smart cities

MDPI

Systematic Review

Threat Modeling and Attacks on Digital Twins of Vehicles: A Systematic Literature Review

Uzair Muzamil Shah [1], Daud Mustafa Minhas [2], Kashif Kifayat [3], Khizar Ali Shah [1] and Georg Frey [4,*]

[1] Department of Cyber Security, Air University, Islamabad 44230, Pakistan; uzairshaaa9@gmail.com (U.M.S.); 231358@students.au.edu.pk (K.A.S.)
[2] Industrial Security Lab, ZeMA—Center for Mechatronics and Automation Technology, D-66121 Saarbrücken, Germany; daud.minhas@zema.de
[3] College of Computing and Intelligent Systems, University of Khorfakkan, Sharjah 18119, United Arab Emirates
[4] Automation and Energy Systems, Saarland University, D-66123 Saarbrücken, Germany
* Correspondence: georg.frey@aut.uni-saarland.de

Highlights

What are the main findings?

- This paper conducts an in-depth review of 23 studies on threat modeling and security testing in automotive digital twins using the PRISMA framework.
- It identifies deficiencies and proposes improved methodologies to enhance current security and safety validation practices for interconnected automotive systems.

What is the implication of the main finding?

- This paper highlights the need for more advanced threat modeling and emphasizes the importance of improving cybersecurity to prevent potential attacks on connected vehicles.
- It suggests future research and practical strategies for secure digital twin system design in the automotive sector, supporting the development of resilient smart urban environments through a robust interconnected vehicle security framework.

Academic Editor: Pierluigi Siano

Received: 7 April 2025
Revised: 9 July 2025
Accepted: 13 July 2025
Published: 28 August 2025

Citation: Shah, U.M.; Minhas, D.M.; Kifayat, K.; Shah, K.A.; Frey, G. Threat Modeling and Attacks on Digital Twins of Vehicles: A Systematic Literature Review. *Smart Cities* **2025**, *8*, 142. https://doi.org/10.3390/smartcities8050142

Abstract

This systematic literature review pioneers the synthesis of cybersecurity challenges for automotive digital twins (DTs), a critical yet underexplored frontier in connected vehicle security. The notion of digital twins, which act as simulated counterparts to real-world systems, is revolutionizing secure system design within the automotive sector. As contemporary vehicles become more dependent on interconnected electronic systems, the likelihood of cyber threats is escalating. This comprehensive literature review seeks to analyze existing research on threat modeling and security testing in automotive digital twins, aiming to pinpoint emerging patterns, evaluate current approaches, and identify future research avenues. Guided by the PRISMA framework, we rigorously analyze 23 studies from 882 publications to address three research questions: (1) How are threats to automotive DTs identified and assessed? (2) What methodologies drive threat modeling? Lastly, (3) what techniques validate threat models and simulate attacks? The novelty of this study lies in its structured classification of digital twin types (physics based, data driven, hybrid), its inclusion of a groundbreaking threat taxonomy across architectural layers (e.g., ECU tampering, CAN-Bus spoofing), the integration of the 5C taxonomy with layered architectures for DT security testing, and its analysis of domain-specific tools such as VehicleLang and embedded intrusion detection systems. The findings expose significant deficiencies in

the strength and validation of threat models, highlighting the necessity for more adaptable and comprehensive testing methods. By exposing gaps in scalability, trust, and safety, and proposing actionable solutions aligned with UNECE R155, this SLR delivers a robust framework to advance secure DT development, empowering researchers and industry to fortify vehicle resilience against evolving cyber threats.

Keywords: cybersecurity; automotive security; attack surface; risk assessment; risk analysis

1. Introduction

Contemporary automobiles are increasingly reliant on sophisticated electronic control systems and vehicle-to-everything (V2X) communication technologies. While these systems enhance automation, safety, and performance, they simultaneously introduce new cybersecurity vulnerabilities. Typical attack vectors include unauthorized access to electronic control units (ECUs), spoofing of sensor data, and malicious manipulation of in-vehicle networks [1]. As a result, proactive threat modeling has become an essential strategy in identifying and mitigating such risks.

One promising approach to address these challenges is the application of digital twin (DT) technology: virtual replicas of physical systems that enable simulation, monitoring, and behavior analysis. In the automotive domain, digital twins can be leveraged to test attack scenarios, evaluate defensive mechanisms, and validate system robustness without endangering actual vehicles. Despite their growing adoption across industries, the use of digital twins for structured threat modeling and cyberattack simulation remains underexplored, particularly in vehicular contexts.

This systematic literature review (SLR), guided by the PRISMA framework, synthesizes cybersecurity challenges for automotive digital twins (DTs), a critical frontier in connected vehicle security. Addressing RQ1-RQ3 (discussed in detail in Section 7.3), we analyze 23 studies to deliver a novel threat taxonomy across architectural layers (e.g., ECU tampering, CAN-Bus spoofing) and integrate the 5C taxonomy for security testing. By exposing gaps in scalability, trust, and safety, and aligning with UNECE R155, this SLR provides a robust framework to advance secure DT development. This SLR is focused on three central research questions: (1) How can threats to automotive digital twins be identified and evaluated? (2) What methodologies are currently employed for threat modeling regarding vehicle digital twins? Lastly, (3) what are the most effective techniques for validating threat models and examining attacks? By synthesizing findings from high-quality studies selected from an initial pool of 882, this review identifies critical research gaps, classifies modeling approaches, and provides structured recommendations to advance secure digital twin development in the automotive sector. The following key insights summarize the major contributions and findings of this study:

- Clarification of Digital Twin Definitions: The review consolidates different interpretations of digital twins present in existing research, classifying them into physics-based, data-driven, and hybrid models. This differentiation lays the groundwork for the analysis and findings of the review [2,3].
- Overview of Digital Twin Implementations: The review highlights the extensive use of digital twins across various sectors, particularly in automotive applications, stressing the significance of threat modeling within this context and identifying existing platforms that support automotive digital twins [4].
- Identification of Passive Security Testing Techniques: A considerable portion of the review is focused on passive testing techniques within digital twins, offering a thor-

ough examination of security challenges that are unique to passive testing in vehicular systems [5].

- Identification of Security Gaps: This review points out multiple security vulnerabilities present in current digital twin applications, providing direction for future research and development aimed at enhancing the security stance of automotive digital twins [6,7].
- Mitigation Recommendations: Drawing from the findings, the review proposes actions to tackle the identified security issues, such as adopting proactive defense strategies, ensuring data privacy, and following best practices for secure deployment [8].

