Elevating TARA: A Maturity Model for Automotive Threat Analysis and Risk Assessment

Manfred Vielberth
manfred.vielberth@continental.com
Continental AG
Regensburg, Germany

Kristina Raab
kristina.raab@ur.de
University of Regensburg
Regensburg, Germany

Magdalena Glas
magdalena.glas@ur.de
University of Regensburg
Regensburg, Germany

Patrick Grümer
patrick.gruemer@continental.com
Continental AG
Porto, Portugal

Günther Pernul
guenther.pernul@ur.de
University of Regensburg
Regensburg, Germany

ABSTRACT

The importance of automotive cybersecurity is increasing in tandem with the evolution of more complex vehicles, fueled by trends like V2X or over-the-air updates. Regulatory bodies are trying to cope with this problem with the introduction of ISO 21434, which standardizes automotive cybersecurity engineering. One piece of the puzzle for compliant cybersecurity engineering is the creation of a TARA (Threat Analysis and Risk Assessment) for identifying and managing cybersecurity risks. The more time security experts invest in creating a TARA, the more detailed and mature it becomes. Thus, organizations must balance the benefits of a more mature TARA against the costs and resources required to achieve it. However, there is a lack of guidance on determining the appropriate level of effort. In this paper, we propose a data-driven maturity model as a management utility facilitating the decision on the maturity-cost trade-off for creating TARAs. To evaluate the model, we conducted interviews with seven automotive cybersecurity experts from the industry.

CCS CONCEPTS

• **Security and privacy → Systems security**; **Embedded systems security**.

KEYWORDS

Threat Analysis and Risk Assessment, Maturity Model, Automotive Cybersecurity

ACM Reference Format:
Manfred Vielberth, Kristina Raab, Magdalena Glas, Patrick Grümer, and Günther Pernul. 2024. Elevating TARA: A Maturity Model for Automotive Threat Analysis and Risk Assessment. In *The 19th International Conference on Availability, Reliability and Security (ARES 2024), July 30-August 2, 2024, Vienna, Austria.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3664476.3670888

ARES 2024, July 30-August 2, 2024, Vienna, Austria

ACM ISBN 979-8-4007-1718-5/24/07…$15.00
https://doi.org/10.1145/3664476.3670888

1 INTRODUCTION

Historically, automotive cybersecurity has been approached in a very superficial way, with ad hoc decisions made about the need to implement cybersecurity controls. However, as cars become increasingly software-defined, the attack surface is growing. As a result, it was not long before the first cyberattacks specifically targeted vehicles [2, 14, 20]. To counter that problem, more sophisticated security management, which is already quite common in IT in the form of an Information Security Management System (ISMS) standardized within the ISO 27001 [11], is now gaining a foothold in the automotive industry. For type approval of new vehicles, a Cybersecurity Management System (CSMS), the automotive counterpart to an ISMS, is mandatory since 2024 and is standardized within ISO 21434 [10]. Within a CSMS, the TARA (Threat Analysis and Risk Assessment) is the key element for identifying and managing risks. A TARA can be created for whole vehicles, but also on smaller scale for single ECUs (Electronic Control Units) within vehicle networks. However, the automotive industry currently lacks a clear understanding on the required level of detail of a TARA. To be compliant with ISO 21434 [10] it is possible to create a TARA in a few days (which then presumably is of low quality and of limited usefulness) or invest several months to have a very high level of detail (but with high costs for its creation). Although certain parts of TARA creation can be automated [23], the determination of the level of detail and effort invested in creating a TARA is presently contingent upon the subjective decision of the responsible expert. From this perspective, two challenges can be identified. First, this security expert not only delineates the elements to encompass within a TARA but also determines the appropriate level of granularity for its content. From this first challenge also the second, and in our opinion more important, challenge arises. There is no means to manage and determine the balance between maturity and cost, which we call the maturity-cost trade-off.

To contribute to the identified challenges, we propose D2TARA, a maturity model for measuring and managing the maturity of a TARA and a self-assessment tool for applying the D2TARA maturity model. As a first step, we focus on a data-driven approach, as it enables maturity assessment in an objective way and thus enables the transition from a subjective ad-hoc approach to a managed and well considered creation of TARAs. The target domain of the maturity model is the automotive industry. Within this domain, the target group comprises cybersecurity managers responsible

for deciding on the desired level of maturity of TARAs as well as cybersecurity experts tasked with their creation.

2 THREAT ANALYSIS AND RISK ASSESSMENT (TARA)

The TARA process broadly adopted by automotive industry is described in clause 15 of the ISO 21434 [10] and constitutes a key component of the automotive security engineering process. TARA is a method to identify cybersecurity threats during the concept and development phases following the security-by-design paradigm. Therefore, it allows for risk management at the earliest phases of development. For creating a TARA, a multitude of methodologies exist [4]. In this paper, we employ the description based on the ISO 21434 [10], due to its broad adoption in industry. As shown in Figure 1 the TARA process is divided into seven main steps.

