Applications of Formal Verification Techniques for Security in the Context of Automotive Diagnostics

a Literature-Survey

Julius Figge[1,2] and David Knuplesch[2]

[1] Institute of Computer Science, Leipzig University, 04109 Leipzig, Germany
[2] Mercedes-Benz Tech Innovation GmbH, 89081 Ulm, Germany
{julius.figge, david.knuplesch}@mercedes-benz.com

Abstract. The automotive industry is shifting from a mechanical engineering focus to an integrated approach emphasizing software development. This transition is marked by the increased performance and responsibilities of Electronic control units (ECUs) in vehicles, combined with in-vehicle systems growing in complexity and external connectivity. Automotive diagnostics (AD), including monitoring, anomaly detection, maintenance and updates, has become a crucial part for maintaining the reliability, safety, and security of these advanced systems. However, new regulatory frameworks, like the UNECE directives for cyber security and Software Update Management, introduce challenges, particularly for over-the-air (OTA)-updates. A promising solution for improving and ensuring security is the application of formal verification methods. Formal methods provide a range of mathematical techniques to systematically and exhaustively validate that a systems design adheres to its specified security requirements, thus helping to prevent security flaws by design and implementation errors. This systematic literature review evaluates the use of formal verification in the combined field of security and AD. Our analysis of the current research indicates that these techniques are underutilized, particularly in areas where formal methods have yet to be applied. Our findings highlight a potential for expanding the use of formal methods in enhancing security within AD.

Keywords: Literature Survey · Remote Diagnostics · Automotive · Formal Verification · Security.

1 Introduction

The architecture of automotive electronics has significantly evolved during the recent years and continues to do so. It is shifting away from configurations comprising up to 150 *Electronic Control Units* (ECUs) [44] with limited computing capabilities, toward more centralized and domain- and zone-based approaches. The number of ECUs is meanwhile being reduced and reorganized again around a few, yet potent, *high-performance computing platform* (HPC) ECUs that serve

as domain- or zone-controllers. These HPCs are more powerful, achieve higher data rates, and are comparable to conventional computers and even run hypervisors supporting multiple virtual machines (VM), including Linux and Android guests [3, 18].

In these advanced architectures, *automotive diagnostics* (AD) play a vital role in ensuring the reliability, safety, and security of vehicles [33]. AD encompasses not only monitoring, anomaly detection, and maintenance functionalities, but also enables vehicle software updates [24]. In particular, standards and regulations, such as ISO 14229 and UNECE R156, do not only require manufacturers to support AD in general, but also demand for comprehensive *Software Update Management Systems* (SUMS) that enable remote and *over-the-air* (OTA) updates as essential part of AD for their vehicles.

SUMS and OTA provide numerous benefits, but also introduce a spectrum of security risks that extend beyond data and software integrity, potentially endangering passenger safety [43]. In the case of a successful attack, malicious entities could potentially exploit OTA mechanisms to alter dashboard displays, turn off headlights, or even trigger airbag deployment while the vehicle is in motion [14].

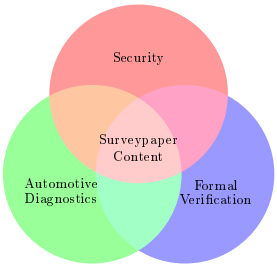

Fig. 1: Thematic target area.

The above mentioned scenarios highlight the need for manufacturers to ensure the security of AD in various ways. In this context, *formal verification* (FV) techniques appear to be a suitable tool as they provide means to unambiguously prove or refute aspects of security [12, 47]. Furthermore, FV is already employed in the automotive domain (e.g., for validating safety [21]) and has yet been successfully applied in security assessments in multiple scenarios [6].

However, to the best of our knowledge it has not yet been discussed to which extent FV is already applied to ensure security in the context of AD (i.e., the current state of research). This raises the following research questions:

RQ1 *What existing work discusses applications of formal verification techniques for security in the context of automotive diagnostics (cf. Fig. 1), and which specific sub-area do they cover?*
RQ2 *What methods and techniques does existing work use?*
RQ3 *What open research directions can be identified that have received little or no attention so far?*

To tackle RQ1-3, this paper provides three major contributions. First, it undertakes a systematic literature search to collate relevant publications applying formal verification techniques to the security of AD. Second, the collected works are clustered according to their application domains and the methodologies utilized. Third, the paper discusses achievements in this field and identifies areas for further investigation.

The structure of this paper is as follows: Sect. 2 reviews related surveys. Sect. 3 introduces the details of the automotive architecture that is relevant to diagnostics. The methodology used in this article is outlined in Sect. 4. Significant

findings are presented and categorized in Sect. 5. Sect. 6 investigates unexplored areas and identifies open requirements and challenges to enhance security in AD via formal verification techniques. Finally, Sect. 7 provides a summary and concludes the paper.

2 Related Work

The objective of this survey is to examine the utilization of formal verification in the domain of AD security. In this section, we discuss related surveys that also address topics relevant to our field of interest. We provide a brief overview of these papers, validate their alignment with our focus, and delimit their scope from that of our survey.

Altinger et al. [1] explored automotive testing-practices, -automation, and -tools. They noted the usage of formal methods in specification, not testing. The survey did not focus on the fields of security and AD. Kim et al. [22] reviewed security for autonomous vehicles, detailing attacks on control systems, components, and communications, alongside defenses like security architecture and detection systems. They observed a research shift from *Controller Area Network* (CAN) and ECUs to risk design and attack scenarios post-2017. The survey emphasizes security within the automotive sector, touching on AD, but formal verification is outside their scope. Sun et al. [45] assessed security in *connected and autonomous vehicles* (CAVs), classifying risks into in-vehicle and vehicle-to-everything network attacks, among others. They presented protection strategies and summarized standards for CAVs security and safety. Their survey did focus on security and diagnostics in the automotive context, whilst formal methods in the automotive domain were outside their scope. Pekaric et al. [41] analyzed security testing techniques in the automotive sector through a systematic mapping study over five dimensions. They identified penetration testing, dynamic analysis, and *model-based testing* (MBT) as common techniques. They highlighted the *Automotive Open System Architecture* (AUTOSAR) application and services layer during various phases. Their survey emphasized the necessity for regression and integrated security-safety testing in the automotive industry, but it did not concentrate on formal methods beyond model-based testing, the field of AD was largely out of their scope. Sommer et al. [44] surveyed MBT and *model-based security testing* (MBST) within the automotive industry, also referencing examples from aerospace, medicine, and IT. They observed that MBST is a recent practice in the automotive domain compared to others. The studies focus was set on formal methods in the automotive sector. Whilst they examined MBST, they otherwise did not focus on security, or AD. Krichen [25] reviewed security analysis and verification methods in the automotive industry, whilst also setting the focus on penetration testing, fault injection, and fuzz testing. They employed code examples and hypothetical attack scenarios for clarity. Their survey was not focused on AD. They focused on the broader context of security and formal methods, rather than being limited to the automotive sector.

