A Systematic Review of Threat Analysis and Risk Assessment Methodologies for Connected and Automated Vehicles

Benyahya, Meriem; Lenard, Teri; Collen, Anastasija; Nijdam, Niels Alexander

A Systematic Review of Threat Analysis and Risk Assessment Methodologies for Connected and Automated Vehicles

Meriem Benyahya
meriem.benyahya@unige.ch
Centre Universitaire d'Informatique, Geneva School of Economics and Management, University of Geneva
Carouge, Geneva, Switzerland

Teri Lenard
teri.lenard@unige.ch
Centre Universitaire d'Informatique, Geneva School of Economics and Management, University of Geneva
Carouge, Geneva, Switzerland

Anastasija Collen
anastasija.collen@unige.ch
Centre Universitaire d'Informatique, Geneva School of Economics and Management, University of Geneva
Carouge, Geneva, Switzerland

Niels Alexander Nijdam
niels.nijdam@unige.ch
Centre Universitaire d'Informatique, Geneva School of Economics and Management, University of Geneva
Carouge, Geneva, Switzerland

ABSTRACT

With the prevalence of high cyber risks within the Connected Automated Vehicle (CAV)'s environment, the core regulation bodies mandated applying Threat Analysis and Risk Assessment (TARA) methodologies. Conducting auspicious TARA is essential to ensure acceptable level of risk by analysing potential threats and determining corresponding mitigation strategies. Albeit plethora of standardised TARA versions are available, they are not-ready-to-use methods or they do not encapsulate heterogeneous CAVs properties. By considering the TARA emerging trends and the CAVs' SAE automation levels, the present work provides a systematic study of salient TARA methodologies in the last ten years. The methodology we applied starts with a systematic review identifying TARA approaches that are relevant to the automotive domain at a large scope. After that, the methods' applicability to CAVs is evaluated based on their threat analysis avenues and risk metrics. We elevate our appraisal further with a focus on how the automation level is considered, how the privacy impact is assessed by each TARA method, and how subjective the experts were while assessing scores to the risk metrics. Our investigation spotlights how different methods are intertwined and joint to meet the compliance with key standards such as ISO/SAE 21434. We believe that the present study's findings identify knowledge gaps and help to shape the next generation of TARA methods to keep pace with rapidly evolving automotive technologies and support the readiness of CAV of SAE levels four and five.

CCS CONCEPTS

• **Security and privacy**; • **Software and its engineering → Risk management**;

KEYWORDS

Connected automated vehicles, Cybersecurity, Data privacy, Threat analysis and risk assessment, ISO/SAE 21434

ACM Reference Format:
Meriem Benyahya, Teri Lenard, Anastasija Collen, and Niels Alexander Nijdam. 2023. A Systematic Review of Threat Analysis and Risk Assessment Methodologies for Connected and Automated Vehicles . In *The 18th International Conference on Availability, Reliability and Security (ARES 2023), August 29–September 01, 2023, Benevento, Italy.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3600160.3605084

ARES 2023, August 29–September 01, 2023, Benevento, Italy

ACM ISBN 979-8-4007-0772-8/23/08.
https://doi.org/10.1145/3600160.3605084

1 INTRODUCTION

The Society of Automotive Engineering (SAE) defines six levels of automation. They vary from L0 (no automation, the entire driving duty is on the human driver); L1 (driver assistance on either steering or speed, handled by the vehicle in a specific context); L2 (partial automation of the driving performance, but the driver is needed to react to external events); L3 (entire driving performance is automated, but human fallback is still required); L4 (entire driving and fallback are automated but in a specific context) to L5 (fully automated with unlimited conditions) [47]. Connected Automated Vehicles (CAVs) of L4 and L5 are anticipated as the new paradigm aimed at shaping the future transportation model where a driver is no longer needed.

To assure the autonomous driving functionalities, CAVs embed multiple cutting edge sensors such as Light Detection and Rangings (LiDARs), cameras, Artificial Intelligence (AI) processing units, advanced Electronic Control Units (ECUs) in addition to numerous Vehicle-to-everything (V2X) connections [4]. Those components turn the autonomous driving from dream into reality, but expose CAVs to fatal consequences if such safety critical systems are not sufficiently prepared for all traffic scenarios, including a cyber attack.

The CAV's technologies come with cybersecurity and data privacy threats, dramatically impacting the vehicle acceptance and jeopardising its passengers' safety and privacy [5]. To illustrate, Miller and Valasek [42] presented the remote take over of the braking and the steering systems of a Jeep Cherokee. Yan et al. [57] demonstrated Tesla S sensors' blinding leading to a crash. Asuquo

et al. [2] showcased a location privacy threat revealing the vehicle and passenger identities for tracking and feeding social profiling.

As there are always risks in the CAV's ecosystem, Threat Analysis and Risk Assessment (TARA) is considered by the new United Nations Economic Commission for Europe (UNECE) R155 regulation [54] and the ISO/SAE 21434 [25] standard as the efficient way to keep systems at an acceptable level of risk. TARA is a valuation methodology whose essence consists of identifying cybersecurity threats and appraising the risks associated to the determined threats [48]. Therefore, as the Automated Driving Systems (ADSs) are safety critical units, TARA is envisioned as the relevant automotive cybersecurity management tool to support the secure development of the highly automated vehicles [13].

Nevertheless, the existing TARA methodologies lack granularity and are no-ready-to-use methods [55]. Moreover, there is still a lack of in-depth descriptions on the appropriateness of TARA framework regarding CAV's specific assets and properties. Furthermore, TARA metrics vary from one methodology to another where, for example, the controllability factor, reflecting either the driver or the ADS reactivity within a threat scenario, remains optional. On the same note, the vehicle software and hardware fluctuate with the SAE automation level [6]. Consequently, L4 and L5 CAVs are supposed to mitigate cyber risks individually and on real time manner, while an L3 vehicle attack is likely to be controlled by human interventions. Inspired by such challenges, our research builds a systematic literature review, comparing the key TARA methodologies in the highly CAV's field, by evaluating how the SAE automation level is considered, how privacy impact is assessed and how the risk is computed.

The present article provides the following contributions:

- An extensive analysis of existing TARA methods applicable to CAVs' landscape, selected according to the methodology's essence, scope and domain.
- An investigation into the connections between generic TARA and CAVs' oriented methodologies.
- An evaluation of how the ISO/SAE 21434 [25] triggered a paradigm shift within the TARA development.

In the course of the present paper, Section 2 provides background definitions while Section 3 describes our methodology. Section 4 presents a granular classification of the existing TARA methodologies. Then Section 5 discusses our findings and leverages the major research gaps with regard to the existing TARA methods leading to outline our future work. After the analysis on the key TARA methodologies, the related work is presented afterwards in Section 6. Finally, the concluding remarks are presented in Section 7.

2 BACKGROUND

To facilitate the technical discussion on different TARA methodologies, we first align the terms used throughout the manuscript. Thereafter, the key standards embedded in TARA are highlighted.

2.1 Definitions

Risk Assessment (RA) and TARA encapsulate common concepts that lead to overlapping definitions or misinterpreted terms. RA is: 'the process of planning, preparing, performing and reporting a risk analysis, and evaluating the results against risk acceptance criteria' [45]. TARA consists of assessing potential cyber threats, rating the associated risks, and recommending appropriate mitigations [48]. A main difference between the two definitions is the term 'threats'. While RA focuses on risks in general, TARA involves threats identification and their link to risks. A common pitfall is to address RA under the TARA name and vice versa. Hence, we delimit the present systematic study to frameworks where the essence of the methodology is aligned with the TARA definition.