The TARA process relies on the **Item Definition**, which encompasses the modeling of the item under development, including its components and interfaces. Based on it, cybersecurity-relevant assets (**Asset Identification**) can be identified. These assets are subsequently associated with cybersecurity properties (e.g., confidentiality, integrity, availability), whose compromise could potentially lead to various damage scenarios. During the **Threat Scenario Identification**, threats are derived from the identified cybersecurity properties. Therefore, automated methodologies like the Microsoft STRIDE threat modeling framework are available [19]. Subsequently, the likelihood of the threat to occur is determined. To achieve this, during the **Attack Path Analysis,** each step an attacker needs to take for a successful attack that leads to the threat scenario is deduced. Therefore, multiple approaches are defined in the ISO 21434, whereby presumably the most common is to model potential attacks with the help of attack trees, that comprise all possible attack paths. To finally determine the likelihood of an attack, during the **Attack Feasibility Rating** phase, the efforts are rated that an attacker has to invest for a successful attack. The **Impact Rating** aims to measure and assess the adverse consequences for road users or other stakeholders for each damage scenario. Therefore, the safety, financial, operational, and privacy impact is rated. In this context, Pape et al. [15] present a methodology specifically designed for addressing automotive privacy management concerns. With the completion of the two TARA branches, the risk level is calculated (**Risk Value Determination**) based on the feasibility (and therefore its likelihood) and the potential impact of the threats, which were determined in the steps before. Based on the risk level, a **Risk Treatment Decision** has to be taken in order to manage the identified risks. Consequently, a risk may be mitigated by avoidance (e.g., refraining from implementing a particular feature that may introduce vulnerabilities), reduced through the implementation of security controls (e.g., encrypting specific connections), shared with other stakeholders, or simply accepted.

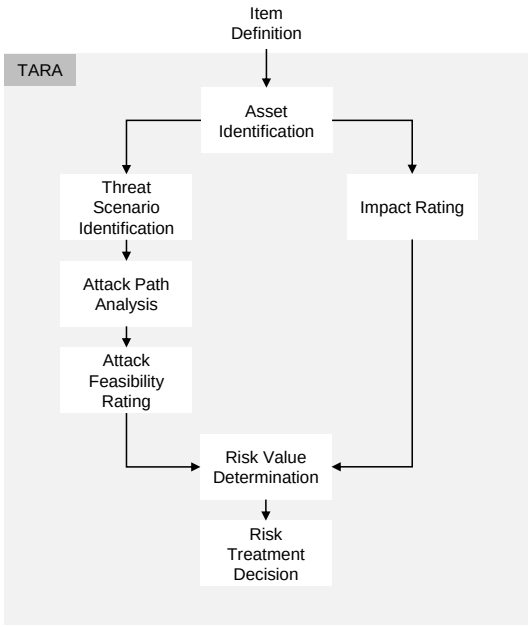

Figure 1: The TARA process based on ISO 21434 [10]

3 RELATED WORK

To contextualize our work within the scientific domain, we initially provide a general overview of capability maturity models. To further narrow down the research direction, we outline maturity models specifically designed for cybersecurity. Finally, for delineating the target domain, we examine research about maturity models for the automotive sector and specifically for TARA.

Probably the most influential work within the domain of Capability Maturity Models (CMM) was presented by Paulk et al. [16] who laid the foundation for this research field and originally defined the five capability levels from initial to optimized, which were broadly adopted by subsequent models [6, 13]. This research evolved and was transferred into practice by the SPICE (Software Process Improvement and Capability Determination) model [9], which is used for maturity assessment of the software development process within many organizations. In contrast to CMMs, SPICE not only defines maturity levels but also gives detailed guidance on how to measure it. Most of CMMs have in common, that they measure the maturity of organizational processes. A more data-centered approach was presented by Weber et al. [21]. They compare industrial reference architectures and derive the M2DDM model. It comprises six levels (Nonexistent IT integration to Self-Optimizing Factory) and measures the maturity of manufacturing, considering the degree of data integration.

Based on a comparative study of cybersecurity-focused CMMs, Rae-Guaman et al.[17] give an overview of C2M2 (Cybersecurity Capability Maturity Model). C2M2 focuses on the maturity of an organization's cybersecurity capabilities. The model was developed collaboratively by the US Department of Energy and the Carnegie Mellon University. It defines four maturity levels and is organized into ten domains, which comprise a grouping of cybersecurity practices. Focused on both, a data-driven approach and cybersecurity, Schlette et al. [18] present with CTI-SOC2M2 a CMM that measures the maturity of Security Operations Centers based on the incorporation of data sources. Therefore, the overall idea and the concept

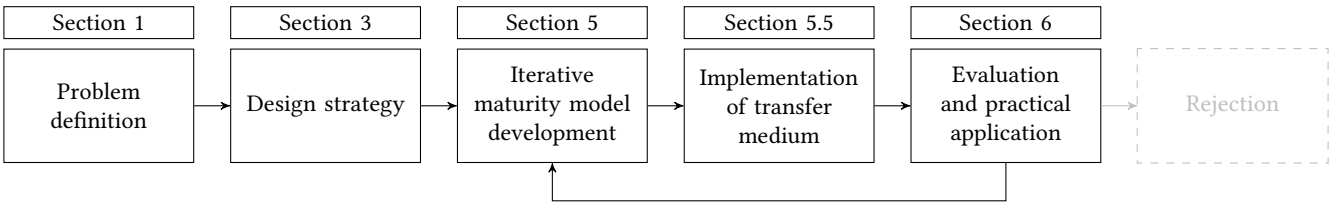

Figure 2: The method of this paper follows six steps based on Becker et al. [3]

of leveraging the degree of data integration to measure maturity is inspired by this model.