To date, no publication specifically addresses formal methods in the context of security for diagnostics within the automotive industry. Our current work aims to illuminate this precise area.

3 Diagnostics Architecture

This section briefly introduces the automotive vehicle *electrical/electronic* (E/E) architecture and its details relevant for AD as illustrated in Fig. 2.

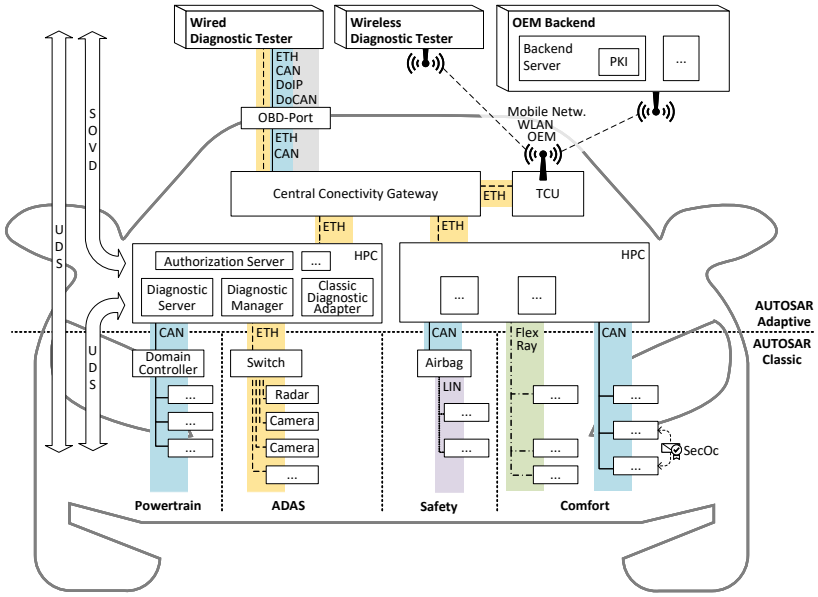

Fig. 2: Exemplary simplified vehicular diagnostic infrastructure. [3, 9, 13, 18, 48]

The architecture can be divided into two main categories: The internal components of the vehicle on the one hand and external systems and components interacting with the vehicle on the other hand.

The internal architecture is evolving from an approach based on a up to 150 specialized ECUs, with limited computing capabilities and isolated functions, to a more centralized design with fewer but more powerful HPCs serving as domain- and zone-controllers. [18] This ongoing transformation is complemented by the addition of the new AUTOSAR Adaptive platform on top of the AUTOSAR Classic architecture, which marks a significant shift for AD [48].

The AUTOSAR Adaptive components relevant in the context of AD are the Central Connectivity Gateway, which serves as the main communication hub of the architecture, as well as several HPCs. These HPCs are more powerful, achieve higher data rates, and are comparable to conventional computers as they are even capable of running hypervisors supporting multiple *virtual machines* (VM), including Linux and Android guests [3, 18]. Among other functions

HPCs also house services that are crucial for AD [9].
The components of the AUTOSAR Adaptive layer communicate via an (Automotive) Ethernet based Network.

AUTOSAR Classic ECUs are arranged around the *AUTOSAR Adaptive* HPCs organized into domains (e.g. Powertrain, Advanced Driver Assistance Systems (ADAS), Safety, or Comfort) (cf. Fig.2). Within these domains, various communication technologies such as CAN, *Local Interconnect Network* (LIN), (Automotive) Ethernet, and FlexRay are employed [48]. Communication among AUTOSAR Classic ECUs in the network is protected by AUTOSAR Secure Onboard Communication (SecOC) [28].

There are two main AD standards: Aligning with the addition of AUTOSAR Adaptive, the previous standard for AD (i.e. the *Unified Diagnostic Services* (UDS)), is being supplanted by the *Service Oriented Vehicle Diagnostics* (SOVD), a new standard by the Association for *Standardisation of Automation and Measuring Systems* (ASAM) consortium [3]. The relevant components for using SOVD diagnostics are situated in the HPCs. These include, among others, the Diagnostic- and Authorization-Server, Diagnostic Manager as well as the Classic Diagnostic Adapter for AUTOSAR Classic ECU communication [3].

Using their *Telematics Control Unit* (TCU) modern vehicles already connect to numerous external entities through the Internet, utilizing mobile communications and Wi-Fi [44], which is generally referred to as *vehicle-to-everything* (V2X) [28]. In the context of AD, V2X also includes interaction with diagnostic entities, i.e., diagnostic adapters and original equipment manufacturers (OEM) backends. The OEM backend plays an essential role in managing vehicle services. It is not only able to initiate AD remotely, e.g., by using SOVD or to conduct OTA updates in order to adhere to compliance and security requirements, but OEM backends also provide the *Public Key Infrastructure* (PKI) crucial for authentication in the context of AD [4]. The TCU itself is connected to the Central Connectivity Gateway via Ethernet.

In addition to Internet-based communication, AD using the UDS and SOVD standards with special diagnostic adapters (for example, during workshop visits or as part of production) continues to play a major role [3]. The diagnostic adapter is either physically connected to the vehicle via *On-board diagnostics* (OBD) connectors or Ethernet, or communicates remotely via a network connection established by the vehicle's TCU (Remote Diagnostics). The AD UDS connection is made via ODB using *Diagnostics over CAN* (DoCAN) or *Diagnostics over IP* (DoIP) [9]. SOVD AD is based on HTTP and REST. The connection is established via OBD in Ethernet mode, wireless via WiFi or even via the OEM backend [3].

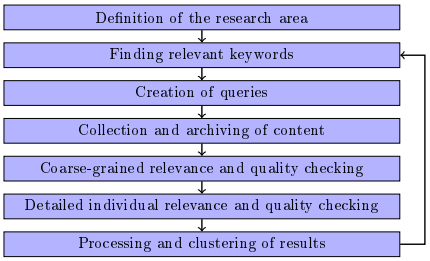

Fig. 3: Research methodology.

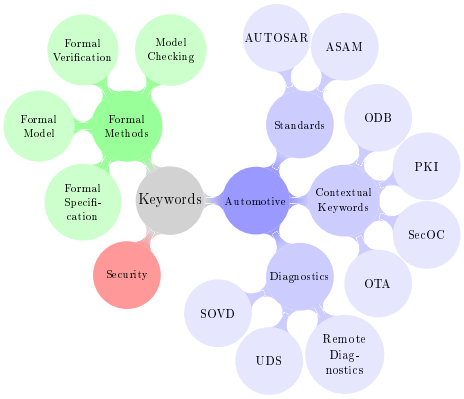

Fig. 4: Relevant Keywords.

