Vehicular Over-the-Air Software Upgrade Threat Modelling

Rudi Mocnik[1] and Daniel S. Fowler[2] and Carsten Maple[2]
[1]Red Bull Media House GmbH, 5071, Salzburg, Austria
[2]WMG, University of Warwick, Coventry, CV4 7AL, UK

Corresponding author: Daniel S. Fowler (e-mail: dan.fowler@warwick.ac.uk).

ABSTRACT

The major vehicle manufacturers deploy Over-the-Air (OTA) software update technology for their vehicle systems. In this research, we review the literature on the cybersecurity of the OTA software update mechanism. This allowed the derivation of a high-level reference architecture for the OTA system. The architecture and review guided the analysis of the OTA system attack surface. A novel asset-centric threat modelling method is derived from the analysis and applied to the OTA software upgrade use case. System assets identification, system decomposition and labelling are three steps of a four-step threat modelling methodology. The final step enables attack vector threat analysis and mitigation. The final contribution comes from actionable cybersecurity recommendations for software upgrade systems, providing threat mitigation recommendations for their secure implementation. Knowledge of potential long-range wireless attacks and other OTA system threats provides a foundation for stakeholders' strategic investment in cybersecurity risk reduction. This investment is needed to address a dilemma. On the one hand, OTA systems are a useful technology for updating the software in cyber-physical systems, however, they do provide a potential conduit for cyber attacks. Whilst this work researched vehicular OTA systems, it could be applied to other cyber-physical systems that require secure software updates over a lifecycle.

INDEX TERMS Communication system security, embedded software, land vehicles, security management, cyber-physical systems.

I. INTRODUCTION

Cars and other vehicle types have become software on wheels as a result of the rapid adoption of digital technology. This software needs to be maintained and updated when bugs are fixed, cybersecurity vulnerabilities are found, and new functionality can be enabled.

A vehicle's cellular, Wi-Fi, or Bluetooth connection, marketed as a beneficial feature by car manufacturers, is a useful channel for software updates of a car's embedded computers. In this work, the term "OTA" refers to a wirelessly connected and remotely provisioned, i.e. "over-the-air", software update or upgrade system. Note, the term "firmware-over-the-air" (FOTA) is sometimes used in the literature.

However, any connected system, as decades of using the Internet have demonstrated, brings cybersecurity issues, and the technology-rich vehicle, including its OTA system, is an attractive cyber target. OTA technologies could be hijacked and used to attack the vehicle or breach into an Original Equipment Manufacturer's (OEM) enterprise network. Yet, OTA systems are seen as a solution to address vulnerabilities that emerge from cyber threats. Furthermore, OTA systems add complexity to the already complex supply chain. Complex supply chains contribute to the obfuscation of the connected vehicle ecosystem, hindering the identification of cyber threats. Therefore, it is sensible for OEMs to adopt strategies to maintain secure OTA systems.

A. ANALYSING OTA CYBER THREATS

In our work, we have taken a qualitative approach to consolidate threat information on OTA systems for OEMs, their suppliers, and other decision-makers. This allows stakeholders to make informed cybersecurity decisions when designing OTA software upgrade solutions. This study addressed the problem in four parts:

1) Performing literature analysis on the OTA system and components, discussing how connectivity and software trends drive a vehicle's cybersecurity exposure and exploring potential attackers' capabilities.
2) Examining the suggested mitigation technologies, the role of the supply chain, and cybersecurity inhibitors, including technological hurdles and cost implications. Technical solutions, for example, digital signatures, and administrative solutions, such as vulnerability

management, are mapped to support threat modelling for a secure OTA software upgrade system. Further, ISO/SAE 21434 "Road vehicles — Cybersecurity engineering" [1] is one of the standards and guidelines that OEMs can use to develop their cybersecurity capabilities.

3) A novel asset-centric threat modelling 4-step method is developed based on the findings and applied to the OTA software upgrade case. The assets identification, system decomposition and labelling steps of the threat modelling allow for final threat analysis.
4) The final contribution comes from actionable cybersecurity recommendations for OEMs regarding securing OTA software upgrade systems.

This study addresses the threat analysis part of the Threat Analysis and Risk Assessment (TARA) present in ISO/SAE 21434 as applied to vehicular OTA systems. Full threat analysis of vehicular systems expands beyond the threat modelling discussed in this research. A vehicle's complex software systems and time limitations restricted this work to OTA threat analysis. Suggestions are given on how the model may be integrated into the full TARA process.

B. ORGANISATION OF THE WORK

Section II provides a background on how connected cars have raised concerns about automotive cybersecurity, the reasons for OTA software delivery, and OTA systems becoming a critical function in vehicles. This motivates the objectives and contribution introduced in Section III and the need to understand OTA cyber threats via threat modelling. The research methodology in Section IV details the literature and data sourcing. It includes the reasoning for threat modelling. The literature findings are then discussed in five sections:

- Section V summarises views on OTA system advantages and disadvantages.
- Section VI examines researchers' understanding of the OTA system architecture.
- Section VII is on the vehicular cyber attack surfaces and vectors.
- Section VIII on mitigation measures, including the role of the supply chain, and security challenges.
- Section IX on existing threat modelling discussions.

In Section X we present the reasoning for the novel asset-centric threat model and its application to the OTA upgrade system. This informs the discussion in Section XI where security recommendations are provided and where further work can be performed. Section XIII concludes with a recap of the work and contribution.

II. AUTOMOTIVE CYBERSECURITY AND OTA BACKGROUND

The advancement of digital technology has enabled the connected car (see Figure 1). The range of connected, i.e., OTA, services is broad. Alongside software updates for bug fixes and activation of new features [2], [3] the connected car provides:

FIGURE 1. Vehicle Internet connectivity, directly or via smartphones, is commonplace. (Image CC BY-SA 4.0 via Wikimedia Commons.)

- The ability to control vehicle functions from a smartphone.
- Cars connecting to smartphone apps.
- Vehicles provisioning a Wi-Fi hotspot.
- Manufacturers selling additional Internet-connected services.

Visit the websites and dealerships of car manufacturers and you will see vehicle connectivity and the services it enables highlighted as beneficial features. The rapid adoption of digital technology and increased connectivity in mass-manufactured vehicles can provide a cyber attacker (i.e., a *threat agent* [4]) motivation to infiltrate vehicle systems. The intrinsic value of vehicles and vehicle parts, plus the size of the vehicle market, indicate high potential rewards for successful cyber attacks. Furthermore, for nation-state actors and other threat agents, there is the potential ability to disrupt road networks via the disabling of vehicles.

In our work vehicles are passenger cars. However, the vehicle ecosystem is much broader, encompassing commercial vehicles and trucks, public transportation including busses, trains and aeroplanes, and services such as ride-hailing apps, car rental, and more. Therefore, although our work addresses a small part of the ecosystem, the OTA upgrade concepts described herein could be applied to the general transportation domain.

The principle of OTA updates is well established. Smartphone users will be familiar with prompts to install updates. Installed *apps* will often update automatically. Handset updates targeted at the operating software emerged in the 1990s with the advent of software-defined radio [5]. Further back, updating space and defence systems using OTA is from the 1980s [6]. Updates for vehicle systems have been researched since the mid-2000s with United States patents issued in the mid-1990s [7]–[9].

OTA software upgrades are important for connected vehicles to help combat emerging cyber threats. Technologically driven car companies use OTA software upgrades to update functionality and patch security vulnerabilities. The OTA software upgrade capability within a car begins with a telematics control unit (TCU), a computer wired into the vehicle systems that has wireless communications capability. The TCU typically establishes a cellular connection to OEM-controlled data servers. The vehicle reports software versions of its systems and the servers then respond with pending updates. The vehicle prompts the driver to authorise the update. Upon successful authorisation, the software is downloaded to the car and installed on the target vehicle's relevant digital components.

Despite its advantages, OTA technology brings additional security challenges to the vehicle, including the potential to endanger occupants' lives (e.g., through the disruption of a vehicle's control system). Cybersecurity issues in the automotive industry were highlighted with the infamous Jeep hack [10]. Although this was an experiment for research aims, the attackers gained control of the vehicle (acceleration, engine and other car functions) from a substantial distance. This was achieved through a multistage exploit via the vehicle's infotainment system. The exploit leveraged a vulnerability in the infotainment's "UConnect" software (i.e., the operating system), without any hardware modifications to the car.

The Jeep incident highlighted the security and safety issues of cyber attacks when they impact a car in its operational environment. Rigorous safety standards exist for vehicles to maintain high safety levels and these safety levels should not be compromised by software issues. Guidance and standards targeting vehicle cybersecurity have been introduced by the automotive industry to mitigate cyber threats. These include type approval [11] regulations (where vehicles need to adhere to certain standards) and the aforementioned ISO/SAE 21434 (which replaced J3061, Cybersecurity Guidebook for Cyber-Physical Vehicle Systems [12]). These exist to guide manufacturers in improving vehicle cybersecurity and aid in assessing a vehicle system's cyber safety over its life cycle.

III. OBJECTIVES AND CONTRIBUTION

Consumer and market demands will see all of the world's mass-manufactured vehicles with wireless connectivity. The assumption is that all connected cars will support a variance of OTA software upgrades, exposing vehicles to potential remote attacks. OEMs are taking different approaches to implementing OTA technologies [2], however, many technical details are omitted due to the automotive industry's proprietary nature. Despite the lack of access to proprietary information research on remote attacks against vehicle systems are possible [13], [14]. This motivates a presentation of factors related to vehicular remote cyber attacks and mitigation strategies.

An overview threat assessment of the OTA software upgrade process was performed based on published research. The guiding question was *how can OTA upgrade system technology be exploited to attack vehicle and OEM systems?* The threat modelling Research Objectives (RO) to address this question are:

1) Analyse published work of cyberattacks on vehicle systems to establish how vehicle systems may be attacked.
2) Evaluate the attack vectors specific to OTA software upgrade technologies and their potential impact and importance.
3) Analyse literature for protective measures that protect against vehicle attacks, to establish the current state of mitigation and cyber resilience.
4) Perform threat modelling for the OTA software upgrade system to establish a framework for threat mitigation.
5) Provide a set of recommendations for OEMs and their tier suppliers to improve the security of OTA software upgrade technologies.

Improving the security of remote software upgrades increases the difficulty of cyber attacking a vehicle system. A lack of concise information was identified for OEMs and other stakeholders for informing cybersecurity investment and strategic decisions on OTA upgrade systems. The developed threat model will aid stakeholders needing to make such decisions. The threat model offers explanations and shows relationships between cyber attack vectors targeting the OTA system components and the mitigation strategies applied. The generic OTA system threat model is then used to provide action-oriented recommendations for OEMs to secure OTA systems. This aids stakeholders in good security design for their OTA software upgrade technologies. Additionally, the work contributes to the broader automotive cybersecurity knowledge base.

IV. METHODOLOGY

A qualitative research approach was used to develop the novel threat model systematically. The analysis was informed by a range of collected data points which include attack, defence, threat modelling, threat actor, and other relevant information. Further, the qualitative approach collated different arguments and approaches applied by researchers in their work. The following two sections describe how we performed the study and the production of the threat model and set of recommendations.

A. INFORMATION SOURCES

Reviewing the literature found that not all relevant automotive cybersecurity literature is published in academic journals. For example, Def Con and Black Hat conferences are popular platforms used to present cybersecurity research; however, people presenting do not always publish academic papers and instead capture results in non-standard format [15]. Furthermore, relevant regulatory documents and standards are not published in academic papers. However, we found that some authors of academic literature use those primary sources to integrate the knowledge as a basis for their work. We do not rely on mainly non-academic sources and opted to use academic literature from specialist databases. In our experience, the reporting of cybersecurity research is not always as rigorous as some other scientific fields,

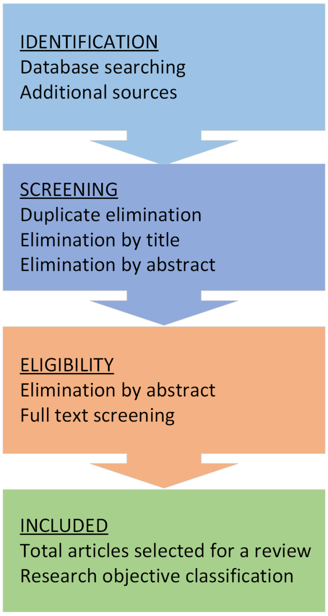

FIGURE 2. Review selection process.

and there are challenges in extracting relevant information from academic and non-academic sources, acknowledging that some information may not be uncovered or qualitative analysis is open to differences in interpretation. Figure 2 summarises the main steps of the literature selection process.

B. OTA REVIEW

Table 1 shows the two search strings and the number of search results for each specialist database used in the Systematic Literature Review (SLR):

1) A search string to capture literature on cyber attacks on vehicle systems;
2) and one to find literature on vehicle OTA or FOTA software update technology.

The results saw that all attacks were performed by white-hat hackers that penetrated the vehicle system using black-box approaches, i.e. reverse engineering and other methods to learn about the systems and find vulnerabilities. It is acknowledged that difficulties in accessing accurate data due to manufacturers' intellectual property (IP) controls may lead to incorrect assumptions by researchers.

TABLE 1. Databases, query strings and the number of results.

Database	Query	Count
Scopus	TITLE-ABS-KEY((vehic* OR automo*) AND (cyber*) AND (attack) AND (review)) AND (LIMIT-TO (PUBYEAR, 2021) OR LIMIT-TO (PUBYEAR , 2020) OR LIMIT-TO (PUBYEAR, 2019) OR LIMIT-TO (PUBYEAR, 2018) OR LIMIT-TO (PUBYEAR, 2017) OR LIMIT-TO (PUBYEAR, 2016)) AND (LIMIT-TO (LANGUAGE, "English"))	72
Scopus	TITLE-ABS-KEY((vehic* OR automo*) AND (cyber*) AND (attack) AND ("software upgrade" OR "OTA" OR "FOTA" OR “over-the-air”)) AND (LIMIT-TO (PUBYEAR, 2021) OR LIMIT-TO (PUBYEAR, 2020) OR LIMIT-TO (PUBYEAR, 2019) OR LIMIT-TO (PUBYEAR, 2018) OR LIMIT-TO (PUBYEAR, 2017) OR LIMIT-TO (PUBYEAR, 2016)) AND (LIMIT-TO (LANGUAGE, "English"))	9
IEEE Xplore	("Document Title":vehic* OR "Document Title":automo*) AND ("Document Title":cyber*) AND ("Document Title":attack*)	34
IEEE Xplore	("Document Title":vehicl* OR "Document Title":automo*) AND ("Document Title":"ota" OR "Document Title":"fota" OR "Document Title":"over-the-air" OR "Document Title":"software upgrade" OR "Document Title":"software update" OR "Document Title":"upgrade")	41
ACM Digital Library	[[Publication Title: auto*] OR [Publication Title: vehic*] OR [Publication Title: car]] AND [Publication Title: cyber*] AND [Publication Title: attack] AND [Publication Date: (01/01/2016 TO 12/31/2021)]	31
ACM Digital Library	[[Publication Title: auto*] OR [Publication Title: vehic*]] AND [[Publication Title: "ota"] OR [Publication Title: "fota"] OR [Publication Title: "over-the-air"] OR [Publication Title: "software update"] OR [Publication Title: "software upgrade"] OR [Publication Title: "upgrade"]] AND [Publication Date: (01/01/2016 TO 12/31/2021)]	19
SAE Mobilus	Title:(auto* OR vehic* OR "car") AND Metadata Only:(attack* OR cyber* OR exploit*) AND Metadata Only:("long-range" OR "wireless" OR "remote")	60
SAE Mobilus	Title:(auto* OR vehic* OR "car") AND Title:("ota" OR "fota" OR "over-the-air" OR "software upgrade" OR "software update" OR "upgrade")	12

Note, where dates are not shown an additional web page filter was applied.