The automotive domain as a very process-driven industry broadly adopted ASPICE[1] (Automotive SPICE). As the name suggests, it adjusts SPICE for the automotive domain and measures the maturity of the development process for software-based systems. More targeted towards our research focus, Grümer and Brandão [7, 8] propose a rating system, which uses the outcome of TARA to calculate a 5-grade rating for evaluating the cybersecurity quality of vehicles. However, to the best of our knowledge, no specific CMM is targeting the TARA process.

To sum up, we encapsulate our work within the scientific context by transferring the domain perspective of the C2M2 model [17] and the model architecture of the CTI-SOC2M2 maturity model of [18] to the new application domain of TARA.

4 MODEL DEVELOPMENT

The method employed for developing our maturity model is based on Becker et al. [3], extended by the practical guidelines proposed by Mettler et al. [13]. The overall method, mapped to the respective sections of this paper, is depicted in Figure 2.

Phase 1: Problem definition. The model development begins with defining the problem, comprising the definition of the intended application domain as well as the intended benefits the model might bring. This includes the identification of the model's intended target group. We have addressed all these topics in Section 1, where we outline the problem scope with a definition of the target domain and group.

Phase 2: Design strategy. In this phase, existing maturity models are analyzed to determine a strategy for using them in our own model. Based on this comparison, we decided to go with a combination of two design strategies. On the one hand, we transferred the structures available from the SOC2M2 maturity model developed by Schlette et al. [18], especially since they are defining a data-driven approach, which we also target for our model. This model primarily serves as a basis for adopting its high-level structure, particularly concerning the determination of maturity levels through the integration of data sources for multiple services (in our case, TARA sections). On the other hand, the TARA-specific parts of our model require the design strategy of developing them from scratch, since there is no maturity model in the target domain of TARA.

[1] https://vda-qmc.de/automotive-spice/

Phase 3: Iterative maturity model development. In this phase, the general structure of the maturity model is defined before specifying the individual tiers and their attributes. Following this approach, we initially drafted the overall model architecture consisting of three tiers. Subsequently, we developed a standard pool of external data sources, which we identified in both academic (e.g., Schlette et al. [18]) and gray literature (e.g., [22]). We then defined which sections of a TARA require the integration of external data sources (in the following referred to as *data-driven TARA sections*). This corresponds to the first tier of the maturity model. Subsequently, the data sources from the data pool were categorized and mapped to the respective data-driven TARA sections (rf. Table 1). In a final step, we defined the capability and maturity levels, corresponding to the second and third tier of the model. The model was evaluated with a group of industry experts (rf. Phase 5) and adapted based on the results of this evaluation. The outcome of this adaptation represents the latest version of the model, which is presented in Section 5.

Phase 4: Implementation of transfer media. A transfer medium aims to streamline the practical implementation of the maturity model. This can take the form of document-based checklists, manuals or software tools. To this end, we developed the D2TARA self-assessment tool (rf. Figure 4) that aims to facilitate employees within an organization to assess the maturity of a TARA based on D2TARA. The concept and technical implementation of the D2TARA tool is described in Section 5.5.

Phase 5: Evaluation and practical application. To evaluate the relevance and application of the maturity model, we conducted semi-structured interviews with seven experts in automotive cybersecurity risk assessment. Through the expert interviews, we investigated the relevance and accuracy of the model, utilizing the developed tool (rf. Phase 4) to showcase the design and application of D2TARA. As described above, the findings of this evaluation phase were incorporated into a subsequent iteration step of the model development. The method we followed for conducting the interviews and the notable findings are described in Section 6. Once successfully deployed, the maturity model requires constant re-evaluation if it still fits the requirements of its application. This is done until the model cannot adapt to the change of requirements or is replaced through a new model, so it needs to be rejected as indicated in Figure 2.

5 D2TARA: DATA-DRIVEN TARA MATURITY MODEL

5.1 Overview of the Architecture

Figure 3 visualizes the architecture of D2TARA. The database icon symbolizes the identified standard pool of external data sources. The arrows leading to the data-driven TARA sections represent the mapping of the external data sources to the data-driven TARA sections. In the second tier, a capability level is determined for each data-driven TARA section based on the extent to which the external data sources are used. Finally, in the third tier, the capability levels are aggregated to the overall TARA maturity level.

5.2 First Tier

The first tier of D2TARA involves identifying a standard pool of external data sources, selecting data-driven TARA sections from the TARA process and mapping them to the data-driven TARA sections.