4 Methodology

This survey aims to offer a thorough review of the current application of formal verification techniques for security in AD. We identify and analyze relevant scientific contributions using a methodical and reproducible approach to ensure qualitative results (Fig. 3)

The initial crucial step was the *Definition of the research area*, which has been predetermined and is illustrated by the intersecting sub-areas in Fig.1.

The next phase, which is also the start of an iteration of the cyclic process, involved *Finding relevant keywords* (Fig. 4). The fields from Fig. 1 were used as a starting point for the keyword search. From this point on, the iterative process was used and, based on the core terms, the search scope was progressively widened by adding related terms.

After identifying keywords, we proceeded to the *Creation of queries* by combining one or more keywords from each identified sub-area. These combinations and their results and relevance assessments are detailed in Tab.1. We prefixed all of our queries with the term *Security* as we chose not to expand this field with additional keywords. *Automotive* was used as the second keyword in every query to address the second relevant topic. Alternatives like "vehicle" and "cyber-physical system" were considered but discarded as they did not yield relevant additional results. To refine the search, we appended a more specific AD-related term to each query.

Search Query	**O**	**I**	**MR**	**R**	**HR**
Security Automotive Model Checking Diagnostics	149	140	2	6	1
Security Automotive Formal Methods Diagnostics	139	123	4	12	0
Security Automotive Formal Specification Diagnostics	40	37	0	3	0
Security Automotive Formal Verification "Remote Diagnostics"	80	60	4	12	4
Security Automotive Formal Verification Diagnostics	126	89	4	12	5
Security Automotive Formal Verification OTA	80	57	4	14	5
Security Automotive Formal Verification SOVD	80	60	4	12	4
Security Automotive Formal Verification UDS	77	56	4	12	5
Security Automotive Formal Verification SecOC	80	60	4	12	4
Security Automotive Formal Verification PKI	130	108	4	14	4
Security Automotive Formal Verification AUTOSAR	90	68	5	13	4
Security Automotive Formal Verification ASAM	80	60	4	12	4
Security Automotive Formal Verification OBD	80	59	4	13	4
Security Automotive Formal Verification HPC	80	60	4	12	4
Overall	420	370	16	27	7

Legend: O=Overall, I=Irrelevant, MR=Minor Relevance, R=Relevant, HR=High Relevance

Table 1: Used queries including results and relevance classification.

The final component consists of terms related to *Formal Methods*. We used a variety of keywords to maximize the retrieval of papers relevant for our topic. Our experience showed that combining multiple formal methods keywords with those from the AD field did not significantly enhance the value of the search results. Thus, we built the queries using the primary keyword *Formal Verification*.

With the queries established we started the *Collection and archiving of content*, systematically saving the search results (linked to the respective queries).

Following that, we conducted a *Coarse-grained relevance and quality check* using the decision criteria outlined in Tab.2. This preliminary sorting served as a pre-classification to reduce and manage the number of papers for subsequent stages, by excluding clearly unsuitable content. Although LLMs are increasingly being used in research for the automated screening of current literature [46], we conducted the reviews manually in order to ensure a high level of accuracy.

	Desired	**Undesired**
General Criteria	English Paper	Non-English Paper
	Peer reviewed Paper	Grey/White Literature
	Paper with scientific Contribution	Duplicate Paper
	Accessible Paper	Paper that is not available
	relevant and up-to-date Paper	non-relevant or outdated Paper
Topic-specific Criteria	Usage of Formal Methods	No use of Formal Methods
	Focus on Automotive Domain	No Focus on Automotive Context, Cyber Physical Systems in general
	Relevance for Automotive Diagnostics	No relevance for Automotive Diagnostics
	Focus on Security	Focus on Safety, No Focus on Security

Table 2: Paper relevance criteria.[3][4]

This was followed by a *Detailed individual relevance and quality check*, using the criteria from Tab. 2. Papers that only partially met the requirements but provided relevant contributions were classified as of minor relevance. Those that met all criteria were deemed relevant, and publications of concrete practical relevance or special contributions were rated as of high relevance. This classification was based on the entire content of the papers.

At this point in the cyclical process, we utilized indirect snowballing to optimize our research queries. If references were found in the papers to be sorted not present in the result set, the search queries were adjusted accordingly. As indicated in Fig. 1, overall 7 papers were classified as of high relevance and 27 papers as relevant.[5] A total of 370 papers were classified as irrelevant and 16 as only of minor relevance, and were therefore filtered out.

Finally, the *Processing and clustering of results* was completed. During this phase, the findings were prepared for inclusion in the survey paper. The relevant insights from the papers were processed, and the papers were grouped into clusters. We utilize the concept based approach of [51]. The following method was employed to classify the concepts: At the highest level, the assignment is

[4] Outdated papers specifically refer to protocols, techniques, and approaches that are no longer relevant in the continuously evolving context of the E/E architecture.

[4] The relevance of a publication in this context refers to its correspondence with the desired target scope.

[5] It should be noted that duplicates occurred when a publication was found via several search queries. These were removed from the overall results.

based on the major subject areas in the field of diagnosis. At the lower levels, the classification is additionally based on sub-areas, tools and approaches used.

The discovered research papers and identified clusters are presented in the follwing Chapter 5.

5 Results

In the following, we address the question of which scientific publications already exist in our observed field and what specific sub-areas they cover (**RQ1**). We present our research findings (as seen in Fig.5), organized by key topics and clustered into concepts where applicable. Beginning at a high-level with frameworks, we pivot to examine SUMS and OTA-Updates, then transition to vehicle external connections within V2X. Progressing towards the vehicle, we explore its internal network and conclude with a focused analysis of AD in the narrower sense.

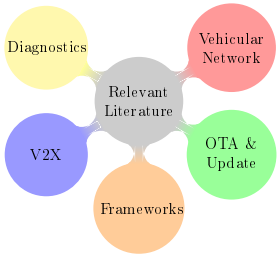

Fig. 5: Concepts resulting from the survey results.

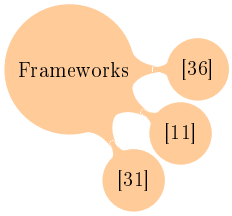

Fig. 6: Relevant research for the area "Frameworks".

