A Review of Threat Analysis and Risk Assessment Methods in the Automotive Context

Conference Paper *in* Lecture Notes in Computer Science · September 2016

DOI: 10.1007/978-3-319-45477-1_11

4 authors, including:

Georg Macher
Graz University of Technology
72 PUBLICATIONS **369** CITATIONS
SEE PROFILE

Eric Armengaud
AVL LIST GMBH
111 PUBLICATIONS **680** CITATIONS
SEE PROFILE

Christian Kreiner
Institute of Electrical and Electronics Engineers
211 PUBLICATIONS **987** CITATIONS
SEE PROFILE

A Review of Threat Analysis and Risk Assessment Methods in the Automotive Context

Georg Macher[1], Eric Armengaud[1], Eugen Brenner[2], and Christian Kreiner[2]

[1] AVL List GmbH
{georg.macher, eric.armengaud}@avl.com
[2] Institute for Technical Informatics
Graz University of Technology
{brenner, christian.kreiner}@tugraz.at

Abstract. Consumer demands for advanced automotive assistant systems and connectivity of cars to the internet make cyber-security an important requirement for vehicle providers. As vehicle providers gear up for the cyber security challenges, they can leverage experiences from many other domains, but nevertheless, must face several unique challenges. Thus, several security standards are well established and do not need to be created from scratch. The recently released SAE J3061 guidebook for cyber-physical vehicle systems provides information and high-level principles for automotive organizations to identify and assess cyber-security threats and design cyber-security aware systems.
In the course of this document, a review of available threat analysis methods and the recommendations of the SAE J3061 guidebook regarding threat analysis and risk assessment method (TARA) is given. The aim of this work is to provide a position statement for the discussion of available analysis methods and their applicability for early development phases in context of ISO 26262 and SAE J3061.

Keywords: TARA, ISO 26262, SAE J3061, automotive, security analysis.

1 Introduction

Numerous industrial sectors are currently confronted with massive difficulties originating from managing the increasing complexity of systems. The automotive industry, for instance, has an annual increase rate of software-implemented functions of about 30% [1]. This rate is only higher for avionics systems and the Internet of Things [9]. New challenges regarding the manageability of systems are emerging caused by the increasing gap between cross-domain expertise required and the pervasiveness of novel technologies and software functions. In the automotive domain this evolution became challenging with the advent of multi-core processors, advanced driving assistance systems and automated driving functionalities, and the thus broadening societal sensitivity for security and safety properties (remote hacking and control of cars). Management of extra-functional properties (e.g. timing, safety, security, memory consumption, etc.) is still one of the core challenges faced by developers of embedded systems [14]. Appropriate systematic approaches to support the development of these properties are thus required. Standards and guidelines, such as ISO 26262 [6] in the automotive safety and more recently SAE J3061 [15] in automotive security domain, have been established to provide guidance during the development of dependable systems and are currently reviewed for similarities and alignment.

In the course of this document, a review of available threat analysis methods and the recommendations of the SAE J3061 guidebook regarding threat analysis and risk assessment method (TARA) is given. The aim of this work is to provide a position statement for the discussion of available analysis methods and their applicability for early development phases in context of ISO 26262 and SAE J3061.

We provide an overview of the recommendations of the SAE J3061 guidebook regarding threat analysis and risk assessment method (TARA) for this paper together with a review of available threat analysis methods. The aim of this work is to provide an evaluation of available analysis methods for the discussion of their applicability for early development phases in the context of ISO 26262 and SAE J3061.

This paper is organized as follows: Section 2 reviews the recommendations of the SAE J3061 guidebook regarding threat analysis and risk assessment method (TARA). Based on this review, Section 3 analyzes the TARA approaches available in the automotive domain. In Section 4 an evaluation of the applicability of the analysis methods for early development phases in context of ISO 26262 and SAE J3061 is provided. Finally, Section 5 concludes the work.

2 SAE J3061 Guidebook TARA Recommendations

Safety and security engineering are very closely related disciplines. They both focus on system-wide features and could greatly benefit from one another if adequate interactions are defined. Safety engineering is already an integral part of automotive engineering and safety standards, such as the road vehicles – functional safety norm ISO 26262 [6] and its basic norm IEC 61508 [2], are well established in the automotive industry. Safety assessment techniques, such as failure mode and effects analysis (FMEA) [3] and fault tree analysis(FTA) [4], are also specified, standardized, and integrated in the automotive development process landscape.