Methodology of Review

To ensure a comprehensive and reproducible literature review, a systematic search and selection protocol was applied, guided by the PRISMA framework. The methodology followed these key steps:

- **Databases:** The search was carried out in three major academic databases: IEEE Xplore, ACM Digital Library, and ScienceDirect. These databases were selected for their wide coverage of peer-reviewed literature in cybersecurity, digital twin, and automotive systems.
- **Keywords:** Search queries used Boolean combinations of relevant terms, such as "digital twin", "cybersecurity", "smart city", "vehicular systems", "automotive", and "threat modeling". The complete Boolean query used across databases was as follows:

  ```
  (''Threat modeling'' OR ''Security analysis'' OR ''Vulnerability assessment'') AND (''Digital Twin'') AND (''Vehicle'' OR ''Automotive'') AND (''Attack'' OR ''Cyberattack'' OR ''Cybersecurity'' OR ''Security threat'')
  ```

  This formulation is also illustrated in Section 6
- **Timeframe:** Publications from January 2015 to February 2024 were considered, with a particular emphasis on works from the last five years (2019–2024) to capture recent developments.
- **Inclusion Criteria:** Only peer-reviewed journal articles, conference proceedings, authoritative standards (e.g., ISO, NIST) and relevant white papers were included. Exclusion criteria included duplicate entries, non-English papers, non-peer-reviewed publications, and inaccessible full texts.
- **Gray Literature:** Although gray literature sources (e.g., industrial tools, expert opinions) were briefly reviewed for contextual understanding, they were excluded from the final analysis due to a lack of methodological rigor and relevance to the research questions.
- **Classification Process:** Selected papers were categorized according to their domain (vehicular, smart city, industrial), architectural layers (physical, communication, application, security) and cybersecurity focus (threat modeling, simulation, validation). An inductive thematic coding approach was applied to extract recurring themes and identify knowledge gaps.
- **Selection Summary:** An initial pool of 854 publications was reduced to 20 high-quality articles after applying inclusion/exclusion criteria, keyword filtering, abstract screening, snowballing and full-text analysis. Details are presented in Section 6.2.4.

2. In-Vehicle Digital Systems: A Testing Challenge

As time has progressed, embedded systems within vehicles have evolved to become more advanced, providing users with innovative features and improved functionalities. However, with the increasing complexity of these systems comes the challenge of conducting effective testing. These systems are required to perform reliably in ever-changing

environments and under diverse conditions. Additionally, since many of these systems are critical to safety, thorough testing is vital to confirm their proper operation. The process of testing and debugging is further complicated by the significant integration of hardware elements and software components. This section explores different cyber systems found in vehicles and highlights the importance of cybersecurity testing in relation to vehicular digital twins.

2.1. Defining Vehicular Cyber Systems

Contemporary vehicles, encompassing cars, trucks, and buses, are integrated with sophisticated electronic and computing systems, described in Figure 1, referred to as "vehicular cyber systems" [9]. These systems consist of a range of electronic elements, including sensors, controllers, communication networks, and software, which together oversee numerous operational functions of a vehicle. As vehicles evolve and become increasingly interconnected, the significance of vehicular cyber systems has grown. Beyond providing safety and entertainment features for both drivers and passengers, these systems are responsible for managing essential functions such as engine performance, braking, steering, and suspension.

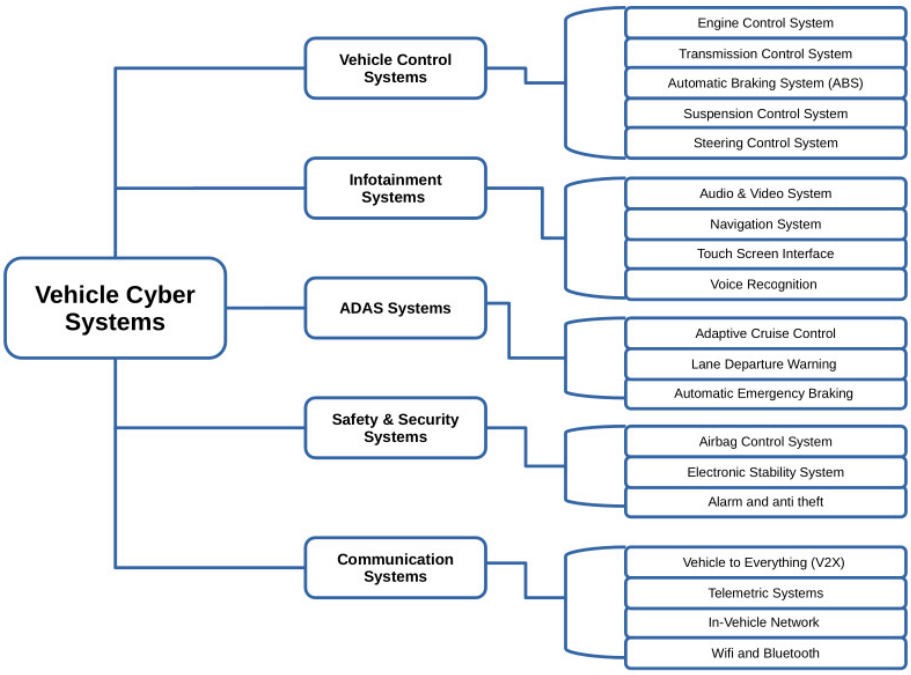

Figure 1. Vehicle cyber automation system.

To enhance the comprehension of in-vehicle systems, we employed a 5C taxonomy that is utilized in automotive system design. This taxonomy serves as a general classification for vehicular units undergoing testing. The automotive industry can be classified into 5C tiers, which are structured around the development processes for complex systems, as illustrated in Figure 2.

This framework presents multiple levels of automotive systems design grounded in the 5C classification, beginning with the fundamental concept layer. It offers a systematic methodology for the creation of intricate automotive systems, guaranteeing that all elements are comprehensively evaluated and managed. This approach has effectively supported the advancement of a variety of automotive technologies, such as advanced driver assistance systems, electric drive trains, and autonomous vehicles.

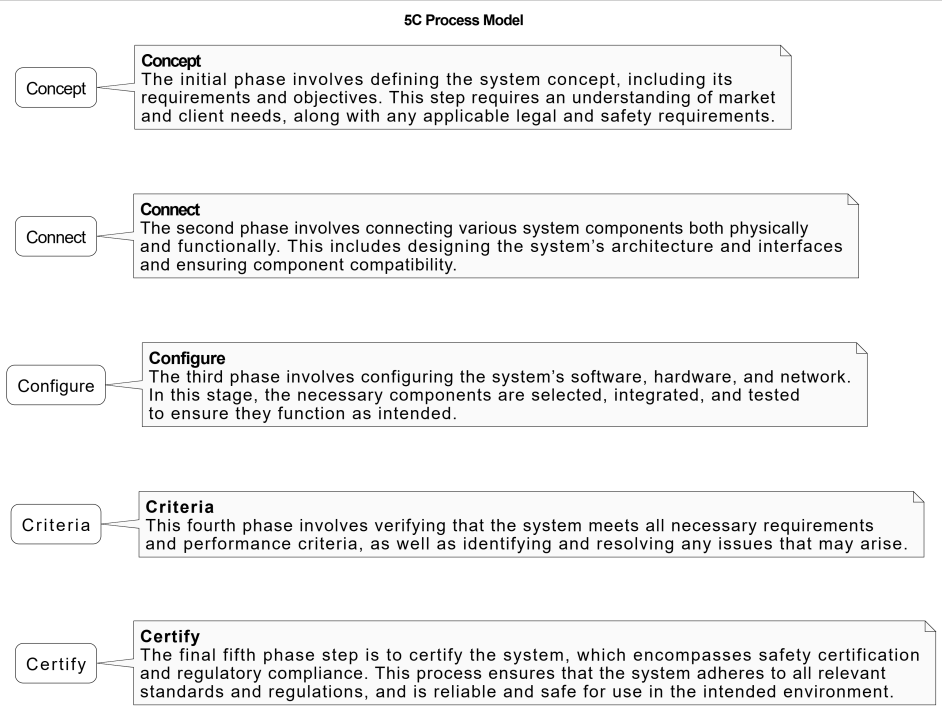

Figure 2. Taxonomy levels of automotive system engineering.