Work published from 2016-2021 was chosen for two reasons. Firstly, vehicle design and development cycles vary in the literature between two to five years, which means the technology in older vehicles is soon outdated. However, assuming that the technology in the design phase was cutting-edge may not always be the case. This is due to the automotive industry's high safety standards and consequential reluctance to adopt new untested technologies. Secondly, the widely publicised Jeep hack that occurred in 2015, see Section II, presents a milestone in automotive cybersecurity. We found this attack referenced very frequently and recognised this as a good delineation point for the research. Therefore, excluding the 2015 and 2022 years, the five-year interval (2016 to 2021 inclusive) is relevant for this study of attack vectors on vehicle systems. Additional database search notes:

- For the IEEE Explore and SAE Mobilus sources the date filter was via an additional web page setting;
- the search strings produce point-in-time results and the databases do change;
- the literature searched was limited to the English language.

The identified search results (n = 278) from the database search engines were imported into the EndNote reference management tool. The references were organised into groups per database/search string pair to gain greater insight into which databases provided good quality and relevant sources.

TABLE 2. Literature review filtering stages.

Stage	Filtering	Number (n)	Total n
Identification	Records identified from databases	278	278
	Records from other sources	0	278
Screening	Duplicates excluded	7	271
	Non-relevant records excluded	209	62
Eligibility	Excluded as full-text unavailable	8	54
	Exclusion after full-text inspection	29	25
Included	Sources analysed	25	25

TABLE 3. Final sources used for analysis, given a rating and matched with relevant Research Objectives (RO).

Source	Rating	RO1	RO3	RO4
Allodi and Etalle (2017) [16]	3			✓
Pan et al. (2017) [17]	1	✓	✓	
Plappert et al. (2021) [18]	3			✓
Kumar et al. (2021) [19]	3	✓	✓	
Malik and Sun (2020) [20]	1	✓		✓
El-Rewini et al. (2020b) [21]	1	✓	✓	
Haas and Möller (2017) [22]	1	✓	✓	
Kent et al. (2020) [23]	4		✓	
Hutzelmann et al. (2019) [24]	5			✓
Ansari et al. (2021) [25]	2		✓	
M et al. (2020) [26]	1		✓	
Luo and Hou (2019) [27]	2		✓	
El-Rewini et al. (2020a) [28]	2	✓	✓	
Khan et al. (2020) [29]	4	✓	✓	✓
Kim et al. (2021) [30]	2	✓	✓	✓
Parkinson et al. (2017) [31]	3	✓	✓	
Xiong et al. (2020) [32]	3			✓
Mbakoyiannis et al. (2019) [33]	4		✓	
Ghosal et al. (2020) [34]	3		✓	
Kexun et al. (2020) [35]	1		✓	✓
Khatun et al. (2021) [36]	2			✓
Steger et al. (2018) [37]	2		✓	✓
Freiwald and Hwang (2017) [38]	4		✓	
Howden et al. (2020) [39]	5		✓	
Aust (2018) [40]	3		✓	

Note, results delineated via the two different search strings.

In the screening phase, see (Figure 2), EndNote's duplicate elimination function eliminated seven papers (n = 7), however, further manual duplicate elimination was required as the duplicate elimination function was found unreliable. Furthermore, we evaluated source titles for relevancy, eliminating most records (n = 209). In the eligibility stage, we downloaded full-text articles for the remaining sources, thereby checking accessibility, and performed a deeper analysis of the abstract, screening the full-text articles to evaluate the relevance to the research objectives. This eliminated more sources (n = 37). After completing the phases, we arrived at a final set of papers (n = 25) which we included in the SLR. Lastly, we assigned a key to every paper in the final set, matching them with a particular research objective for clarity and easy reference. In summary, Table 2 shows the number of sources identified and eliminated at each phase of the screening process.

Table 3 shows a table of the sources included in the review. The list is delineated by a line to show the two sets of sources. The top section of the table represents the first search string, and the bottom section represents the second search string (Table 1 shows the search strings). In addition, each source was assigned a rating based on a qualitative judgement on the relevancy and the quality of the source. Finally, each paper was assigned to one of the three relevant Research Objectives (see Section III for the ROs). From the top part of Table 3, we can see that attacks (RO1) and mitigation (RO3) are represented, with authors often addressing both sides. The second search string is related to OTA software upgrades (RO4), most authors proposed mitigation solutions, though not addressing how such a system may be attacked. The highest quality articles, rated 4 or higher, represent 24% of the final sources, and 28% for those rated 3. The remaining 2s and 1s are rated at 24% each.

As mentioned in the introduction (Section I), in the following sections we examine the literature for the views on OTA system advantages and disadvantages, the architecture, the attack vectors, describe the attack surface and highlight critical OTA-specific vulnerabilities mentioned. We touch on threat actors and their motivation when targeting automotive systems. In the mitigation section, we evaluate technologies, attack detection and prevention techniques, and, importantly, inhibitors to security. The supply chain in the automotive industry is extensive and we discuss its role in securing OTA technologies. Finally, we examine the threat modelling approaches adopted in the literature and use the review results to construct our asset-based threat model.

C. THREAT MODELLING: WHY DO WE NEED IT AND WHERE DOES IT FIT?

Open Web Application Security Project (OWASP) is a non-profit foundation that works to improve software security. Their definition of threat modelling is: "Threat modeling works to identify, communicate, and understand threats and mitigations within the context of protecting something of value." [41]. Further, the UK's National Cyber Security Center (NCSC) states that threat modelling can "... help you discover the ways in which an attacker could realise their goals." [42] further explaining the merits of it being used in setting up countermeasures.

Threat modelling is not a prescribed activity but is viewed as valuable to enterprises as part of a broader risk management system. In the automotive domain, this could be scoped as an area within product risk management. Whatever the scope, threat modelling needs to be correctly located in the product/system development process to inform the design of a system and help satisfy the security requirements in the most efficient manner.

Figure 3 depicts the role of the threat model in the overall system design. The solution to be assessed may assume a new system or an existing product. We should take two important ideas from Figure 3; firstly, the positioning of the threat modelling stage, and secondly, its purpose. As soon as solutions are proposed, manufacturers should validate the security of the design early to identify vulnerabilities in the system and feedback to the design process with proposed mitigation (security-by-design). This iterative use of threat modelling

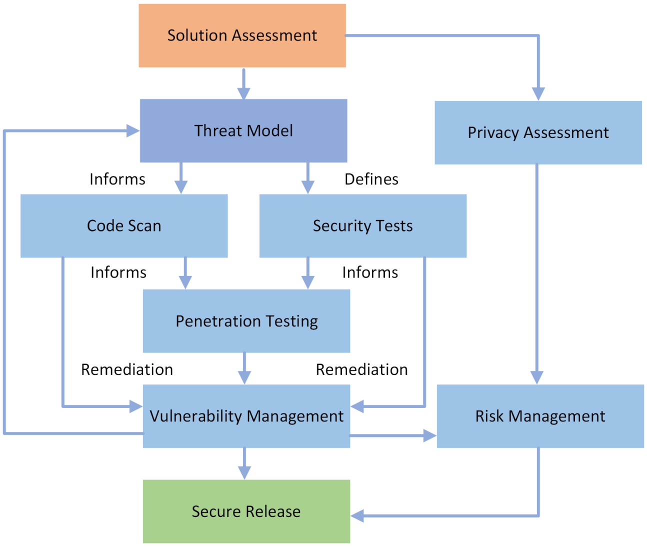

FIGURE 3. The role threat modelling in overall system security assessment and testing, derived from [43].

could improve the cybersecurity of the final product. The connected car increases the relevancy of threat modelling in the automotive domain. This allows us to use the review to influence our design of a novel asset-centric OTA upgrade system threat model.

V. FINDINGS ON OTA SYSTEM ADVANTAGES AND DISADVANTAGES

The reason for OTA systems was given in the background discussion, see Section II. One argument for OTA adoption is the benefits for the OEM. For example, the Jeep hack, see Section II, incurred high costs because Fiat Chrysler recalled 1.4 million cars to update the software due to security concerns [44]. Further, Toyota recalled 1.9 million Prius cars sold worldwide due to a software bug in their hybrid system [45]. These recalls were a large financial expense to the company, however, damage to brand reputation and weakened customer trust is another potential impact [20]. In [37] emphasis is on the benefits of integrating OTA technology into standard engineering practice, the development and production phases, improving the speed of vehicle production and time-to-market (TTM). Furthermore, customers should enjoy cost savings as they will not need to drive to a service location for non-mechanical repairs (e.g., software bugs). Finally, OTA will enable the evolution of new business models enabling OEMs and their partners to sell new services and features to customers [37].

On the other hand, OTA software upgrades have the disadvantage of raising cybersecurity issues and potential safety threats. At least 25% of the authors directly mentioned OTA software upgrades being a new attack vector. Others suggested it indirectly by proposing defence solutions to the system. In [38] they highlighted the safety implications of updating safety-critical electronic control units (ECU) via OTA systems. Moreover, they mention a so-called "brain-dead" scenario, a.k.a. "bricking" [46], where an ECU's update fails unrecoverably and consequently limits the vehicle's functionality. This scenario could diminish the cost-saving advantage.

The legislation and compliance issue should not be disregarded when updating a vehicle [39]. For example, in March 2020 the United Nations Economic Commission for Europe (UNECE) introduced Software Update Management Systems (SUMS) [47] to address vehicle software upgrades. UNECE proposals are the foundation for the Vehicle Type Approval, ensuring vehicles are manufactured to a standard. That UNECE proposal includes a requirement for OEMs to certify their SUMS with an "Approval Authority". In the UK the Vehicle Certification Agency (VCA) handles Type Approval. Further, explicit approval from the authority will be required should the update modify the car's technical performance. The proposal gives guidance on the requirements of the OTA system; cybersecurity is addressed, referring to OTA software code validation and security, as well as the security of the process itself. Lastly, in [34], [39] they mention scalability issues hinting at a new solution requiring an extended supply chain utilising cloud providers' infrastructure for efficient OTA upgrade dissemination.

In summary, the OTA upgrade system has business benefits for OEMs, enabling them to save costs, improve the production process, aid vehicle maintenance, and increase revenue through new services. Nevertheless, new technology presents a new attack vector (covered further in the following sections). Finally, implementing OTA software upgrades is a non-trivial objective encompassing legislative and regulatory uncertainties and safety considerations along with challenging technological requirements. There is guidance available for those implementing OTA systems. ISO 24089, "Road vehicles - Software update engineering" [48] is an international standard that is suitable for addressing UNECE SUMS requirements.

VI. FINDINGS ON OTA SYSTEM ARCHITECTURE

Authors in the literature proposed different architectures and solutions based on their understanding of the threats and components in the vehicle. However, none of the authors focused explicitly on the details of the OTA software upgrade architecture. Instead, the architecture is often described at a high level. Since the authors did not state how they came up with their specific architectures, we can make an educated assumption that the knowledge of the architectural components and their relationships came from researchers' testing the OTA software upgrade system and trying to understand it by studying its behaviour. Some authors proposed technological solutions to the OTA upgrade system based on their electrical and electronics (E/E) architectural assumption, which may be incomplete or entirely false and not beneficial for OEMs. It is recognised that OEMs would not disclose their E/E architecture details and system topologies because this is not a regulatory requirement and is proprietary IP. Therefore, we

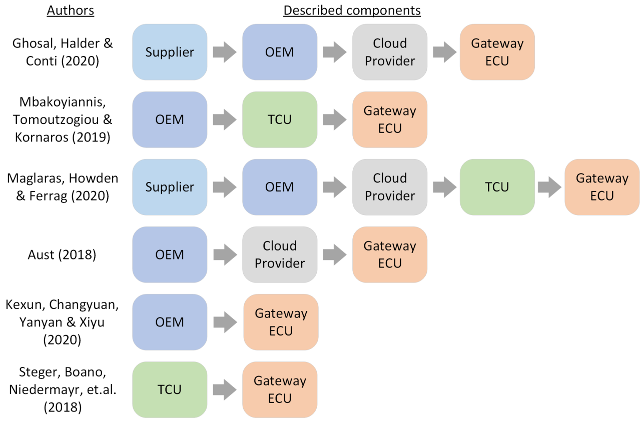

FIGURE 4. OTA software upgrade components comparison.

acknowledge that the information in this section may be built on unreliable assumptions. Nevertheless, the objective was to find common themes in the literature and synthesise it into an architecture diagram.

Figure 4 summarises components within the OTA upgrade system described by different authors. Some propose a very high-level simple picture; others scope the system around the car and entirely disregard the serving or "backend" infrastructure. Overall we can see a noticeable lean towards the vehicle and less on the backend side. Those that mentioned backend infrastructure often involved the OEM servers storing the software image itself and disseminating it to the vehicle. Additionally, [34], [39] added suppliers while [34] and [40] proposed an additional component for the dissemination of software, the cloud provider. The reasoning behind the cloud provider was to address concerns of capacity, which, unlike OEMs, big cloud providers could handle. From the car's perspective, a common approach by most authors was a staged system. The entry component was represented by TCU which integrates different modems (cellular, Wi-Fi). Then a second gateway unit operates as a parent ECU of a target ECU needing a software update.

For our representation of the system, we decided to include all of the components proposed by the authors. Figure 5 presents the high-level architecture of the system. **Supplier** represents a generic component which may represent software vendors developing ECU code or a component supplier. We can appreciate that vehicle production heavily depends on a complex chain of suppliers to keep up with demanding production. Therefore, it is reasonable to assume they will play a part in the ECU software life cycle. Next, the **OEM** is the aggregator with a central database, the software update management server holding data on each vehicle and their ECUs and software version numbers. The OEM will be a critical component in authorising a software upgrade, as we will discuss in the mitigation section. The **Cloud Provider** (CP) will store encrypted ECU images and distribute them to vehicles. Moreover, CPs will provide the capacity and high availability and manage risks associated with those requirements, e.g., denial-of-service (DOS) protection and disaster recovery. The cloud icon represents a generic **Transport** type which could be public Internet or a private Access Point Name (APN) network from a telecommunications provider. On the car side, the **TCU** will take care of the communication channel with the outside world. It will then pass the image over the vehicle's high-bandwidth backbone to the **Gateway ECU**, acting as the OTA reception client. The gateway will then communicate with the **Target ECU** for image installation.

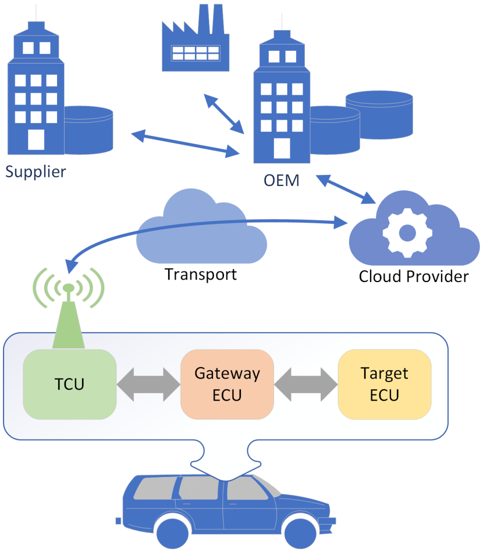

FIGURE 5. Generic reference architecture for OTA software upgrade.

This section synthesised the literature on the OTA software architectures and proposed a high-level model. We will use the OTA component model (Figure 5) to aid comprehension in the following sections reviewing attack and mitigation actions on vehicle OTA systems.

VII. FINDINGS ON VEHICLE ATTACKS: HOW, WHAT, WHO AND WHY?

The cyber threat landscape has evolved with the change in digital technology adoption in vehicles, from requiring direct connections with laptops in the late 1990s and early 2000s to the capability of remote wireless access [49]. We have identified four themes, Figure 6, relevant to cyber threat evaluation and recorded the authors' ideas, assumptions and highlighted limitations. Here we critically analyse the themes, note the contrasts and collate the different views and ideas.