Frameworks Our first area of focus comprises frameworks (Fig.6), which encompass approaches such as metamodels, requirement management systems, and architecture security analysis methods. Mundhenk et al. [36] introduced a system-level security analysis method for automotive architectures. The method is used to evaluate architecture security variants as early as the design process. They utilized a *Continuous-Time Markov Chain* (CTMC) model, built from ECUs and networks modeled on system-level, including exploitability scores and patch levels to analyze the systems. The model allows for probabilistic model checking based analysis of confidentiality, integrity and availability. Cimatti et al. [11] suggested a framework for analyzing and verifying automotive systems, extending AUTOSAR with a unified, modular metamodel and an Eclipse-based framework. Their framework allows for timing analysis and functional verification via model checking, using the Kratos model checker and OCRA platform. Future enhancements aim to verify AUTOSAR client-server operations and improve timing tools for network-level coverage. Luo et al. [31] proposed a *cyber security Requirements Management System* (CRMS) framework for the automotive sector, utilizing the UML-based *Eclipse Modeling Framework* (EMF). This approach encompasses the entire development lifecycle, including AD and ECUs, enabling automated threat analysis and risk assessment. The CRMS allows system modeling with UML-EMF for engineers and a formal threat and

security requirement library in Alloy for security experts. The *component channel and messaging interface* (CCMI) middleware facilitates integration between these elements.

OTA The next key concept are Software Updates in the broader sense (Fig.7). The UN Regulation (UN R156) requires, among other things, a SUMS for vehicles. Seo et al. [43] proposed a secure SUMS that poses stricter security requirements than UN R156 and is formally verified using Event-B. Pedroza et al. [40] proposed a profile extension with a focus on security to the automated verification of real time software (AVATAR) UML, which in turn is based on SysML. They also utilized it, amongst other goals, to formally verify an OTA-protocol for trusted firmware updates of ECUs called "FU Update". Mansor et al. [32] presented a secure OTA firmware update protocol that incorporates a mobile phone for authentication and data transmission. They successfully verified their protocol with Scyther and CasperFDR, tools for formal protocol security analysis (finding no attacks). Mundhenk et al. [35] introduced the *Lightweight Authentication for Secure Automotive Networks* (LASAN), a full-lifecycle authentication method for integration into manufacturing, maintenance, and software updates. LASAN secures firmware and ECU replacements and updates throughout a vehicle's lifecycle. The core protocol protects internal networks while meeting real-time requirements and has been formally verified with Scyther using a Dolev-Yao model. An alternative method was proposed by [17], using OTA software updates as an example to demonstrate their solution. They concentrated on automatic, systematic security testing of ECU components and broader systems through model-checking, employing process algebra CSP models verified by an FDR refinement checker. Kirk et al. [23] also offered a solution using an FDR refinement checker and CSP to model and confirm the vulnerability of Uptane, an OTA Software Update Framework. Using CSP, FDR4 and a Dolev-Yao model, they found that Uptane was vulnerable to three of four attacks. Mukherjee et al. [34] also focussed on the Uptane Framework, deploying it within a *trusted execution environment* (TEE) on *commercial off-the-shelf* (COTS) hardware. They used the ARM TrustZone for isolation during OTA updates in a simulated *battery electric vehicle* (BEV) and confirmed the deployments functional and logical consistency using SAWScript.

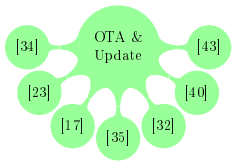

Fig. 7: Relevant research for the area "OTA & Update".

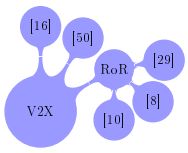

Fig. 8: Relevant research for the area "V2X".

V2X V2X is used as the umbrella term for vehicle communication with external systems [50]. As part of communication, vehicles require access to more services than just the OEM backend for obtaining OTA updates, for example. They should have the capability to interact with third-party services and each other within the scope of V2X communication (Fig.8). Gürgens et al. [16] introduced a security model for in-car field bus communication, subject to formal analysis. Their model,

is based on asynchronous product automata and includes a field bus, TCU, backend server, and terminal clients. They employed the *SH Verification Tool* (SHVT) to validate a known vulnerability in a smartphone-based remote unlocking system. Wang et al. [50] suggested a certificateless aggregate signature (CLAS) scheme for 5G based vehicular networks. They employed a *random oracle model* (ROM) for security analysis, demonstrating the schemes security.
In the V2X domain, another common method is the application of *random-or-real* (RoR) models in proof constructions. Lee et al. [29] applied RoR models to their *Vehicular Ad Hoc Network* (VANET) authentication protocol, which incorporates mutual authentication, for vehicle-to-vehicle communication. They have formally analyzed their protocol with the *Automated Validation of Internet Security Protocols and Applications* (AVISPA) software tool, in conjunction with the use of a RoR model. Bojjagani et al. [8] proposed another protocol using RoR models for their Secure Authentication and Key Management Protocol on the *Internet of Vehicles* (IoV). Named AKAP-IoV, it was formally analyzed for security with a RoR model and verified with the Scyther and Tamarin tools. Chen et al. [10] introduced a *digital twin* (DT) model and constructed a DT-enabled autonomous vehicle framework with a secure authenticated key agreement protocol to ensure data privacy in entity communication. They formally verified their protocol using *Burrows-Abadi-Needham* (BAN) logic and a RoR model.

Vehicular Network Having examined the overall car architecture and external communications, this section shifts focus to the CAN bus and in-vehicle communications (Fig.9). Feng et al. [15] evaluated an *Intra-Vehicular Networks* (IVNs) protocol using model detection, identifying security flaws and proposing a new protocol. They employed *Colored Petri Nets* (CPN) and the Dolev-Yao model to validate the proposed protocol and to analyze the CAN2.0-based IVN, uncovering two man-in-the-middle attacks in the latter. Kim et al. [21] introduced MAuth, a message authentication extension for the CAN vehicle bus. They validated MAuth using timed automata with model checking and demonstrated obtaining ISO 26262 safety and security certifications through formal methods. Jahandiden et al. [19] proposed an extension to the actor based language Rebeca, called Hybrid Rebeca as a language for the modeling of cyber-physical sytems. They demonstrated the language on the example of a *Brake-By-Wire* (BBW) system with an *Anti-lock Braking System* (ABS) and analyze the case study using the SpaceEx framework.

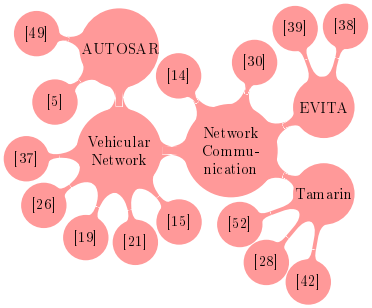

Fig. 9: Relevant research for the area "Vehicular Network".

In the vehicle internal networking domain, two key studies address the AUTOSAR standard. Bahig et al. [5] proposed a framework for the automated verification of UML based designs. Their approach is to compile UML *finite state machines* (FSM) into formal notations, mapping requirement specifications to

model theorems, and utilizing SAT/SMT solvers to validate compliance to specification. They exemplarily applied their methodology to the AUTOSAR FlexRay State Manager state machine. Trinh et al. [49] formalized and verified the AUTOSAR OS standard memory protection, using Event-B specification language and verification with RODIN, revealing ambiguities in the original specification. Lampe and Meng [26] used temporal logic for automotive intrusion detection by formalizing *indicators of compromise* (IoC) in *linear temporal logic* (LTL), *metric temporal logic* (MTL), and *signal temporal logic* (STL). They demonstrated feasibility with a Python implementation, with the goal to implement a formal monitor in the future.