IEC 61508 Ed 2.0 provides a first approach of integrating safety and security; security threats are to 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 Ed 3.0 is about to be more elaborated on security-aware safety topics. Also ISO 26262 Ed 2.0, which is still in progress, is likely to include recommendations for fitting security standards and appropriate security measure implementations.

The recently published SAE J3061 [15] guideline establishes a set of high-level guiding principles for cyber-security by:

- defining a complete lifecycle process framework
- providing information on some common existing tools and methods
- supporting basic guiding principles on cyber-security
- summarizing further standard development activities

SAE J3061 states that cyber-security engineering requires an appropriate lifecycle process, which is defined analogous to the process framework described in ISO 26262. Further, no restrictions are given on whether to maintain separate processes for safety and security engineering with appropriate levels of interaction or to attempt direct integration of the two processes. Apart from that, the guidebook recommends an initial assessment of potential threats and an estimation of risks for systems that may be considered cyber-security relevant or are safety-related systems, to determine whether there are cyber-security threats that can potentially lead to safety violations.

In paragraph 3.88 of SAE J3061 TARA is defined as: *'an analysis technique that is applied in the concept phase to help identify potential threats to a feature and to assess the risk associated with the identified threats...' [15]*

In paragraph 8.3.3 of SAE J3061 this threat analysis and risk assessment (TARA) method is further specified as a method identifying threats and assessing the risk and residual risk of the identified threats by following three steps:

1. Threat Identification
2. Risk Assessment (includes classification of the risk associated with a particular threat)
3. Risk Analysis, which ranks threats according to their risk level

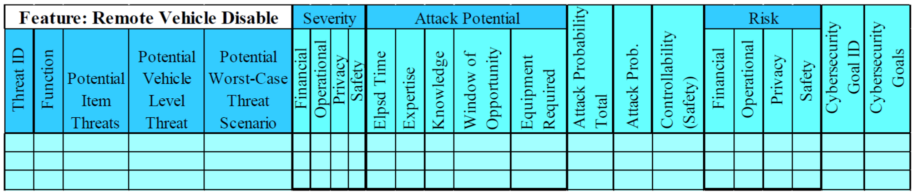
Beyond this the guidebook does not give any restrictions on how to excerpt the TARA analysis. *'It is left to an organization to determine which TARA method is appropriate for their purposes, and to determine what an acceptable level of risk means ...' [15]*

Appendices A-C of the SAE J3061 provide an overview of the techniques for threat analysis and risk assessments and threat modeling and vulnerability analysis. These TARA methods proposals will also be analyzed in the following section of this document, and are:

- EVITA method
- TVRA
- OCTAVE
- HEAVENS security model
- Attack trees
- SW vulnerability analysis

3 TARA Approaches Available for the Automotive Domain

This section of the document analyzes the TARA approaches available in the automotive domain. Some TARA approach suggestions are already given by Appendix A of the SAE J3061 guidebook [15]. This section thus mentions those TARA approaches already introduced by SAE J3061 (recommended or not-recommended) and those not mentioned in the guidebook separately. Additionally, SAE J3061 already mentions a limited applicability of some of the methods introduced for the automotive domain. These methods are only mentioned briefly in this document for the sake of completeness and are not further detailed.



Feature: Remote Vehicle Disable					Severity				Attack Potential								Risk					
Threat ID	Function	Potential Item Threats	Potential Vehicle Level Threat	Potential Worst-Case Threat Scenario	Financial	Operational	Privacy	Safety	Elpsd Time	Expertise	Knowledge	Window of Opportunity	Equipment Required	Attack Probability Total	Attack Prob.	Controllability (Safety)	Financial	Operational	Privacy	Safety	Cybersecurity Goal ID	Cybersecurity Goals

Fig. 1. The EVITA method using THROP spreadsheet example (from [15])