Furthermore, there is a large misunderstanding on safety and security requirements within the TARA scope. A starting step in the TARA process is the asset identification. In safety engineering, an asset is defined as anything of value that can be protected from significant accidental harm prompting remedial action [11]. In security engineering, an asset represents valuable properties that needs to be protected from malicious harm, such as data privacy and software integrity [45]. On one hand, safety methods derived from Hazard Analysis and Risk Assessment (HARA) evaluate the likelihood and impact of accidental and hazardous harm. On the other hand, the security methods derived from TARA are focused on intended harm conducted by attackers. As the safety and security concepts can be overlapping, we therefore constrain our research to TARA with a focus on security issues, yet with safety implications.

2.2 Key standards

Within the last decade, efforts have been made to provide standardised TARA guidelines related to the CAV's ecosystem. SAE J3061 [48] evoked a complete cybersecurity management for the driverless landscape representing a first draft of the TARA. The final standardised TARA draft came along with the joint efforts from International Organization for Standardization (ISO) and SAE through the ISO/SAE 21434 [25]. Further ISO standards remain inspiring for the elaboration of other TARA methods. ISO 26262 [23] brought the basic principles of safety recommendations into the automotive environment and recommends the Automotive Safety Integrity Levels (ASIL) [21] determination approach for system's failure quantification and ranking. ISO 31000 [24] orients towards risk management foundations and efficiency. Additional standards are required within the assessment process to rate the impact and assign attack feasibility values within the TARA process as per ISO/IEC 15408 [26] and ISO/IEC 18045 [27] that were constructed on the top of The Common Methodology for Information Security Evaluation (CEM) V3.1 [9]. More focused on Cooperative Intelligent Transport Systems (C-ITS) scope, European Telecommunication Standards Institute (ETSI) released multiple standards on identifying threats and their countermeasures including dedicated guidelines on TARA deployment through the ETSI TS 102 165 [17].

3 METHODOLOGY

Based on Kitchenham and Charters [33] guidelines, known for their rigour review instructions, the present section describes the adopted methodology for our systematic review. As the first and most important step, research questions are elaborated to drive the entire research process. Then, research questions are addressed through primary and secondary studies where a set of relevant sources are selected and fully investigated to meet the inclusion and exclusion criteria. Followed by the data extraction step, the

Table 1: Search string.

(threat **OR** risk) **AND** (assessment **OR** analyses **OR** evaluation **OR** test) **AND** (connected **OR** automated **OR** autonomous) **AND** (vehicle **OR** automotive)

findings are filtered and ready to be synthesised and compared to meet the research purpose.

3.1 Research questions

The deployment of highly automated vehicles cannot occur apart but in a symbiotic way with the development of robust threat and risk assessment methodologies. The present work aims to assess how the existing TARA methodologies are coping with the CAVs' evolving technologies and how such topic is addressed by current research. This factor motivates our systematic review which is driven by the following research questions:

- RQ1: What are the existing TARA methods that can be applied to the highly automated and connected vehicles?
- RQ2: What are the limitations of TARA methods, including the trending methodology defined by ISO/SAE 21434 [25], to address the properties of CAVs of SAE L4 and L5?

3.2 Primary studies selection

The primary research was conducted by using the advanced search feature in publication platforms such as ACM digital library and IEEExplore, as spotlighted in Table 2. Not limited to academic and scientific search engines, the Standard Development Organisations (SDOs)' databases were also used to complement our findings with standardised methods. The search string drawn in Table 1 consists of boolean operators as per OR and AND to fetch relevant publications. The query was adjusted depending on the source database for a comprehensive search. Within the advanced search interfaces, only publications from January 2014 to April 2023 were filtered.

3.3 Secondary studies selection

The secondary studies overviewed the primary findings through two steps. First, only peer-reviewed publications as well as journals and conference proceedings were selected. Such selection was further elevated by studying the manuscripts' titles and abstracts. Second, 215 selected publications were screened for context relevance where 79 papers were finally chosen.

3.4 Final inclusion and exclusion

With the aim of drawing a systematic review on TARA methods specific to CAVs, the 79 manuscripts were fully read and assessment methods were thoroughly evaluated. To that end, only methodologies that are aligned with TARA essence and scope were considered. The inclusion criteria relies on selecting methods wrapping up both threat modelling and RA. Following such procedure, generic RA methodologies, which are lacking the threat analysis, were excluded from our analysis, as well as methods that are not focused on the automotive or CAVs' domain. Additionally, HARA methods that are assessing system failures or hazardous events without tackling the cyber threats properties are beyond the scope of our selection. Further guided by the key standards, we excerpt standardised methods and those aiming the compliance to crucial ISO, SAE or ETSI standards. Based on such inclusion and exclusion criteria, 23 manuscripts out of 79 were selected to be deeply evaluated in Table 2.

3.5 Data extraction and comparison factors

The data extraction step was conducted using data collection forms that were elaborated, edited and adjusted by the present work's authors. The results were cross-checked afterwards and compared among involved researchers where disagreements were resolved by consensus or arbitration. To that end, the investigation into TARA methods was guided by evaluating the following factors per selected model: (i) clear definition of the method acronym; (ii) year/s of release (depending if there was one or multiple versions per model); (iii) type of the method (to be quantitative QT and/or qualitative QL); (iv) category of the method as standardised by ISO 27001 [28] (asset-based or scenario-based indicating whether the methodology is guided by a targeted asset or a risk scenario accordingly); (v) level or group of levels with regard to the SAE automation level [47]; (vi) privacy impact reflecting how the privacy weight was approached by the method; (vii) metrics considered for risk determination as entitled by the method's authors; (viii) rating methodology or scaling reference that the experts used to assign values and scores for the metrics involved in the assessment; (ix) standards for which the method aims compliance; and (x) related TARA methods constituting the bases of the identified methodology. Table 3 reflects how the aforementioned factors were analysed, while the following section provides a detailed discussion per TARA method.

4 THREAT AND RISK ASSESSMENT METHODS

Given the intertwined concepts between traditional TARA methods and recent releases, we believe that the exploration of TARA applicable to the CAV's landscape occurs interdependently with an investigation into fundamental TARA methodologies. It is noteworthy to mention that classical, yet salient, threat modelling or risk scoring methods constitute the bases for the emerging TARA methodologies.

4.1 Fundamental methods

The present discussion spotlights popular methods that were not identified in the primary studies selection phase of our systematic review as they are not relevant to the predefined research time period. Though, such methods remain pertinent to leverage granular insights for TARA properties as well as their applicability into the highly connected and automated driving ecosystem.

Spoofing, Tampering, Repudiation, Information disclosure, Denial-of-service and Elevation of privilege (STRIDE) [41] is a threat modelling technique provided by Microsoft, identifying six types of security threats, categorised per the attacker intentions and known vulnerabilities. The method is based on graphical classification without imposing any risk metrics computation. STRIDE was designed for the Information Technology (IT) industry, but

Table 2: Paper selection results.

Source	Primary selection	Secondary selection		Final inclusion/exclusion
	Search string	Title & abstract	Content screening	Full text analysis
ACM digital library	641	54	15	4
IEEExplore	540	28	17	7
MDPI	136	10	2	0
Science Direct	966	42	10	1
SDOs portals (ISO, SAE, ETSI, UNECE, ENISA)	384	29	15	5
Springer	824	41	14	5
Wiley Online Library	438	11	6	1
Total	**3929**	**215**	**79**	**23**

since it was recommended by the SAE J3061 [48], it started to be part of multiple automotive TARAs.