The vehicular network literature features multiple studies focused on network communication. Dürrwang et al. [14] proposed a method for automating security testing and *Threat Analysis and Risk Assessment* (TARA) by modeling attacker privileges. They applied these privileges to formally model a vehicles internal network, creating attack trees and security tests from the model. The authors demonstrated the potential attack of detonating an airbag via OBD Diagnostics. Lenard et al. [30] proposed the *Lightweight Cryptographic Key Distribution* (LOKI) 2 Protocol for automotive systems, with both the initial and new variants formally verified for security. The older version lacked in security properties and had design flaws, while the new variants correctness was established through BAN logic analysis.

There are also two relevant papers dealing with network communication in the context of the *E-safety vehicle intrusion protected applications* (EVITA) project. Pedroza et al. [39] proposed the aforementioned ([40]) AVATAR UML standard, which allows capturing both safety- and security-elements in the same SysML model. Their proposed environment allows the verification of those properties with UPPAAL for safety and ProVerif Toolkit for security. They illustrated this by applying it to a keying protocol where a key master distributes randomly generated keys to ECUs. Pedrozas PhD thesis [38] covered extending the AVATAR SysML language with the AvatarSE profile to model security concerns and define formal model transformations for verification. The author demonstrated this with a case study by verifying the EVITA keying protocol, an automotive cryptography protocol for ECU key distribution using *Hardware Security Modules* (HSM).

There are three relevant papers that analyze in vehicular network communication using Tamarin. Püllen et al. [42] introduced the *Automotive Service-Oriented Architecture* (ASOA) framework for the design, deployment and maintenance of automotive software architecture and presented a security process for ASOA communications. They detailed a central component for converting communication models into securely distributed tokens for ASOA services (ECUs) The token distribution protocol was formally verified using Tamarin. Lauser et al. [28] used Tamarin for tool based formal analysis of the AUTOSAR *Secure Onboard Communication* (SecOC). The authors validated the integrity and authentication guaranteed by SecOC, whilst noting the lack of confidentiality. The paper goes further, discussing security properties for automotive protocols, the state

of protocol verification tools, and the overall landscape of protocol analysis. The same author group joined by Kern (Zelle et al.) [52], conducted a Tamarin-based formal security analysis of the Scalable *service-Oriented MiddlewarE over IP* (SOME/IP), identifying vulnerabilities to *Man-in-the-Middle* (MitM) attacks in two real-world libraries. Three different MitM attacks were found, even with security mechanisms on OSI-Layer 2 enabled. To mitigate these, they proposed two security extensions, SESO-RC for resource-rich ECUs using asymmetric cryptography, and SESO-AS for lower overhead symmetric cryptography, both validated through formal analysis.
Palaniswamy et al. [37] analyzed a proposed protocol for the SAE J1939 Commercial Vehicles Bus, which facilitates ECU communication Using Tamarin, they identified vulnerabilities to replay, masquerading, and MitM attacks. To address these, they proposed a new protocol suite *certificateless key insulated manageable signature* (CL-KIMS), encompassing key exchange, time synchronization protocols, and a signature scheme, which they formally verified via a ROM and Tamarin.

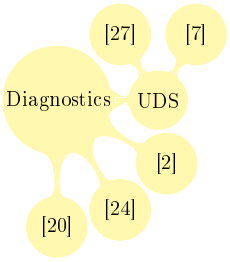

Fig. 10: Relevant research for the area "Diagnostics".

Diagnostics We have now covered the broader context surrounding and enabling diagnostics and now focus on topics directly related to AD in the narrower sense (Fig.10).
There are two papers focusing on the security of the UDS protocol. Lauser et. al [27] also utilized Tamarin, to formally analyze UDS, uncovering vulnerabilities in the "Security Access" and the newer "Authentication Service" standards. For the old Security Access they identified lack in the standards detail, that could lead to room for interpretation in the implementation. As for the newer Authentication Service, they were able to identify two vulnerabilities in the standard. Becker et al. [7] analyzed a UDS implementation on an OEMs ECU using a model-based classification algorithm for bug identification, incorporating symbolic execution and Hoare logic into their methodology.
Apvrille et al. [2] introduced SysML-Sec, a SysML extension for a model-driven engineering environment that enhances security analysis by integrating requirements and threats, enabling formal verification with ProVerif. They demonstrated its application through an ECU firmware flashing process example. Kleberger and Moulin [24] verified a previously proposed authorization protocol for remote diagnostics to prevent unauthorized access, ensuring mutual authentication, key secrecy, and authorization information freshness. These properties were formally analyzed and proven utilizing BAN logic and the ProVerif tool.
Karray et al. [20] presented a graph transformation-based method for the conceptual phase of vehicle development. They formally modeled vehicle architecture and state evolution with their method, using the Groove (*GRaph- based Object-Oriented VErification*) tool to build an architectural graph and transformation

rules. The method facilitates the construction of attack trees for analyzing potential vehicle attacks.

6 Discussion

In the previous section, we presented the curated relevant papers and clustered them based on their concepts. This clustering involved a top-level classification according to areas within AD, followed by a sub-level classification based on specific domains, as well as methods and tools of formal verification. We aim to elaborate on these findings, focusing on the remaining two research questions. Firstly, we seek to pinpoint areas within the field that have received minimal scientific attention to date (**RQ3**). Secondly, we aim to examine the various approaches, frameworks, and tools utilized for formal verification in the scientific literature related to our area of interest (**RQ2**). Lastly, we will identify open research questions that emerge from our analysis.

Regarding **RQ3**, while the in-vehicle network and OTA approaches have been covered by research, these areas are evolving and relevant components are changing or being replaced. Not only is there a shift towards domain and zone-based networking with the introduction of AUTOSAR Adaptive and HPC ECUs, but legislation is also mandating OTA updates [43, 48]. This makes the integration of formal methods in security particularly relevant to this area. While two papers have been identified that examine the UDS standard [7, 27], research on the successor standard SOVD, who continues to support UDS, is lacking. Given SOVDs likewise design for next-generation connected cars with HPC ECUs [3], it represents a critical area for security analysis through formal methods that should be covered. The AUTOSAR standard defines the usage of a PKI based security infrastructure among other things for AD purposes [4]. Similarly, AD standards like UDS and SOVD incorporate PKI-based authentication [3]. However, there is little research on the OEM backend infrastructure, the connection and communication with this and in particular on PKI implementations within the current scope.