2.2. Cybersecurity Testing

In the past decade, the cyber technologies embedded in vehicles have grown substantially. Although these systems offer numerous functions and benefits, they also present substantial risks related to cyber threats. Therefore, conducting comprehensive security assessments of cyber systems in vehicles is crucial to identify and address possible vulnerabilities [9].

An essential aspect of security testing for cyber systems within vehicles is threat modeling [5]. This process identifies possible threats and weaknesses in the defense mechanism of the system, assessing their impact on overall security. Utilizing this approach, it becomes easier to comprehend the security requirements of the system and to formulate an effective security testing strategy. Through threat modeling, developers can identify potential attack vectors that malicious actors may use to leverage system loopholes.

Penetration testing can be employed to evaluate the security of in-vehicle cyber systems. This method involves simulating a cyber-attack to identify potential vulnerabilities and assess the system's resilience against such threats. By utilizing this testing approach, weaknesses within the system can be detected and subsequently fortified. The results obtained from penetration testing inform the implementation of security measures designed to protect against cyberattacks.

Several security testing methods can be employed in addition to penetration testing to evaluate in-vehicle cyber systems. Fuzz testing, for example, involves inputting random data into the system to find potential security holes. Another technique for examining the system's code to find potential security flaws is code review. Below are a few examples of the various security testing of automotive systems:

- **Penetration Testing:** This simulates a cyber-attack on the car to find any potential holes and gauge how well the system can fend off threats.
- **Fuzz Testing:** Sending random data to a vehicle's systems is known as "fuzz testing", which aims to find any potential flaws and gauge how the system handles unexpected inputs.

- **Code Review:** Reviewing the vehicle's source code to look for any security flaws such as buffer overflows or SQL injection vulnerabilities is known as a "code review".
- **Vulnerability Scanning:** Vulnerability scanning entails looking for known weaknesses in vehicle systems using automated technologies.
- **Wireless Security Testing:** Testing the security of the vehicle's wireless network, which includes Wi-Fi, Bluetooth, and cellular connections, is known as wireless network security testing.
- **Physical Security Testing:** Testing the vehicle's physical security, including its locks, alarms, and anti-theft equipment, is known as physical security testing.
- **User interface testing:** This examines the safety of the information system and other components of the user interface in the car to find any potential security holes or vulnerabilities.
- **Threat modeling:** This is the process to identify possible threats and vulnerabilities that the vehicle may encounter and to assess how they may affect vehicle security.
- Hardware-in-the-Loop Testing: This is worth mentioning because it is a similar step of digital twin testing. ECU's that manage different vehicular operations, including cybersecurity-related systems, are tested using a technique called hardware in the loop (HIL). HIL testing is crucial for ensuring that vehicle's cybersecurity systems work properly and can detect and respond to cyberattacks in the context of automotive cybersecurity. HIL testing involves coupling the ECU to a simulation environment that resembles the actual driving environment in which the car will function [9]. The ECU can interact with the simulated vehicle environment in the same way as in the actual world thanks to a variety of inputs that can be included in this simulation environment, including sensors, actuators, and communication networks [9]. HIL testing is particularly crucial in the domain of automotive cybersecurity for testing the cybersecurity systems created to recognize and react to cyberattacks. Firewalls, intrusion detection systems, and other security measures might be a part of these systems. HIL testing can assist in locating any flaws or vulnerabilities in the cybersecurity systems and ensuring that they are operating properly by simulating actual cyber-attacks on the vehicle's systems.

While hardware-in-the-loop testing offers a simulation-based evaluation of ECU behavior, digital twin technology extends this paradigm by integrating real-time data, system modeling, and cyber-physical interactions across the entire vehicle ecosystem. Within this context, the 5C taxonomy and layered architecture serve as foundational frameworks for structuring digital twin-based security testing. The *Concept* and *Connect* stages of the 5C model support early-phase threat identification and risk assessment, addressing the objectives outlined in RQ1 established in Section 6.1. The *Configure* and *Validate* stages facilitate the simulation and testing of attack scenarios, aligning with RQ2. The layered architecture comprising the *Physical*, *Communication*, *Application*, *Data*, and *Security* layers enables a systematic mapping of threats to specific system domains and supports security validation across multiple abstraction levels, directly contributing to RQ3. This layered modeling approach aligns with broader CPS security frameworks [10,11] adopted in smart urban systems [12]. Together, these models enhance the precision and depth of automotive cybersecurity assessments performed through digital twin frameworks [13].

2.3. Role of Standards: UNECE R155 and Digital Twin Security Protocols

The United Nations Economic Commission for Europe (UNECE) Regulation No. 155 (R155) [14] defines the mandatory requirements for cybersecurity management systems (CSMS) in the automotive sector. It compels manufacturers to systematically identify, assess, and mitigate cybersecurity risks across the entire vehicle lifecycle. Digital twin

technology is increasingly recognized as a key enabler for achieving R155 compliance, offering capabilities for continuous threat modeling, safe simulation of attack scenarios, and validation of cybersecurity controls in a virtualized environment without compromising physical systems.

Specifically, digital twin platforms can support the following compliance efforts, referred to Table 1:

- Simulating CSMS audit trails to meet Article 6.2 of R155 [14].
- Validating secure software update mechanisms and over-the-air (OTA) protocols, as required by Annex 5. of Article 6.
- Testing and monitoring detection mechanisms across all R155-defined threat categories, including emerging threats.
- Enabling continuous vulnerability assessment and incident response, in alignment with Article 7.
- Modeling supply chain risks and third-party components, fulfilling the expectations of Annex 8 of Article 7.

Table 1. UNECE R155 Compliance via DT Security Protocols.

