification of these factors is better aligned with the HARA classification common in the automotive domain. Additionally, for the design phase the likelihood estimation of an attack must be assumed to be 100% and it is more likely that required know-how and resources required to exert a threat remain the same over the whole life-time of the SuD. The SAHARA method further mentions, that after this quantification of threats, adequate reduction or prevention by appropriate design and countermeasures shall be performed. In the case of safety-related security threats, the threat can be analyzed and resulting hazards evaluated according their controllability, exposure, and severity. This improves, as mentioned earlier in this document, the completeness of the required situation analysis of the HARA approach by implying factors of reasonably foreseeable misuse (security threats) in a more structured way. Moreover, a combined review of the safety analysis by security and safety experts also helps to improve the completeness of security analysis. The combination of the different mindsets and engineering approaches of safety engineers and security engineers, which are able to work independently from another and mutually benefit from each other's findings, are more likely to be result in higher maturity of their analysis.

3.1. Enhancements of the Threat Quantification Scheme

The previously mentioned SAHARA method is geared towards the needs of an analysis of security threats in the automotive domain at an early development phase (concept level). Nevertheless, this analysis focuses on the development of a single car, the identification of security threats and safety risks at early development phases and their mutual dependencies. For analysis of remote cyber-security attacks and attacks geared towards whole car fleets the SAHARA threat quantification scheme is lacking in terms of measures for damage potential and affected users.

Therefore, this work provides a novel approach to the quantification of threats. The quantification of threats according to the risks they pose allows threats with the highest risk level to be resolved first and therefore make risk management more economical. The novel threat classification approach we propose is an adapted DREAD classification scheme[3], which can be promising for a more detailed analysis of the system design.

The DREAD acronym stands for:

- Damage Potential - determines the damage if vulnerability is exploited
- Reproducibility - identifies the repeatability of the attack
- Exploitability - defines the applicability of the attack for repetition
- Affected Users - represents an estimation of how many users might be affected
- Discoverability - determines how easy the vulnerability can be found in the field

The proposed classification should quantify each category with none (0), low (1), medium (2), or high (3) impact factors. Adding up these factors results in a risk priority number (RPN) for each of the threats, as known by the failure mode and effects analysis (FMEA)[9] in the safety domain. This scheme better determines the damage potential differences of threats and also represents an impact on the number of users affected.

4. Application of the Approach

This section describes the application of the SAHARA approach for an automotive battery management system (BMS) and evaluates the new threat quantification scheme. The BMS use-case is an illustrative material, reduced for training purposes; technology-specific details have been abstracted for commercial sensitivity and analysis results presented are not intended to be exhaustive. The SAHARA analysis is done in a classical way, by determining the SecL, and with the newly proposed DREAD approach to analyze the difference between these two rating systems.

The SAHARA method allows the description of the hazard and the worst situation in which this hazard may occur in conventional ISO 26262 aligned manner. The 'hazardous situations' are classified by an ASIL via severity, exposure, and controllability and a high-level safety target (safety goal) and safety function (safe state) can be done (established HARA analysis).

The security related analysis part of the SAHARA method is shown partially in Figure 2. The components of the system and their possible attack vectors (taken from initial system design and the STRIDE approach respectively) are used to generate a list of possible attacks. This list is detailed with a general situation description in which this attack may be performed and the high level system service malfunction to which the attack will lead. The first phase of the SAHARA method is concluded by the classification of the security risk by a SecL via resource, know-how, and

Security Risk description					Security Risk		Security Risk related Safety goal description				
Security Hazard ID	STRIDE Function	Attack description	General Situation	attacker generated malfunction	Threat Level 'T'	Resulting SecL	Severity 'S'	Exposure 'E'	Controlability 'C'	Resulting ASIL	Safety Goal
SH_1	Spoofing	spoofing of HV system ready signals	all	HV system ready without ensured overall system safety	3	1	3	4	3	ASIL D	Prevent from electric shock
SH_4	Spoofing	spoofing actual sensor readings	all	extending safe operation areas of HV battery (temp, cell current, cell voltages)	3	3	2	4	3	ASIL C	Battery outgasing and fire shall be prevented
SH_5	Denial of service	DoS communication with charger	charging	communication with charger jammed	3	0	3	4	3	ASIL D	Battery outgasing and fire shall be prevented