Another compelling threat modelling method is the Attack Tree Analysis (ATA) [45]. Based on a tree structure, the ATA sets the attack target as a parent node while children nodes depict the events triggering the attack. On one hand, the top-down analysis showcases the attack paths. On the other hand, the bottom-up interpretation spotlights the attack surfaces and the potential vulnerabilities. The ATA is foreseen to be a powerful tool for the threat scenario identification step, though, it needs to be combined with other risk scoring methods for risk determination.

Similar to ATA, being a scenario-based and a graphical representative tool, FAIR is a riveting method but for risk analysis instead of threat modelling. FAIR [20] is a quantitative method providing a taxonomy of risks to systems of different scales. FAIR's tree graphical view breaks down every risk into discrete factors, computing a value per factor and summing the overall risk through a range representation instead of a single number score. FAIR combines the loss event frequency, determining the susceptibility of a threat event to become a loss event, and the loss magnitude, assessing the impact from an event.

Common Vulnerability Scoring System (CVSS) [45] is an industry free and open standard providing quantitative measurements and qualitative ranking. Based on a CVSS calculator, the vulnerability severity is determined for decision-making process. The score is computed based on the attack ease and impact. The attack ease evaluates how close an attacker is from the asset or how the authentication can be passed to reach the asset while the impact factor reflects the threat severity and eventual consequences.

One of the pioneering comprehensive methods combining both threat modelling and RA is the Failure Mode and Effects Analysis (FMEA) [55]. It is an industry wide accepted process which evaluates the modes, causes and effects of a failure based on the IEC 60812 standard [55]. The methodology was initially developed for safety analysis, but it was extended to cover cyber-physical security. The threat analysis in FMEA is provided by determining how the security attributes fail while the risk is assessed by combining severity and probability properties.

A more comprehensive method was initiated in 1999 through Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) [1] and its variants: OCTAVE-S, OCTAVE Allegro, OCTAVE Forte. OCTAVE was released to evaluate cyber risks from the management, organisational and technical perspectives. The methodology encapsulates assets, threats and vulnerability assessments where risks to be mitigated are prioritised. Being customisable, easily self-directed and with high interoperability [35], OCTAVE represents the foundation of the TARA from the ISO/SAE 21434.

E-safety Vehicle Intrusion proTected Applications (EVITA) is another pillar of the TARA from the ISO/SAE 21434. Over a decade ago, the EVITA project was the pioneer to present asset-based TARA methodology for the automotive environment. It evaluates risks based on severity and attack probability where the threats are rated and prioritised with the consideration of the driver controllability [46]. Though, EVITA remains limited to CAVs of SAE L0, L1 and L2 requiring the driver presence and intervention.

Less popular threat modelling methodologies, yet interesting to consider when constructing TARA for CAVs, are Process for Attack Simulation and Threat Analysis (PASTA) [53], Visual, Agile, and Simple Threat (VAST) [32], and Linkability, Identifiability, Nonrepudiation, Detectability, Disclosure of data, Unawareness, and Noncompliance (LINDDUN) [37]. Such methods can be selected based on the scale and complexity of the system. For the purpose of the present research, our analysis is constrained to only those methods that were evoked in constructing dedicated automotive TARA methodologies discussed Table 3.

4.2 TARA methods applied to CAVs

Table 3 overviews TARA methods that were designed for automotive systems generally and CAVs specifically. Based on the inclusion/exclusion criteria (Section 3.4), we selected methods varying from those derived from research projects, standardised methods, to the most recent improved methodologies.

Failure Mode, Vulnerabilities and Effects Analysis (FMVEA) [49] represents an improved version of the FMEA method. As elicited in Section 4.1, FMEA is a powerful quality control methodology used to assess the entire product life-cycle; though, it is not efficient to handle multiple failures at a time and over complex systems. To overcome such limitations, FMVEA [49] was developed in a combination to STRIDE to serve the C-ITS domain.

Risk Analysis for Cooperative Engines (RACE) [7] is an extension of the EVITA methodology which assesses risks using the same metrics but with a consideration of the C-ITS's architecture [4]. Though, as it was perceived for highly connected environments,

Table 3: Threat Analysis and Risk Assessment methods.

Method	Description	Year	QL/QT†	Type	SAE Lx	Privacy	Metrics	Rating practice	Aimed compliance	Based on
FMVEA [49]	Failure Mode Vulnerabilities and Effects Analysis	2014	QL	Asset	N/A	✗	Severity Probability of occurrence	Experts knowledge	ISO 26262 IEC 60812	FMEA, ATA
RACE [7]	Risk Analysis for Cooperative Engines	2015	QL	Asset	≤ L2	✓	Severity Attack probability Controllability	ISO/IEC 15408 ISO/IEC 18045	ETSI TS 102 165	EVITA, TVRA
SAHARA [40]	Security-Aware Hazard and Risk Analysis	2015	QL	Asset	≤ L2	✗	User profile User knowledge Safety impact	ASIL	ISO 26262	HARA, STRIDE
HEAVENS [22, 36]	HEAling Vulnerabilities to Enhance Software Security and Safety	2016	QL	Asset	≤ L3	✓	Threat level Impact level	ASIL CEM V3.1 Experts knowledge	ISO 26262 ISO/SAE 21434	EVITA, STRIDE
Dominic et al. [15]	Risk Assessment for Cooperative Automated Driving	2016	QL	Scenario	≥L1	✓	Impact Motivation Attack feasibility	NHTSA [8] ISO/IEC 15408 Experts knowledge	N/A	HEAVENS
TVRA [16, 17]	Threat, Vulnerability, Risk Analysis	2017	QL	Scenario	Not specified	✗	Occurrence likelihood Impact value	ISO/IEC 15408	ETSI TS 102 165 ISO/IEC 15408	EVITA
SARA [43]	Security Automotive Risk Analysis Method	2018	QL QT	Asset	L3 L4	✓⋆	Attacker profile Vehicle controllability	ISO/IEC 15408 ISO/IEC 18045	SAE J3061 ISO 26262	ATA
SPMT [52]	Start, Predict, Mitigate, and Test	2018	QL QT	Asset	Not specified	✓	Occurrence likelihood	Experts knowledge	SAE J3061	HEAVENS, STRIDE, ATA
TARA+ [6]	Controllability-aware TARA for L3 Automated Driving Systems	2019	QL	Asset	L3	✓	Impact Attack feasibility Controllability	ISO/IEC 18045 Experts knowledge	SAE J3061 ISO 26262	TARA 1.0, HEAVENS
VeRA [12]	Vehicles Risk Analysis	2020	QL QT	Asset	L3 L4	✓	Attack probability Severity Human control	Experts knowledge	SAE J3061	EVITA
Khatun et al. [31]	Scenario-Based Threat Analysis and Risk Assessment	2021	QL	Asset	≥ L3	✓	Attack probability Severity	ASIL	SAE J3061	STRIDE, EVITA, HEAVENS
TARA 1.0 [25, 48]	Threat Analysis and Risk Assessment	2021	QL	Asset	Not specified	✓	Impact Attack feasibility	ISO/IEC 18045 Experts knowledge	ISO/SAE 21434 SAE J3061	OCTAVE, EVITA, TVRA, HEAVENS
ThreatGet [50]	Asset Driven Automotive Cybersecurity Analysis	2021	QL	Asset	Not specified	✓	Threat level Impact level	ISO/IEC 18045 Experts knowledge	ISO/SAE 21434	SAHARA, TARA 1.0, STRIDE
Dobaj et al. [13, 14]	Security-driven automotive development lifecycle	2021	QL QT	Scenario	≥ L3	✓	Threat level Impact level	FAIR ISO/IEC 18045 Experts knowledge	ISO/SAE 21434	TARA 1.0
Vogt et al. [55]	Comprehensive Risk Management in Intelligent Transport Systems	2021	QL QT	Scenario	Not specified	✓	Severity Failure probability	FAIR Monte Carlo simulation Experts knowledge	ISO 26262 ISO/SAE 21434	FMEA, FAIR
Wang et al. [56]	A Systematic Risk Assessment Framework of Automotive Cybersecurity	2021	QT	Asset	Not specified	✓	Impact Attack feasibility	BSI 100–4 [18] ISO/IEC 18045	ISO/SAE 21434	HEAVENS
ThreatSurf [58]	Threat Surface assessment in automotive cybersecurity engineering	2022	QL	Asset	L3	✓	Threat level	ISO/IEC 18045 Experts knowledge	ISO/SAE 21434	TARA 1.0
PIER [44]	Probability, Impact, Exposure, and Recovery	2022	QT	Scenario	≤ L3	✓	Occurrence likelihood Impact Exposure likelihood Recovery	Experts knowledge	ISO/SAE 21434	TARA 1.0
Zhou et al. [59]	Data Security Risk Assessment Method for Connected and Automated Vehicles	2022	QT	Asset	≥ L3	✓⋆	Data value Feasibility Impact	National regulations (GB/T 20984-2007) [51]	ISO/SAE 21434	EVITA, HEAVENS, TARA 1.0