For **RQ2**, the analysis reveals that (cryptographic) protocol provers are the leading approach, with 16 papers employing them. The Tamarin protocol prover is the most favored tool, used in 6 studies, while Scyther is the next preferred, appearing in 3 papers. Often, multiple protocol provers are utilized within a single publication. The second most common method is model checking, featured in 14 publications, with no single tool dominating; a diverse range of tools is noted. Equally prevalent are UML/SysML-based and Oracle-based approaches, each used in 5 papers. The combined use of different methods, especially protocol provers with UML-based approaches, is also significant. At the same time, the range of tools used is limited, prominent examples of model checking and theorem proving such as TLA+ or approaches of functional languages such as Lean, Coq, Idris as well as approaches of HoTT are not to be found.

Finally, we would like to mention relevant *open issues* (OI) that should be addressed and clarified as part of further research. The current status of soft-

ware development for vehicles and control units is defined, on the one hand, by applicable legal framework conditions for creating OTA updates and update frameworks like the UNECE R159 [43]. And on the other hand by standards such as the ISO/SAE 21434 standard, which define the vehicle life cycle [41]. The present publications covered either proposed protocols or existing solutions, standards and implementations. Whilst [35] does cover the whole lifecycle, their focus is solely on authentication. No work could be identified focusing on the entire lifecycle of components. In this context the lifecycle, exemplary in the context of an ECU, begins with the manufacturing of the hardware as well as development of the software and ends with the decommissioning of the hardware as waste. Therefore, we identify **OI1**. Aside from expanding the focus of formal verification to the entire lifecycle, it would be interesting to validate larger partial areas and systems of the vehicle or even the entire vehicle itself with formal methods. The underlying approach is to validate the entire vehicle rather than a subdomain or individual ECUs. We summarize this circumstance by defining **OI2**. The prior section highlighted gaps in the application of formal methods within scientific literature, particularly in areas like the new SOVD diagnostic standard, PKIs, and HPC ECUs. In this context, we identify **OI3**. Vehicle manufacturers and OEMs in general base their development and implementation on common, sometimes mandatory standards. These standards include frameworks such as AUTOSAR (Classic and Adaptive) as well as diagnostic standards like SOVD and UDS (ASAM). Currently, there are publications that utilize formal verification to validate parts of the standards (e.g. [28, 52]), but these have not been incorporated into the standards themselves. Thus, we identify **OI4** in relation to work in this direction. In this paper, we have examined the approaches and techniques of formal verification used in scientific publications for the security of automotive diagnostic systems. Future research should evaluate the efficiency of the tools used for identifying and addressing security vulnerabilities. Additionally, the various characteristics of the employed tools should be compared. For instance, by comparing model checkers with theorem provers or by assessing their accuracy, efficiency, and scalability. Therefore we define **OI5**.

OI1 *Can the use of formal verification throughout the ECU lifecycle add value outside the development process ?*

OI2 *Is it possible to extend the analysis of components and protocols with formal methods to larger parts or the whole vehicle, and what added value can be achieved by doing so?*

OI3 *Which of the currently least analyzed areas and protocols are the most important to validate using formal verification?*

OI4 *What are the challenges and solutions to include formal models or proofs for automotive protocols in the respective standards and what added value can be achieved hereby?*

OI5 *How effective are the currently utilized formal verification methods in identifying and mitigating security vulnerabilities, and how do they compare in terms of accuracy, efficiency, and scalability?*

7 Conclusion

The field of *automotive diagnostics* (AD) includes monitoring, anomaly detection, maintenance and updates. Although, AD is intended to analyze and fix defects, AD could potentially be exploited by attackers, which could have far-reaching consequences. Accordingly, it is crucial to ensure the security of AD, including supporting and related components, in various ways, which might also include formal verification techniques.

This paper provides the first comprehensive overview of the state of research on the use of formal verification for security in AD, as underpinned by our analysis of related literature surveys in Sect. 2. Based on an introduction of the AD architecture and associated components in Sect. 3, we determined relevant key words. Following a clear and iterative methodology (cf. Sect. 4), these key words were employed to identify a total of 420 publications out of which 34 papers were recognized as relevant.

We were able to discover five primary research clusters (Diagnostics, Vehicular Network, OTA & Update, Frameworks and V2X) and also identified further sub-clusters. These are RoR models for vehicle-to-everything (V2X), as well as the sub-clusters EVITA, Tamarin and Vehicular Network with their own sub-cluster AUTOSAR for Network Communication and the sub-aspect UDS for the Diagnostics cluster (cf. Sect. 5).
Research mainly targets two use-cases: in-vehicle networks, like the CAN bus, and vehicle communication with external services, such as V2X and over-the-air (OTA) updates. Despite the general focus on individual protocols, components, and rare references to meta-models or frameworks, there is a notable lack of research examining AD as a whole.
While academic research primarily focuses on proposed protocols and the validation of theoretical or academic frameworks and protocols, there are still several publications that focus on standards, protocols, and frameworks that are either established in the industry or used by manufacturers and OEMs as a basis for their own implementations (e.g. AUTOSAR).
The analysis of tools and methodology used in publications shows a preference for cryptographic protocol provers, especially Tamarin or model checkers.
It is notable, that the need for further research on in-vehicle networks and OTA updates is driven by continuously evolving technologies like AUTOSAR Adaptive and *high-performance computing platform* (HPC) ECUs, alongside new legislative requirements for OTA updates. There are studies on the UDS standard for AD, but the emerging SOVD standard, which is essential for future connected cars, needs further investigation in terms of security with formal methods. The same applies to the OEM backend infrastructure, the connection and communication with it and PKI implementations require further investigation in terms of security with formal methods.

Our survey has revealed that while the use of formal methods in the domain of AD security is established, there are significant gaps in validation by and application of these methods. Future research should address these gaps and aim

for a more comprehensive approach that extends beyond the currently narrowly focused segments, individual protocols, and subsystems.

In the course of the discussion in Sect. 6, we identified four *open issues* (OI). **OI1** concerns the benefits of extending the use of formal methods to the entire ECU lifecycle. **OI2** addresses the feasibility and advantages of extending the use of formal methods from an isolated component or protocol to the entire vehicle. **OI3** refers to the selection of the most urgent field for validation using formal methods. **OI4** addresses the potential added value of including formal proofs in automotive standards and the necessary steps to achieve this. **OI5** focuses both on the evaluation of methods for their effectiveness in finding and fixing vulnerabilities, and the comparison of different approaches based on their specific characteristics.

In future work we plan to expand this literature survey further and include exploring the coherences between scientific domains, thematic areas, and the tools and approaches used. In addition to the present grouping, an alternative clustering based on frameworks and tools was created during the survey preparation process, which would also be worth to investigate further. Finally, we intend to address the current areas of AD security that have not been formally verified yet. An obvious first target could be the SOVD standard.