Standard Pool of External Data Sources. We have identified a set of TARA-relevant external data sources in the categories of (i) standards and enumerations, (ii) weaknesses and vulnerabilities, (iii) TTPs, (iv) advisories, and (v) CTI communities (rf. Table 1). Note that these data sources are not intended to be exhaustive, but rather represent a standard pool of relevant sources that can be expanded and customized to meet an organization's specific needs. The mapping of data sources and data-driven TARA sections suggests how to use external data sources and is a first step in integrating them into the TARA process. Web links to the data sources and further details about the mapping can be found on the project's GitHub page[2].

Data-Driven TARA Sections. Data-driven TARA sections benefit greatly from external data, as it is essential for their analysis to incorporate current threat data to ultimately provide the most complete risk assessment possible. The data-driven TARA sections are (i) the damage scenarios identification task during Asset Identification (DAMAGE), (ii) Impact Rating (IMPACT), (iii) Attack Path Analysis (ATTACK), (iv) Attack Feasibility Rating (FEASIB), and (v) Risk Treatment Decision (RISK TREAT).

Three TARA sections are not data-driven for the following reasons. First, Asset Identification is highly dependent on the specific item and thus on the preceding Item Definition. Since information from the item definition is proprietary, assets cannot be identified using public data sources. Second, Threat Scenario Identification is based on the automated threat modeling technique STRIDE, which does not require any additional data. Third, for Risk Value Determination, the calculation is based on values from previous TARA sections. Again, no additional data from external sources is required.

For each of the data-driven TARA sections, the required data input from the external data sources is specified in the following. In DAMAGE, descriptions of the impact on the item's cybersecurity properties are of interest. IMPACT asks for ratings of the damage scenarios in the categories of safety, financial, operational, and privacy. To create attack paths in ATTACK, it is fundamental to understand the adversary's behavior by examining tactics, techniques, and procedures (TTPs) and analyzing weaknesses and vulnerabilities. FEASIB asks for the feasibility rating of each attack path. And finally, in RISK TREAT, risk treatment options must be determined for the identified risks. This is supported by mitigation and detection strategies.

[2]https://github.com/d2tara/D2TARA

5.3 Second Tier

The second tier of D2TARA captures the extent to which external data sources are used. For each data-driven TARA section (DAMAGE, IMPACT, ATTACK, FEASIB, and RISK TREAT), a capability level ranging from Undefined (0) to Augmentation (4) is determined based on the answer to an indicative question. The five capability levels build upon each other. This means that completion of the lower levels is a necessary condition for achieving the next higher level. The capability levels (CLs) and their associated indicative questions are listed in Table 2.

At CL 0, no external data sources are used. CL 1 requires the use of external data sources in an ad hoc manner, meaning that external data sources are used on the initiative of the expert without a standardized process. For example, the expert searches the internet for data sources. CL 2 requires the definition of a standard pool of external data sources. At CL 3, the standard pool of external data sources must be integrated into the TARA process. This means that it is specified how the external data sources are to be used for each data-driven TARA section. At the highest capability level, CL 4, the external data sources within the standard pool must be continuously monitored for information suggesting a repetition of the TARA process. The goal is not only the highest level of security, but also economic efficiency, since, for example, a new mitigation strategy may provide a less costly risk treatment option. Schlette et al. [18] define another level between CLs 3 and 4: the automation level. We deviate from this scale because automation does not contribute to the goals of the maturity model in terms of a data-driven approach, but is aimed at process efficiency (e.g., automated creation of TARA sections).

5.4 Third Tier

The third tier of D2TARA aggregates the capability levels of the data-driven TARA sections into an overall TARA maturity level ranging from Initial (1) to Visionary (4). Table 3 lists the maturity levels (MLs) and shows how the aggregation is applied.
At ML 1, DAMAGE, ATTACK, and FEASIB must meet CL 1. We have chosen these three of the five data-driven TARA sections because the use of external data sources is straightforward in these TARA sections. At ML 2, CL 2 must be achieved by all data-driven TARA sections. This establishes a core data-driven TARA process.

Building on this, at ML 3, CL 3 must be accomplished in all data-driven TARA sections. Finally, at the highest maturity level, ML 4, all data-driven TARA sections must realize CL 4. MLs 3 and 4 are, as the names suggest, ambitious goals that can be daunting for organizations with limited resources and those new to the concept. We encourage organizations to view the maturity levels as an evolutionary path that can be taken in small steps. In addition, organizations do not have to reach the final stage. This is why we

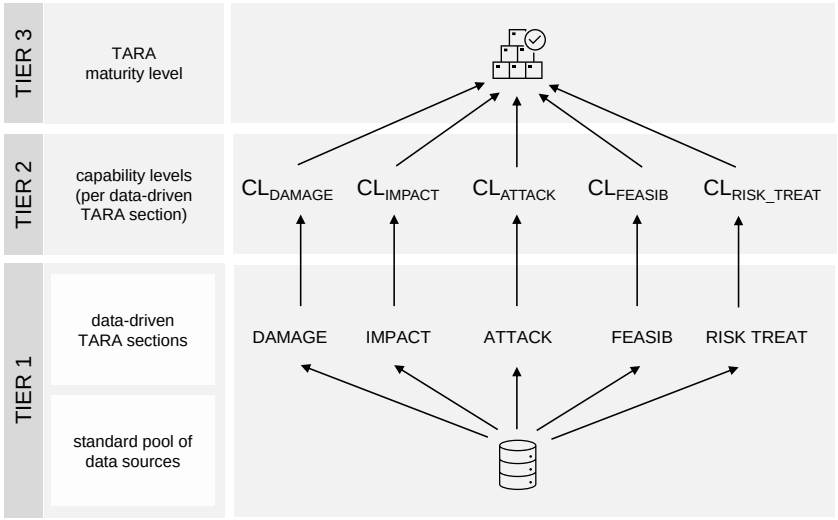

Figure 3: The D2TARA architecture composed of three tiers.