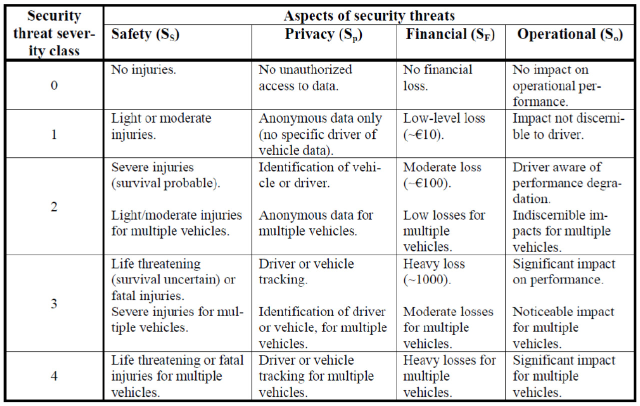
3.1 TARA Approaches recommended in SAE J3061

The EVITA method is part of a European Commission funded research project (EVITA - E-Safety Vehicle Intrusion Protected Applications) and is an adaptation of ISO 26262 HAZOP analysis for security engineering. The method is named threat and operability analysis (THROP) and considers potential threats for a particular feature from a functional perspective. Threats are defined at the functional level based on the primary functions of the analyzed feature using attack trees. Thus, THROP first identifies the primary functions of the feature, second applies guide-words to identify potential threats and third determines potential worst-case scenario outcomes from the potential malicious behavior. **Fig. 1** shows a THROP spreadsheet example.

The risk level determination is also adopted from ISO 26262 (ASIL determination) based on a combination of severity, attack probability, and controllability measures. The severity classification separates different aspects of the consequences of security threats (operational, safety, privacy, and financial); as shown in **Fig. 2**. Similar to the determination of the ASIL, controllability, severity, and attack probability are mapped to a qualitative risk levels (R0 to R7 and R7+) for classification of the security threats. This risk level determination reveals some issues of the approach: (a) the classification of severity as standardized in ISO 26262 is adopted and thus no longer conforms to the ISO 26262 standard, (b) the classification of safety-related threats and non-safety-related (operational, privacy, and financial) threats differs and could thus lead to imbalance of efforts and (c) the sufficient accuracy of attack potential measures and expression as probabilities is still an open issue, as also the combination of these probabilities by summing, minimum, and maximum operations.

Nevertheless, the classification of attack potentials and the analysis based on threat trees is suitable at feature or system level and thus applicable for embedded automotive systems. Although not explicitly mentioned this method seems to be the method that is most recommended in the SAE J3061 guidebook for an initial assessment of potential threats and estimation of risks for cybersecurity relevant or safety-related systems.

HEAVENS security model analyzes threats based on Microsoft's STRIDE [8] approach and ranks the threats based on a risk assessment. This risk assessment consists of three steps: (a) determination of threat level (TL), (b) determination of impact level (IL), and (c) determination of security level (SL), which corresponds to the final risk ranking.



Security threat severity class	Aspects of security threats			
	Safety (S_S)	Privacy (S_p)	Financial (S_F)	Operational (S_o)
0	No injuries.	No unauthorized access to data.	No financial loss.	No impact on operational performance.
1	Light or moderate injuries.	Anonymous data only (no specific driver of vehicle data).	Low-level loss (~€10).	Impact not discernible to driver.
2	Severe injuries (survival probable). Light/moderate injuries for multiple vehicles.	Identification of vehicle or driver. Anonymous data for multiple vehicles.	Moderate loss (~€100). Low losses for multiple vehicles.	Driver aware of performance degradation. Indiscernible impacts for multiple vehicles.
3	Life threatening (survival uncertain) or fatal injuries. Severe injuries for multiple vehicles.	Driver or vehicle tracking. Identification of driver or vehicle, for multiple vehicles.	Heavy loss (~1000). Moderate losses for multiple vehicles.	Significant impact on performance. Noticeable impact for multiple vehicles.
4	Life threatening or fatal injuries for multiple vehicles.	Driver or vehicle tracking for multiple vehicles.	Heavy losses for multiple vehicles.	Significant impact for multiple vehicles.

Fig. 2. The EVITA Severity Classification Scheme (from [11])

The determination of the threat level (TL), which corresponds to a 'likelihood estimation', is based on four parameters (expertise of the attacker, knowledge about the system, window of opportunity, and equipment), which are individually estimated using values between 0 and 3 (referring to the different levels: none, low, medium, and high).