Acknowledgments. This study was funded by Mercedes-Benz Tech Innovation GmbH (As part of the doctoral student position of Julius Figge).

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article. All authors are employees of Mercedes-Benz Tech Innovation GmbH.

References

1. Altinger, H., Wotawa, F., Schurius, M.: Testing methods used in the automotive industry: Results from a survey. In: JAMAICA@ISSTA 2014. pp. 1–6. ACM, San Jose CA USA (Jul 2014). https://doi.org/10.1145/2631890.2631891
2. Apvrille, L.: SysML-sec: A sysML environment for the design and development of secure embedded systems. In: APCOSEC 2013. Yokohama (Aug 2013)
3. ASAM e.V.: Asam Sovd Service-Oriented Vehicle Diagnostics (Jun 2022)
4. AUTOSAR GbR: Specification of Cryptography (Nov 2023)
5. Bahig, G., El-Kadi, A.: Formal Verification Framework for Automotive UML Designs. In: AMECSE '16. pp. 21–27. ACM, Cairo Egypt (May 2016). https://doi.org/10.1145/2944165.2944169
6. Basin, D.: The Cyber Security Body of Knowledge v1.1.0. University of Bristol (2021)
7. Becker, M., Meyer, R., Runge, T., Schaefer, I., Van Der Wall, S., Wolff, S.: Model-Based Fault Classification for Automotive Software. Programming Languages and Systems **13658**, 110–131 (Nov 2022). https://doi.org/10.1007/978-3-031-21037-2_6

8. Bojjagani, S., Reddy, Y.C.A.P., Anuradha, T., Rao, P.V.V., Reddy, B.R., Khan, M.K.: Secure Authentication and Key Management Protocol for Deployment of Internet of Vehicles (IoV) Concerning Intelligent Transport Systems. IEEE Trans. Intell. Transport. Syst. **23**(12), 24698–24713 (Dec 2022). https://doi.org/10.1109/TITS.2022.3207593
9. Carlson, B.: The Rise and Evolution of Gateways and Vehicle Network Processing (Jul 2019)
10. Chen, C.M., Miao, Q., Kumar, S., Wu, T.Y.: Privacy-preserving authentication scheme for digital twin-enabled autonomous vehicle environments. Trans Emerging Tel Tech **34**(11), e4751 (Nov 2023). https://doi.org/10.1002/ett.4751
11. Cimatti, A., Corfini, S., Cristoforetti, L., Di Natale, M., Griggio, A., Puri, S., Tonetta, S.: A comprehensive framework for the analysis of automotive systems. Proceedings of the 25th International Conference on Model Driven Engineering Languages and Systems pp. 379–389 (Oct 2022). https://doi.org/10.1145/3550355.3552408
12. Dijkstra, E.W.: E.W. Dijkstra Archive: On the reliability of programs. (EWD303). https://www.cs.utexas.edu/~EWD/transcriptions/EWD03xx/EWD303.html (Jun 2005)
13. dos Santos, E., Schoop, D., Simpson, A.: Formal models for automotive systems and vehicular networks: Benefits and challenges. In: 2016 IEEE Vehicular Networking Conference (VNC). pp. 1–8 (Dec 2016). https://doi.org/10.1109/VNC.2016.7835940
14. Dürrwang, J., Sommer, F., Kriesten, R.: Automation in Automotive Security by Using Attacker Privileges. In: ESCAR 2021 Europe. Frankfurt, Germany (Nov 2021)
15. Feng, T., Zheng, L., Xie, P.S.: Formal Security Evaluation and Research of Automotive CAN Protocol Based on CPN. IJNS **24**(2), 352–363 (Mar 2022). https://doi.org/10.6633/IJNS.202203_24(2).18
16. Gürgens, S., Lahr, N., Zelle, D.: On Formal Security Analysis of Automotive Systems. In: ESCAR 2017. Berlin, Germany (Nov 2017)
17. Heneghan, J., Shaikh, S.A., Bryans, J., Cheah, M., Wooderson, P.: Enabling Security Checking of Automotive ECUs with Formal CSP Models. 2019 49th Annual IEEE/IFIP DSN-W pp. 90–97 (Jun 2019). https://doi.org/10.1109/DSN-W.2019.00025
18. Huelsewies, M.: Transformation in Products (Jul 2021)
19. Jahandideh, I., Ghassemi, F., Sirjani, M.: Hybrid Rebeca: Modeling and Analyzing of Cyber-Physical Systems. Cyber Physical Systems. Model-Based Design **11615**, 3–27 (Jul 2019). https://doi.org/10.1007/978-3-030-23703-5_1
20. Karray, K., Danger, J.L., Guilley, S., Abdelaziz Elaabid, M.: Attack Tree Construction and Its Application to the Connected Vehicle. In: Koç, Ç.K. (ed.) Cyber-Physical Systems Security. pp. 175–190. Springer International Publishing, Cham (Dec 2018). https://doi.org/10.1007/978-3-319-98935-8_9
21. Kim, J.H., Jo, H.J., Lee, I.: Model Checking Resiliency and Sustainability of In-Vehicle Network for Real-Time Authenticity. Applied Sciences **11**(3), 1068 (Jan 2021). https://doi.org/10.3390/app11031068
22. Kim, K., Kim, J.S., Jeong, S., Park, J.H., Kim, H.K.: Cybersecurity for autonomous vehicles: Review of attacks and defense. Computers & Security **103**, 102150 (Apr 2021). https://doi.org/10.1016/j.cose.2020.102150
23. Kirk, R., Nguyen, H.N., Bryans, J., Shaikh, S., Evans, D., Price, D.: Formalising UPTANE in CSP for Security Testing. 2021 IEEE 21st QRS-C pp. 816–824 (Dec 2021). https://doi.org/10.1109/QRS-C55045.2021.00124