Table 1: The standard pool of external data sources mapped to the data-driven TARA sections (Tier 1).

Data Source	DAMAGE	IMPACT	ATTACK	FEASIB	RISK TREAT
Standards & Enumerations					
CWE (MITRE)	•			•	•
CVE (MITRE)		•		•	
CVSS (FIRST)		•		•	
CAPEC (MITRE)	•	•	•	•	•
Weaknesses and Vulnerabilities					
NVD (NIST)		•		•	
KEV Catalog (CISA)					•
JVN (JPCERT/CC, IPA)	•	•		•	•
Vulnerability Notes Datab. (SEI)	•				•
Vulnerability & Exploit Datab. (Rapid7)	•	•		•	•
TTPs					
ATT&CK (MITRE)			•		•
ATM (AutoISAC)			•		•
D3FEND (MITRE)					•
Advisories					
Cybersecurity Advisories (CISA)	•		•		•
ICS Advisories (CISA)	•	•		•	•
CTI Communities					
AutoThreat (Upstream)	•		•		
OTX Endpoint Security (AlienVault)	•	•		•	
VulDB	•	•	•	•	•

have defined D2TARA as a decision support tool for setting organizational goals, communicating associated operational requirements, and ultimately managing the maturity-cost trade-off.

5.5 Transfer Medium: D2TARA Self-Assessment Tool

The goal of the transfer medium is to make the model accessible to the previously defined target group [3]. Therefore, we decided to develop a web-based tool (rf. Figure 4), enabling security experts to self-assess a TARA. On the left side, a questionnaire is provided that allows the expert to specify the capability level for each data-driven TARA section based on the indicative questions defined within the model (rf. Table 2). Based on the answers, on the right side, the achieved maturity level, from Initial to Visionary is shown. To give a good overview of the current state of the TARA and to identify possible areas of improvement, a radar chart visualizes the selected

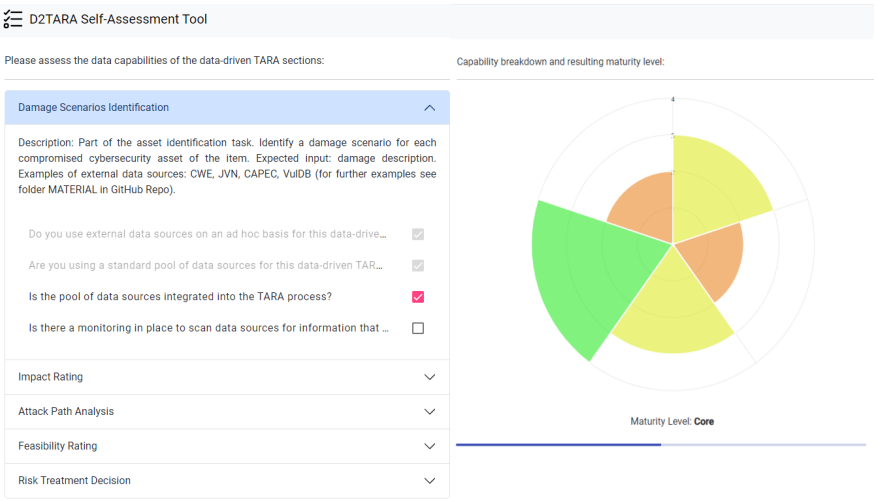

Figure 4: The D2TARA self-assessment tool.

Table 2: Capability levels of the data-driven TARA sections (Tier 2).

CL	Caption	Indicative Question
0	Undefined	No external data sources are used for this data-driven TARA section.
1	Ad Hoc	Do you use external data sources on an ad hoc basis for this data-driven TARA section?
2	Standardization	Are you using a standard pool of data sources for this data-driven TARA section?
3	Integration	Is the pool of data sources integrated into the TARA process?
4	Augmentation	Is there a monitoring in place to scan data sources for information that could lead to a reiteration of the TARA process?

Table 3: TARA maturity levels (Tier 3).

ML	Caption	Description
1	Initial	CL 1 (Ad Hoc) is reached for DAMAGE, ATTACK, and FEASIB.
2	Core	CL 2 (Standardization) is achieved in all data-driven TARA sections.
3	Extended	CL 3 (Integration) is achieved in all data-driven TARA sections.
4	Visionary	CL 4 (Augmentation) is achieved in all data-driven TARA sections.

capability levels. The tool is publicly available[3] and the source code is provided under open source license on GitHub[4] to allow broad adoption.