The threat impact level (IL) estimates the impact on four categories (safety, financial, operational, and privacy and legislation). For the IL quantification the impact level of the attack on these four categories is parametrized with no impact (value 0), low (value 1), medium (value 10), or high impact (value 100). The summation of the values of the impact parameters is then quantified via 5 IL values (no impact for 0, low for 1 -19, medium 20 -99, high 100 -999 and critical $\geq$ 1000)

The threat level factors (TL) and threat impact level (IL) further derive the security level (SL) and thus the ranking of risks. This approach clearly benefits from the structured and systematic STRIDE approach to exploit threats, but requires a huge amount of work to analyze and determine the SL of individual threats; which implies lots of discussion potential for each individual IL and TL factor of each single threat.

3.2 TARA Approaches also proposed in SAE J3061

The methods mentioned in this section are also proposed by the SAE J3061 guide book, but are not recommended for application in the automotive context. Thus, these methods are only mentioned in this document for the sake of completeness.

TVRA Threat, vulnerabilities, and implementation risks analysis (TVRA) identifies assets in the system and their associated threats by modeling the likelihood and impact of attacks. The analysis was developed for data - and telecommunication networks and is scarcely applicable for cyber physical systems in vehicles.

OCTAVE stands for Operationally Critical Threat, Asset, and Vulnerability Evaluation and is a process-driven threat assessment methodology. OCTAVE focuses on bringing together stake holders of security through a progressive series of workshops; thus this approach is best suited for enterprise information security risk assessments but not readily applicable for embedded automotive systems.

Attack tree analysis (ATA) is analogous to the safety fault tree analysis (FTA) and thus adequate for exploiting combinations of threats (attack patterns), but requires more details of the system design (thus not appropriate for an initial TARA at early development phases).

SW vulnerability analysis , as the name implies, examines software code for known software constructs that should be avoided to prevent from potential vulnerabilities. This method aims at SW development level and is thus in-appropriate for early development phases.

3.3 TARA Approaches not mentioned by SAE J3061

FMVEA method is based on an FMEA as described in IEC 60812 [3]. Schmittner et. al [13] present this failure mode and failure effect model for safety and security cause-effect analysis. This work categorizes threats via quantification of threat agents (respectively attacker), threat modes (via STRIDE model), threat effects and attack probabilities. A general limitation of this analysis is the restriction to analyze only single causes of an effect and multi-stage attacks could be overlooked, thus the combination of FTA and ATA for supporting the FMVEA is considered. Nevertheless, the FMVEA method is based on the FMEA (safety pendant) and is thus in-appropriate for early development phases (TARA).

SAHARA method [7] quantifies the security impact on dependable safety-related system development on system level. The SAHARA method combines the automotive HARA [6] with the security domain STRIDE approach [8] to trace impacts of security issues on safety concepts on the system level.

For the safety analysis an ISO 26262 conform HARA analysis can be performed in a conventional manner. Also a security focused analysis of possible attack vectors of the system can be done using the STRIDE approach independently from the safety team. For a combined approach, the SAHARA method combines the outcome of this security analysis with the outcomes of the safety analysis. Thus, the ASIL quantification concept is applied to the STRIDE analysis outcomes. Threats are quantified aligned with ASIL analysis, according to the resources (R), know-how (K) required to exert the threat, and the threats criticality (T). **Table 1** shows the determination schemes for the different elements.

These three factors determine the resulting security level (SecL). The SecL determination is based on the ASIL determination approach and is calculated according to (1).

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, partially 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

$$SecL = \begin{cases} 4 & \text{if } 5 - K - R + T \geq 7 \\ 3 & \text{if } 5 - K - R + T = 6 \\ 2 & \text{if } 5 - K - R + T = 5 \\ 1 & \text{if } 5 - K - R + T = 4 \\ 1 & \text{if } T = 3, K = 2, R = 3 \\ 0 & \text{if } 5 - K - R + T < 4 \text{ } or \text{ } T = 0 \end{cases} \tag{1}$$

The SAHARA quantification scheme is less complex and requires less analysis effort and fewer details of the analyzed system than other proposed approaches. This quantification enables the possibility for determining limits on resources allocated to prevent the system from a specific threat (risk management for security threats) and the quantification of the threats impact on safety goals (threat level 3) or not (all others).