24. Kleberger, P., Moulin, G.: Short paper: Formal verification of an authorization protocol for remote vehicle diagnostics. In: 2013 IEEE VNC. pp. 202–205 (Dec 2013). https://doi.org/10.1109/VNC.2013.6737613
25. Krichen, M.: Formal Methods and Validation Techniques for Ensuring Automotive Systems Security. Information **14**(12), 666 (Dec 2023). https://doi.org/10.3390/info14120666
26. Lampe, B., Meng, W.: Can-logic: Automotive Intrusion Detection via Temporal Logic. In: IOT 2023. pp. 113–120. ACM, Nagoya Japan (Nov 2023). https://doi.org/10.1145/3627050.3627059
27. Lauser, T., Krauß, C.: Formal Security Analysis of Vehicle Diagnostic Protocols. ARES 2023 pp. 1–11 (Aug 2023). https://doi.org/10.1145/3600160.3600184
28. Lauser, T., Zelle, D., Krauß, C.: Security Analysis of Automotive Protocols. Computer Science in Cars Symposium pp. 1–12 (Dec 2020). https://doi.org/10.1145/3385958.3430482
29. Lee, J., Kim, G., Das, A.K., Park, Y.: Secure and Efficient Honey List-Based Authentication Protocol for Vehicular Ad Hoc Networks. IEEE Trans. Netw. Sci. Eng. **8**(3), 2412–2425 (Jul 2021). https://doi.org/10.1109/TNSE.2021.3093435
30. Lenard, T., Genge, B., Collen, A., Nijdam, N.A.: LOKI-2: An Improved Lightweight Cryptographic Key Distribution Protocol for Automotive Systems. 2023 IEEE 19th ICCP pp. 187–194 (Oct 2023). https://doi.org/10.1109/ICCP60212.2023.10398644
31. Luo, F., Jiang, Y., Wang, J., Li, Z., Zhang, X.: A Framework for Cybersecurity Requirements Management in the Automotive Domain. Sensors **23**(10), 4979 (May 2023). https://doi.org/10.3390/s23104979
32. Mansor, H., Markantonakis, K., Akram, R.N., Mayes, K.: Let's Get Mobile: Secure FOTA for Automotive System. In: Qiu, M., Xu, S., Yung, M., Zhang, H. (eds.) Network and System Security. vol. 9408, pp. 503–510. Springer International Publishing, Cham (Nov 2015). https://doi.org/10.1007/978-3-319-25645-0_38
33. Marksteiner, S.F., Schmittner, C., Christl, K., Nickovic, D., Sjödin, M., Sirjani, M.: From TARA to Test: Automated Automotive Cybersecurity Test Generation Out of Threat Modeling. In: 7th CSCS. pp. 1–10. ACM, Darmstadt Germany (Dec 2023). https://doi.org/10.1145/3631204.3631864
34. Mukherjee, A., Gerdes, R., Chantem, T.: Trusted Verification of Over-the-Air (OTA) Secure Software Updates on COTS Embedded Systems. AutoSec 2021 (Feb 2021). https://doi.org/10.14722/autosec.2021.23028
35. Mundhenk, P., Paverd, A.J., Mrowca, A., Steinhorst, S., Lukasiewycz, M., Fahmy, S.A., Chakraborty, S.: System Level Design Approaches to Security in Automotive Networks. TODAES (Mar 2017)
36. Mundhenk, P., Steinhorst, S., Lukasiewycz, M., Fahmy, S.A., Chakraborty, S.: Security analysis of automotive architectures using probabilistic model checking. 52nd DAC pp. 1–6 (Jun 2015). https://doi.org/10.1145/2744769.2744906
37. Palaniswamy, B., Ansari, K., Reddy, A.G., Das, A.K., Shetty, S.: Robust Certificateless Authentication Protocol for the SAE J1939 Commercial Vehicles Bus. IEEE Trans. Veh. Technol. **72**(4), 4493–4509 (Apr 2023). https://doi.org/10.1109/TVT.2022.3227281
38. Pedroza, G.: Assisting the Design of Secured Applications for Embedded Systems. (Conception Assistée Des Logiciels Sécurisés Pour Les Systèmes Embarqués). Ph.D. thesis, TELECOM ParisTech, Paris, France (Jan 2013)
39. Pedroza, G., Apvrille, L., Knorreck, D.: AVATAR: A SysML Environment for the Formal Verification of Safety and Security Properties. 2011 11th NOTERE pp. 1–10 (May 2011). https://doi.org/10.1109/NOTERE.2011.5957992

40. Pedroza, G., Idrees, M.S., Apvrille, L., Roudier, Y.: A Formal Methodology Applied to Secure Over-the-Air Automotive Applications. 2011 IEEE VTC Fall pp. 1–5 (Sep 2011). https://doi.org/10.1109/VETECF.2011.6093061
41. Pekaric, I., Sauerwein, C., Felderer, M.: Applying Security Testing Techniques to Automotive Engineering. In: ARES 2019. pp. 1–10 (Aug 2019). https://doi.org/10.1145/3339252.3340329
42. Püllen, D., Frank, F., Christl, M., Liu, W., Katzenbeisser, S.: A Security Process for the Automotive Service-Oriented Software Architecture. IEEE Trans. Veh. Technol. **73**(4), 5036–5053 (Apr 2024). https://doi.org/10.1109/TVT.2023.3333397
43. Seo, J., Kwak, J., Kim, S.: Formally Verified Software Update Management System in Automotive. VehicleSec 2023 (2023). https://doi.org/10.14722/vehiclesec.2023.23087
44. Sommer, F., Kriesten, R., Kargl, F.: Survey of Model-Based Security Testing Approaches in the Automotive Domain. IEEE Access **11**, 55474–55514 (Jun 2023). https://doi.org/10.1109/ACCESS.2023.3282176
45. Sun, X., Yu, F.R., Zhang, P.: A Survey on Cyber-Security of Connected and Autonomous Vehicles (CAVs). IEEE T-ITS **23**(7), 6240–6259 (Jul 2022). https://doi.org/10.1109/TITS.2021.3085297
46. Syriani, E., David, I., Kumar, G.: Screening articles for systematic reviews with ChatGPT. Journal of Computer Languages **80**, 101287 (Aug 2024). https://doi.org/10.1016/j.cola.2024.101287
47. Ter Beek, M.H., Gnesi, S., Knapp, A.: Formal methods and automated verification of critical systems. Int J Softw Tools Technol Transfer **20**(4), 355–358 (Aug 2018). https://doi.org/10.1007/s10009-018-0494-5
48. Tischer, M.: The Computing Center in the Vehicle AUTOSAR Adaptive. Vector Informatik GmbH (Sep 2018)
49. Trinh, L.K., Chiba, Y., Aoki, T.: Formalization and Verification of AUTOSAR OS Standard's Memory Protection. 2018 TASE pp. 68–75 (Aug 2018). https://doi.org/10.1109/TASE.2018.00017
50. Wang, Z., Wang, H., Wang, Y., Yang, X.: CLASRM: A Lightweight and Secure Certificateless Aggregate Signature Scheme with Revocation Mechanism for 5G-Enabled Vehicular Networks. Wireless Communications and Mobile Computing **2022**, 1–20 (Apr 2022). https://doi.org/10.1155/2022/3646960
51. Webster, J., Watson, R.: Analyzing the Past to Prepare for the Future: Writing a Literature Review. MIS Q. (Jun 2002)
52. Zelle, D., Lauser, T., Kern, D., Krauß, C.: Analyzing and Securing SOME/IP Automotive Services with Formal and Practical Methods. In: ARES 2021. pp. 1–20. ARES '21, ACM, New York, NY, USA (Aug 2021). https://doi.org/10.1145/3465481.3465748