6 EVALUATION

In the following section, we describe the method we employed to evaluate D2TARA and present the key findings of the evaluation.

6.1 Evaluation Method

The evaluation should assess the maturity model for comprehensiveness, consistency, and problem adequacy to evaluate if the proposed model provides a viable solution for the defined problem. Building upon the method outlined by Becker et al. [3] and previously utilized in related studies [18, 21], we evaluated D2TARA through expert interviews. We recruited seven experts (rf. Table 4) who belong to the D2TARA target group, i.e., experts who work in the automotive sector and are directly (i.e. cybersecurity analysts and architects) or indirectly (i.e. decision makers) involved in the TARA process. To this end, we employed purposive sampling, selectively recruiting participants who meet the target group criteria from the authors' professional networks. Table 4 provides an overview of the demographics of the participants. The seven participants were grouped based on their job roles (*Cybersecurity Manager* or *Cybersecurity Senior Consultant*) to ensure their anonymity. To allow for individual thoughts without limiting the range of possible responses, the expert interviews were conducted in a semi-structured manner [1, 12]. To this end, an initial interview guide was developed through several rounds of discussion between the authors. To assess the interview guide, we conducted a test interview with one expert. Since only a few minor adaptions were made to the guideline after the test interview, the interview was included in our sample. The final interview guide consists of three phases:

[3]https://d2tara.github.io/D2TARA/

[4]https://github.com/d2tara/D2TARA

(1) **Introduction.** The interview begins with mutual introductions and an overview of the project. Respondents are then presented with D2TARA. Throughout the interview, they are encouraged to express any ambiguities or criticisms directly.
(2) **Evaluation of D2TARA.** After being introduced to the project, this second phase aims to evaluate D2TARA with a focus on its problem relevance, comprehensibility and comprehensiveness. Participants are also asked to indicate if they are missing any aspects or need further clarification.
(3) **Maturity Assessment Using D2TARA.** This phase focuses on the applicability of D2TARA. For this purpose, the D2TARA self-assessment tool[3] was presented to the interviewees. The aim is to find out if D2TARA is practicable and if the tool enables its use in a comprehensible way. As in the second interview phase, the participants are asked about open points or insufficient explanations.

Every phase consists of a set of interview questions. The full guide is made available on GitHub[5].

The interviews took place in March 2024 and lasted, on average, 57 minutes. One author conducted all seven interviews. For the majority of interviews, at least one second author participated in the session, allowing for additional questions and brief discussions after the participant left. Interviews were conducted over an online conferencing tool and held in English (n=3) and German (n=4). The participants were informed that their data was anonymized before analysis and is published in an aggregated manner. With the participants' consent, the interviews were recorded using a digital voice recorder and later transcribed.

We used inductive coding as elaborated by Corbin and Strauss [5] for data analysis. The first round of coding was done by the author who conducted the interviews, identifying recurring patterns according to predefined themes. On this basis, the authors inductively drew conclusions from the interviews in several rounds of discussion. All findings were approved by the interviewees and are presented below.

6.2 Results

In the following, we describe the key findings of the experts interviews. First, we present the results obtained with respect to the D2TARA model. Then we describe the feedback we received on the application of D2TARA through the self-assessment tool.

D2TARA model. Respondents agreed that a data-driven approach is important and that the associated maturity-cost trade-off needs to be managed appropriately. One of the reasons given for a data-driven TARA was that results can vary widely from expert to expert when different data sources are used. A standard repository of data sources would help to overcome this problem. Second, participants considered it very important that TARA results are up-to-date. According to them, this is well ensured by the data-driven approach, especially in CL 4 (Augmentation). Third, the addition of external data sources to the internal data sources to broaden knowledge was strongly supported by respondents.

While some of the external data sources presented in the standard pool were already known and used manually, which corresponds to CL 1 (Ad hoc), many data sources were rather unfamiliar to the respondents. A summary of all internal and external data sources available to the experts in a standard pool was therefore highly appreciated. However, which data sources are included and considered most important by the participants depends very much on the specific organization. As a result, we found that the standard pool can vary greatly from one organization to another.

There were significant differences among the participants in the selection of data-driven TARA sections. One participant stated that they not considers IMPACT and FEASIB to be data-driven TARA sections because of the discrepancy between the IMPACT and FEASIB rating schemes specified in ISO/SAE 21434 and the Common Vulnerability Scoring System (CVSS)[6], which is predominantly used in external data sources. Specifically, IMPACT is rated in the automotive categories of safety, financial, operational, and privacy, but CVSS uses the cybersecurity categories of confidentiality, integrity, and availability for its impact rating. For FEASIB, ISO/SAE 21434 distinguishes between three different rating schemes, only one of which explicitly uses the CVSS rating system, while the other two schemes do not. A mapping between TARA and public rating schemes therefore needs to be explicitly defined. This could be discussed, for example, as part of CL 4, i.e., the integration of the standard pool into the TARA process. While this respondent did not consider IMPACT and FEASIB to be data-driven TARA sections, others stated that external data sources can indeed be a valuable reference point for conducting these ratings, albeit based on different schemes. Another participant mentioned close relationships between TARA sections, especially between DAMAGE and IMPACT, so that relevant data sources can be used in both and are thus equally data-driven. Finally, one respondent stated that in their specific organizational context, the risk treatment decision is driven solely by internal data sources, so RISK TREAT is not data-driven for him or her.