† QL = Qualitative, QT = Quantitative
⋆ Higher weight on privacy

the severity metric in RACE is computed at a coarse level. RACE is advertised as an improvement of EVITA through its compliance to ETSI TS 102 165 [16].

Security-Aware Hazard and Risk Analysis (SAHARA) [40] is one of the original methodologies combining hazard analysis methods such as HARA and threat modelling tools as per STRIDE. SAHARA aims to harmonise safety and security methods by assessing security threats over safety-critical systems at the vehicle conceptual phase. The method was evaluated over a battery management system of a hybrid vehicle where additional threats were identified with regard to a simple HARA deployment.

HEAling Vulnerabilities to Enhance Software Security and Safety (HEAVENS) [22] adopted the EVITA methodology, yet with an alignment to the ISO 26262 [23] and SAE J3061 [48] requirements. As

an outcome of the HEAVENS methodology, the security level of an asset is derived by combining the 'threat level' and 'impact level' being the key metrics of the approach. It combines the threat likelihood which is computed by considering the attacker expertise, the knowledge about the target, the window of opportunity and the equipment required to conduct an attack, and estimation on the expected loss per stakeholder from the Safety Finance Operations Privacy (SFOP) perspectives. To meet the ISO/SAE 21434 [25] compliance, an improved version entitled HEAVENS 2.0 [36] was recently delineated. Both HEAVENS versions intend to cope with the evolving risks within the automotive industry including CAVs, though, the SAE automation level was not imposed within the assessment. In Table 3 we consider both methods to be adapted to vehicles of SAE L3 rearward as the methodologies were validated through the vehicle speed limiter use cases, requiring the driver presence.

Dominic et al. [15] were the first authors who dug beneath the surface of SAE automation levels and their impact on conducting TARA within the CAVs landscape. By extending the STRIDE method and developing a CAV's reference architecture, the researchers proposed an agile TARA that can be adjusted to every automobile manufacturers (OEM)'s design and to each automation level. Unlike the other TARA methods of that era, Dominic et al. [15] advertised the customisation of the threat model and matrix within every different system as well as the values, weights and parameters of the risk assessment. While demonstrating the methodology over driverless valet parking as an SAE L4 component, the authors depicted the TARA outcome through a threat matrix plot with visual priorities ranking.

The Threat, Vulnerability and Risk Assessment (TVRA) method was standardised by ETSI in 2011 [16] and upgraded by 2017 [17]. With a focus on vehicular telecommunication threats, the method relies on the occurrence likelihood and the impact value to assess the risk. The TVRA generates quantified risks of an asset and maps them to security mitigation techniques with the aim to bring the risks to an acceptable level [10]. Nevertheless, as the TVRA method is more adapted to V2X threats, it misses in-vehicle components perils. Also, it does not consider the safety and privacy within its risk computation approach [43].

Security Automotive Risk Analysis Method (SARA) [43] is one of the first asset-based methods targeting the assessment of risks related to the automation features and one of the unique methods focusing on the privacy weight. The methodology claims further metrics impacting the risk computation including the attacker profile and the self-controllability of the ADS reflecting the method adaptability to SAE L3 & L4. The SARA feasibility was showcased by privacy and safety scenarios on vehicle tracking and comfortable emergency brake failure.

The Start, Predict, Mitigate, and Test (SPMT) [52] came up with security enhancements over the entire vehicle life-cycle. It is a methodology wrapping up several security models including HEAVENS, ATA and STRIDE. The SPMT process is foreseen as a virtuous cycle based on prediction, security testing, mitigation and reassessment over any asset in each phase of the automotive development. Although, the methodology targets CAV's assets, the SAE automation level weight is not specified in assessment. Another limitation of the method is that it does not consider multiple metrics in computing the risk, mostly focused on the probability of occurrence.

Based on earlier drafts of TARA from the SAE J3061 [48], TARA+ [6] was built with an additional metric assessing both the driver and ADS controllability over vehicles of SAE L3. The TARA+ model is a proof of concept demonstrated by threat scenarios over the surface attacks: ADS on-board units, LiDAR and vision sensors.

Vehicles Risk Analysis (VeRA) [12] is a method inspired from the SAE J3061 but in a simplified way. The methodology captures the risk through a compilation of the attack probability, severity and the human control. Unlike other methods, the human control property in VeRA considers the SAE automation level. Nevertheless, it attributes a constant risk value for SAE L3, L4 and L5 as they are merged together in the risk classification matrix. VeRA's performance was assessed to be quicker and less complex than EVITA.

In a combined perspective of safety and security analysis, Khatun et al. [31] designed a TARA methodology, which takes a list of hazardous events as a further input to build a scenario-based threat analysis. The method relies on the main TARA steps recommended by the SAE J3061 to assess the Over-the-Air (OTA) software update system of CAVs of SAE L3 onward. The OTA system was selected by the authors as a complex safety critical asset, yet required within automated vehicles. The proposed method followed STRIDE for damage scenario definition while it was built upon HEAVENS and EVITA methodologies to identify the attack potential and severity level.