A. FACTORS IN INCREASED CYBERSECURITY EXPOSURE

The speed at which digital technology is changing cars is a challenge to OEMs and suppliers alike. In [29] they found that "84% of OEM employees and their vendors are concerned that cybersecurity measures are not keeping up with emerging technologies". Figure 7 synthesises from the litera-

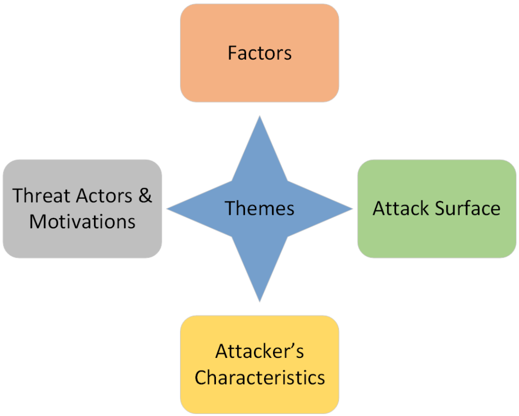

FIGURE 6. Themes in cyber-threat and attack surface analysis.

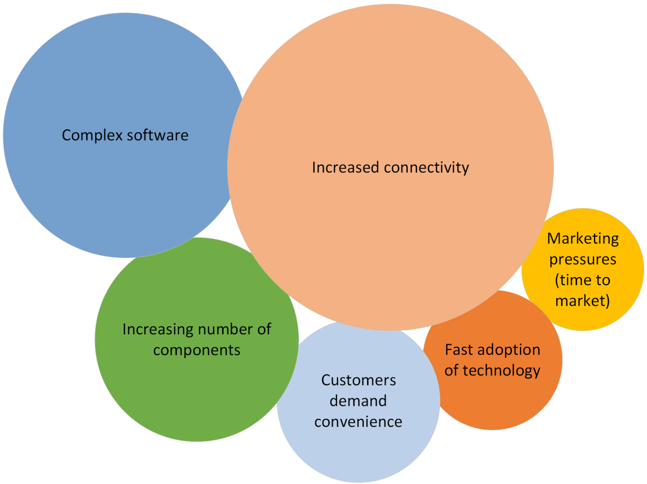
Complex software
Increased connectivity
Marketing pressures (time to market)
Increasing number of components
Fast adoption of technology
Customers demand convenience

FIGURE 7. Factors in increasing cybersecurity exposure.

ture factors supporting the expanded cybersecurity exposure causing concern. The bigger circles represent the increasing frequency of the idea discussed in the literature.

As seen from Figure 7, increased connectivity is the most significant concern to cyber exposure. It is recognised as the main driver and enabler for attackers to target and efficiently exploit vehicle systems. At least 40% of the authors mentioned connectivity as a primary concern. Authors highlighted vehicle-to-everything (V2X), vehicle-to-vehicle (V2V) and the vehicle-to-infrastructure (V2I) coupled with the number of external communicating interfaces expanding the attack surface and growing network complexity. Moreover, [22] gives a new perspective to increased connectivity, referencing the changing mobility culture. For example, car-sharing, valet-parking, e-mobility, and fleet management systems are becoming popular, with Uber and similar companies expanding their businesses in global markets. Modern mobility services need to share data with different systems to enable their functionalities, driving the demand for increased connectivity. Further, as a consequence of the increased connectivity a car's critical components are at risk [25], as was demonstrated by the 2015 Jeep hack (see Section II).

Increased technology adoption and customers accepting more and more convenience features are emphasised in [18]. Adding technology features confirms the concerns raised by OEMs and tier suppliers in the quote from [29] above, that cybersecurity measures may not keep up with technology adoption. As an example, Advanced Driver Assistance Systems (ADAS), used to aid vehicle driving safety, is a convenience technology increasingly integrated into mass-manufactured vehicles. Analysis by [50] shows rapid year-on-year growth since 2015 in the global ADAS market size. Functional and cybersecurity concerns over ADAS systems are driving additional type approval regulations, for example, the 2021 regulation on the provision of an Automated Lane Keeping System [51].

Vehicle software complexity has been emphasised in the literature as one of the top issues threatening vehicle security. Four papers stress the issue of code complexity in terms of the exploding count in lines of code (LOC). In [28], [39] they report that high-end cars can have over 100 million LOC, allegedly ten times more than a Boeing 787. Although several authors use that LOC number none presented quantitative proof. The two themes of software complexity and increased connectivity are connected within OTA systems. In [35] there are concerns around OTA upgrade technologies maintaining software integrity and the challenges of providing a tamper-proof copy of the image over an untrusted transport to the target ECU.

Lastly, the literature discusses a common concept in the automotive industry, and business in general, of time-to-market (TTM). In [22] it mentions the high pressure and competitiveness of the automotive market. This can be tied to OEM concerns over the rapid integration of technology as a theme.

B. ATTACK SURFACE

Literature authors approached the classification of attack vectors and cyber attacks in different ways. For example, [19] categorised cyber attacks into active and passive. They used survey data [52] from Upstream (a private company) as a basis for their work. Despite being a commercial report it provides valuable insights by analysing more than 700 automotive cyber-incidents (as they claim). The significance of active vs passive attacks is that active attacks are easier to detect compared to passive as they require physical access and are more invasive to the vehicle [19]. In contrast, passive attacks, e.g., man-in-the-middle or eavesdropping attacks are harder to detect and mitigate. Moreover, the survey categorised attacks into different channels used for hacking, showing servers, keyless entry systems, and the OBD port as the top three vectors. Finally, more analysis of the survey data confirmed the trend towards long-range wireless attacks, further validating the justification for OTA software upgrade significance as a remote attack vector.

TABLE 4. 2020 & 2021 Cyber incidents assessed against WP.29 threats & vulnerabilities, incidents can appear in more than one category, adapted from [53]

Description	Percentage
Threats to vehicles regarding their communication channels	89.3%
Threats to vehicle data/code	87.7%
Potential vulnerabilities that could be exploited if not sufficiently protected or hardened	50.8%
Threats to vehicles regarding their external connectivity and connections	47.1%
Threats regarding back-end servers related to vehicles in the field	24.1%
Misuse or compromise of update procedures	4.3%
Threats to vehicles regarding unintended human actions facilitating a cyber attack	3.2%

Another approach to attack categorisation was made by [19], [28], highlighting the types of attacks. The latter also assigned qualitative scores for "ease of attack" and "detection probabilities" for each type of attack. Unfortunately, the additional metrics were not justified or described, so it is hard to evaluate their reasoning. Still, both of the papers above show higher frequency and importance of the attacks that result in the ability to control the vehicle, modification of data through eavesdropping and spoofing to enable car theft, and tracking or service interruption via DOS attack.

The final approach demonstrated by [30] categorised attacks into seven categories representing different aspects of the connected car (ECU, in-vehicle network, key, sensor, mobile app, vehicle-ad-hoc-network (VANET), infotainment attacks). They performed frequency analysis on the attacks, showing the top three vectors as the in-vehicle network, ECU, and VANET attacks. The results of this study signal a strong preference for the manipulation of data through external and in-vehicle networks to perform an attack on an ECU.

We compared our literature review with Upstream's report [53]. The report confirmed the rise in remote vs physical attacks, with almost 90% of incidents assessed as using communications channels, see Table 4. Moreover, despite addressing cyber incidents from 2020 and with incidents put into more than one category, [53] matches claims made by academic authors confirming the emphasis around communication channels and ECU code security. However, an impact analysis by [53] may signal a different conclusion to academia regarding the attack impacts. Analysis by [53], Table 5, confirms the significance of car system denial of service attacks recognised by [19], [28]. Interestingly, Table 5 shows a relatively low percentage for "manipulate car systems" but a high number for "control car systems". Unfortunately, the report lacked information on the two categories. Still, this may indicate that despite a large percentage of attack vectors aiming to control the car [19], [28], the impact of attacks or their success may be relatively low [53], hinting towards the difficulty of such attacks.

We analysed the collected attack data and visualised it in Figure 8 to show the various attack surfaces and vectors mentioned in the literature. The number of different attack vectors signifies the importance of a particular component.

TABLE 5. Vehicle cyber incidents impacts breakdown 2010-2021, incidents can appear in more than one category, adapted from [53]

Impact	Percentage
Data/privacy breach	39.9%
Car theft/break-ins	27.9%
Control car systems	24.2%
Service/business disruption	18.2%
Fraud	4.2%
Manipulate car systems	4%
Location tracking	2%
Policy violation	1.5%

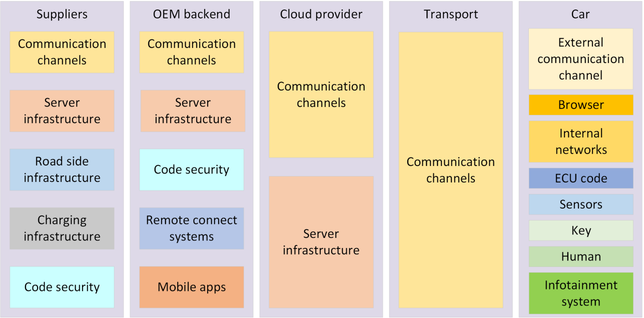

FIGURE 8. Attack vector analysis categorised into OTA software upgrade architectural components.

The attack surface categories were defined based on the OTA software upgrade high-level architecture component model shown in Figure 5. The categories are:

1) Suppliers
2) OEM backend
3) Cloud provider
4) Transport
5) Car

Some attack vectors are applied to more than one category based on relevancy. Figure 8 shows many attack vectors concentrated at the car, followed by suppliers and the OEM's backend. The communication channel is present on all surfaces, whether an external or internal channel or both. Plus the connected car is dependent on external communication infrastructure, therefore, proven enterprise security will still be required to secure against threats that originate from suppliers, the OEM backend, or the cloud provider. Server infrastructure can be considered a remote attack vector as attacks must traverse several networks, as when distributing an OTA software upgrade (Figure 5). In addition, [19] emphasised the bidirectional nature of the attacks; the vehicle can be attacked from the backend infrastructure and vice versa.

Finally, humans are generally thought of as a significant attack vector in traditional enterprise security and were acknowledged as weak point [29]. The authors discussed a lack of cybersecurity awareness may mean, for example, users trigger malicious software updates via mobile applications or infotainment systems. However, the literature examined did not generally point to the human component as a vector. General trust in technology was mentioned in [29], an observation that is hard to quantify and analyse without supporting data. They argued that drivers might not question technology and rely too much on it to "do the right thing." These points hint at the need to raise cybersecurity awareness among OEM customers.

In summary, authors analysing attacks have shown that external connections are being leveraged to impact the functions of ECUs, raising the need not only for a robust OTA software upgrade solution but also for end-to-end network security. Furthermore, backend infrastructure was recognised as a legitimate attack vector, meaning traditional enterprise security should be part of OTA system cybersecurity. Secure coding practices, if not in use by an organisation, should be adopted to minimise critical software bugs. Finally, vehicle users should be considered when designing automotive technology, they must not be tricked into installing malicious software.

C. THREAT ACTORS, THEIR CHARACTERISTICS AND MOTIVATIONS

This section focuses on the attacker's capabilities, motivations and characteristics. This aids in the understanding of threat sources to help develop the final threat model. One observation is that automotive cyber attacks are not pervasively present, with most of the variety of attacks performed in controlled environments inside a lab. No OTA attacks executed by black-hat hackers were seen in the review. However, grey-hat attacks did appear in the past [19], e.g., to unlock limitations in Tesla's software, increasing vehicle power. With limited information, we turned to [54] which reported that from 2010-2020 49% of the attacks were performed by black hat hackers. Unfortunately, the report's details are behind a paywall, preventing accessibility to evaluate data credibility; however, it suggests automotive hacking is an issue, even if not widespread.

In [16], [30] they touched on the skill levels of anyone trying to attack a car. While [16] argued that most attackers use exploit kits accessing a limited number of vulnerabilities, despite the potential for the number of low-level attacks to be large. Whilst [30] argued that the attackers needed to be very skilled, despite the equipment to execute the attacks being cheap. Neither of the authors presented significant justification for their claims; however, [28] did attribute an "ease of attack" score to each attack in their summary paper. Despite a vague explanation of how the metric was calculated, 87% of the attack types identified were marked as *High* or *Moderate* on a three-level scale. This shows that an automotive attack may not be so trivial, or the motivation for attacks has not matured.

The attacker's motivation was found to be lacking in [16], stating attackers quickly abandon the system if they face barriers in their attack, turning to another vector. The authors presumed the attacker is low-skilled using exploit kits to execute attacks. However, the papers mentioning exploit tools lacked information on how an attacker might acquire such tools. Further, [30] acknowledged a lack of research on the topic of attacker motivation and threat actor identification, acknowledging that more information on the topic could help mitigate the threats.

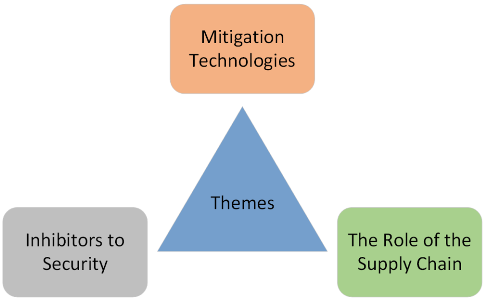

FIGURE 9. Themes in protective measures.

The motivation was found to be related to the impact of cyber attacks, with safety implications a common concern, followed by the privacy of vehicle and user data. In today's connected world, the privacy of Personally Identifiable Information (PII) has become tightly regulated, for example, with Europe's General Data Protection Regulation (GDPR). The failure to protect, or the misuse of, PII can result in a fine of up to 4% of global annual turnover. This could run to several billion for large OEMs. Furthermore, the loss of PII may result in trust erosion, and reputational and further financial damage resulting from loss of customers [20]. Lastly, human life was mentioned to be endangered if the automotive cyber threat increases.

Summarising, there is a lack of data to help determine the type of threat actors exploiting automotive vulnerabilities and the level of threat activity. The skill level of threat actors likely needs to be at a moderate to a high level, though more information is required. Authors acknowledge that information sharing between OEMs themselves, and the research community should be stimulated to improve cybersecurity. Knowing more about threat actors' motivations and skills will improve the efficiency of threat mitigation. Finally, concerns around the impacts of cyber attack primarily revolve around safety aspects and the potential to incur financial damages.

VIII. FINDINGS ON PROTECTIVE MEASURES AND CHALLENGES TO SECURITY

In examining the mitigation solutions proposed from the literature the approach is to appreciate that technology is not the only aspect of cybersecurity. The consideration of people and processes (an OEM's policies and procedures) is important when engineering the software-driven vehicle. The three themes for this section in support of cybersecurity objectives for OTA systems are technologies for mitigation, inhibitors to achieving security, and the role of supply chains, see Figure 9.

A. MITIGATION TECHNOLOGIES

The literature proposes novel cybersecurity solutions to the relatively opaque automotive technologies (it was mentioned in Section IV-B that OEMs protect their IP). A quote from [29] states: "Orthodox cybersecurity approaches are not adequate to counter cyber attack in CAVs" (a CAV is a connected autonomous vehicle). This signals the challenges of integrating known enterprise-type countermeasure technology into cars. Others see established concepts as relevant, from [30]: "Use security methods already known and not invent new ideas" suggests the adoption of proven technologies. A unified viewpoint is not necessarily required. Well-established techniques can be applied, plus techniques that can address some of the unique digital systems present in vehicles. Then there is the regulatory weight on the automotive industry, where components and systems need to be certificated and comply with safety and security standards. Proven technologies may offer an advantage over novel solutions, assuming that the former can be effectively integrated into vehicles within the regulatory approvals process. Balancing established enterprise security techniques with new security methods is an interesting problem, though we have not collected enough data to address the question here. However, the observed split in researchers' views demonstrates challenges in addressing cybersecurity in the automotive domain.

In Table 6, we have collated the mitigation techniques proposed by the authors and mapped them to the cybersecurity categories of **Technology**, **People**, and **Process**. Under Technology the method discussed is provided. Additionally, mitigation is assigned to the OTA domains shown in Figure 5 and Figure 8 to show relevancy to the OTA software upgrade process.