Regarding the capability levels, one respondent expressed confusion about the wording of the indicative questions. He or she pointed out that data sources can be used not only in the TARA creation process, but also afterward, e.g., in a review or update. As a result, we changed *TARA creation process* to *TARA process* in the indicative question for CL 3 (Integration). One respondent also discussed whether the maturity assessment nomenclature could be aligned with existing automotive standards (in particular ASPICE[1]) to ensure standardization and thus ease of use. This concerned in particular the labeling of the CLs (i.e., from Undefined to Augmentation), which is not identical to the terms used in ASPICE (i.e., from Incomplete to Innovating). While some participants were in favor of alignment, others were opposed because of the risk of confusion. As explained in Section 3, ASPICE and D2TARA have different objectives and therefore cannot be directly compared. Alignment would only make sense in a much higher level context (e.g., a suite of maturity models for automotive) and is therefore not considered significant at this time.
In summary, the participants agreed with the definition of the capability levels and their aggregation to a specific maturity level. They were particularly supportive of maturing towards ML 4 (Visionary), as this will have a significant impact on current practices

[5]https://github.com/d2tara/D2TARA/tree/main/material

[6]https://www.first.org/cvss/

Table 4: Information on Interview Participants. *TARA Scope* indicates whether the TARA is performed at the whole vehicle level or at the component level. The column *Avg. Experience* gives the average cybersecurity experience in years, and the column *Avg. TARAs* shows the average number of TARAs the participants in the respective group have created.

Job Role	Number of Participants	TARA Scope	Avg. Experience	Avg. TARAs
Cybersecurity Manager	5	component level	7	7
Cybersecurity Senior Consultant	2	vehicle level	13	15

and is indeed considered a visionary goal to achieve in automotive cybersecurity.

Practical application. The possibility to use D2TARA through a web-based tool was considered very helpful by the participants, as it makes it easier to understand how D2TARA works and more practical to use. Regarding the individual data-driven TARA sections, the participants suggested to specify what input from external data sources is required and to provide examples together with links to external data sources. As a result, we have added an expected input and several examples of external data sources to the tool's description of each data-driven TARA section. More details about the external data sources (specifically, the provider and a web link) are available on GitHub[5].

When asked about the next steps necessary for an organizational integration of D2TARA, the participants suggested similar approaches. On the one hand, D2TARA needs to be introduced to a wider user base. On the other hand, D2TARA needs to be linked to existing TARA software tools and platforms in order to facilitate the use of D2TARA by experts and thus achieve broad acceptance.

Conclusions from the Interviews. An important result of the interviews is that D2TARA is an initial model that needs to be adapted to the respective business context. This was made clear by the considerable differences in the selection of relevant data sources for the standard pool, as well as in the definition of which TARA sections are data-driven. Furthermore, a core statement regarding the practical application is the integration of D2TARA into existing software platforms to enable an end-to-end TARA workflow. Since the data-driven goals of D2TARA were described as very promising for the future, all participants supported further development.

7 LIMITATIONS AND FUTURE WORK

As with any research endeavor, our work is not without limitations, which we aim to acknowledge while outlining strategies for their potential mitigation in future work. The D2TARA model has a data-driven focus, as we believe this is the most decisive factor in assessing the degree of maturity. Therefore, other dimensions were not considered. However, it would be worthwhile to include the TARA process itself as an additional factor in the maturity assessment in future work. In this case, an alignment with the ASPICE model would be useful, as it measures process maturity. This could also be advantageous for practical adaptation, as ASPICE is already widely used in the automotive industry. This leads to another open topic. Although we have demonstrated the practical relevance through expert interviews, the model has not been used in real projects yet, which we leave to future work. Challenges in this regard that emerged from the expert interviews are, that it may be difficult to integrate the maturity model into already established processes. In addition, the degree of automation of integrating external data sources should be decided, as the model leaves open whether they are integrated purely manually by a security expert or whether their integration is supported by software tools. Future research could contribute to these challenges by providing guidance for practical application.

8 CONCLUSION

In this work, we have presented D2TARA, a data-driven maturity model for TARA. Structured in three tiers, D2TARA measures the overall TARA maturity by assessing the degree of data integration for each step within the TARA creation process. Expert interviews demonstrated the practical relevance of the model and provided insight for future research and next steps towards practical application. To ensure a high level of comprehensibility and reproducibility, we followed a methodical approach to both model development and expert interviews. In conclusion, the D2TARA model takes a step to a more sophisticated and structured TARA and ultimately contributes towards making the mobility of the future more secure.

ACKNOWLEDGMENTS

We would like to thank all the experts for their valuable time and the insights they provided during the interviews.

REFERENCES

[1] William C. Adams. 2015. Conducting Semi-Structured Interviews. In *Handbook of Practical Program Evaluation*. John Wiley & Sons, Ltd, 492–505. https://doi.org/10.1002/9781119171386.ch19

[2] Amir Alipour-Fanid, Monireh Dabaghchian, Hengrun Zhang, and Kai Zeng. 2017. String stability analysis of cooperative adaptive cruise control under jamming attacks. In *2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE)*. IEEE, 157–162.