TARA method in ISO/SAE 21434 (hereinafter, referred as TARA 1.0) was initially introduced within the SAE J3061 standard [48] which was developed based on OCTAVE, EVITA, TVRA and HEAVENS. The new ISO/SAE 21434 [25] evoked a different, yet detailed, workflow. Depicted in Figure 1, the blue section draws the boundaries of the TARA scope as outlined by the ISO standard. TARA 1.0 brought out a detailed description of the asset identification which can be represented through a data flow diagram supporting on enumerating the assets. Based on the cybersecurity properties, the threat scenarios are identified and the attack paths are analysed. The ISO/SAE 21434 standard suggested STRIDE or ATA as potential tools to accomplish these two steps accordingly. Similar to HEAVENS, the risk in TARA 1.0 compiles the impact rating using the same factors. The attack feasibility can be driven through three methods varying from 'attack potential-based' where feasibility rates are retrieved from the ISO/IEC18045, 'CVSS-based' using FIRST scoring system [19] to the qualitative 'attack vector-based'. From the risk value, a decision should be derived which represents the main outcome of the TARA 1.0 process. Such key output feeds the cybersecurity goals and claims afterwards to update the general vehicular cybersecurity governance. Despite the process clarity and agility of the TARA 1.0, the method remains generic and does not elicit any specific treatment per SAE automation level.

ThreatGet [50] represents a concrete implementation of TARA 1.0 method through a tool-supported approach. Not limited to the compliance with ISO/SAE 21434 [25] only, ThreatGet wraps other TARA methodologies such as SAHARA for the asset identification and HEAVENS for the risk computation. ThreatGet

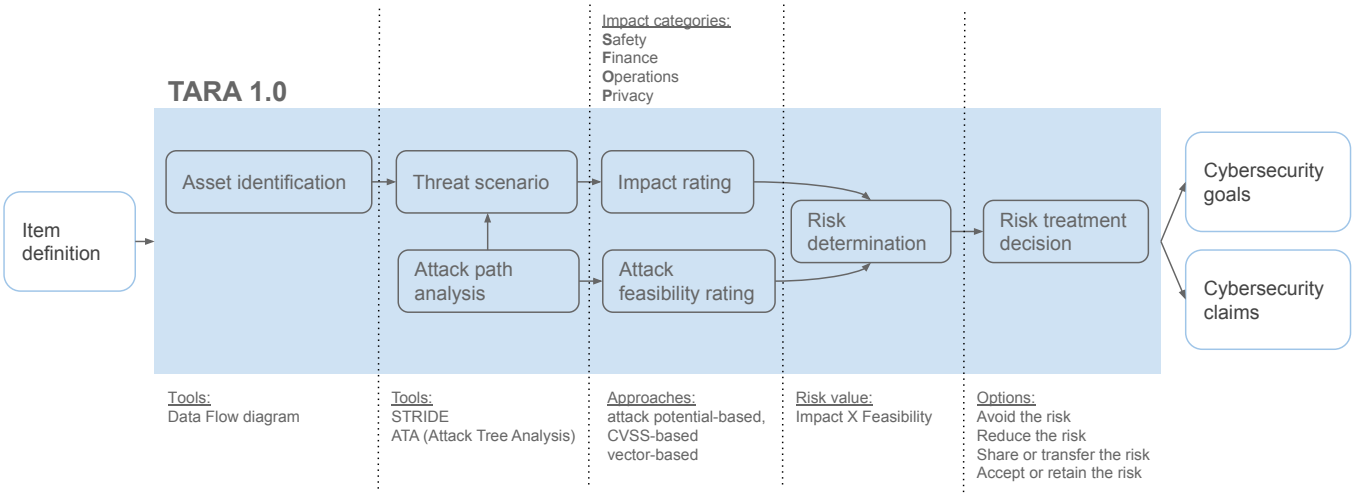

Figure 1: TARA 1.0 as defined by ISO/SAE 21434.

extended the combined TARA methodologies with automated determination of threat scenarios and attack paths. Though, the SAE automation level was not imposed by the tool parameters.

Dobaj et al. [13] proposed additional steps to the TARA 1.0 process, especially at the threat scenario modelling phase. The model maps the additional steps to the relevant vehicle lifecycle phases. To illustrate, it distinguishes between TARA actions to be taken during the concept phase and those that are applicable at design or implementation phases. Additionally, the method targets highly automated vehicles of SAE L3 onward. Nevertheless, it assesses L3, L4 & L5 equally.

Inspired from the core standards for safety, security and risk management, Vogt et al. [55] introduced a comprehensive TARA method for C-ITS including CAVs. The method combines qualitative and quantitative threat modelling and risk scoring tools such as FMEA and FAIR to offer flexibility for any C-ITS's asset assessment. For uncertain values, a Monte Carlo simulation was used to generate ranges instead of a fixed score supporting the impact and attack feasibility rates' computation. Although, the authors proposed a model wrapping the advantages of other TARA methodologies,the SAE automation level was not pushed within the assessment.

Wang et al. [56] shifts the focus from procedural adjustments to quantitative suggestions with the aim to improve the risk matrix and hence elevate the assessment's objectivity. The authors proposed different rating schemes supporting the risk calculation that can be adapted through the vehicle development lifecycle. Though, the methodology shares several commonalities with the TARA 1.0 without any explicit citation to the ISO/SAE 21434. Additionally, the vehicle's SAE automation level was not considered within the method's analysis scope.

Similar to ThreatGet, ThreatSurf [58] introduced an automated assessment of the vehicle attack surface per TARA 1.0 and hence compliant to ISO/SAE 21434. The methodology also aims to align with the UNECE R155 [54] as it is evaluated through the regulation's threat categories. ThreatSurf demonstrated an in-depth assessment of threats in modern vehicles of SAE L3. Nevertheless, the process excludes the impact rating and risk determination steps from the automation process, as it is manufacturer specific.

Probability, Impact, Exposure, and Recovery (PIER) [44] is a recent TARA methodology dedicated for CAVs of SAE L3 onward. The method focuses on assessing how the assets are exposed to risk from internal and external connections and how resilient they are on real-time base. PIER is considered as another improved version of the TARA 1.0 by embedding the recovery and rapid resilience over mission-critical components within the CAV. The method was theoretically validated through a vehicular software update and collision avoidance scenarios and a concrete implementation of the attack scenarios over a real CAV remains absent.

A more privacy focused methodology was drawn by Zhou et al. [59]. The authors merged together the data security risk assessment recommended by national regulations to TARA 1.0 steps. Furthermore, the risk computation imposes data security factors such as data value (reflecting the data sensitivity) as well as the feasibility and impact metrics involved on the TARA 1.0 risk computation. While considering the data privacy risks in the CAV's environment and the data life-cycle, the researchers demonstrated their methodology on the Telematics box data as the assessment's asset. However, the methods remains limited to national regulations requiring major adaptation for different markets.

5 DISCUSSIONS AND FUTURE WORK

In the following, we summarise our key findings, demonstrating the discrepancy between the existing TARA methods and CAVs readiness:

Despite being called by different terms, the main two TARA steps are threat modelling and risk analysis. While few TARA methods, such as TARA 1.0, have clear boundaries, others may include further steps like item definition and mitigation. To that end, we urge for the need on more unified and standardised terminologies and scope.

OCTAVE, EVITA and HEAVENS are ubiquitous TARA methods which literally geared up today's models. They even represent the foundations for TARA 1.0 which can be foreseen as the most

pervasive method. By analysing the aims of the TARA developed within the last three years, we assert that they all either comply to ISO/SAE 21434 [25] or suggest an improvement to TARA 1.0.

Although, there is a continuous improvement to build the most auspicious TARA methodology with regard to the driver and the ADS controllability, there is no explicit distinction in addressing highly CAVs of SAE L4 and L5. There are limited efforts in distinguishing the assessment of SAE L3, L4 and L5 respectively as the majority of the reviewed TARA methodologies consider their risks to be equal. Fortunately, a potential method was initiated by Dominic et al. [15] but the methodology did not emerge with current cyber threats and today's technologies advances. Taking into account the evolving cyber risks with the increase of every automation level, there is a scarcity on TARA methods dedicated to SAE L4 and L5. A risk that can be low on SAE L3 may be defined as high in L4 and even higher in an L5 CAV where a driver control is substituted by the ADS self-risk mitigation.