The most apparent observation from Table 6 is the empty People category. This information may be captured in other papers not explicitly related to OTA upgrades. However, customers, supply chain and OEM employees still interact with the OTA software upgrade process, so it is valuable to consider people when proposing solutions in this space. The fact that this information was missing in the reviewed literature shows a lack of consideration or understanding of the role people play in cybersecurity. For example, none of the authors mentioned security awareness training within the R&D supply chain or for OEM engineers. In [31] it was recognised that the consumers are not very skilled and could be misled into installing malicious software or plugin a malicious device into their cars, however, no mitigation was proposed. It would be an interesting study to see if any cybersecurity guidance is, or could, be provided by the user guide or instruction manual that is supplied with vehicles, and its potential to improve the cybersecurity awareness of vehicle customers.

The categories of Technology and Process have good coverage, though Technology has a higher number of references. Under Technology, ECU code validation and intra-vehicle network attack prevention received frequent attention. For the former, the most used terms are digital signatures and digital certificates. ECU code signing and validation should be performed not only by the vehicle's ECUs but also on the code supplier's and OEM's side. On the in-vehicle network protection side, authors focused on different IDS algorithms, firewalls and AI solutions. These solutions aim to detect and prevent in-vehicle denial-of-service attempts due to automotive network protocol deficiencies. Moreover, threats such as spoofing, message injection, and man-in-the-middle type of attacks were addressed. There was less attention given to in-vehicle network encryption, with only 8% of the papers proposing that mitigation strategy.

The security of external communication was relevant for all OTA domain components, reflecting connectivity as a factor in attack vectors in Section VII-A. Several sources indicated the importance of adding security to V2X communications. Most authors propose traditional cryptography concepts to ensure the confidentiality, integrity and authenticity (CIA) of communications, though common V2X protocols can support certificate-based security. In [26] they propose a high-level blockchain solution; however, the paper lacked detail. Despite the experimental approach of those authors, a distributed technology, i.e., blockchain, would require a larger number of infrastructure nodes and full-time dependency on available communication, not practical for normal vehicle usage.

A good portion of mitigation strategies was dedicated to Trusted Platform Modules (TPMs) and Trusted Execution Environments (TEEs). Once cryptographic algorithms are integrated, the TPM and TEE should ensure secure crypto key storage, crypto operations and secure code execution. The divergence between the authors was on the type of implementation of these technologies as these can be implemented in software or hardware. TPMs experience concerns about the economic feasibility of mass-scale use (though they are increasingly built into microcontroller cores). Further, a TPM is recognised as a critical component in conjunction with ECU code validation on the vehicle side during the OTA software upgrade. A quote by [33], "ECUs that are not able to verify signatures should not be updated over-the-air", shows the importance of verifying code signing as a mitigation strategy.

Proposed mitigation under Process varied, most are referenced by a single source. Again, referring to Section VII-A, software was identified as a factor in increased cyber exposure, so it is good to see mitigation strategies, e.g., secure coding and static code analysis, addressing the issue. Further, a concept of air-gaping was proposed in the context of network segmentation. Despite it being a technological concept, it is included in Process as this would be a design decision. Three papers mentioned vulnerability reviews, another consideration in managing increases in software complexity. Data classification was discussed, recognising that cars may be storing personal data (discussed in Section VII-C). In [31] they called for anonymisation and strong protection of data. Besides conventional audits and software patching, threat intelligence was proposed by [22]. The latter addresses

TABLE 6. Analysis of mitigation technologies

Category	Mitigation	Method	Supplier	OEM	Cloud	Transport	Car	Source
Technology	ECU code signing/validation	Digital signatures and certificates	✓	✓			✓	[17], [23], [27], [28], [31], [33], [37]
	Intra-car communication encryption	Network encryption and segmentation					✓	[17], [28]
	In-vehicle network attack prevention	Intrusion Detection System (IDS), Firewall, Artificial Intelligence (AI)					✓	[17], [19], [21], [22], [27], [28], [30], [33], [37]
	External communication security	Encryption, Blockchain	✓	✓	✓	✓	✓	[21], [22], [26], [28], [37]
	Key storage and crypto operations	Trusted Platform Module (TPM)	✓	✓	✓	✓	✓	[22], [27], [37], [38]
	Secure execution environment	Trusted Execution Environment (TEE), TPM, Hardware Security Module (HSM)	✓	✓	✓	✓	✓	[22], [25], [27]
People								
Process	Vulnerability reviews		✓	✓	✓	✓	✓	[19], [29], [31]
	Software Patching		✓	✓	✓	✓	✓	[19]
	Air-gaping		✓	✓	✓	✓	✓	[19], [24]
	Security testing		✓	✓	✓	✓	✓	[20], [29]
	Static code analysis		✓	✓			✓	[21]
	Threat intelligence		✓	✓	✓	✓	✓	[22]
	Data classification		✓	✓			✓	[24], [31]
	Secure coding		✓	✓			✓	[39]
	Audits		✓	✓	✓	✓	✓	[29], [39]

the issue recognised in the section on threat actors where information sharing was stressed. To conclude on Process, with exceptions for code-related mitigation for cloud and transport domains, the mitigation list is applicable for all OTA domain components. However, OEMs are likely to need processes to guide them in managing each component's security requirements and the interconnections with other components.

B. THE ROLE OF THE SUPPLY CHAIN

This section assesses the authors' ideas on the responsibilities and contributions of supply chain players to the cybersecurity of a car. In Figure 5 there are three dedicated components that function as suppliers in the OTA software upgrade architecture:

1) parts and software suppliers;
2) the cloud provider offering storage and a content distribution network (CDN) to disseminate software images efficiently;
3) the transport representing, most often, a cellular network provider that is the bridge between the wired and the wireless worlds.

In [23] it states that "Security has been slow due to complexity of automotive supply chain". It does not offer much insight into what is meant by "complexity". However, in [23] it explains that suppliers are responsible for most of the car's ECUs and code. Further, OEMs hire domain experts, i.e., suppliers for a specific part, thus requiring different suppliers [24]. In [23] it additionally discusses that ECU suppliers may outsource software development to lower-tier suppliers. Plus, different OEMs may share parts of their supply chains. These findings have significance not only to cybersecurity but also to IP rights and protection, including opening doors to cyber espionage. However, not all authors acknowledged the long and complex supply chain or offer solutions to its cybersecurity management, opening the need for additional research. Yet, some suggestions are present.

Firstly, [33] proposed a hierarchical certificate-based solution where suppliers would encrypt the ECU software and deliver it to the target ECU in a car preinstalled with encryption keys for decryption. Unfortunately, despite a good approach to using certificates to establish trust, no consideration was given to key management and it ignored the problem of not having a reliable time source on the ECU to validate the certificates. In addition, they did not consider key storage, yet Table 6 shows that many papers have proposed TPMs for that function.

Secondly, attribute-based encryption (ABE) was proposed in [34] for the cloud provider to use when distributing the software to the vehicles as an access control policy, ensuring only a vehicle with specific attributes will generate and decrypt the image. ABE is based on common asymmetric cryptography (public/private keys) with decryption only possible if the receiving vehicle's key attributes (e.g., model ID or VIN) matches the attributes assigned to the ciphertext. Therefore, if multiple parties (vehicles) match the ciphertext attributes they can all decrypt the message. ABE appears a good solution for the "last mile" distribution but does not seem practical for the supplier-to-OEM relationship, coupled with the OEM needing to perform testing on the image before publishing the update. Nevertheless, the authors claim ABE offers advantages over classic cryptography with lower network load, energy consumption, storage and computation requirements. The overheads mentioned are indicators of the limitations of the vehicle environment when compared to traditional computing systems.

Aside from certificate and ABE solutions, other papers offered more general recommendations. Mentioned in [31] are the supplier aims to fulfil contractual requirements and not add extra features that are not required, e.g., over-engineered security solutions. A view not derived from automotive suppliers and one that may be based on an assumption, though no contradictory argument was presented by other authors. However, it offers an insight into commercial sensitivities and the balance of costs versus security.

In [29] is suggested a trust model where each supplier would be required to digitally sign their outputs for easier tracking, accountability and remediation in case of software issues. This approach connects well with the potential reputational impact on OEMs from cyberattacks as a consequence of mismanagement of the supply chain. In addition, the traceability aspects of such a trust model offer good incident response capabilities, aiding the speed of software bug remediation.

Lastly, [21] and [39] propose managing the supply chain risks through policies and contractual obligations with strict cybersecurity requirements. A policy-based solution may seem quick and cheap for the OEM; however, it does not offer a full defence-in-depth approach. Product and enterprise-wide audits may be helpful to enforce the policies, along with security testing of finished components, which could be helpful to evaluate the overall cybersecurity resilience of the complete system.

In summary, a lack of primary data research was evident on supply chain cybersecurity in the automotive industry. Furthermore, the technical solutions proposed by two papers need further validation to justify their feasibility. Lastly, suppliers, in some cases, have complete autonomy over the design and the code of an ECU. In those cases, the OEM's job is to enforce cybersecurity requirements into the design within the contract and perform independent security testing of complete parts before installation.

C. INHIBITORS TO SECURITY

In this section, we gather insight into limiting factors for OEMs in adopting countermeasures proposed in research. A qualitative reflection on the data gathered is made, based on the mitigation proposed, or derived from implied limitations and assumptions. Figure 10 depicts a word cloud with the increasing size of bubbles indicating the higher frequency of the factor.

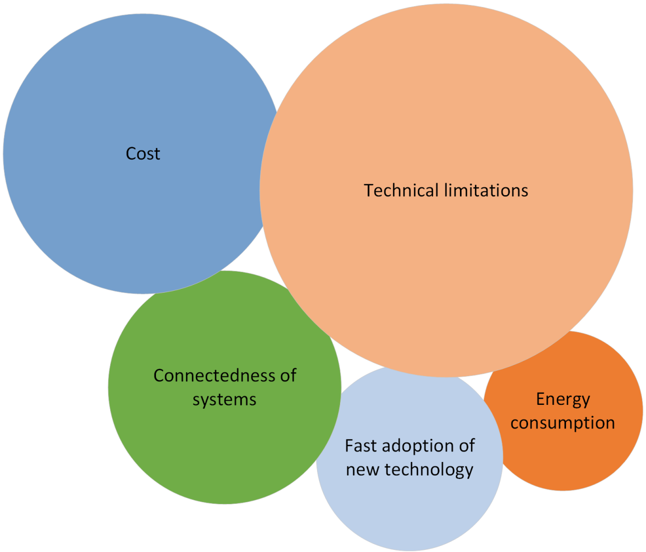

FIGURE 10. Factors that hinder cybersecurity adoption in vehicle security.

Technical limitations appeared to be the most considered factor. In [25], [39] they critique countermeasures with crypto capabilities because of their hardware resource requirements that are unavailable in the automotive environment. Additionally, crypto operations take too long for the real-time requirements of certain ECUs [39]. In [28] it claims that not all OEMs have the OTA software upgrade capability for every ECU. The latter paper on cybersecurity challenges was published in 2020 with over 300 referenced papers. Their statement may signal the maturity of the OTA software upgrade systems up to that point. In [39] it states OEMs support non-safety critical systems such as infotainment for OTA, therefore, the ECU software upgradeability was still moving towards full maturity, potentially requiring service technician visits for updates for hard-to-patched vulnerabilities. Further, OEMs need certainty with the challenges in supporting OTA software upgrades on safety-critical ECUs, indicated by references to "brain-dead" ECU situations. Finally, the certification requirement to support SUMS in the recent UNECE type approval regulation (see Section V) will require OEMs and suppliers to coordinate and adapt to the regulations. Further, code updating can only be done in specific situations for some ECUs, e.g., when the vehicle is not moving [38]. The heterogeneity of vehicle systems and their usage indicates the complexity of deploying a vehicle-wide OTA software upgrade system.

Regulations were not widely addressed in the literature; however, it was noted that it is not uncommon for technology to outpace policymakers. Still, several standards and guides are available to automakers on automotive cybersecurity matters. Aside from the international ISO/SAE 21434, there is the U.S. Department of Transportation's National Highway Traffic Safety Administration (NHTSA) published guidance titled "Cybersecurity Best Practices for the Safety of Modern Vehicles" [55]. The European Union Agency for Cybersecurity raises awareness under the slogan "cybersecurity for safety" [56]. There is the US-based Automotive Information Sharing and Analysis Center (Auto-ISAC)[1] organisation providing guidance and information for OEMs and suppliers. Further, a factor in Figure 10 is cost, mentioned several times in different contexts. In [23] it states that manufacturers will only adopt a technology if it makes solid economic sense or if there is a known consequence of not adopting it. The former is logical for any business. No business is keen on investing in something that customers will not ultimately be funding. However, any commercial organisation should

[1] https://automotiveisac.com/

have a process or model for a cybersecurity investment cost-benefit analysis [57]. Further, the cost consequences of not adopting cybersecurity are linked with regulation and policy contexts. Aside from cyberattacks potentially leaking IP, cars are now data sinks with systems storing personal data and, as previously mentioned, GDPR threatens high penalties to companies that leak such data. Further, it was noted that cost assessments are not presented with proposed countermeasures despite, as appreciated in other parts of this analysis, automotive's sensitivity to cost.

The primary factor in exposing vehicles to threats is system connectivity (see Figure 7). It presents difficulties in protecting automotive systems as in [40] it stresses the requirement of a vehicle to "always be online". Therefore, this always-on connectedness can hinder cybersecurity as the protection measures need to interact with multiple in-use systems concurrently [38]. This may result in complex design challenges when integrating cybersecurity measures into real-time and safety-critical vehicle systems. Further, dedicated cybersecurity and crypto-based solutions increase energy consumption [31]. They presented the argument in the context of electric vehicles, which may need to charge more often, impacting battery life. Related is the power consumption differences between symmetric and asymmetric algorithms, demonstrated by [34], with symmetric showing an increased consumption. However, [34] lacked justification for the chosen microcontroller, so it is not clear if the simulations were performed on a vehicle-type microcontroller, questioning the results of this study. Nevertheless, power consumption, as with all vehicle systems, is to be considered when designing cybersecurity solutions.

The pace of new technology was discussed as a limiting factor in adopting cybersecurity. Concern for the growing software adoption in vehicles becoming unmaintainable and difficult to audit. A vehicle's life cycle, maintenance, and backward compatibility will be affected should the manufacturers bolt on more digital technology [28]. When considering the life cycle of a car OEMs may look for "future-proof" protection systems that can be adapted to emerging digital technologies. This helps avoid overreliance on further research and development (R&D) costs. This is an area where remote system updates have a role to play.

In summary, this section presented limiting factors that need to be addressed to stimulate the growth of cybersecurity in vehicles. OTA software upgrade technology may have not fully matured and yet regulation and standardisation are here. The approval and standards bodies are concerned with digital technology, introducing guidance and promoting security by design for automotive systems. Cybersecurity costs have been recognised as a significant consideration, and technological change, digital connectivity, and power consumption are all presenting challenges.

IX. FINDINGS ON THREAT MODELLING

This section examines the threat modelling approaches. The analysis of different threat modelling techniques informed our threat model for the OTA software upgrade use case, presented in Section X. The terminology around threat modelling can differ, therefore, examples from the reviewed literature are presented to help define threat modelling in our context.

An Attack Tree (AT) or Attack Graph is composed of nodes (vertices) connected with paths (edges) and is used to show steps an attacker can follow to reach a resource or goal in a system. The "leaves" of the tree are tasks to be completed to achieve the goals of the higher-level nodes (and the final goal). At a given level a single task out of several may need completing (OR tasks), or all tasks at a level may need completing (AND tasks). There are many variations [58] on this AT concept that adds additional features and rules. Figure 11 shows an example of a simple attack tree model for a key relay attack (where a signal from a wireless car key is amplified to compromise a vehicle [59]).

Presented in [27] was an AT for an in-vehicle network attack. Each node is carrying a probability of exploitation so that each attack path can be quantitatively evaluated for feasibility. However, it was unclear how each element's probability score was calculated, possibly undermining the presented work. The authors acknowledged that subject matter expert knowledge is required to justify the exploitation scores assigned to each component.