SHIELD is a methodology for assessing security, privacy, and dependability (SPD) of embedded systems and part of a European collaboration of the same name. SHIELD is a multi-metric approach to evaluate the system's SPD level and compares it with use case goals for SPD. The main objective of the methodology is to evaluate multiple system configurations and select those which address or achieve the established requirements. To achieve this aim a triplet is composed of the system's security, privacy and dependability levels (each element is described by a value in a range between 0 and 100). This approach implies a high discussion potential for each of the triplets, due to the lack of a guidance on how to estimate the security, privacy, and dependability values. Additionally, the method becomes increasingly suitable the more details and variants of a system exist and is therefore not optimally applicable for the early design phase TARA analysis.

CHASSIS also combines safety and security methods for a combined safety and security assessments approach. The approach relies on modeling misuse cases and misuse sequence diagrams within a UML behavior diagram, which implies additional modeling expenses for the early development phase. CHASSIS aims at unifying safety and security in the trade-off analysis, to define whether there are features that are mutually dependent or independent of each other. The activity specifies the safety/security requirements by structuring the harm information in the form of HAZOP tables and in combination with the BDMP technique (see next paragraph). Thus, the CHASSIS approach also requires a higher level of detail that is given at the TARA analysis stage.

Boolean logic Driven Markov Processes (BDMP) represent an approach where fault tree and attack tree analysis are combined and extended with temporal connections. In addition to its logical structuring, this method also enables activation of top events based on triggers or the state of basic events. Furthermore, leave nodes have failure in operation or failure in demand fault behaviors, which extends the abilities of the FTA and ATA depiction of threats. Nevertheless, BDMP is in-appropriate for an early development phase TARA.

Threat Matrix approach proposed by US Department of Transportation [10] is used to consolidate threat data. The threat matrix is spreadsheet based, allowing the matrix to be sorted by various categories as needed. Categories of severity, sophistication level, and likelihood are indicated as high, medium, or low based on expert opinion. Other categories of the matrix are, among others, attack zone safety relation, system involved, vulnerability exploited, attack vector, access method, attack type, and resources required. Thus the threat matrix is another variation of the FMEA approach, which is geared towards the establishment of a threat database but is not the best approach for the early development phase TARA.

Binary Risk Analysis (BRA) [12] is a lightweight qualitative open license risk assessment and included, among others, by OCTAVE and NIST SP800-30. The BRA determines the asset and the threat a system must be protected from and quantizes their impacts by following these steps:

1. Answering the ten (yes/no) questions
2. Mapping the answers to each of the five 2x2 matrices which give a metric for individual attack and system features
3. Using the results from the five 2x2 matrices to select results from three 3x3 matrices (representing attack effectiveness, threat likelihood and impact).
4. Using these factors to final get the risk metric from a final 3x3 matrix.

The Binary Risk Analysis can be used for: (a) a quick risk conversations to enable discussion of a specific risk in just a few minutes, (b) helping to identify where perceptions about risk elements differ. Nevertheless, the Binary Risk Analysis is neither a full risk management methodology nor a quantitative analysis based on statistics and monetary values, nor does it eliminate subjectivity completely from the analysis. BRA is also not a threat discovery or threat risk assessment techniques on its own, which is a requirement for TARA in the early development phases.

4 Evaluation of Methods in ISO 26262 and SAE J3061 Context

This section briefly evaluates the applicability of the analysis methods presented in the previous section for early development phases in context of ISO 26262 and SAE J3061. **Table 2** summarizes all the presented methods and the earliest suitable development phase, assets and drawbacks of the methods. As can be seen in the table, in addition to the SAE J3061 recommended EVITA method, two other methods (SAHARA and BRA) are well suited for an early concept analysis (TARA). These methods were already available at the release date of SAE J3061, but are not mentioned in the guide book. Besides this, SAE J3061 recommends two methods (TVRA and OCTAVE), which are scarcely applicable for TARA of embedded automotive systems and no hints are given for application in the automotive context.