[3] Jörg Becker, Ralf Knackstedt, and Jens Pöppelbuß. 2009. Developing Maturity Models for IT Management. *Business & Information Systems Engineering* 1, 3 (June 2009), 213–222. https://doi.org/10.1007/s12599-009-0044-5

[4] 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 *Proceedings of the 18th International Conference on Availability, Reliability and Security* (Benevento, Italy) *(ARES '23)*. ACM. https://doi.org/10.1145/3600160.3605084

[5] Juliet Corbin and Anselm Strauss. 2008. *Basics of Qualitative Research (3rd ed.): Techniques and Procedures for Developing Grounded Theory*. https://doi.org/10.4135/9781452230153

[6] Adamu Garba, Maheyzah Sirat, and Siti Othman. 2020. An Explanatory Review on Cybersecurity Capability Maturity Models. *Advances in Science Technology and Engineering Systems Journal* 5 (Aug. 2020), 762–769. https://doi.org/10.25046/aj050490

[7] Patrick Grümer and Pedro Brandão. 2023. Computing an Automotive Cybersecurity Maturity Level Assessment Programme. In *Proceedings of the 7th ACM*

Computer Science in Cars Symposium (Darmstadt, Germany) *(CSCS '23)*. Association for Computing Machinery, New York, NY, USA, Article 4, 10 pages. https://doi.org/10.1145/3631204.3631865

[8] Patrick Grümer and Pedro Brandão. 2023. An Automotive Cybersecurity Maturity Level Assessment Programme. In *2023 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*. 84–91. https://doi.org/10.1109/DSN-W58399.2023.00035

[9] ISO/IEC 15504:2011(E) 2011. *Information technology – Process assessment*. Standard. International Organization for Standardization.

[10] ISO/IEC 21434:2022(E) 2021. *Road vehicles – Cybersecurity engineering*. Standard. International Organization for Standardization.

[11] ISO/IEC 27001:2022(en) 2022. *Information technology — Security techniques — Information security management systems — Requirements*. Standard. International Organization for Standardization.

[12] Beth L. Leech. 2002. Asking Questions: Techniques for Semistructured Interviews. *PS: Political Science & Politics* 35, 4 (Dec. 2002), 665–668. https://doi.org/10.1017/S1049096502001129 Publisher: Cambridge University Press.

[13] Tobias Mettler and Omar Ballester. 2021. Maturity Models in Information Systems: A Review and Extension of Existing Guidelines.

[14] Charlie Miller and Chris Valasek. 2015. Remote exploitation of an unaltered passenger vehicle. *Black Hat USA* 2015 (2015), 1–91.

[15] Sebastian Pape, Sarah Syed-Winkler, Armando Miguel Garcia, Badreddine Chah, Anis Bkakria, Matthias Hiller, Tobias Walcher, Alexandre Lombard, Abdeljalil Abbas-Turki, and Reda Yaich. 2023. A Systematic Approach for Automotive Privacy Management. In *Proceedings of the 7th ACM Computer Science in Cars Symposium*. 1–12.

[16] Mark C Paulk, Bill Curtis, Mary Beth Chrissis, and Charles V Weber. 1993. Capability maturity model, version 1.1. *IEEE software* 10, 4 (1993), 18–27.

[17] Angel Marcelo Rea-Guaman, Tomás San Feliu, Jose A. Calvo-Manzano, and Isaac Daniel Sanchez-Garcia. 2017. Comparative Study of Cybersecurity Capability Maturity Models. In *Software Process Improvement and Capability Determination*, Antonia Mas, Antoni Mesquida, Rory V. O'Connor, Terry Rout, and Alec Dorling (Eds.). Springer International Publishing, Cham, 100–113.

[18] Daniel Schlette, Manfred Vielberth, and Günther Pernul. 2021. CTI-SOC2M2 – The quest for mature, intelligence-driven security operations and incident response capabilities. *Computers & Security* 111 (Dec. 2021), 102482. https://doi.org/10.1016/j.cose.2021.102482

[19] Adam Shostack. 2014. *Threat Modeling: Designing for Security*. John Wiley & Sons, Ltd.

[20] Zhendong Wang, Haoran Wei, Jianda Wang, Xiaoming Zeng, and Yuchao Chang. 2022. Security Issues and Solutions for Connected and Autonomous Vehicles in a Sustainable City: A Survey. *Sustainability* 14, 19 (2022), 12409.

[21] Christian Weber, Jan Königsberger, Laura Kassner, and Bernhard Mitschang. 2017. M2DDM–a maturity model for data-driven manufacturing. *Procedia Cirp* 63 (2017), 173–178.

[22] Jackson Wynn and MITRE. 2017. MITRE ICS/SCADA Cyber Repository. (2017). https://www.mitre.org/sites/default/files/2021-11/pr-17-0876-mitre-ics-scada-cyber-repository-briefing.pdf

[23] 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 (2022), 104461.