Other graph-type models are presented to analyse system security and attacks. In [32] they presented models focused on network communications and data flows inside vehicles. The models are then used to generate a risk matrix and attack path.

In [24] they adopt a model with interlinked elements representative of an attacker, defences, and system parts. The use of Unified Model Language (UML) class or object style notation reinforces the meaning of the links between the model elements, see Figure 12 which is drawn from [24].

The model depicted in Figure 12 acknowledges that not all exploits can be resolved, so mitigation strategies should reduce the attacker's capabilities to exploit a system part. If a vulnerability (called a "Weakness" in their model) can be mitigated, e.g., with an OTA software upgrade, exploiting a system component is no longer possible because the weakness was patched. This model allows the modelling of different systems from a high-level view. Yet, this model needs to be expanded to include a metric that would aid manufacturers in decision-making when analysing different mitigation strategies. For example, in [32] a commercial modelling tool "securiCAD" was used to automatically generate probabilistic attack graphs based on given system requirements. However, the paper lacked information on why this tool is suitable for the automotive domain's specific technology requirements. The experiment used an ordinary computer with a traditional operating system to represent an ECU, the model predicted threats based on approximation. For example, the model allowed the ECU to be vulnerable to Address Resolution Protocol (ARP) cache poisoning attacks, which is irrelevant in the automotive domain. Therefore it is

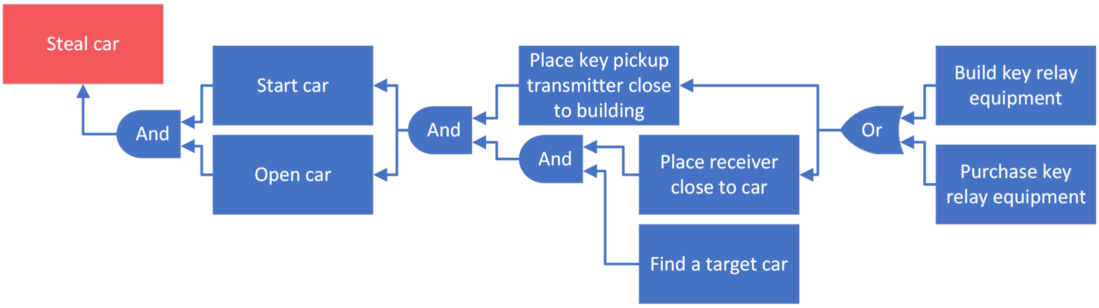
Steal car
And
Start car
Open car
And
Place key pickup transmitter close to building
And
Place receiver close to car
Find a target car
Or
Build key relay equipment
Purchase key relay equipment

FIGURE 11. Example of an attack tree for a key relay attack.

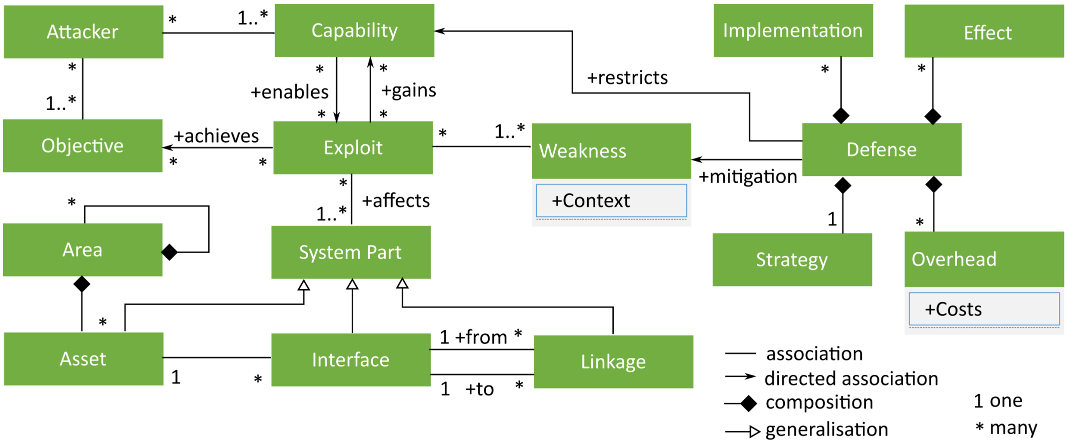

FIGURE 12. Automotive threat model drawn from [24].

not clear how applicable the threats generated by this tool are.

In [20] the vehicle simulation and visualisation tool "CARLA" was used. They appreciated the tool could not simulate all the threats identified. However, simulated attacks show the usefulness of speedily illustrating outcomes of threats and evaluating attack paths through a system.

Several authors used a multi-step approach to threat modelling, combing it with risk assessment. For example, [36] first identified assets in a system. Then, each asset was evaluated for cybersecurity threats. Next, damage scenarios were created based on the threat with different impacts on assets, e.g., the driver, or data. Finally, the risk level was evaluated based on financial, privacy, safety and operational aspects. Although complex, the TARA presented a well-rounded approach unlike others mainly concerned with confidentiality, integrity and availability of impacted assets. The authors used the EVITA method [60] to express attack potential and the HEAVENS method [61] to calculate the severity level, though both lacked justification of the scores derived from these methods.

Regarding the philosophy behind threat modelling, [16] presented a "realistic threat-modeling approach", stressing the need to focus on the threat actors to filter through the number of threats to the system accurately. This ties in with the previous model approach in [24] to limit the attacker's capabilities. Thus, the attacker's motivations and objectives need to be considered when modelling threats to a system [16]. The latter was also part of the attack model in [24]; however, it was superficially described, supporting the discussion in Section VII-C on a lack of information on threat actors and their motivations when targeting the automotive domain.

A tiny fraction of all possible vulnerabilities will get exploited in the wild when considering the number of possible attacks [16]. This may signal lower-skilled attackers using exploit tool kits. Further, they claim attacks do not change very often, with novel attacks coming out every 600 days, and some vulnerabilities have higher volumes than others. The arguments presented by [16] was based on an analysis of others' work, and the paper was not aligned with the automotive domain. Still, its content helped with the thinking on how threat modelling may be approached.

In summary, there was no unified approach to representing automotive cybersecurity threats. From a high level, some authors only looked at the attack side; others combined the attack and defence, and others appended more model elements. Moreover, a well-argued quantitative evaluation of threats appears to be lacking throughout. Several papers undertook automated threat modelling addressing the complexity of automotive systems and the amount of attack surface

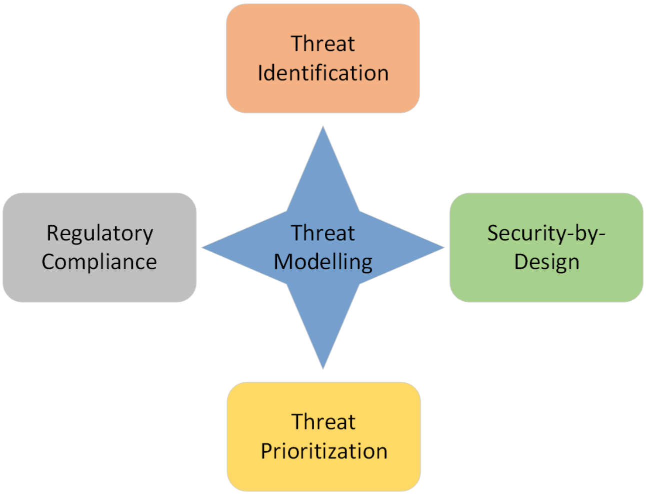

FIGURE 13. The purpose of threat modelling.

available to the attacker to exploit. However, some work is required to equip tools with automotive-specific components for better relevance of the generated models. A multi-step approach of using threat modelling in combination with asset identification, impact and feasibility analysis and risk assessment was observed, a useful aid for decision-makers prioritising threats. Finally, there is an approach stemming from threat actors, their capabilities and motivations as a basis for relevant threat modelling and mitigation.

X. THREAT MODELLING THE OTA SOFTWARE UPGRADE USE CASE

This section presents the synthesis and application of the results presented in the preceding sections. A generic methodology will provide the process of developing a threat model of a system. Then we apply the method to the automotive OTA software upgrade system.

We have already introduced threat modelling in Section IV-C. Our review shows that threat modelling is an activity that can be implemented in different ways following a variety of different methodologies. However, based on the results, it was not clear whether manufacturers yet perform threat modelling in their development cycle.

Figure 13 depicts four aims of threat modelling, enabling vehicle systems engineers to look at their applications from a security perspective. Moreover, the automotive industry has long moved its development into computer-aided design (CAD) and adopted digital technology in its development processes, increasing engineering speed and efficiency [21]. Therefore, programmatic threat modelling could be integrated into the manufacturer's digital development process, as additional computer-based tooling.

This security perspective will enable OEMs to spot issues in their designs that enable threat actors to exploit the system. Furthermore, stakeholders can use a threat model to prioritise mitigation according to their risk mitigation strategy. Threat prioritisation is helpful as not all threats identified in a system have the same probability of being encountered or being effective. Some threat models from the review involved exploitation probability scores. Alternatively, prioritisation and scoring could be done in a product risk register fed from a threat model. Finally, the modelling aids regulatory compliance being considered early in development, as some regulations (e.g., GDPR) impose security requirements depending on the data held or processed within a system.

A. AN ASSET-CENTRIC THREAT MODEL

An alternative to listing out all attack vectors, as some authors proposed, threats can be modeled by identifying the system assets an attacker might target. An attacker profile aids in determining which assets may have a higher probability of exploitation. Then evaluate the impact on the vehicle and the driver from an assent-centric attack. The assumption is we have the threat actors' information and a method to score threats. However, our literature review shows there is limited information on this topic. Information from commercial threat intelligence sources (e.g., the Upstream Security report [53]) may aid in gathering missing data to make better-informed decisions.

Threat modelling and risk scoring are separate activities and demand different methodologies. This work focused on the first of the two due to time constraints. The threat modelling we describe can serve as the first part of the TARA process outlined in the ISO/SAE 21434 standard. The methodology can be used to develop threat models for other aspects of automotive systems beyond this OTA use case. The developed threat models enable a threat analysis to inform the analysis processes where risks would be scored for prioritisation by OEMs. The three guiding principles for the threat model were:

1) data should be treated as an asset;
2) data should be classified;
3) and the technology that is storing, processing or transferring the data should impose security to protect the data.

Microsoft's STRIDE threat modelling is well established [62], designed to aid software developers to build secure software. STRIDE is an acronym for potential threats: **S**poofing, **T**ampering, **R**epudiation, **I**nformation disclosure, **D**enial of service, and **E**levation of privilege. Unlike STRIDE, our approach addresses less technical stakeholders with a focus on the OTA data. Nevertheless, STRIDE shares a few features with the proposed method, such as the system decomposition approach to identify threats, data flows and trust boundaries. Further, STRIDE's roots in enterprise software development pay less attention to automotive-specific technologies, making it less of a fit for modelling automotive threats. Figure 14 summarises our 4-phase threat modelling methodology.

In the **Identify Assets** stage the scope of the system is established. This includes identifying all the system and data

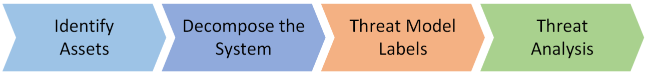

FIGURE 14. The 4-phase threat modelling methodology.

components, mapping the relationships between the system components and adding any parties (“actors”) accessing the system. Upon completion of this phase, one should have a high-level view of the system involving all the components. The initial diagram generated should inform the decision-makers of what needs to be protected.

Next, the **Decompose the System** phase takes deeper dive into the system to better understand its workings. More information is imposed on the initial diagram to show how data flows between components, revealing interdependencies between components.

The use of **Threat Model Labels** in the third phase adds depth around the thinking on the system operation and its secure design. Three types of labels are added onto the diagram as needed. The types of labels used are:

1) Assets;
2) Controls;
3) Threat agents (actors interacting with the system).

The labels for assets identify the type of data assets to protect and aid the choice of security controls to apply around those assets. For example, if the assets are of type customer information, we consider the regulations that may apply to that data and the controls to meet them. Another example would be IP, e.g., ECU code, which is identified to enable the addition of controls to prevent theft. In the literature, authors discussed aspects of encryption, therefore, the storage and usage of encryption keys as assets are identified for protective controls.

The types of controls to apply include usual cybersecurity controls, for example, authentication and authorisation. These can encompass concepts around a certificate, password or public key-based authentication. Digital signatures are considered a type of authentication control for a code image signing scenario. Authorisation helps accomplish the least privilege and need-to-know principles that aim to limit the damage if an account is compromised. Encryption controls are applicable for the protection of communication channels and for encrypting data at rest, including keying material. Lastly, threat agent labels consider external and internal actors, and whether the actors are authorised or unauthorised for their actions.

The last phase of the 4-phase methodology is the **Threat Analysis**. This is where the interpretation of the final threat model diagram is made. The central idea is that authorised actors and threat agents want to reach an asset. Therefore, to interpret the threat model, start with an actor or threat agent and follow the data flows to reach an asset. Assets missing security controls or with too few controls will be recognised. Any issues discovered will be cost-beneficial as threat modelling is performed in the early design stage (see Figure 3). During the analysis different threat scenarios can be examined from a single diagram for the particular system. Moreover, each threat scenario should be scored using a scoring system (not developed in this work) to help prioritise threats. However, reiterating findings from the literature review, all attack vectors in a system may not pose a high risk, therefore, it is essential to consider a "probability" factor when scoring threats. Threat frameworks such as OWASP Top 10 [63] and MITRE ATT&CK [64] may be helpful to develop a deeper understanding of how attackers may overcome security controls when developing a scoring metric.

B. APPLYING ASSET-CENTRIC THREAT MODELLING TO THE OTA USE CASE

This section applies the "asset-centric" methodology described in the previous section to the OTA software upgrade use case. The architecture from Figure 5 is the basis for the first phase (see Figure 14) of Identify Assets.

1) Identify Assets in the OTA Upgrade System

Figure 15 shows the system’s high-level view upon completion of the first phase of the methodology. We refer to each party interacting with the system as an "actor". Actors in red circles are a) vehicle operators or b) external service providers accessing an OEM’s internal SUMS and the vehicle systems. Access is via untrusted external networks (UEX0), indicated with the color red. Dashed lines are used to represent the logical connections, and a solid line shows a physical path for the true data flow via the transport actor. These different labelled connections are helpful when establishing controls per type of connection. The transport actor represents the internet or a cellular provider facilitating the physical connections to and from the OEM’s private cloud as well as the car’s TCU.

The driver can trigger an update directly via the infotainment system (PHY0) or indirectly via a mobile application using a transport provider (UEX0). Both are considered untrusted interactions. The large dashed line square represents the trust boundary inside which the OEM has full authority to enforce its policies and apply necessary controls. We have included only one actor in blue, to indicate the manufacturer’s IT employees. They will be interacting with the system over a trusted internal network (TIN0), again indicated in blue. Finally, each communication uses arrows to indicate the expected initialisation of the connection. The arrows will help determine the nature of the systems, whether they are expected to be initiating or accepting incoming connections or both.