Thus, in the context of the EMC^2 project[3] and in cooperation with the experts of the SOQRATES working group[4] an analysis of the 13 methods referred to has been performed and evaluated based on an electric steering column lock use-case for a connected vehicle. This safety-critical and security-related use-case application revealed the four most applicable TARA methods (EVITA method, HEAVENS, SAHARA and BRA) for early development phase analysis of the system. Additionally, if a combined approach for safety and security engineering is utilized the methods SAHARA (for combined analysis of security and safety of the development concept), BDMP (combination of FTA and ATA) and FMVEA (combination of security and safety FMEA) are recommended for use. The following paragraphs provide a brief extract of the use-case application outcomes:

TVRA not applicable for automotive application.

OCTAVE not applicable for automotive application.

Attack tree security pendant to FTA and thus for identification of nested attacks. Detailed system design required, thus not applicable for concept evaluation, but recommended for system design analysis.

SW vulnerability only applicable for SW codes, thus not applicable for concept evaluation.

FMVEA security pendant to FMEA. More details of the system design required, thus recommended for system design analysis. Best suitable for a combined safety and security engineering process landscape.

SHIELD guidance for estimation of security, privacy and dependability value triplet missing. The purpose of the analysis is the evaluation of different system configurations, but due to the lack of quantitative determination for the evaluation of the triplets mostly leading to long discussions.

CHASSIS relies on modeling of use-cases and misuse sequences, and is thus appropriate for identification of nested attacks but not applicable for early concept evaluation. Method might only be applied when detailed modeling of use-cases and sequences are available.

BDMP Combination of ATA and FTA, is thus not applicable for concept development evaluation. It is best suited for a combined safety and security engi-

[3] http://www.artemis-emc2.eu/

[4] http://www.soqrates.de/

neering process landscape.

Threat Matrix Variant for providing input for establishing a database. Not recommended for concept analysis due to confusing size of table and thus not easy to focus on identification of new threats or threat vectors.

EVITA is a suitable approach for concept evaluation, but requires too many details for classification. These details are estimated based on concept design and thus involves the disadvantage of a huge potential for discussion. The separation of functional, safety, privacy and operational severity adds further potential for discussion but does not result in a significant difference in the resulting risk level. There is too much classification effort based on estimations for the concept evaluation phase.

HEAVENS involves less classification efforts requirements than the EVITA method. The STRIDE threat modeling approach brings additional support structuring for the estimation of threat scenarios.