UNECE R155 Ref. [14]	Requirement	DT Application	Example	RQ Alignment
Article 6.2	CSMS Audits	Simulate ECU integrity checks	Tampering detection	RQ3: Attack simulation
Annex 5	Secure Updates	Validate OTA protocols	Secure software updates	RQ3: Attack simulation
Article 7	Continuous Monitoring	Real-time threat detection and vulnerability management	CAN-Bus spoofing detection	RQ1: Threat identification
Annex 8	Supply Chain Risk Assessment	Model third-party and V2X vulnerabilities	STRIDE analysis for supplier components	RQ2: Threat modeling

Despite their potential, most current digital twin implementations only address a subset of the compliance areas summarized in Table 1. Notable gaps remain in persistent threat monitoring, secure software update validation, and comprehensive supply chain security modeling. Bridging these limitations is essential not only for fulfilling regulatory obligations under UNECE R155 but also for aligning digital twin frameworks with practical cybersecurity assurance protocols and the objectives set out in research questions RQ2 and RQ3.

3. Digital Twin: A New Era of Automotive Security Testing

Digital twin technology has introduced a new dimension to automotive security testing. These virtual models replicate vehicle system behaviors using sensor and environment data. They allow engineers to evaluate cybersecurity defenses and test various scenarios in a risk-free environment. This facilitates early detection of vulnerabilities and supports the design of more resilient security solutions before deployment in real vehicles.

3.1. Definition of Digital Twin

It is essential to accurately define the concept of a digital twin in order to conduct a structured and systematic analysis of the topic. Having a clear definition of a digital twin is necessary to ensure that the literature reviewed is relevant and aligned with the research objectives. A digital twin, which is a virtual representation of a physical system or process, replicates its physical and functional attributes and can be utilized for various purposes, such as design, simulation, optimization, and maintenance [15,16]. A digital twin serves as a virtual model of a physical system that allows for the reproduction and forecasting of the operation, maintenance, and behavior of the physical entity while also capturing its dynamic interactions with the surrounding environment [4].

The behavior, performance, and state of a physical system can be anticipated and assessed through a digital twin [17], which serves as a comprehensive, multi-domain model that enables optimization and enhancement of the system throughout its lifecycle [18].

A digital twin refers to a virtual representation of a physical object or system that facilitates data-driven modeling, analysis, and simulation to enhance the operation, maintenance, and effectiveness of the actual entity [5]. To maintain focus and precision in the systematic literature review, it is beneficial to establish clear criteria for including or excluding aspects of the digital twin concept. Digital twins utilize real-time data to model and examine the physical behavior, performance, and condition of a tangible entity, system, or process that correlates with its real-world counterpart [19]. Foundational works on smart city CPS design [10] also emphasize the use of digital twins as instruments of predictive control and situational awareness across multiple domains [20].

In [21], the authors examined the various definitions of digital twins and assessed their level of ambiguity [22]. In the remainder of this review, we will concentrate on the definition of a digital twin presented in this research [19]. According to their functional outputs, digital twins can be categorized into five distinct types:

- Simulation-Based Digital Twins: These digital twins simulate a physical system or process's behavior, functionality, and interactions using physics-based models. They can be used to forecast how a physical system or process will operate under various circumstances [23].
- Data-driven Digital Twin: To predict the behavior and effectiveness of a physical system or process, digital twin evaluate and interpret real-time data from sensors and other data sources using data analytics and machine learning methods. They can be applied to process optimization, quality assurance, and predictive maintenance.
- Hybrid Digital Twin: Hybrid digital twins combine the advantages of simulation-based and data-driven digital twins to precisely and fully capture a physical system or process [24]. In addition to simulating complex, multi-domain systems and processes, they can be used to merge various types of data and models.
- Analytical-Digital Twin: These types of digital twins assess and improve the functionality and behaviors of a physical system or process using mathematical models and algorithms. In complex systems, they can be applied for decision-making, control, and optimization [25].
- Control-Based Digital Twin: The behavior and efficiency of a physical system or process are regulated and optimized by these digital twins via real-time feedback control and monitoring [26]. They can be applied to the closed-loop optimization and control of dynamic systems.

Each type of digital twin presents distinct advantages and limitations when applied to threat modeling and attack simulation in the automotive domain. Simulation-based digital twins, which rely on physics-based models, are effective for replicating known system behavior and testing deterministic attack vectors such as sensor spoofing or ECU command

injection. However, they often lack the flexibility to adapt to unforeseen or zero-day attack patterns. Data-driven digital twins, on the other hand, utilize machine learning and real-time data to capture system behavior dynamically. This enables them to detect anomalies and learn from novel threat scenarios, but introduces risks related to data poisoning and interpretability. Hybrid digital twins, which integrate both approaches, offer a more robust framework for security testing by combining model fidelity with real-time adaptability, allowing for comprehensive threat modeling and simulation across multiple attack surfaces. Thus, understanding the functional distinctions among these types is critical for selecting the appropriate digital twin architecture in security-sensitive automotive applications.

Recent advancements in artificial intelligence (AI) and machine learning (ML) have significantly enhanced the capabilities of data-driven and hybrid digital twins in security contexts. AI/ML techniques allow digital twins to detect zero-day attacks, learn evolving threat behaviors, and adapt to complex cyber-physical scenarios in real. As detailed in recent surveys [27,28], the integration of AI enables anomaly detection, predictive threat modeling, and more resilient simulations. These contributions reinforce the need to incorporate intelligent digital twins into security validation frameworks for modern vehicles.

While these classifications are widely referenced, their practical implications for automotive cybersecurity particularly in ECU security testing require deeper analysis. Table 2 compares the strengths and limitations of physics-based, data-driven, and hybrid digital twins in the context of ECU threat detection and validation.

Table 2. Comparison of digital twin types for ECU security testing.

Digital Twin Type	Security Testing Characteristics
Physics-Based	Detection of Known Attacks: High. Accurately replicates ECU behavior under defined conditions. Detection of Novel Attacks: Low. Lacks adaptability to emerging threats. Computational Cost: High. Requires detailed system modeling. Adaptability: Low. Rigid and difficult to generalize. Transparency: High. Model logic is interpretable. Data Requirements: Moderate. Primarily specification-based.
Data-Driven	Detection of Known Attacks: Moderate. Matches statistical patterns in past data. Detection of Novel Attacks: High. Uses anomaly detection via ML. Computational Cost: Moderate. Depends on data size and model complexity. Adaptability: High. Easily retrains on new patterns. Transparency: Low. Often opaque (black-box behavior). Data Requirements: High. Requires large, labeled datasets.
Hybrid	Detection of Known Attacks: High. Leverages physics-based accuracy. Detection of Novel Attacks: High. Adds ML adaptability. Computational Cost: High. Combines two modeling paradigms. Adaptability: Moderate. Better than physics only, less than ML. Transparency: Moderate. Mix of logic-based and data-driven behavior. Data Requirements: High. Uses both structured and real-world data.

Physics-based, data-driven, and hybrid digital twins (DTs) exhibit distinct strengths and weaknesses in ECU security testing, addressing RQ1-RQ3 established in Section 6.1. Physics-based DTs, rooted in deterministic models, excel in detecting known ECU command injections with high precision, supporting structured threat modeling with STRIDE (RQ2) and aligning with UNECE R155's deterministic testing requirements. However, their static nature limits adaptability to zero-day attacks (RQ3). Data-driven DTs, leveraging Bayesian networks, enable real-time threat identification (RQ1) by detecting CAN-Bus anomalies, yet face vulnerabilities to data poisoning and noisy inputs, compromising validation

(RQ3). Hybrid DTs integrate deterministic accuracy with adaptive learning, facilitating robust attack simulations for dynamic threats like zero-day attacks (RQ3), though at higher computational cost.