2) Further Decompose the OTA System

The next stage is Decompose the System to reveal the OTA system’s sub-components for additional detail (Figure 16). The OEM may not have insight into suppliers’ infrastructure, so we will treat them as "black boxes". SUMS is further divided into an image store for storing ECU code and the

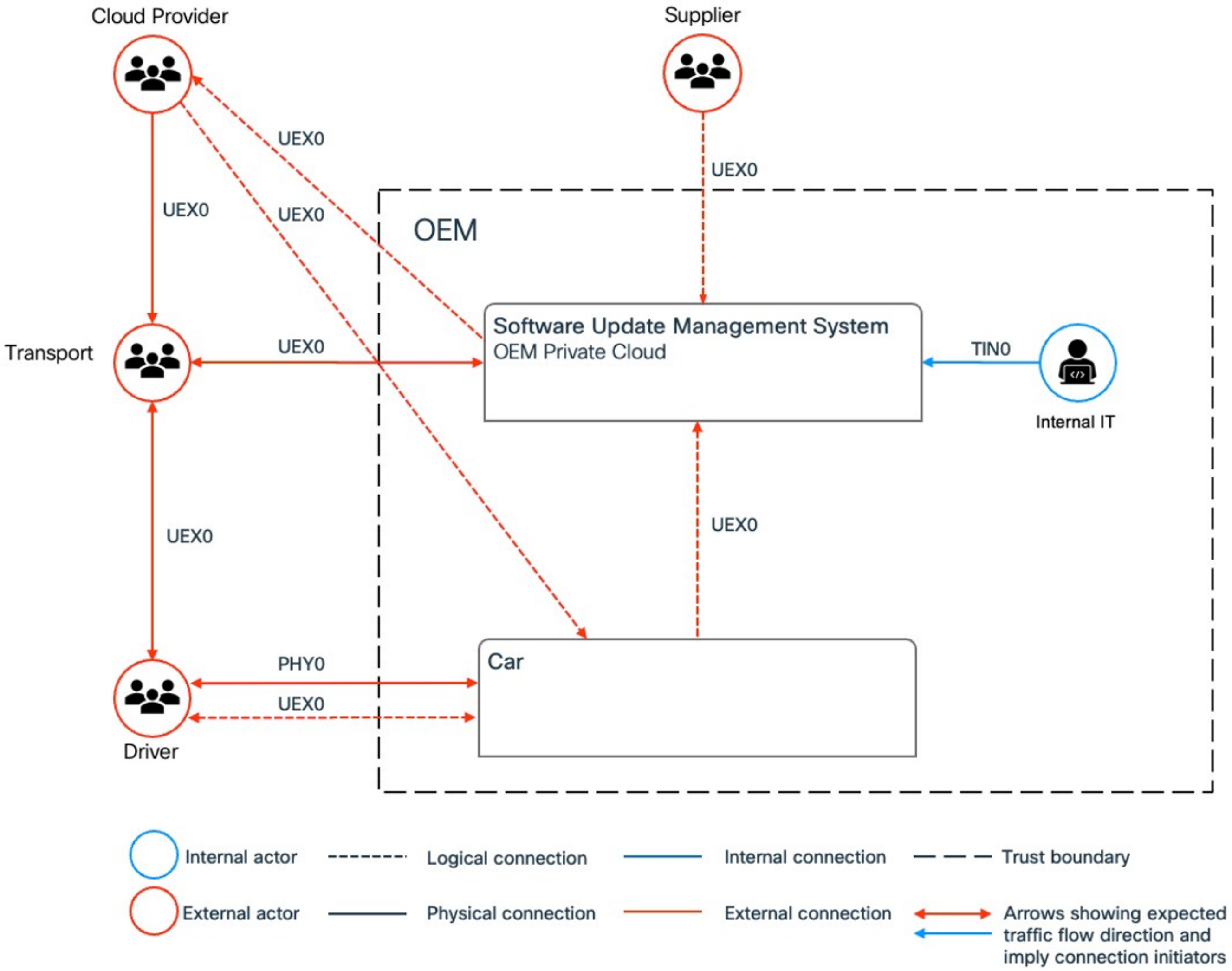

FIGURE 15. OTA software upgrade threat model after step 1, Identify Assets.

vehicle database. The database can be used to record the vehicle's software image version for verifying if a car needs an update, record logs for regulatory purposes, collect logging data, and any other data management requirements. Additionally, identity and access management (IAM) and encryption services may not be part of the SUMS; however, we added them to support controls imposed on the system.

We assumed internal IT will have full access to an OEM's private cloud for administrative purposes. The supplier and the cloud provider will require access to the image store to publish and disseminate updates. Further, the TCU will require vehicle database access via the transport provider to check for updates and send log data. Transport will also need a connection with the cloud provider to enable an image download to the car. The sub-system components inside the car show the chain of interdependence and implied attack vectors resulting from those relationships. Automotive networks (ANX) will show different communication technologies within a car that will help to identify possible mitigation strategies available to those technologies. We show only one vehicle network (AN1) in this example, however, a production vehicle is likely to have several networks.

3) Label the OTA Threat Model

Phase three of the methodology is to add the Threat Model Labels. The OTA labels for the assets, security controls and threat agents are itemised in Table 7. The labels are provided with a tag to aid clarity within the threat model diagram. The tags added to the model diagram provide a cross-reference to the threat label table.

Aside from the typical security controls introduced in Section X-A, the controls for the OTA use case are informed by the analysed mitigation strategies from Table 6. Technology control C4 is related to the discussion around TPM and TEE that is found in the literature (see Section VIII-A). The controls from C5 to C9 relate to the mitigation categories of People and Process. These administrative controls can

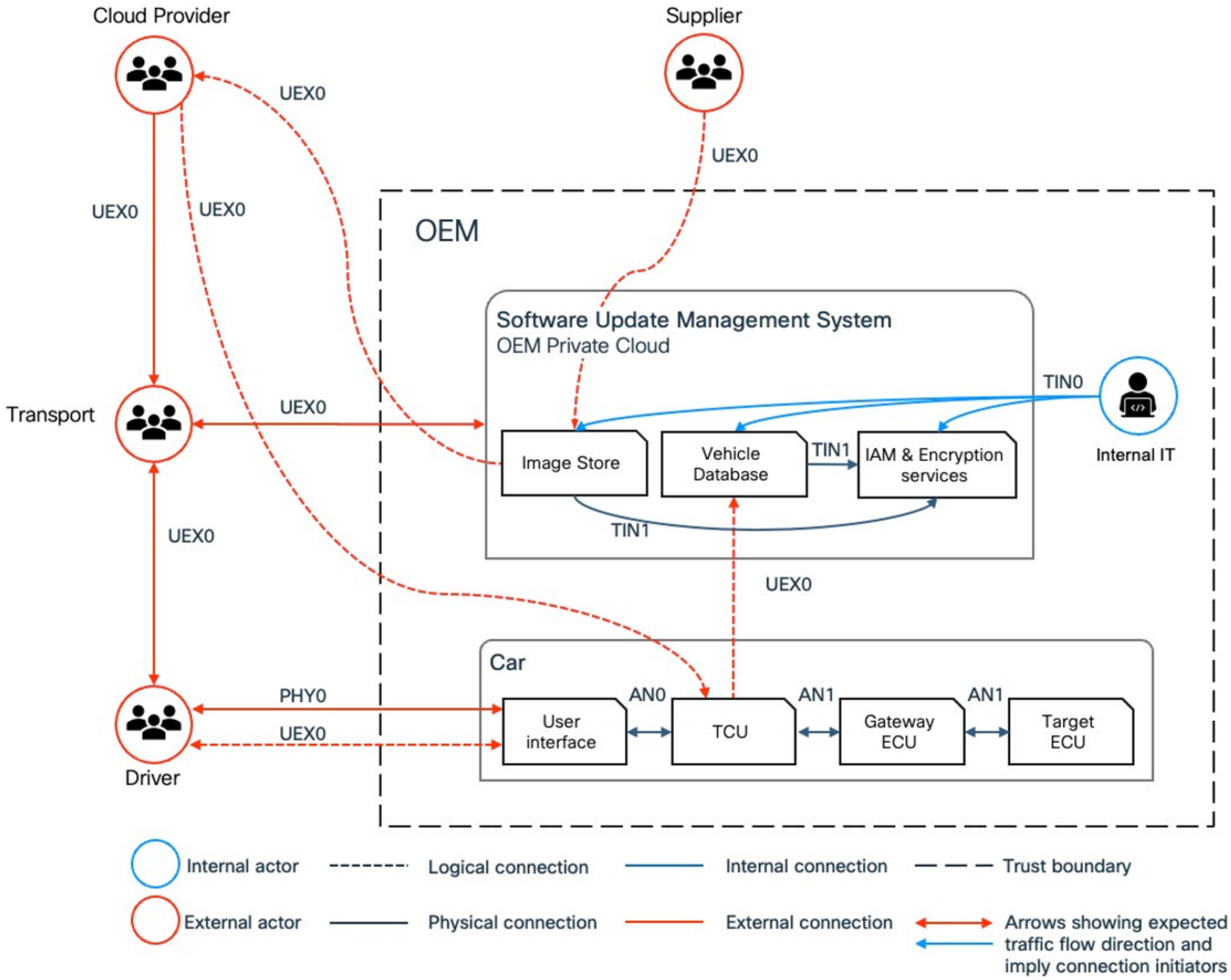

FIGURE 16. OTA software upgrade threat model after step 2, Decompose the system.

augment the overall security posture of a system, following the principle of security in depth.

An example of an external authorised (T1) actor would be a software developer employed by an external supplier to write the code for an ECU. An unauthorised external threat agent (T2) would be an attacker that is not expected to interact with that process or system component. The internal authorised actor (T3) could be a customer buying a car or an internal IT operations team member. Lastly, an example of an internal unauthorised (T4) actor would be a privileged employee acting as an "insider threat". This last type of threat agent was not detected in the literature review; however, it is a valid threat in the wider workforce involved in developing an automotive system.

The threat labels were assigned to appropriate components in the diagram to produce the completed OTA threat model, see Figure 17. The labels have been color coded to aid with identification. Threat agent labels T1 and T2 are assigned on all external actors because external parties could be authorised legitimate or unauthorised malicious actors. The authorised threat, either internal or external, covers the insider threat, for example, a disgruntled developer employee at an ECU code supplier. An external unauthorised could be a supply chain attack scenario where an adversary gained access to a supplier's network and compromised a privileged account that has access to the OEM's private cloud. The agent labels T3 and T4 are assigned to internal IT, again covering normal operations and the insider threat scenario.

Asset labels are assigned to components and threat actors. For example, the supplier and the cloud provider would develop and store proprietary code respectively, so they were assigned label A4 indicating sensitive IP data. Likewise, in-car components have various types of software IP. The TCU is a central point for external connections, it may need to store encryption keys (A3) and access credentials (A2) to support the proposed security controls of authentication (i.e., secure

TABLE 7. The threat modelling labels mapping table for the OTA use case.

Assets		Controls		Threat Agents	
Key	Description	Key	Description	Key	Description
A1	Customer information	C1	Authentication	T1	External authorised
A2	Access credentials	C2	Authorisation	T2	External unauthorised
A3	Encryption keys	C3	Encryption	T3	Internal authorised
A4	Intellectual property	C4	Secure execution environment	T4	Internal unauthorised
		C5	Security testing		
		C6	Secure coding		
		C7	Audit		
		C8	Security awareness training		
		C9	Logging and monitoring		

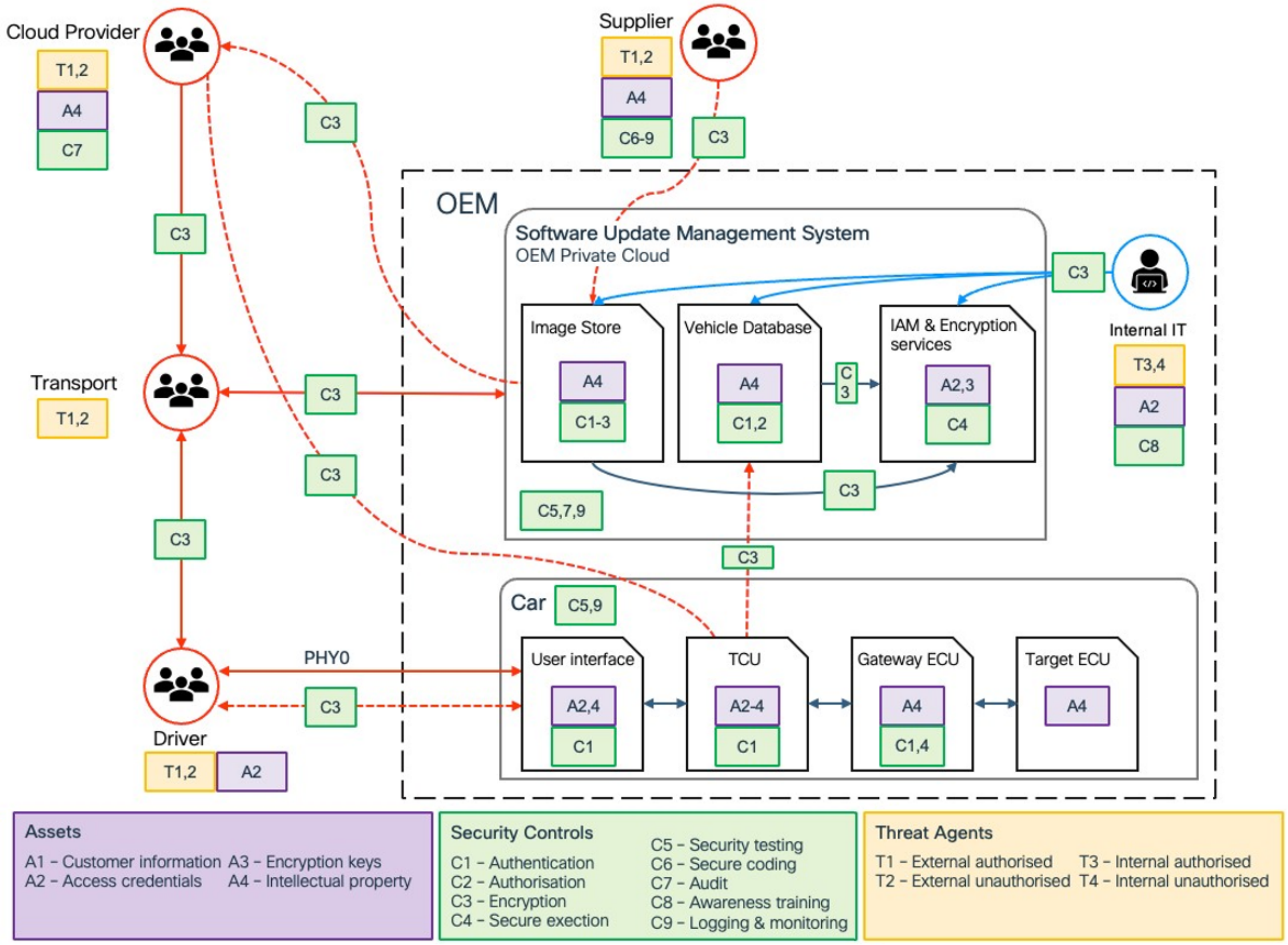

FIGURE 17. Completed OTA software upgrade threat model, after step 3, the labelling, aided with color coding.

connections). Similarly, the "IAM and encryption services" could store such sensitive information to perform their roles.

The application of security controls starts with the literature results where external connections are discussed as cybersecurity threats. The mitigation widely supported is encryption as a strategy to deal with insecure channels. Therefore, encryption control, C3, is used on all communication channels, external and internal. Further, we opted to apply audit (C7) as a Process measure to establish baseline security for all the suppliers. Additionally, suppliers (e.g., ECU code developers) may require a control providing staff security awareness training and suitable secure coding standards (C6, C8). We imposed the security controls of security testing, audit, and logging (C5, C7, C9) on the SUMS as overarching security on the technological and procedural level as good practices for any information system.

On the vehicle side, as shown in the literature results, technology may not be mature enough to integrate all security controls proposed by the literature. Therefore, in-vehicle communication networks did not adopt any security control, instead concentrating on inter-ECU authentication and vehicle user authentication (authentication is control C1). The TCU is a relatively recent addition to the history of vehicle engineering and can support external authentication (C1) alongside external network encryption (C3) via the external cellular or Wi-Fi broadband connection. Further, the gateway ECU, being a parent ECU of the target ECU, should use a secure environment (C4) for decryption and verification of the image before forwarding it to the final target. Vehicle systems should be subjected to security testing (C5) and be monitored and use logging (C9) for situational awareness.