By considering the high privacy risks within the CAV's ecosystem [5], several TARA methods assigned a privacy weight while measuring the risk. Except the methodologies demonstrated by SARA [43] and Zhou et al. [59], which emphasised on privacy, all other TARA methodologies assigned a weight to the privacy which remains equal to the other SFOP categories as safety, finance and operations.

A common point about the metrics used in all the methods is that they are based on feasibility and impact, while very few TARA methods consider the controllability metric. The terminology varies from attack ease, occurrence to exposure likelihood to quantify the feasibility of a threat to occur. Similarly, there are multiple terms to represent the severity impact. While the majority of the methods are focused on these two metrics, others such as RACE, SARA, VeRA and TARA+ added the controllability metric to assess either the driver or ADS control in case of an attack. We believe that the controllability metric should be imposed differently while assessing CAVs of SAE L4 and L5.

Regarding the rating values, Table 3 demonstrates that ISO/IEC 15408, ISO/IEC 18045 and experts knowledge represent the main sources to assign scores. In other words, Appendix I from the ISO/SAE 21434 guided several TARA methods where such sources are recommended. Nevertheless, both ISO/IEC 15408 and ISO/IEC 18045 were elaborated for IT systems without considering the CAV's features which are wrapping both IT and automotive aspects. Furthermore, as long as the experts subjectivity is involved, we consider that a confidentiality factor should be imposed. On the same note, when the estimation depends on experts evaluation, it is prone to over-confident or under-confident results. Consequently, we believe that risks computation can be biased if there is no further metric reflecting the experts confidence.

The presented TARA methods commonly provide threat modelling, risk ratings, determinations and treatments; though the scales remain not specific to cope with today's CAVs challenges including the vehicle connection maturity and SAE automation level. As a future work, it is required to build an improved TARA that will be adapted to the SAE L4 and L5 particularities. The new method aims to consider the vehicle automation level and the evolving privacy impact while computing the risk. Moreover, the process intends to add further metrics such as the experts confidence and the residual risk estimation (risk related to unknown threats) while assessing CAVs's of L4 and L5. Furthermore, the methodology should add further layers of the assessment by including the Cybersecurity Assurance Level (CAL) concept to reflect the ideal level of assurance and protection for the asset. Such parameters were briefly introduced in the ISO/SAE 21434 [25] and will be the focus of the underdeveloped ISO/SAE AWI 8475 [29].

6 RELATED WORK

While a plethora of research works provided reviews on safety assessments, limited comparative studies on CAV's TARA exist. At a general security engineering scope, Kumar et al. [34] studied six TARA methods including CVSS, ATA and OCTAVE. The research work asserted the need of making the methodology specific to its domain as the TARA results depend on the experts knowledge and proficiency. More focused on the automotive domain, Luo et al. [37] provided a comparative study with a taxonomy on TARA methodologies. The authors classified the methods into formula-based (representing the asset-based methods) and model based (grouping scenario-based methods). Albeit a granular presentation of TARA models was presented, the research lacks comparative discussions among the identified methods with regard to the vehicle automation and connectivity properties. In another survey, Luo et al. [38] overviewed TARA as a powerful risk-based testing tool. The authors evoked nine fundamental methods where only the application scope and the threat model of every methodology were evaluated. Similarly, Benyahya et al. [3] studied TARA methodologies and selected TARA 1.0 to be demonstrated over an L4 vehicle. The authors elevated further the assessment results by conducting penetration tests over risky damage scenarios. While the authors demonstrated the advantages and limitations of TARA over a highly automated vehicle, the research work lacks a granular comparative study.

Kawanishi et al. [30] studied threat analyses methods by comparing the performance of their risk scoring approaches through a CAV use case. Though, the study was limited to three techniques and only to the national JASO TP15002 standard requirements. In a more detailed review, Monteuuis et al. [43] provided a critical review of ten TARA methods including EVITA, TVRA and HEAVENS. The authors compared them through multiple criteria such as the vehicle type (connected or automated), the attack type (mono or multi threat) and the driver's controllability. To that end, the comparative study remains at a high scale without determining the corresponding SAE automation level.

The European Union Agency for Cybersecurity (ENISA) [10, 35] evaluated RA frameworks by categorising them into asset or scenario based, qualitative or quantitative, and based on their risk calculation methodology. Though, the ENISA's reports sought the interoperability evaluation of risk management frameworks in general without addressing neither TARA models nor the CAV's domain. For more standards related studies, Cui and Sabaliauskaite [11] evaluated TARA and HARA common phases by investigating into the ISO 26262 [23], SAE J3016 [47] and SAE J3061 [48]. Similarly, Macher et al. [39] provided a review comparing the TARA methods from SAE J3016, EVITA, HEAVENS, TVRA, OCTAVE and FMVEA. Nevertheless, as with the rapid evolving CAV's standards,

both studies [11, 39] remain outdated and limited to generic automotive methodolgies without covering the new trending standards such as ISO/SAE 21434 [25].

Our contribution is different from the aforementioned works as it not only identifies the key TARA methods, but also spotlights their consonance and limitations with regard to the highly CAV's readiness. Moreover, our systematic review brings an innovative comparison using specific CAV's properties including: (i) SAE automation level and high connectivity implications; (ii) privacy impact; (iii) experts subjectivity; and (iv) standardisation evolution and compliance.

7 CONCLUSIONS

We seldom have enough data to build a set of accurate analysis and assumptions as input to any TARA model. Though, high certainty is much required within the CAV's environment and hence a thorough knowledge about TARA methodologies is crucial in identifying adequate cybersecurity threat modelling for highly automated driving. Our research goal was threefold: conduct a systematic review of the existing TARA methods, analyse them in relation to the ISO/SAE 21434 requirements, and build intensive understanding about how CAVs' properties are considered by the existing methodologies. The outcome shows that the automation level and privacy impacts are barely the main focus of TARA methods. On the same note, more emphasis is needed to appropriately address the specifications CAVs of SAE L4 and L5. We further rationalise a set of recommendations and needs that are driving our insights in providing an improved TARA methodology as a future work.

ACKNOWLEDGMENTS

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under grant agreement No 875530, Horizon Europe Research and Innovation programme under grant agreement No 101077587, and from the Swiss State Secretariat for Education, Research and Innovation (SERI). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or CINEA. Neither the European Union nor the granting authority can be held responsible for them.

REFERENCES

[1] Christopher Alberts, Audrey Dorofee, and James Stevens. 2005. *OCTAVE -S Implementation Guide, Version 1.0.* Technical Report. Carnegie Mellon Software Engineering Institute, Pittsburg.

[2] Philip Asuquo, Haitham Cruickshank, Jeremy Morley, Chibueze P.Anyigor Ogah, Ao Lei, Waleed Hathal, Shihan Bao, and Zhili Sun. 2018. Security and Privacy in Location-Based Services for Vehicular and Mobile Communications: An Overview, Challenges, and Countermeasures. *IEEE Internet of Things Journal* 5, 6 (2018), 4778–4802.