3.2. Digital Twin: A Transformation of Automotive Systems

The integration of cutting-edge technologies like AI, ML, IoT, and digital twins is the main focus of Industry 4.0. This is included in order to improve efficiency and performance. The creation of a secure digital twin solution for automotive systems can be used to simulate physical models, visualize physical systems, and monitor and forecast vehicle behavior. Digital twin technology has significantly enhanced the development and testing of vehicular systems by enabling virtual representations of physical components and behavior [29]. These models allow engineers to simulate a range of operational scenarios in controlled environments, facilitating the identification of vulnerabilities and validation of cybersecurity mechanisms. Recent advancements further introduce autonomous digital twins capable of proactive threat detection and adaptive cyber response, enhancing the resilience of vehicular systems against evolving attack surfaces [30]. Within automotive applications, the 5C framework outlined in Section 2 maps naturally to the digital twin lifecycle and can be interpreted in the following security-focused context:

- Concept: In the context of digital twin in automotive security testing, the idea phase comprises establishing the goals and parameters of the digital twin model, identifying possible security threats and vulnerabilities, and formulating a plan to mitigate them [4,31]. One could think of this phase as threat modeling.
- Connect: To enable real-time testing and monitoring, the connect phase integrates the digital twin model with the actual vehicle system. Installing sensors and other monitoring tools and connecting them to the physical system may be necessary for the digital counterpart [32,33] to achieve this.
- Configure: During the setup stage, the digital twin model is altered to replicate various security situations and possible cyberattacks. To do this, it may be necessary to modify the digital twin model's properties to account for different system configurations and security settings [3].
- Validation: The accuracy and effectiveness of the digital twin in detecting and blocking security threats are tested. This may involve simulating different security situations and comparing the results with empirical data to ensure that the model accurately depicts the behavior of the real system [34,35].

The aforementioned taxonomy provides a high-level overview of the digital twin system for vehicles. The layered design shown in Figure 3, which mimics earlier work, can also be used to explain the vehicle digital twin for attack simulation [36].

- Physical Layer: The vehicle's physical components, including the engine, gearbox, brakes, and other mechanical components, are a part of the physical layer. The installation of sensors and other monitoring devices on the physical system would be required for this layer in order to gather real-time data [37] about the vehicle in the context of a vehicular digital twin for security testing and attack simulation [38,39].
- Communication Layer: The communication layer comprises the interfaces and protocols that allow different components of the automotive system to communicate with one another [40]. In order to facilitate real-time monitoring and testing for attack simulation and security testing, this layer would use the twin model in conjunction with the physical layer [41].
- Application Layer: This layer consists of the software applications and services that run on top of the communication layer. To verify the security of the vehicle system, this layer would involve creating a digital twin model and a variety of attack scenarios [42].

- Data Layer: This layer contains the data that the vehicle system collects and processes [35]. This layer would involve gathering and analyzing data from the physical system and using that data to make sure the digital twin model is accurate [43].
- Security Layer: This layer contains the security procedures and methods that are employed to protect the car system against cyberattacks [44]. This layer will model several types of cyberattacks to assess the security systems' efficacy and identify any possible vulnerabilities in the system [37].

Creating digital twins of vehicles for attack simulation and security testing is a challenging, multi-stage process that requires the fusion of several physical components, software applications, communication protocols, data processing, and security mechanisms. That's why a layered approach is more feasible. Also, this understanding can be used to spot potential research gaps and opportunities for future work. It is important to use vehicular digital twins for attack simulation and security testing to ensure safety and security. This can assist in finding potential flaws and fixing them before cyberattackers can take and use them. Figure 4 Shows different security standards in automotive domain that at some level contribute to vehicle safety.

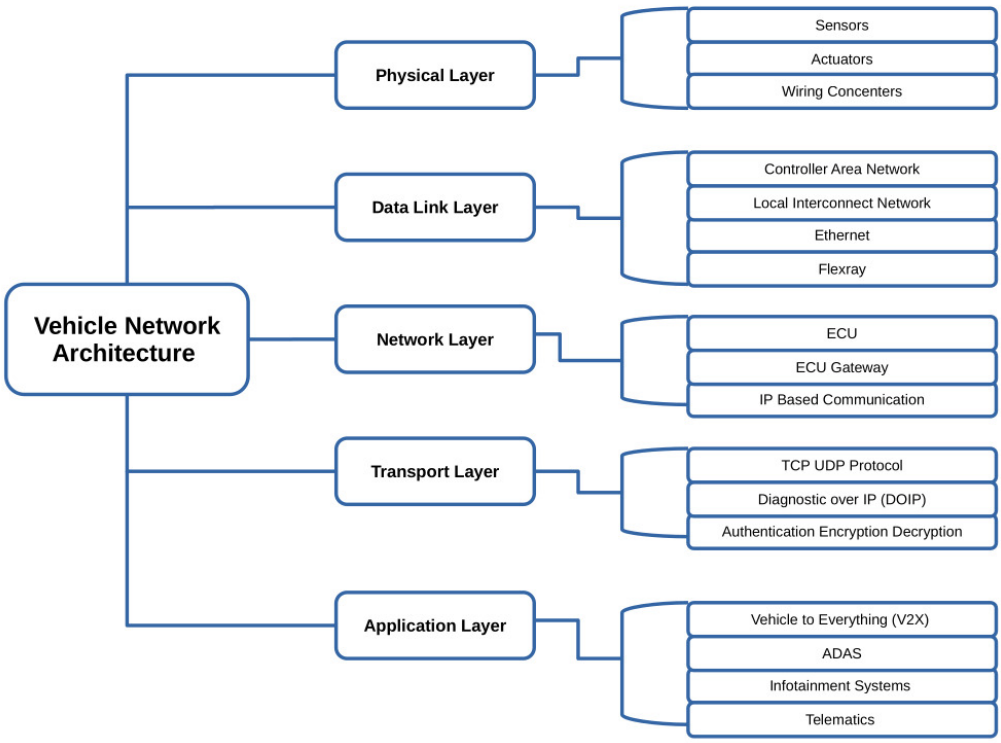

Figure 3. Layered architecture.