Fig. 2. Screenshot of application of SAHARA method

Table 3. Classification Extracts of SAHARA and DREAD Threat Rating Systems

Security Threat	'K'	'R'	'T'	'SecL'	'D'	'R'	'E'	'A'	'D'	'RPN'
spoofing of HV system ready signals	2	2	3	1	3	2	1	1	1	8
DoS communication with charger	2	3	3	0	2	2	2	2	1	9
tampering of cycle status	2	2	2	0	2	2	3	1	2	10

threat level of the security attack. This SecL classification provides means for assigning adequate efforts to mitigate the security risk and also states high-level security requirements to close these attack vectors. Figure 2 also highlights level 3 threats. These security threats are handed over to the safety analysis for further analysis of their safety impact.

Table 3 shows the comparison of security threats analyzed in the classical SAHARA way and with the newly proposed DREAD analysis. As can be seen by these extracts, the SecL of these threats is relatively low (1 or 0); the resulting RPN are nearly equal but show the significant difference that those threats which have a $SecL = 0$ have a higher RPN than the threat with the $SecL = 1$. This results on one hand due to the fact that the threat 'DoS communication with charger' is assumed to be done on the side of the external charger and therefore also has a potential impact on more users. On the other hand, the exploitability of the threat 'spoofing of HV system ready signals' is, although having a high threat criticality, lower compared to the other example threats.

5. Conclusion

In conclusion, safety and security are two challenging research domains for future automotive systems. Nevertheless, as stated by Firesmith[6], safety and security engineering are very closely related disciplines and could mutually benefit from one another if their similarities are recognized and adequate interactions are established in a correct manner.

This paper examines threat and risk assessment techniques available for the automotive domain and presents an approach to classify cyber-security threats and safety risks. The safety-aware hazard analysis and risk assessment (SAHARA) approach combines the automotive HARA (hazard analysis and risk assessment) with the security domain STRIDE. This classification can be used to determine the appropriate number of countermeasures that need to be considered. The application of the SAHARA method has been demonstrated for an automotive battery management system use-case. Additionally, an evaluation of the typical way of applying the SAHARA method, by determining the SecL, and with the DREAD approach has been done to analyze the difference between these two classification schemes. This novel threat classification scheme is more appropriate for the analysis of remote cyber-security attacks and attacks affecting whole car fleets due to its incorporation of measures for damage potential and affected users. While the authors do not claim completeness or representativeness of the BMS use-case, the benefits of the approach are already evident.

Acknowledgments

This work is supported by the EMC^2 project. The research leading to these results has received funding from the ARTEMIS Joint Undertaking under grant agreement nr 621429 (project EMC^2).