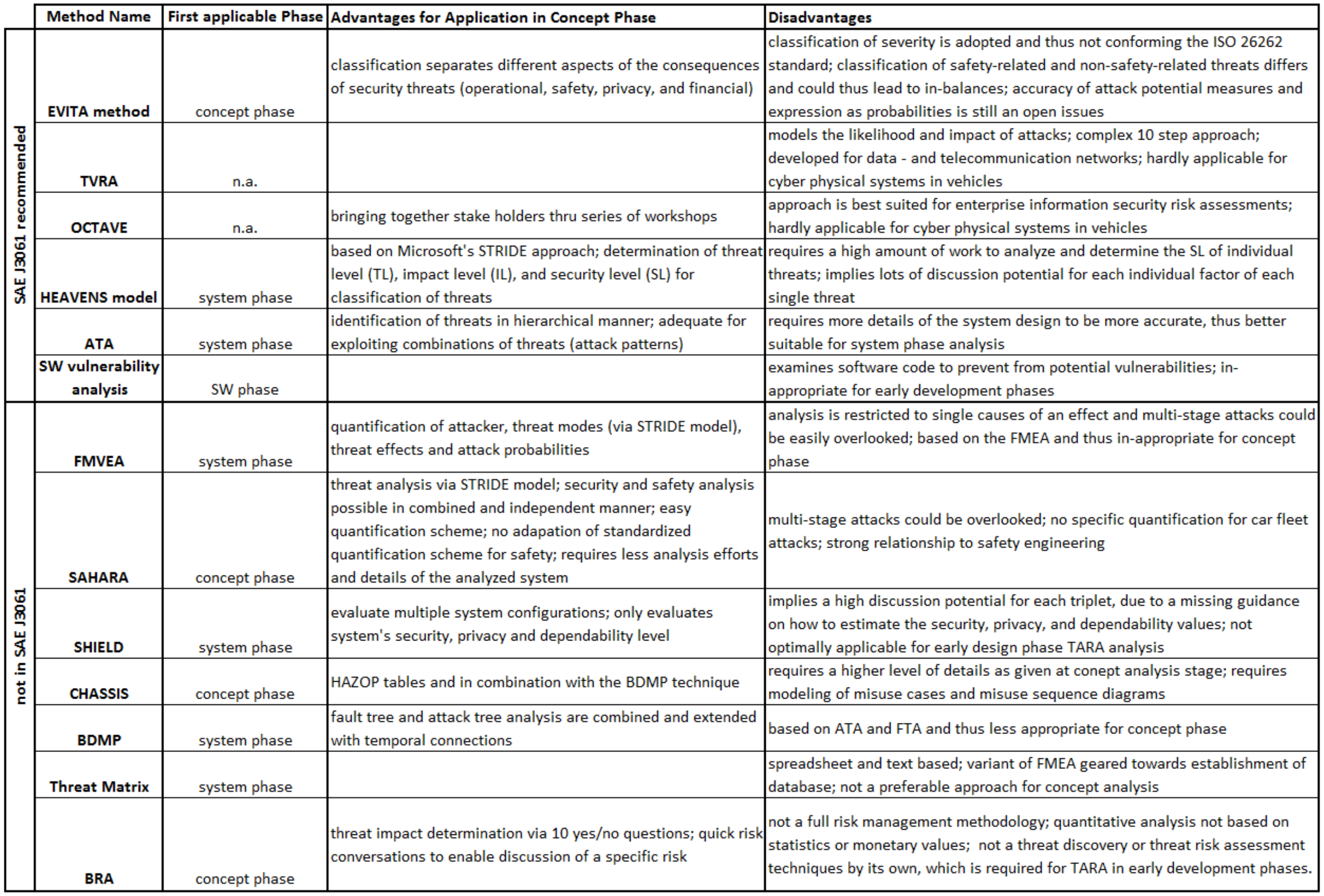
SAHARA achieves easy classification of threats in combination with STRIDE threat modeling. It was evolved from HARA and STRIDE, thus originally focusing on safety, but redesigned for security evaluation. The basic classification aligned with ASIL classification and is thus optimal for use in combined security and safety engineering processes.

BRA brings easy classification by means of 10 binary decisions in the form of questions. Nevertheless, the resulting risks are only classified as high, medium or low and a conservative analysis trend leads to threat classification solely of high risks. Additionally, no structured estimation of threat scenarios is given and the resulting threat classification is too rudimentary for concept development phases.

5 Conclusion

In conclusion, this work highlights how security standards, such as IEC 62443 [5], or security guidelines, such as SAE J3061 [15], are currently still incomplete or not directly applicable in practice. Their current state is often fragmented, and each typically assumes that their open issues are covered by other guidelines or standards. For this reason a review of novel work by researchers and research projects is highly recommended. This work is thus solely focused on the evaluation of the analysis methods available (presented in SAE J3061 and other research projects) for threat analysis and risk assessment (TARA) method at concept phase. The work briefly summarizes a review of 13 TARA methods done in the context of the EMC^2 project and in cooperation with the experts of the SOQRATES working group. This review, based on a safety critical and security related automotive use-case (electric steering column lock) revealed the four most applicable TARA methods (EVITA method, HEAVENS, SAHARA and BRA) for early development phase analysis of the system. Additionally, it discovers a set of recommended techniques for a combined approach of safety and security engineering processes.