Linking 5C Taxonomy and Layered Architecture to DT Security Testing:

The 5C taxonomy (Connection, Conversion, Cyber, Cognition, Configuration) and layered architecture (Physical, Connectivity, DT Data, DT Virtual, Service) provide a structured framework for digital twin (DT) security testing, addressing RQ1–RQ3. The Connection stage, aligned with the Connectivity layer, supports threat identification (RQ1) by testing V2X security with Bayesian-network-based IDS to detect CAN-Bus spoofing. The Cyber stage, paired with the DT Virtual layer [45], enhances threat modeling (RQ2) using STRIDE to mitigate data poisoning risks in virtual DT models. The Cognition stage, linked to the Service layer, drives attack simulations (RQ3) with VehicleLang to validate defenses against zero-day attacks. Configuration, spanning all layers, ensures lifecycle security testing per

UNECE R155, safeguarding ECU firmware updates. Table 3 maps these elements to testing functions, underscoring their role in advancing automotive DT security.

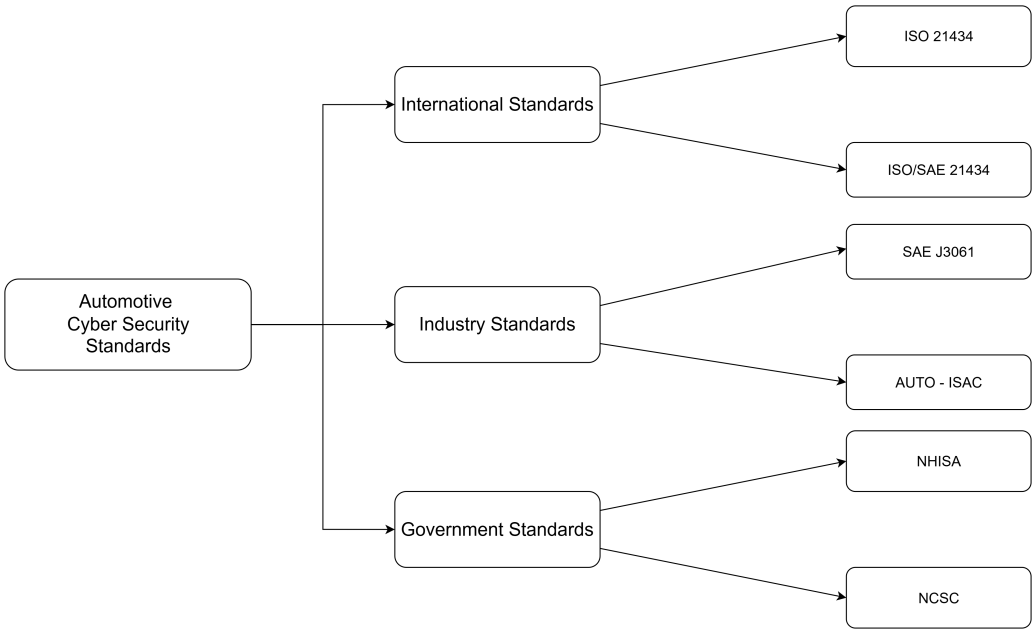

Figure 4. Automotive cybersecurity standards.

Table 3. Mapping of the 5C taxonomy and layered architecture to digital twin security testing and research question alignment.

5C Stage	Layer	Security Testing Function	Example	RQ Alignment
Connection	Connectivity	Threat detection via IDS	CAN-Bus spoofing detection	RQ1: Threat identification
Conversion	DT Data	Data integrity testing	ECU data validation	RQ1: Threat identification
Cyber	DT Virtual	Threat modeling with STRIDE/PASTA	Data poisoning mitigation	RQ2: Threat modeling
Cognition	Service	Attack simulation with VehicleLang	Zero-day attack validation	RQ3: Validation/attack simulation
Configuration	All Layers	Lifecycle security testing	Firmware update security	RQ3: Validation/attack simulation

4. Definitions of Terminologies

Different terms that could be included in the review are mentioned in Table 4.

Table 4. Terminologies used in this work.

Terminology	Explanation
Automotive Systems	A system that incorporates all of a vehicle's parts, both physically and through the software programs that operate on them.
Digital Twin	A digital replica of a physical system in the actual world, used to simulate real-time functioning.

Table 4. *Cont.*

Terminology	Explanation
Attack Simulation	The process of simulating different cyberattacks to test a system's security.
Security Testing	The procedure of testing a system to find and address any security risks and vulnerabilities.
Physical Layer	The section of a car's system that houses its mechanical parts, such as the engine, transmission, and brakes.
Communication Layer	The layer of a vehicle system that contains the interfaces and communication protocols that permit communication between various components.
Application Layer	The portion of a vehicular system that houses the programs and services that operate on top of the communication layer.
Data Layer	The portion of a vehicle system that contains the data that the system has collected and processed.
Security Layer	The portion of a vehicle's system that contains security measures and procedures used to guard against cyberattacks.
Cyberattack	An attempt to exploit a vulnerability in a system to steal, destroy, or gain unauthorized access.
Black-Box Modeling	A modeling strategy where the system is modeled based on its inputs and outputs without knowledge of its internal workings.
White-Box Modeling	A modeling strategy where the inner workings of a system can be directly modeled because they are known.
Hybrid Modeling	A modeling strategy that combines principles of black box and white box modeling.
Attack Surface	The collection of vulnerabilities and entry points that an attacker can exploit to compromise a system.
Threat Modeling	The process of identifying and evaluating potential threats and system weaknesses.

5. Related Systematic Reviews

Although a comprehensive literature study on this topic may not exist in exact similarity, there are many relevant studies available. Threat modeling and attacks on automobile digital twin is a relatively new and developing research area. Studies on automotive cybersecurity and digital twin technologies that are closely related can offer a lot of knowledge and insights that can be used to inform and direct the evaluation. The systematic review presented in [46] states that this work is worthy for academia as well as research gaps in the literature. A focused gap area is supply chain security, which is not ensured from a manufacturing point of view. The authors recommend a multidimensional implementation by policymakers.

The significance of automobile diagnostics is discussed in another systematic review paper as vehicles become more complicated and consumers expect higher levels of comfort and safety. The study examines the body of literature already in existence and lists the most typical themes, resources, and methods applied in the discipline. A total of 40 articles were chosen for additional research after a thorough evaluation of more than 1000 articles. According to the survey, data extraction from vehicles utilizing OBD and transmission to an online server via cellular interfacing are the most often employed techniques. Techniques for voice recognition are also common since they lessen driver distraction. However, there

are not many strategies for dealing with problems with human–machine interaction. The papers generally have a technical bent and place more of an emphasis on testing and finding faults than driver adaptability [47].