References

1. http://sesamo-project.eu/.
2. http://soqrates.eurospi.net/.
3. https://www.owasp.org/index.php/threat_risk_modeling.
4. Robin Bloomfield, Kateryna Netkachova, and Robert Stroud. Security-Informed Safety: If Its Not Secure, Its Not Safe. In Anatoliy Gorbenko, Alexander Romanovsky, and Vyacheslav Kharchenko, editors, *Software Engineering for Resilient Systems*, volume 8166 of *Lecture Notes in Computer Science*, pages 17–32. Springer Berlin Heidelberg, 2013.
5. European Organization for Civil Aviation Equipment (EUROCAE WG-72) and Radio Technical Commission for Aeronautics (RTCA SC-216). Airworthiness security process specification, ED-202, 2010.
6. Donald Firesmith. Common Concepts Underlying Safety, Security, and Survivability Engineering. Technical Report CMU/SEI-2003-TN-033, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, 2003.
7. Ilir Gashi, Andrey Povyakalo, Lorenzo Strigini, Martin Matschnig, Thomas Hinterstoisser, and Bernhard Fischer. Diversity for Safety and Security in Embedded Systems. In *International Conference on Dependable Systems and Networks*, volume 26, 06 2014.
8. ISO - International Organization for Standardization. IEC 61508 Functional safety of electrical/ electronic / programmable electronic safety-related systems.
9. ISO - International Organization for Standardization. IEC 60812 Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA) , 2006.
10. ISO - International Organization for Standardization. IEC 61025 Fault tree analysis (FTA) , December 2006.
11. ISO - International Organization for Standardization. IEC 62443 - Industrial communication networks Network and system security , 2009.
12. ISO - International Organization for Standardization. ISO 26262 Road vehicles Functional Safety Part 1-10, 2011.
13. ISO - International Organization for Standardization. ISO/IEC 15408. In Henk C. A. van Tilborg and Sushil Jajodia, editors, *Encyclopedia of Cryptography and Security (2nd Ed.)*. Springer, 2011.
14. Ahmad Y. Javaid, Weiqing Sun, Vijay K. Devabhaktuni, and Mansoor Alam. Cyber Security Threat Analysis and Modeling of an Unmanned Aerial Vehicle System. In *IEEE Conference on Technologies for Homeland Security (HST)*, pages 585–590, Nov 2012.
15. Olaf Kath, Rudolf Schreiner, and John Favaro. Safety, Security, and Software Reuse: A Model-based Approach. In *Fourth International Workshop in Software Reuse and Safety Proceedings*, Sept 2009.
16. G. Macher, H. Sporer, R. Berlach, E. Armengaud, and C. Kreiner. SAHARA: A security-aware hazard and risk analysis method. In *Design, Automation Test in Europe Conference Exhibition (DATE), 2015*, pages 621–624, March 2015.
17. Microsoft Corporation. The STRIDE Threat Model, 2005.
18. Michael Paulitsch, Rupert Reiger, Lorenzo Strigini, and Robin Bloomfield. Evidence-Based Security in Aerospace. *ISSRE Workshops 2012*, pages 21–22, 2012.
19. Christian Raspotnig, Vikash Katta, Peter Karpati, and Andreas L. Opdahl. Enhancing CHASSIS: A Method for Combining Safety and Security. In *2013 International Conference on Availability, Reliability and Security, ARES 2013, Regensburg, Germany, September 2-6, 2013*, pages 766–773, 2013.
20. Michael Roth and Peter Liggesmeyer. Modeling and Analysis of Safety-Critical Cyber Physical Systems using State/Event Fault Trees. 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.
21. SAE International. Guidelines and Mehtods for Conductiong the Safety Assessment Process on Civil Airborne Systems and Equipment, 1996.
22. SAE International. Guidelines for Development of Civil Aircraft and Systems, 2010.
23. 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.
24. Christoph Schmittner, Thomas Gruber, Peter Puschner, and Erwin Schoitsch. Security Application of Failure Mode and Effect Analysis (FMEA). In Andrea Bondavalli and Felicita Di Giandomenico, editors, *Computer Safety, Reliability, and Security*, volume 8666 of *Lecture Notes in Computer Science*, pages 310–325. Springer International Publishing, 2014.
25. Giorgio Scuro. Automotive industry: Innovation driven by electronics. http://embedded-computing.com/articles/automotive-industry-innovation-driven-electronics/, 2012.
26. Cristina P. Simion, Olga M. C. Bucovtchi, and Cristian A. Popescu. Critical Infrastructures Protection Through Threat Analysis Framework. *Annals of the ORADEA UNIVERSITY*, 1:351–354, May 2013.
27. Special Committee 205 of RTCA. DO-178C Software Considerations in Airborne Systems and Equipment Certification, 2011.
28. Max Steiner and Peter 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.
29. The Common Criteria Recognition Agreement Members. Common Criteria for Information Technology Security Evaluation. http://www.commoncriteriaportal.org/, 2014.
30. Vehicle Electrical System Security Committee. SAE J3061 Cybersecurity Guidebook for Cyber-Physical Automotive Systems.
31. 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.