[3] Meriem Benyahya, Pierre Bergerat, Anastasija Collen, and Niels Alexander Nijdam. 2023. Symbiotic Analysis of Security Assessment and Penetration Tests Guiding Real L4 Automated City Shuttles. *Telecom* 4, 1 (3 2023), 198–218. https://doi.org/10.3390/telecom4010012

[4] Meriem Benyahya, Anastasija Collen, Sotiria Kechagia, and Niels Alexander Nijdam. 2022. Automated city shuttles: Mapping the key challenges in cybersecurity, privacy and standards to future developments. *Computers & Security* 122 (11 2022), 102904. https://doi.org/10.1016/j.cose.2022.102904

[5] Meriem Benyahya, Sotiria Kechagia, Anastasija Collen, and Niels Alexander Nijdam. 2022. The Interface of Privacy and Data Security in Automated City Shuttles: The GDPR Analysis. *Applied Sciences* 12, 9 (4 2022), 4413. https://doi.org/10.3390/app12094413

[6] Anastasia Bolovinou, Ugur-Ilker Atmaca, Al Tariq Sheik, Obaid Ur-Rehman, Gerhard Wallraf, and Angelos Amditis. 2019. TARA+: Controllability-aware Threat Analysis and Risk Assessment for L3 Automated Driving Systems. In *2019 IEEE Intelligent Vehicles Symposium (IV)*. IEEE, Paris, 8–13. https://doi.org/10.1109/IVS.2019.8813999

[7] Aymen Boudguiga, Antoine Boulanger, Pascal Chiron, Witold Klaudel, Houda Labiod, and Jean-Christophe Seguy. 2015. RACE: Risk analysis for cooperative engines. In *2015 7th International Conference on New Technologies, Mobility and Security (NTMS)*. IEEE, Paris, France, 1–5. https://doi.org/10.1109/NTMS.2015.7266516

[8] C. McCarthy, K. Harnett, and A. Carter. 2014. *Characterization of Potential Security Threats in Modern Automobiles: A Composite Modeling Approach.* Technical Report. National Highway Traffic Safety Administration (NHTSA). www.ntis.gov

[9] Common Criteria. 2017. *Common Methodology for Information Technology Security Evaluation Evaluation methodology.* Technical Report.

[10] Costas Lambrinoudakis, Stefanos Gritzalis, Christos Xenakis, Sokratis Katsikas, Maria Karyda, Kostas Papadatos, Konstantinos Rantos, Yiannis Pavlosoglou, Stelios Gasparinatos, and Alexandros Zacharis. 2022. *Compendium of Risk Management Frameworks with Potential Interoperability.* Technical Report. ENISA.

[11] Jin Cui and Giedre Sabaliauskaite. 2017. On the Alignment of Safety and Security for Autonomous Vehicles. In *Cyber 2017: The Second International Conference on Cyber-Technologies and Cyber Systems*. IARIA XPS Press, Barcelona, Spain, 59–64.

[12] Jin Cui and Biao Zhang. 2020. VeRA: A Simplified Security Risk Analysis Method for Autonomous Vehicles. *IEEE Transactions on Vehicular Technology* 69, 10 (10 2020), 10494–10505. https://doi.org/10.1109/TVT.2020.3009165

[13] Jürgen Dobaj, Georg Macher, Damjan Ekert, Andreas Riel, and Richard Messnarz. 2021. Towards a security-driven automotive development lifecycle. *Journal of Software: Evolution and Process* (11 2021), 1–22. https://doi.org/10.1002/smr.2407

[14] Jürgen Dobaj, Christoph Schmittner, Michael Krisper, and Georg Macher. 2019. Towards Integrated Quantitative Security and Safety Risk Assessment. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 11699 LNCS (2019), 102–116. https://link.springer.com/chapter/10.1007/978-3-030-26250-1_8

[15] Derrick Dominic, Sumeet Chhawri, Ryan M. Eustice, Di Ma, and André Weimerskirch. 2016. Risk Assessment for Cooperative Automated Driving. In *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy*. ACM, New York, NY, USA, 47–58. https://doi.org/10.1145/2994487.2994499

[16] ETSI. 2011. *TS 102 165-1 - V4.2.3 - Method and proforma for Threat, Risk, Vulnerability Analysis.* Technical Report. ETSI.

[17] ETSI. 2017. *ETSI TS 102 165 Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA).* Technical Report. ETSI, Sophia Antipolis.

[18] Federal Office for Information Security. 2009. *BSI-Standard 100-4 Business Continuity Management.* Technical Report. Federal Office for Information Security (BSI), Bonn.

[19] FIRST. 2023. Common Vulnerability Scoring System SIG. https://www.first.org/cvss/

[20] Jack Freund and Jack Jones. 2015. The FAIR Risk Ontology. In *Measuring and Managing Information Risk*. Elsevier, 25–41. https://doi.org/10.1016/B978-0-12-420231-3.00003-8

[21] Youcef Gheraibia, Sohag Kabir, Khaoula Djafri, and Habiba Krimou. 2018. An Overview of the Approaches for Automotive Safety Integrity Levels Allocation. *Journal of Failure Analysis and Prevention* 18, 3 (6 2018), 707–720. https://doi.org/10.1007/s11668-018-0466-9

[22] Mafijul Md. Islam, Aljoscha Lautenbach, Christian Sandberg, and Tomas Olovsson. 2016. A Risk Assessment Framework for Automotive Embedded Systems. In *Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security*. ACM, New York, NY, USA, 3–14. https://doi.org/10.1145/2899015.2899018

[23] ISO. 2018. *ISO 26262 Road vehicles - Functional safety.* Technical Report. ISO.

[24] ISO. 2018. *ISO 31000:2018 - Risk management - Guidelines.* Technical Report. ISO.

[25] ISO. 2021. *ISO/SAE 21434 Road vehicles-Cybersecurity engineering.* Technical Report. ISO/SAE.

[26] ISO. 2022. *ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Introduction and general model.* Technical Report. ISO.

[27] ISO. 2022. *ISO/IEC 18045: Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Methodology for IT security evaluation.* Technical Report. ISO.

[28] ISO. 2022. *ISO/IEC 27001:2022, Information security management systems.* Technical Report. ISO.

[29] ISO. 2023. *ISO/SAE AWI 8475 - Cybersecurity Assurance Levels (CAL) and Target Attack Feasibility (TAF).* Technical Report. ISO.

[30] Yasuyuki Kawanishi, Hideaki Nishihara, Daisuke Souma, Hirotaka Yoshida, and Yoichi Hata. 2019. A Comparative Study of JASO TP15002-Based Security Risk Assessment Methods for Connected Vehicle System Design. *Security and Communication Networks* 2019 (2 2019), 1–35. https://doi.org/10.1155/2019/4614721

[31] Marzana Khatun, Michael Glass, and Rolf Jung. 2021. An Approach of Scenario-Based Threat Analysis and Risk Assessment Over-the-Air updates for an Autonomous Vehicle. In *2021 7th International Conference on Automation, Robotics and Applications (ICARA)*. IEEE, Xi'an, China, 122–127. https://doi.org/10.1109/ICARA51699.2021.9376542

[32] Shiho Kim and Rakesh Shrestha. 2020. *Automotive Cyber Security*. Springer Singapore, Singapore. https://doi.org/10.1007/978-981-15-8053-6

[33] Barbara Kitchenham and Stuart M Charters. 2007. *Guidelines for performing Systematic Literature Reviews in Software Engineering*. Technical Report. Software Engineering Group School of Computer Science and Mathematics Keele University, Durham, UK. https://www.researchgate.net/publication/302924724

[34] Santosh Kumar, Ashish Joshi, and Aditya Raturi. 2022. Study on Smart Security Measures in Threat and Risk Assessment. In *ICAN 2022 - 3rd International Conference on Computing, Analytics and Networks - Proceedings*. Institute of Electrical and Electronics Engineers Inc., Rajpura, Punjab, India, 1–4. https://doi.org/10.1109/ICAN56228.2022.10007166

[35] Costas. Lambrinoudakis, Stefanos. Gritzalis, Christos. Xenakis, Sokratis. Katsikas, Maria. Karyda, Aggeliki. Tsochou, Kostas. Papadatos, Konstantinos. Rantos, Yiannis. Pavlosoglou, Stelios. Gasparinatos, and Alexandros. Zacharis. 2022. *Interoperable EU risk management framework*. Technical Report. ENISA.