To conduct a thorough analysis of threats and defenses against autonomous vehicles, the authors of this study [48] examined 151 papers published between 2008 and 2019. Security architecture, intrusion detection, and anomaly detection for autonomous attacks were the three categories into which defense tactics were separated. Artificial intelligence and machine learning techniques for anomaly identification are emerging alongside the rapid development in big data and communication technologies. The authors feel that autonomous attacks and defenses should be a significant component of smart cities [49], and that future research in these areas should be strongly related to artificial intelligence. This article addresses the challenges of assessing cyberattack simulations in a variety of computer security domains, which has resulted in inconsistent and fragmented research. To offer a shared baseline, a comprehensive literature review of attack simulations published between 1999 and 2019 was conducted, with an emphasis on those that looked at the phases that led to successful attacks. Eleven significant contributions were eventually selected from the first 647 things that the search turned up. Despite being scattered throughout numerous fields, the publications [6] had comparable objectives, contributions, and problem statements, and the data suggests that attack simulations have not yet been investigated as a distinct field of study. The article's conclusion states that the findings should help researchers and practitioners interested in attack simulations with their present and future efforts. Jones et al., [50] conducted a comprehensive review of the literature and a thematic analysis of 92 digital twin articles from the past decade. The final characterization of digital twins consists of 13 characteristics and a comprehensive operating framework. The perceived benefits, real-world uses, and integration of virtual entities [51] are among the seven knowledge gaps and possible study areas mentioned. In order to progress this field of study, this study highlights the necessity of a shared understanding of digital twins. Schwarz et al., [52] focused on the use of digital twins in automated and connected automobiles. However, there are still a number of limitations and challenges in the development of digital twin applications. When models are connected to physical systems, digital twins will become more unique, flexible, and comprehensible, which will encourage the creation of new digital twin services. Despite the intricacy of the new CAV testing methods, digital twins promote the use of numerous models at different scales and model reuse. The history of digital twins, their role in automotive systems, and the testing techniques currently accessible to such systems are all covered in these linked publications [7,53]. Our investigation encompasses both sectors where the digital twin is used in cyber-physical system testing techniques.

6. Systematic Literature Review Methodology

Beginning with a clear definition of the research questions, this part sets the stage for Section 7 including methodology and study selection. We present a detailed methodology for developing a search protocol and retrieving pertinent studies. The approach was carefully crafted to guarantee that the studies chosen are pertinent, trustworthy, and satisfy the requirements outlined in the research questions. With this procedure, we hope to give a thorough and rigorous study of the research questions, illuminating key issues and advancing knowledge of the field as a whole.

6.1. Defining the Scope: Research Questions and Objectives

This paper mostly summarizes previous studies on various approaches used for threat modeling and attacks in the area of automotive digital twins. Therefore, the following

research questions were developed as a fundamental phase of our SLR in order to examine pertinent information linked to our study.

6.1.1. RQ1: How to Identify and Assess Threats to Automotive Digital Twin?

This research question's objective is to look into efficient methods for identifying and evaluating cybersecurity threats to digital twins in the context of automotive systems. While crucial for testing and replicating car systems, digital twins are susceptible to numerous hacks that could compromise their security.

6.1.2. RQ2: What Are the Current Methodologies Used for Threat Modeling in the Context of Digital Twins of Vehicles?

Threat modeling is a structured technique that aids in the identification and analysis of potential system threats, enabling the creation of efficient security policies. Understanding the current threat modeling techniques applied in this situation is essential given the growing use of digital twins to mimic and test vehicle systems.

6.1.3. RQ3: What Are the Most Effective Methods for Validating Threat Models and Assessing Attacks on Digital Twins of Vehicles?

Threat models are used in the context of cybersecurity to pinpoint potential threats and weaknesses as well as create efficient security measures. Validating these models and evaluating their performance in spotting and thwarting possible assaults are nevertheless crucial.

6.2. Review Protocol

According to the processes outlined by [54], a review protocol is created to provide a systematic literature review. These standards help us make sure the review is fair and repeatable. Other methods, like a review of systematic mapping, were taken into consideration. We made the decision to do a systematic literature review since the mapping review would have been challenging to design and would have lacked relevant gray literature if the topic area, as described in Section 5, had not been explored.

6.2.1. Digital Databases

The digital databases consulted to find studies for this review are listed in Table 5. We selected these three digital libraries based on their repute, capacity to handle complex search requests, and availability of studies on the topic. We created a test set of research to make sure the selected digital libraries were comprehensive enough. This test set includes studies that, in our opinion, met the review's criteria and belonged in the first searches. To guarantee that each study was included in at least one of the digital libraries, we evaluated each one against them. This ensured that pertinent studies would be available.

Table 5. Details of selected databases.

Selected Database	Web Address
IEEE	https://ieeexplore.ieee.org/
Science Direct	https://www.sciencedirect.com/
ACM	https://dl.acm.org/

6.2.2. Search Stings

By connecting portions using "AND" and "OR" statements between each word in the segment, a search string was created. The population of this search string has been split into two sections to make it possible to capture more variance in how a study might describe a cyber-physical system. We now create search strings based on operators to look

for our study topics in well-chosen databases. The collective search string from RQ1, RQ2, and RQ3 is given in Figure 5.

("Threat modeling" OR "Security analysis" OR "Vulnerability assessment") AND ("Digital Twin") AND ("Vehicles" OR "Automotive") AND ("Attacks" OR "Cyberattacks" OR "Cybersecurity" OR "Security threats")

Figure 5. Search string derived from research questions.

6.2.3. Criteria for Selection

The time span to collect research papers for our SLR is from 1 January 2012 to 28 February 2023. To obtain our desired results, there should be a predefined criterion for paper selection and rejection. This step will eliminate any loose literature that may enter the screening process.

1. Inclusion Criteria:
    - Include papers that show work on security aspects in automotives.
    - The digital twin, namely in the automotive sector, should be the main topic of the paper.
    - Articles that are focused on firmware and methodologies.
2. Exclusion Criteria:
    - Papers that are not fully accessible.
    - Non-published, non-peer reviewed.
    - Papers that do not have proper methods or are not verified with valid scientific methodology.

6.2.4. Gray Literature

Further research into gray literature was conducted in order to gain a better knowledge of this emerging technology. Because automotive digital twins are still a relatively new topic. According to this study, gray literature can be found in many different contexts. Though it only turned up tool-related literature rather than examples of commercial testing implementations, this topic did yield a few examples of commercial digital twin-based projects [55,56].

Instead of relying on search engines and attending digital twin-specific conferences, industry experts were asked for their advice on where to look for relevant literature [57]. Although the gray literature around these technologies [55–57] was excluded from the study since it did not provide answers to the research questions, the attention they attracted from industry professionals demonstrated their influence on the developing field of digital twins. While not being pertinent to this analysis, we think that more research should be conducted to examine the assistance that these tools offer for evaluating Automotive digital systems. As digital twins are still a relatively new technology, it was decided that the lack of a clear description would increase the likelihood that the review would be misled rather than provided with useful information. Therefore, gray literature is not included in this review's purview.

7. Findings

7.1. Results After Query Execution

We ran the query against the digital databases listed in Table 5 after finalizing the search term. Table 6 lists the studies that were found in each digital database following the initial search as well as how many of them were full-text accessible. Some digital libraries displayed inconsistencies between the availability of their studies and the search results.

We discovered that this was a result of digital libraries displaying results for documents that were only accessible through various digital libraries, introducing their search results with identical records. In the end, every study was accessible since it could be downloaded from its original digital library.

Table 6. SLR Process Summary.