Note, we did not impose any security control on the transport actor because they only take care of the routing and have no visibility into the data as we assume it is encrypted via control C3. Although meta-data can be exploited, even with an encrypted data flow, that would be a topic for further research. Here, the transport actor is a conduit covered by C3. That does not mean further technical controls should not be in place. For example, in the 2015 Jeep hack (see Section II) the researchers could enumerate thousands of vulnerable vehicles using a common cellular connection. This means the cellular provider of the vehicle's subscriber identity module (SIM) card did not implement any security controls (e.g., network segmentation or an access control list), which may have prevented communication from the public consumer cellular network from reaching the automotive end of the network. Therefore, contractual or other administrative controls could be placed on the transport providers to enforce security and mitigate a similar attack vector.

4) Using the OTA Threat Model for Threat Analysis

The availability of a final OTA upgrade system threat model provides stakeholders with the opportunity to perform the final and fourth phase of the methodology, Threat Analysis. The number of potential threats is high, and a full threat analysis would be an extensive body of work, particularly developing a required quantitative probability-based threat ranking for later use in risk assessment and management. Therefore, the final full threat analysis is not covered in this work. However, a straightforward example threat scenario is useful as an illustration of using the threat model. A supply chain attack seeks to use a supplier organisation as an entry point into a larger organisation's valuable assets [65].

An external unauthorised actor, T2, could gain access to supplier systems despite the security controls, C6-9, in place. Typically a supplier employee falls for a socially engineered or phishing attack, or a supplier system is not updated to patch recently discovered security issues. This allows the threat agent a foothold into the system. Once inside they pivot onto OEM's SUMS cloud or enterprise server. This type of attack is not uncommon, and despite the controls in pace could be rated with a 60% probability of an attempt in a given year. With this threat scenario what mitigation could be made by the OEM or supplier? The OEM could add extra layers to the authentication procedure, requiring the use of a multi-factor authenticating (MFA) device to generate an additional access code. This could reduce the risk, e.g., by half [66] to a lower risk of 30%. The OEM and supplier could further agree to process changes to further lower the risk to an acceptable operational level. The changes could include annual employee security refresher training and sharing of metrics on updating of systems software.

As seen from this one scenario, threat analysing of the complete threat model will require substantial work by the OEM. This work could be helped with tools designed to support building these types of threat models and automating some of the threat analysis and risk management. Especially as digital tools are a large part of any vehicle system design cycle.

XI. OUTCOMES FROM THE OTA THREAT MODELLING

OTA systems are a mechanism to enable vehicles to be patched for cyber vulnerabilities, but OTA is a potential cyber target itself (see the research question in Section III). We used data leveraged from a qualitative SLR to study and build a model for threat analysis of an automotive OTA system. This aided in addressing the research objectives and using their outcomes to frame the OTA security recommendations for OEMs and suppliers below, addressing the last research objective.

The results from the review (with the methodology covered in Section IV) allowed a high-level reference architecture and understanding of OTA systems to be formulated. This helped address objective RO1, with findings on how vehicle systems may be attacked, expanding upon potential threat actors, attacker characteristics (the who) and motivations (the why). Results showed that increasing cyber exposure of the vehicle is driven by increased connectivity, growing software complexity and a growing number of components as the top three drivers (Figure 7). Sources claim almost 80% of attacks are wireless, with external connectivity, communication channels, vehicle data and code vulnerabilities recognised as the most significant threats (Table 4). Common threats are often the low-skilled communication relay attacks used to steal or break into cars (Table 5). Additionally, attacks divulged data, indicating weak protection mechanisms.

In Figure 8 we analysed the attack surface in the context of the OTA software upgrade. The threat modelling performed in Section X-B gives further insight into threats to the OTA system to address R02 and allow us to summarise the attack surface:

- OTA software upgrade systems require connections to the backend system, presenting a recent attack vector for the vehicle and the OEM system, i.e., the infrastructure and its communication channels being potential sources of cyber attacks. This includes the possibility of vehicles being leveraged to attack OEM services. Therefore, backend security controls are required to mitigate threats.
- The vehicle exhibits the most attack vectors in number and variety, indicating the potential difficulty in protecting its systems. Cars have many interfaces, examples

include sensors, infotainment systems, and telematics ECUs with wireless connections. These interfaces could be manipulated to trigger a software vulnerability within the vehicle's ECU code.

- The number of possible threat agents has expanded to suppliers, cloud and transport providers, the driver and ultimately to the OEM itself. Each agent in the system presents internal and external threats that could affect the vehicle. Therefore, OEMs need to oversee security controls not directly managed within its trust boundary.
- Code security was a topic that touches almost all attack vectors enumerated in Figure 8. Malicious code can be injected into the process at numerous spots during the development and code delivery phase. Security controls (e.g., security audits, secure coding techniques, security awareness training) should be placed within the supply chain.
- Drivers could be socially engineered to aid an attack via a vehicle's connected mobile applications or infotainment system.

Additional data on the possibility of active automotive threat actors should be obtained from further research. However, a lack of detailed public data on automotive systems does not seem to stop people from attacking vehicle systems. The results show that researchers perform most attacks and the attacks require specialised technical knowledge. Despite that, cheap tool kits can be purchased that enable less-capable actors to exploit automotive systems remotely with the key-relay attack. Responsible data sharing, suggested previously for the automotive domain [67], may aid researchers in helping OEMs and suppliers mitigate some of the most obvious threats.

For R03 we evaluated three themes to inform the final threat model, mitigation strategies and technology, inhibitors to security and the role of the supply chain. Most authors in the literature review focused on technology solutions (see Table 6). For example, digital signatures, certificates, and TPM/TEE/HSM to improve vehicular security, which should mitigate most low-level attacks. Though, care should be taken when adding new technology as it could introduce additional attack vectors.

The Process (policies and procedures) part of a mitigation strategy needs further detail which was lacking in the review. To fully develop that aspect, research on administrative security controls could be conducted. For example, administrative controls such as vulnerability reviews, software patching and data classification (again, see Table 6), could be measured for impact in the OTA software upgrade supply chain. Lastly, the findings of mitigation analysis informed the security controls listed in Table 7 and applied to the threat model.

To address the OTA threat modelling objective, RO4, we contrasted threat models (Section IX) from the literature and proposed a threat modelling method (Section X). To show the applicability of the proposed model, we applied the proposed method to the OTA software upgrade scenario (Section X-B). Threat modelling is part of a bigger threat analysis process (Figure 3). If implemented in system design stages, it could support early threat identification and prioritisation, and aid regulatory compliance, and support security by design philosophy (see Figure 13). These findings illustrate how threat modelling could aid the mitigation of threats to OTA systems. Further, the asset-centric modelling technique abstracts the system to enable flexibility of the model and for it to be used early in the engineering process to achieve risk reduction benefits.

The proposed threat modelling method integrates the literate review findings from the attack side, the mitigation side, the threat actors, along with the concepts of trust boundary, interconnections, and system decomposition to achieve the final OTA threat model in Figure 17. This serves as a basis to identify critical points in the system and ensure appropriate security controls are in place. The literature review findings, modelling process, and the final model aided the final objective below, RO5, security recommendations for OTA system stakeholders.

A. RECOMMENDATIONS ON VEHICLE CYBERSECURITY

It is important to act on findings from any type of threat modelling process. This section takes the main security findings from the research and summarises them in a set of four actionable recommendations. Whilst this research focused on OTA systems, the recommendations are applicable to broader vehicle security. The recommendations can be used by automotive industry decision-makers to aid in their design of OTA management processes.

1) Use Threat Intelligence

This study indicated concerns over the continuous adoption of new digital technologies that potentially bring new vulnerabilities to vehicles. This pace of engineering in the automotive industry requires approaches that include addressing security aspects in system design. New information on threat agents and their techniques will emerge or needs to be found as automotive systems evolve. Therefore, studying sources of automotive threat intelligence and analysing the available information needs to be undertaken. New threat information needs to be synthesised and the new knowledge leveraged, feeding into design and testing processes. Early consideration of relevant threats can result in a securer system design. This potentially offers a competitive advantage and cost savings due to reduced recalls from cybersecurity breaches or regulatory requirements. Auto-ISAC is the type of organisation that could perform that role, though its closed-shop nature does lend to opaqueness in measuring the organisation's effectiveness in the automotive cybersecurity domain.

2) Adopt New In-vehicle Technologies in Safety-Critical Components

The ubiquitous connectivity of cars has increased the interest in automotive cyber attacks due to the ability to access vehicle systems from a distance. Further, researchers have demonstrated that legacy technology has limited or no security controls. This exposes a high potential impact that could put passengers' lives at risk, i.e., safety-critical vulnerabilities. Much academic research has focused on bolting security onto legacy technology with little evidence of commercially implemented success. This highlights limitations in some protocols, for example, the Controller Area Network (CAN). Integrating security onto established vehicle technologies presents an engineering challenge, considering those protocol limitations and restricted in-vehicle compute resources (power consumption is an automotive engineering consideration). In addition, applying appropriate security measures can require novel, unproven technologies raising the cost of implementation. Therefore, OEMs could prioritise newer technologies that support adding security, for example, automotive Ethernet for in-vehicle networks, initially targeting the security of safety-critical systems as they present the highest financial and safety risk. The aim of integrating new technology is to lower barriers to security implementation. However, complacency should not follow new technology introduction, all technology has potential vulnerabilities for attackers to exploit. No design can guarantee a fully secure end-to-end solution for the OTA software upgrade system. Hence the need to consider all these recommendations.

3) Apply Cybersecurity to the Supply-Chain using an Asset-Centric Modelling Technique

The large supply chain in the automotive industry is acknowledged, however, the suppliers' role in overall cybersecurity may be underestimated. This study recognised the supply chain as one of the risk factors. The code needs to be protected end-to-end for OTA systems, starting in the development phase. The OWASP organisation emphasises the role of establishing a Software Development Life Cycle (SDLC) to detect bugs and lower costs: "When a bug is detected early within the SDLC, it can be addressed faster and at a lower cost. A security bug is no different from a functional or performance-based bug in this regard" [68]. Therefore, policies for code suppliers should be reviewed, they must include secure coding awareness training for employees. Finally, code suppliers should demonstrate robust SDLC and perform independent security testing of the code.

4) Review Internal Processes to Support Security-by-Design

This research demonstrated that threat modelling can aid regulatory compliance and threat identification and prioritisation, and contribute to a secure design. Importantly, this could lead to competitive advantage and cost savings through maintaining OEM reputation and reducing the need to address after-sales vulnerabilities. As we showed, threat modelling can be approached from many angles and we proposed an asset-centric approach. Despite this work's focus on threat modelling, other processes need to be established, e.g., vulnerability management and security testing that works in tandem to support secure system design. To develop robust processes organisations can leverage standards, best practices, guidelines and regulations published by different entities, e.g., the US National Highway Traffic Safety Administration, ENISA, ISO (Figure 18) and UNECE.

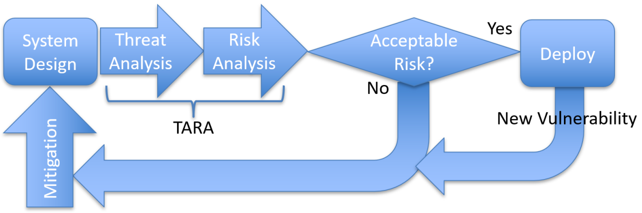

FIGURE 18. The ISO/SAE 21434 cybersecurity engineering process supports security-by-design and OTA lifecycle requirements.

B. FUTURE WORK

The ISO/SAE 21434 standard is designed for OEMs and suppliers to adopt mandated processes. For example, a TARA process is recognised to be an essential part of cybersecurity engineering, see Figure 18. Our research addressed the Threat Analysis part of an automotive TARA, therefore, it would be valuable to address Risk Assessment solutions, and how the automotive industry could integrate and adopt full TARA solutions. Doing so will aid in addressing and maintaining cybersecurity in vehicles, and aid OEMs and suppliers to comply with standards and regulations. As part of this, attack feasibility may be an important factor in mitigation and investment prioritisation. Therefore, a quantitative method addressing the attack feasibility of a threat actor exploiting a vulnerability would benefit from research. Furthermore, the presumed information on threat actors' characteristics and capabilities is known. However, the results of this research indicate that this topic may need further analysis. A good analysis of threat agents will add context to the overall TARA process and could be used as a metric in scoring. With this information, a practical automotive-specific risk-scoring method may be developed. Finally, computer software may be developed for our asset-centric threat modelling technique to fully evaluate its use in automotive systems design.

XII. SUMMARY

Mass-manufactured vehicles are complex, connected, and software-controlled cyber-physical systems. Despite OEMs protecting the IP of their vehicle systems, they are potentially the cyber target of remotely located threat agents. This research investigated vehicular OTA software upgrade systems as a cyber target. The data on vehicle attacks, mitigation technologies and OTA technologies were collected using an SLR and analysed qualitatively. From 278 search results sourced from 4 different specialised databases, 25 relevant papers were identified through the screening process and examined in detail for their themes.

The OTA software upgrade architecture consists of (code) suppliers, OEM, a cloud provider for image distribution, transport (cellular) providers that connect the backend to the vehicle, and the vehicle systems. This high-level architecture was used to understand the attack surface and the placement of mitigation controls when threat modelling OTA systems. The findings allowed a novel asset-centric threat modelling technique to be developed. It was applied to the OTA software upgrade process, illustrating the security considerations of the OTA system and the exploitation paths.

Some sources recognised OTA system as an attack vector itself, to attack the car and to breach corporate networks through the connected backend infrastructure. Therefore, the backend infrastructure and suppliers need to be considered for cybersecurity when threat modelling the OTA system. In this regard, the UNECE's SUMS regulation is a certification requirement that aids in securing the backend connection. Further aid comes from the ISO/SAE 21434 and ISO 24089 standards, supporting OEMs in protecting the car's systems with systematic handling of vehicle cybersecurity and software update process requirements.

The increasing cyber exposure of the vehicle has increased connectivity, growing software complexity and a growing number of components as the top three drivers. Furthermore, customer demand for features and time-to-market were also identified as challenges. The car itself possessed the highest number of attack vectors in the context of OTA software upgrade architecture, see Figure 5, followed by, in descending order, suppliers and the OEM backend, cloud providers, and lastly the transport provider. In summary, the main threats were around code/data stored in the vehicle, the backend infrastructure, or suppliers, though the security of data in transit was another concern. Nevertheless, more data should be collected regarding attack actors and their characteristics as results showed that white hat hackers still perform the most attacks. However, non-academic literature was found to hold data that may contradict that statement.

We saw several technological solutions proposed for cyber defence, however, people and processes techniques had less attention. The most frequent proposed technological solutions included ECU code signing and validation, in-vehicle and external network attack prevention, key storage and crypto operations. Crypto-related technologies are especially applicable when considering code verification and authentication in OTA software upgrades. These mitigation strategies do appear applicable to the attack landscape identified. Further, we addressed the supply chain in the context of attack mitigation. It is considered that suppliers will handle the most significant part of software development with some ECU code likely under their complete autonomy. In such cases issues of code integrity, code management, IP, and supply-chain cybersecurity management emerges. Some proposed technological solutions for code integrity include digital signatures and certificates, others leaned on "softer" controls such as contractual obligations and enforcing standards with suppliers. In addition, automotive supply chain security could be treated as an independent research topic to gain greater insights.

Inhibitors to security were considered. Integrating security into a vehicle is seen as challenging, with technical limitations as the biggest obstacle. A car's technology is resource-constrained and runs on different network technologies than traditional enterprise information technology, so copying known protective measures is problematic. The cost of additional security measures is another inhibitor. With regulations still maturing and customers being cost-conscious, OEMs are looking to justify any investments in cybersecurity. Then there are factors that include fast technological transformation, the connectedness of systems, and energy consumption, all impact rapid improvements in a car's cybersecurity maturity.