Table 2. Evaluation of TARA Methods and Applicability for Concept Phase Analysis



	Method Name	First applicable Phase	Advantages for Application in Concept Phase	Disadvantages
SAE J3061 recommended	**EVITA method**	concept phase	classification separates different aspects of the consequences of security threats (operational, safety, privacy, and financial)	classification of severity is adopted and thus not conforming the ISO 26262 standard; classification of safety-related and non-safety-related threats differs and could thus lead to in-balances; accuracy of attack potential measures and expression as probabilities is still an open issues
	TVRA	n.a.		models the likelihood and impact of attacks; complex 10 step approach; developed for data - and telecommunication networks; hardly applicable for cyber physical systems in vehicles
	OCTAVE	n.a.	bringing together stake holders thru series of workshops	approach is best suited for enterprise information security risk assessments; hardly applicable for cyber physical systems in vehicles
	HEAVENS model	system phase	based on Microsoft's STRIDE approach; determination of threat level (TL), impact level (IL), and security level (SL) for classification of threats	requires a high amount of work to analyze and determine the SL of individual threats; implies lots of discussion potential for each individual factor of each single threat
	ATA	system phase	identification of threats in hierarchical manner; adequate for exploiting combinations of threats (attack patterns)	requires more details of the system design to be more accurate, thus better suitable for system phase analysis
	SW vulnerability analysis	SW phase		examines software code to prevent from potential vulnerabilities; in-appropriate for early development phases
not in SAE J3061	**FMVEA**	system phase	quantification of attacker, threat modes (via STRIDE model), threat effects and attack probabilities	analysis is restricted to single causes of an effect and multi-stage attacks could be easily overlooked; based on the FMEA and thus in-appropriate for concept phase
	SAHARA	concept phase	threat analysis via STRIDE model; security and safety analysis possible in combined and independent manner; easy quantification scheme; no adapation of standardized quantification scheme for safety; requires less analysis efforts and details of the analyzed system	multi-stage attacks could be overlooked; no specific quantification for car fleet attacks; strong relationship to safety engineering
	SHIELD	system phase	evaluate multiple system configurations; only evaluates system's security, privacy and dependability level	implies a high discussion potential for each triplet, due to a missing guidance on how to estimate the security, privacy, and dependability values; not optimally applicable for early design phase TARA analysis
	CHASSIS	concept phase	HAZOP tables and in combination with the BDMP technique	requires a higher level of details as given at conept analysis stage; requires modeling of misuse cases and misuse sequence diagrams
	BDMP	system phase	fault tree and attack tree analysis are combined and extended with temporal connections	based on ATA and FTA and thus less appropriate for concept phase
	Threat Matrix	system phase		spreadsheet and text based; variant of FMEA geared towards establishment of database; not a preferable approach for concept analysis
	BRA	concept phase	threat impact determination via 10 yes/no questions; quick risk conversations to enable discussion of a specific risk	not a full risk management methodology; quantitative analysis not based on statistics or monetary values; not a threat discovery or threat risk assessment techniques by its own, which is required for TARA in early development phases.

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. C. Ebert and C. Jones. Embedded Software: Facts, Figures, and Future. *IEEE Computer Society*, 0018-9162/09:42–52, 2009.
2. ISO - International Organization for Standardization. IEC 61508 Functional safety of electrical/ electronic / programmable electronic safety-related systems.
3. ISO - International Organization for Standardization. IEC 60812 Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA) , 2006.
4. ISO - International Organization for Standardization. IEC 61025 Fault tree analysis (FTA) , December 2006.
5. ISO - International Organization for Standardization. IEC 62443 - Industrial communication networks – Network and system security , 2009.
6. ISO - International Organization for Standardization. ISO 26262 Road vehicles Functional Safety Part 1-10, 2011.
7. 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.
8. Microsoft Corporation. The STRIDE Threat Model, 2005.
9. M. Miller. *The Internet of Things: How Smart TVs, Smart Cars, Smart Homes, and Smart Cities are Changing the World.* Que, 2015.
10. National Highway Traffic Safety Administration. Characterization of Potential Security Threats in Modern Automobiles - A Composite Modeling Approach, October 2014.
11. C. Petschnigg, M. Deutschmann, A. Osterhues, L. Steden, S. Botta, M. Krasikau, S. Tverdyshev, J. Diemer, L. Ahrendts, D. Thiele, C. Bernardeschi, M. D. Natale, G. Dini, and Y. Sun. D2.1 Architecture models and patterns for safety and security (Alpha). Report ICT-644080-D2.1, SAFURE Project Partners, February 2016.
12. B. Sapiro. *Binary Risk Analysis.* Creative Commons License, 1.0 edition.
13. 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.
14. S. Sentilles, P. Štěpán, J. Carlson, and I. Crnković. *Component-Based Software Engineering: 12th International Symposium, CBSE 2009 East Stroudsburg, PA, USA, June 24-26, 2009 Proceedings* , chapter Integration of Extra-Functional Properties in Component Models, pages 173–190. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.
15. Vehicle Electrical System Security Committee. SAE J3061 Cybersecurity Guidebook for Cyber-Physical Automotive Systems.