[36] Aljoscha Lautenbach, Magnus Almgren, and Tomas Olovsson. 2021. Proposing HEAVENS 2.0 – an automotive risk assessment model. In *Computer Science in Cars Symposium*. ACM, New York, NY, USA, 1–12. https://doi.org/10.1145/3488904.3493378

[37] Feng Luo, Yifan Jiang, Zhaojing Zhang, Yi Ren, and Shuo Hou. 2021. Threat Analysis and Risk Assessment for Connected Vehicles: A Survey. *Security and Communication Networks* 2021 (9 2021), 1–19. https://doi.org/10.1155/2021/1263820

[38] Feng Luo, Xuan Zhang, Zhenyu Yang, Yifan Jiang, Jiajia Wang, Mingzhi Wu, and Wanqiang Feng. 2022. Cybersecurity Testing for Automotive Domain: A Survey. https://doi.org/10.3390/s22239211

[39] Georg Macher, Eric Armengaud, Eugen Brenner, and Christian Kreiner. 2016. A Review of Threat Analysis and Risk Assessment Methods in the Automotive Context. In *35th International Conference, SAFECOMP 2016*, Vol. 9922 LNCS. Springer, Cham, Trondheim, 130–141. https://link.springer.com/chapter/10.1007/978-3-319-45477-1_11

[40] Georg Macher, Harald Sporer, Reinhard Berlach, Eric Armengaud, and Christian Kreiner. 2015. SAHARA: A Security-Aware Hazard and Risk Analysis Method. In *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2015*. IEEE Conference Publications, New Jersey, 621–624.

[41] Microsoft. 2023. Microsoft Threat Modeling Tool. https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats#stride-model

[42] Charlie Miller and Chris Valasek. 2015. Remote Exploitation of an Unaltered Passenger Vehicle. *Defcon 23* 2015 (2015), 1–91.

[43] Jean Philippe Monteuuis, Aymen Boudguiga, Jun Zhang, Houda Labiod, Alain Servel, and Pascal Urien. 2018. Sara: Security automotive risk analysis method. In *CPSS 2018 - Proceedings of the 4th ACM Workshop on Cyber-Physical System Security, Co-located with ASIA CCS 2018*. Association for Computing Machinery, Inc, New York, 3–14. https://doi.org/10.1145/3198458.3198465

[44] Seunghyun Park and Hyunhee Park. 2022. PIER: cyber-resilient risk assessment model for connected and autonomous vehicles. *Wireless Networks* (8 2022). https://doi.org/10.1007/s11276-022-03084-9

[45] Marvin Rausand and Stein Haugen. 2020. *Risk Assessment* (2020 ed.). Wiley, New Jersey. https://doi.org/10.1002/9781119377351

[46] Alastair R Ruddle and Michael Friedewald. 2009. *Security requirements for automotive on-board networks based on dark-side scenarios*. Technical Report. European Commission. https://www.researchgate.net/publication/46307752

[47] SAE. 2018. *J3016B Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*. Technical Report. SAE. 35 pages.

[48] SAE. 2021. *SAE J3061- Cybersecurity Guidebook for Cyber-Physical Vehicle Systems*. Technical Report. Society of Automotive Engineering.

[49] Christoph Schmittner, Zhendong Ma, and Paul Smith. 2014. FMVEA for Safety and Security Analysis of Intelligent and Cooperative Vehicles. In *International Conference on Computer Safety, Reliability, and Security SAFECOMP 2014*. Springer, Cham, 282–288. http://link.springer.com/10.1007/978-3-319-10557-4_31

[50] Christoph Schmittner, Bernhard Schrammel, and Sandra Konig. 2021. Asset Driven ISO/SAE 21434 Compliant Automotive Cybersecurity Analysis with ThreatGet. In *European Conference on Software Process Improvement EuroSpi2021*, Springer Nature Switzerland AG (Ed.), Vol. 1442. Springer Nature Switzerland AG, Cham, 548–563.

[51] Standardization Administration of PRC. 2007. *GB/T 20984-2007 Information security technology - Risk assessment specification for information security*. Technical Report. General Adminstration of Quality Supervision Inspection and Quarantine. https://www.chinesestandard.net/PDF.aspx/GBT20984-2007

[52] Kim Strandberg, Tomas Olovsson, and Erland Jonsson. 2018. Securing the Connected Car: A Security-Enhancement Methodology. *IEEE Vehicular Technology Magazine* 13, 1 (3 2018), 56–65. https://doi.org/10.1109/MVT.2017.2758179

[53] Tony Ucedavélez and Marco M. Morana. 2015. *Risk Centric Threat Modeling*. John Wiley & Sons, Inc, Hoboken, NJ, USA. https://doi.org/10.1002/9781118988374

[54] UNECE. 2020. *R155*. Technical Report. UNECE. 1–194 pages.

[55] Tom Vogt, Edvin Spahovic, Thomas Doms, Rainer Seyer, Heinz Weiskirchner, Klaus Pollhammer, Thomas Raab, Stefan Rührup, Martin Latzenhofer, Christoph Schmittner, Markus Hofer, Arndt Bonitz, Carina Kloibhofer, and Sebastian Chlup. 2021. A Comprehensive Risk Management Approach to Information Security in Intelligent Transport Systems. *SAE International Journal of Transportation Cybersecurity and Privacy* 4, 1 (5 2021), 11–04. https://doi.org/10.4271/11-04-01-0003

[56] Yunpeng Wang, Yinghui Wang, Hongmao Qin, Haojie Ji, Yanan Zhang, and Jian Wang. 2021. A Systematic Risk Assessment Framework of Automotive Cybersecurity. *Automotive Innovation* 4, 3 (8 2021), 253–261. https://doi.org/10.1007/s42154-021-00140-6

[57] Chen Yan, Wenyuan Xu, and Jianhao Liu. 2016. Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-driving Vehicle. *DEFCON* 24, 8 (2016), 109.

[58] Daniel Zelle, Christian Plappert, Roland Rieke, Dirk Scheuermann, and Christoph Krauß. 2022. ThreatSurf: A method for automated Threat Surface assessment in automotive cybersecurity engineering. *Microprocessors and Microsystems* 90, 104461 (4 2022), 104461. https://doi.org/10.1016/j.micpro.2022.104461

[59] Shiying Zhou, Xuezhu Yang, Muxi Li, Huawei Yang, and Haojie Ji. 2022. Data Security Risk Assessment Method for Connected and Automated Vehicles. In *2022 IEEE 7th International Conference on Intelligent Transportation Engineering, ICITE 2022*. Institute of Electrical and Electronics Engineers Inc., Beijin, China, 379–387. https://doi.org/10.1109/ICITE56321.2022.10101389