XIII. CONCLUSION

We applied the methodology proposed in Section X-A to the OTA software upgrade system. The threat model was built using the first three phases of the methodology summarised in Figure 14, adding more information at each stage. The final threat model diagram in Figure 17 shows types of assets and their location, and internal/external actors interacting with the system's components. We added security controls needed to promote security by design. The final threat analysis phase of the methodology can be used to evaluate specific threats, which we did not elaborate on fully due to their extensive nature. The asset-centric threat modelling activity can be used to elicit attack scenarios against the OTA software upgrade system. Each derived scenario should describe the attack vector, and provide a measure of feasibility and impact as some form of quantitative score to be used for risk assessment and management.

The asset-centric threat modelling method is a high-level approach applicable to automotive and similar systems. For example, it could be applied to use cases that include smart manufacturing systems, smart cities, healthcare systems, space systems, and home automation. The asset-based model enables less technical stakeholders to comprehend the threat through various levels of abstraction. Firstly, assets and potential threat actors were identified and overlayed on the OTA software upgrade system model. Next, the OTA architectural components were decomposed into sub-components and connected with lines to show data flow. Finally, data assets, threat agents and security controls were added to the final model. This final model represents a framework for threat mitigation and the work allows us to derive four resultant industry recommendations:

1) Use threat intelligence to aid cybersecurity design decisions.
2) Adopt new technologies in safety-critical components to support the OEM stakeholders in prioritising investments.
3) Insure supply chain security processes and procedures are correctly implemented, including secure software development, as a vital part of the OTA software upgrade process.
4) Revise internal processes to support security-by-design, adding the integration of threat modelling into system design.

Using these recommendations, stakeholders should be able to comply with recent and revised automotive cybersecurity regulations, understand the cyber attack landscape, and make informed cybersecurity decisions for automotive system design. Without systematic and audited threat modelling cybersecurity-related automotive regulation will be an administrative burden on vehicle development due to compliance requirements. Furthermore, a lack of understanding of cybersecurity issues may result in vulnerable components and data breaches that could damage brand reputations and possibly result in financial costs for OEMs, whether in remediation work, regulatory fines, or litigation costs.

Standards ISO/SAE 21434 and ISO 24089 do promote systematically addressing vehicular cybersecurity and OTA updates, providing guidance for those needing to implement processes and auditing. Integrating threat modelling into the OTA software upgrade process design, ideally incorporated within systems software engineering tools, will help identify threats to the OTA and other vehicle systems. This will be beneficial to all stakeholders in the vehicle ecosystem.

Finally, the qualitative approach to the research allowed us to address some of the broader implications of automotive cyber attacks and the factors around them. The research touched on regulation, standardisation, and supply chain as inherent parts of the automotive industry, and we appreciate that some topics may not have been fully elaborated on and may require further focused work.

ACKNOWLEDGEMENTS

This work was supported by the UK Engineering and Physical Sciences Research Council (EPSRC) through the Trustworthy Autonomous Systems Hub (EP/V00784X/1), the platform grant entitled "AutoTrust: Designing a Human-Centred Trusted, Secure, Intelligent and Usable Internet of Vehicles" (EP/R029563/1).

REFERENCES

[1] ISO and SAE International, “Road vehicles – Cybersecurity engineering (ISO/SAE 21434),” Geneva, 2021.

[2] S. Halder, A. Ghosal, and M. Conti, “Secure over-the-air software updates in connected vehicles: A survey,” *Computer Networks*, vol. 178, p. 107343, 2020.

[3] D. P. F. Möller and R. E. Haas, *Guide to Automotive Connectivity and Cybersecurity*. Cham: Springer International Publishing, 2019.

[4] International Organization for Standardization, “ISO/IEC 15408-1:2009(E) Information technology - Security techniques - Evaluation criteria for IT Security,” Geneva, 2014.

[5] W. Tuttlebee, “Software-defined radio: facets of a developing technology,” *IEEE Personal Communications*, vol. 6, no. 2, pp. 38–44, 1999.

[6] ——, “Software radio-impacts and implications,” in *1998 IEEE 5th International Symposium on Spread Spectrum Techniques and Applications - Proceedings. Spread Technology to Africa (Cat. No.98TH8333)*, vol. 2, 1998, pp. 541–545 vol.2.

[7] S. Mahmud, S. Shanker, and I. Hossain, “Secure software upload in an intelligent vehicle via wireless communication links,” in *IEEE Proceedings. Intelligent Vehicles Symposium, 2005.*, 2005, pp. 588–593.

[8] M. Shavit, A. Gryc, and R. Miucic, “Firmware update over the air (fota) for automotive industry,” in *Asia Pacific Automotive Engineering Conference*. SAE International, aug 2007.

[9] D. K. Nilsson and U. E. Larson, “Secure firmware updates over the air in intelligent vehicles,” in *ICC Workshops - 2008 IEEE International Conference on Communications Workshops*, 2008, pp. 380–384.

[10] A. Greenberg, “Hackers Remotely Kill a Jeep on the Highway—With Me in It,” 2015. [Online]. Available: http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway

[11] UNECE World Forum for Harmonization of Vehicle Regulations (WP.29), “Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system,” United Nations Economic Commission for Europe, Geneva, Tech. Rep., 2020. [Online]. Available: http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf

[12] SAE International, “J3061 - Cybersecurity Guidebook for Cyber-Physical Vehicle Systems,” Warrendale, p. 128, 2016.

[13] I. Foster, A. Prudhomme, K. Koscher, and S. Savage, “Fast and vulnerable: A story of telematic failures,” in *9th USENIX Workshop on Offensive Technologies (WOOT 15)*. Washington, D.C.: USENIX Association, Aug. 2015. [Online]. Available: https://www.usenix.org/conference/woot15/workshop-program/presentation/foster

[14] S. Nie, L. Liu, and Y. Du, “Free-fall: Hacking Tesla from Wireless to CAN Bus,” *Black Hat USA 2017, Briefings*, 2017.

[15] C. Miller and C. Valasek, “A Survey of Remote Automotive Attack Surfaces,” in *Defcon 22*, 2014.

[16] L. Allodi and S. Etalle, “Towards realistic threat modeling: Attack commodification, irrelevant vulnerabilities, and unrealistic assumptions,” in *Proceedings of the 2017 Workshop on Automated Decision Making for Active Cyber Defense*, ser. SafeConfig ’17. New York, NY, USA: Association for Computing Machinery, 2017, p. 23–26.

[17] L. Pan, X. Zheng, H. Chen, T. Luan, H. Bootwala, and L. Batten, “Cyber security attacks to modern vehicular systems,” *Journal of Information Security and Applications*, vol. 36, pp. 90–100, 2017.

[18] C. Plappert, D. Zelle, H. Gadacz, R. Rieke, D. Scheuermann, and C. Krauß, “Attack surface assessment for cybersecurity engineering in the automotive domain,” in *2021 29th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP)*, 2021, pp. 266–275.

[19] S. V. Kumar, G. A. A. Mary, P. Suresh, and R. Uthirasamy, “Investigation on cyber-attacks against in-vehicle network,” in *2021 7th International Conference on Electrical Energy Systems (ICEES)*, 2021, pp. 305–311.

[20] S. Malik and W. Sun, “Analysis and simulation of cyber attacks against connected and autonomous vehicles,” in *2020 International Conference on Connected and Autonomous Driving (MetroCAD)*, 2020, pp. 62–70.

[21] Z. El-Rewini, K. Sadatsharan, N. Sugunaraj, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, “Cybersecurity attacks in vehicular sensors,” *IEEE Sensors Journal*, vol. 20, no. 22, pp. 13 752–13 767, 2020.

[22] R. E. Haas and D. P. F. Möller, “Automotive connectivity, cyber attack scenarios and automotive cyber security,” in *2017 IEEE International Conference on Electro Information Technology (EIT)*, may 2017, pp. 635–639.

[23] D. Kent, B. H. Cheng, and J. Siegel, “Assuring vehicle update integrity using asymmetric public key infrastructure (pki) and public key cryptography (pkc),” *SAE International Journal of Transportation Cybersecurity and Privacy*, vol. 2, no. 2, pp. 141–158, aug 2020.

[24] T. Hutzelmann, S. Banescu, and A. Pretschner, “A comprehensive attack and defense model for the automotive domain,” *SAE International Journal of Transportation Cybersecurity and Privacy*, vol. 2, no. 1, pp. 5–20, jan 2019.

[25] A. Ansari, S. Thekkumbadan, S. Das, J. JOSE, and I. Sana, “Mechanism for secure storage without a trusted execution environment for low/mid automotive segments,” in *SAE WCX Digital Summit*. SAE International, apr 2021.

[26] V. K. M, R. Koduri, S. Nandyala, and M. Manalikandy, “Secure vehicular communication using blockchain technology,” in *WCX SAE World Congress Experience*. SAE International, apr 2020.

[27] F. Luo and S. Hou, “Security mechanisms design of automotive gateway firewall,” in *WCX SAE World Congress Experience*. SAE International, apr 2019.

[28] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, “Cybersecurity challenges in vehicular communications,” *Vehicular Communications*, vol. 23, p. 100214, 2020.

[29] S. K. Khan, N. Shiwakoti, P. Stasinopoulos, and Y. Chen, “Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions,” *Accident Analysis & Prevention*, vol. 148, 2020.

[30] K. Kim, J. S. Kim, S. Jeong, J.-H. Park, and H. K. Kim, "Cybersecurity for autonomous vehicles: Review of attacks and defense," *Computers & Security*, vol. 103, 2021.

[31] S. Parkinson, P. Ward, K. Wilson, and J. Miller, "Cyber threats facing autonomous and connected vehicles: Future challenges," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 11, pp. 2898–2915, 2017.

[32] W. Xiong, F. Krantz, and R. Lagerström, "Threat modeling and attack simulations of connected vehicles: Proof of concept," in *Information Systems Security and Privacy*, P. Mori, S. Furnell, and O. Camp, Eds. Cham: Springer International Publishing, 2020, pp. 272–287.

[33] D. Mbakoyiannis, O. Tomoutzoglou, and G. Kornaros, "Secure over-the-air firmware updating for automotive electronic control units," in *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing*, ser. SAC '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 174–181.

[34] A. Ghosal, S. Halder, and M. Conti, "Stride: Scalable and secure over-the-air software update scheme for autonomous vehicles," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, 2020, pp. 1–6.

[35] H. Kexun, W. Changyuan, H. Yanyan, and F. Xiyu, "Research on cyber security technology and test method of ota for intelligent connected vehicle," in *2020 International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE)*, 2020, pp. 194–198.

[36] M. Khatun, M. Glaß, and R. Jung, "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)*, 2021, pp. 122–127.

[37] M. Steger, C. A. Boano, T. Niedermayr, M. Karner, J. Hillebrand, K. Roemer, and W. Rom, "An efficient and secure automotive wireless software update framework," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 5, pp. 2181–2193, 2018.

[38] A. Freiwald and G. Hwang, "Safe and secure software updates over the air for electronic brake control systems," *SAE International Journal of Passenger Cars - Electronic and Electrical Systems*, vol. 10, no. 1, pp. 71–82, sep 2016.

[39] J. Howden, L. Maglaras, and M. A. Ferrag, "The security aspects of automotive over-the-air updates," *International Journal of Cyber Warfare and Terrorism (IJCWT)*, vol. 10, no. 2, pp. 64–81, 2020.

[40] S. Aust, "Software downloads in trusted zones with wake-up sensors for connected vehicles," in *2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*, 2018, pp. 1–5.

[41] V. Drake, "Threat Modeling." [Online]. Available: https://owasp.org/www-community/Threat_Modeling

[42] NCSC, "Secure design principles," 2019. [Online]. Available: https://www.ncsc.gov.uk/collection/cyber-security-design-principles

[43] W. Grunbok and M. Cole, "Security in Development, The IBM Secure Engineering Framework," International Business Machines Corporation, Tech. Rep., 2018. [Online]. Available: https://www.redbooks.ibm.com/redpapers/pdfs/redp4641.pdf

[44] A. Greenberg, "The Jeep Hackers Are Back to Prove Car Hacking Can Get Much Worse," 2016. [Online]. Available: https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/

[45] Reuters, "Toyota to recall 1.9 million Prius cars for software defect in hybrid system." [Online]. Available: https://www.reuters.com/article/us-toyota-recall-idUSBREA1B1B920140212

[46] H. Mansor, K. Markantonakis, R. N. Akram, and K. Mayes, "Don't brick your car: Firmware confidentiality and rollback for vehicles," in *2015 10th International Conference on Availability, Reliability and Security*, 2015, pp. 139–148.

[47] UNECE World Forum for Harmonization of Vehicle Regulations (WP.29), "Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to software update and software updates management system," United Nations Economic Commission for Europe, Tech. Rep., 2020. [Online]. Available: https://undocs.org/ECE/TRANS/WP.29/2020/80

[48] International Organization for Standardization, "Road vehicles – Software update engineering (ISO 24089)," Geneva, 2023.

[49] D. S. Fowler, "Automotive Cyber Security Timeline," 2022. [Online]. Available: https://tekeye.uk/automotive/cyber-security/timeline

[50] Netscribes, "Projected global ADAS market size between 2015 and 2023." [Online]. Available: https://www.statista.com/statistics/591579/adas-and-ad-systems-in-light-vehicles-global-market-size/

[51] UNECE World Forum for Harmonization of Vehicle Regulations (WP.29), "Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to Automated Lane Keeping System," United Nations Economic Commission for Europe, Tech. Rep., 2020. [Online]. Available: https://undocs.org/ECE/TRANS/WP.29/2020/81

[52] Upstream Security Ltd, "Global Automotive Cybersecurity Report 2019," 2018.

[53] ——, "2022 Global Automotive Cybersecurity Report," 2021.

[54] U. S. Ltd., "2020 Global Automotive Cybersecurity Report," 2019.

[55] National Highway Traffic Safety Administration, "Cybersecurity Best Practices for the Safety of Modern Vehicles," NHTSA, Washington, DC, Tech. Rep., 2020.

[56] ENISA, "ENISA Good Practices for Security of Smart Cars," European Union Agency for Cybersecurity, Tech. Rep., 2019.

[57] L. A. Gordon, M. P. Loeb, and L. Zhou, "Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model," *Journal of Cybersecurity*, vol. 6, no. 1, 03 2020.

[58] B. Kordy, L. Piètre-Cambacédès, and P. Schweitzer, "Dag-based attack and defense modeling: Don't miss the forest for the attack trees," *Computer Science Review*, vol. 13-14, pp. 1–38, 2014.

[59] A. Francillon, B. Danev, and S. Capkun, "Relay attacks on passive keyless entry and start systems in modern cars," in *18th Annual Network & Distributed System Security Symposium Proceedings*. Internet Society, 2011.

[60] A. Ruddle, "Security risk analysis approach for on-board vehicle networks," in *The Fully Networked Car Workshop at the Geneva International Motor Show*, 2010.

[61] The HEAVENS Consortium, "Security models," Vinnova, Tech. Rep., 2016.

[62] J. Hao and G. Han, "On the Modeling of Automotive Security: A Survey of Methods and Perspectives," *Future Internet*, vol. 12, no. 11, 2020.

[63] OWASP, "OWASP Top Ten." [Online]. Available: https://owasp.org/www-project-top-ten/

[64] The MITRE Corporation, "Enterprise Matrix." [Online]. Available: https://attack.mitre.org/matrices/enterprise/

[65] I. Lella, M. Theocharidou, E. Tsekmezoglou, A. Malatras, S. García, and V. Valeros, "Enisa threat landscape for supply chain attacks," European Union Agency for Cybersecurity, Tech. Rep., 7 2021.

[66] G. Kim, "Making you safer with 2SV," 2022. [Online]. Available: https://blog.google/technology/safety-security/reducing-account-hijacking/

[67] WMG, Cisco, and Telefonica, "Project BeARCAT: Baselining, Automation and Response for CAV Testbed Cyber Security: Connected Vehicle & Infrastructure Security Assessment," Zenzic, Tech. Rep., 2020. [Online]. Available: http://wrap.warwick.ac.uk/141491/

[68] OWASP, "The OWASP Testing Project." [Online]. Available: https://owasp.org/www-project-web-security-testing-guide/stable/2-Introduction/