Database	First Results	IC/EC	Titles & Keywords	Snowballing	Abstract Reading	Full-Text Selection
IEEE Xplore	100	29	26	32	2	12
Science Direct	657	55	23	39	27	2
ACM	97	22	10	6	4	4
Total	854	116	59	77	33	18

Search from the selected string shows that there has been little work performed on the above-mentioned research questions. After a search, we found that there was a total of 854 research works. A total of 104 papers met our selection and exclusion requirements after our criteria were applied. Then, filter of keywords and titles is applied which covered only 60 papers. After that, snowballing is performed to check for missing papers, which resulted in 83 papers. After briefly reviewing the abstracts there were only 100 papers remaining. In the end, only 20 papers were selected to study for answering our research questions. Followed PRISMA framework to perform systematic review. A detailed diagram of overall steps involved during this review are presented in Figure 6.

7.2. Research Question 1: How to Identify and Assess Threats to Automotive Digital Twin?

First, we will explore how digital twins are being applied in the automotive industry. The performance of vehicular systems can be improved and simulated using digital twins, which are simulated reproductions of the physical counterparts. In the context of threat identification, digital twins serve as dynamic environments for simulating attack scenarios across various vehicle subsystems, aiding in early vulnerability detection. Due to the incredibly diverse electronic systems, we observed in our findings, it was challenging to create a classification for all fields of use of digital twins in testing. This approach required a taxonomy that offered simple groups that were pertinent to the systems discovered. Based on the research question, Table 7 is a taxonomy of possible use cases for digital twins in automotive systems. This taxonomy was appropriate since it could be applied at many levels of granularity and encompassed a wide range of vehicular systems.

Table 7. Digital twin classification from literature.

Areas	Relevant Systems
Design and Optimization	Cyber Systems
	Powertrain
	Suspension and Steering
	Electrical and Electronics
	Autonomous Driving
Maintenance	Cybersecurity maintenance
	Predictive maintenance

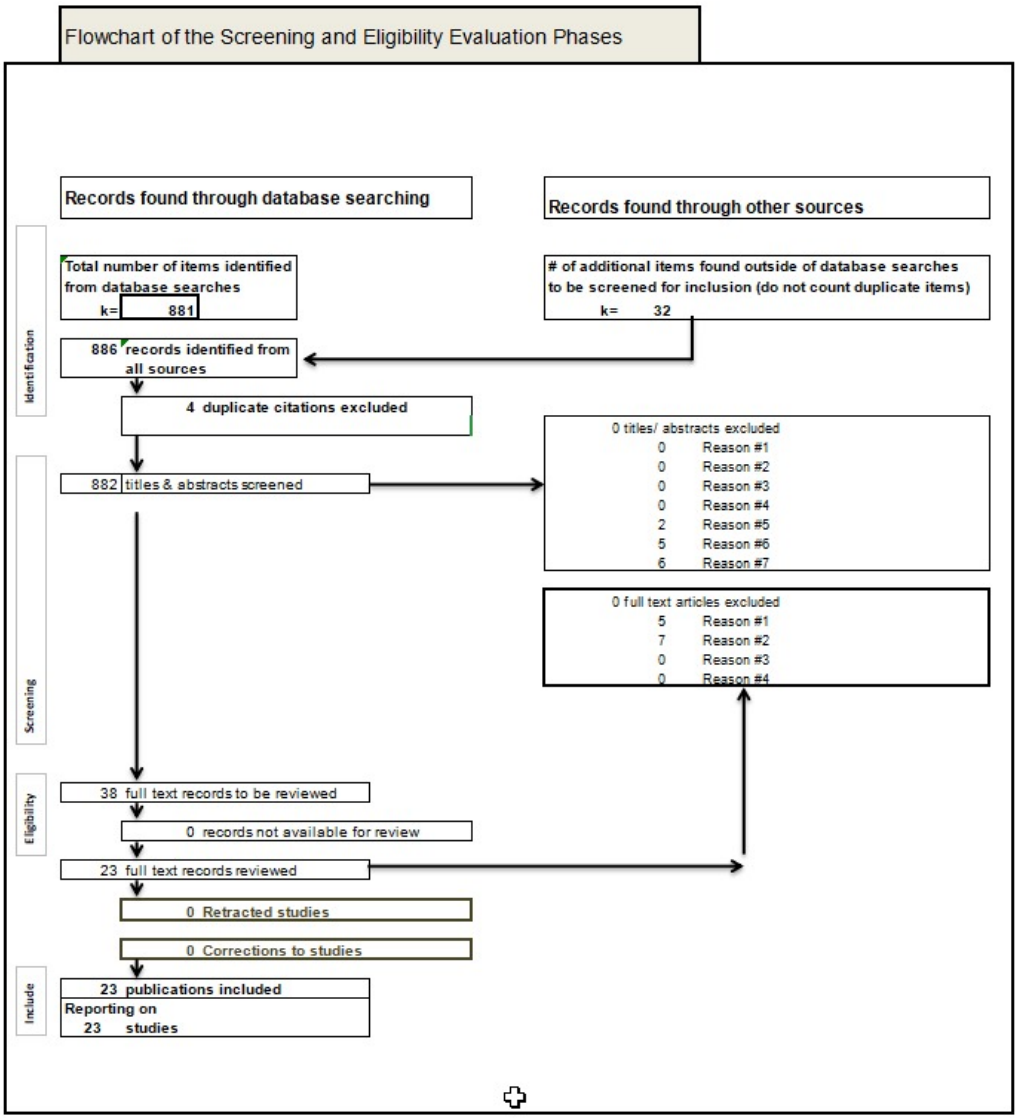

Figure 6. Detailed PRISMA framework protocol.

The design and optimization phase is key in finding potential threats in the creating phase of digital twins. The data we gathered from research contains errors, so we finalized following key areas for our review and discarded all other data to answer our research question:

- Cyber Systems;
- Electrical and Electronic Systems ;
- Autonomous Systems.

Different sub-systems of vehicle that lies in above three types are mentioned in Table 8. A detailed comparison of the selected studies is shown in Table 9.

7.2.1. Cyber Systems: Vulnerabilities and Attack Vectors

Modern automobiles' safety and functionality are greatly enhanced by their use of cyber technologies. These systems include the vehicle network, electronic control units (ECUs), infotainment systems, telematics systems, and other elements linked to the communication and control systems of the vehicle. In [58], the authors explained that security and privacy of vehicle users are threatened by several threats that can affect communication and other VANET assets. The authors suggested an asset-based approach to VANET security that identifies pertinent assets, offers a taxonomy of threats and vulnerabilities on these

assets, and categories potential assaults on VANET while analyzing them. Another work that explained practical DoS attack on in-vehicle CAN bus networks [59] can be regarded as potential threat to digital twins of vehicle. The author highlights the possibility of hardware intrusions on embedded circuits makes this link a security issue as well. The author specifically highlights hardware Trojan (HT) as a potential concern and a key source of backdoor access for hackers. It also states that CAN bus communication is possible without gaining physical access.

As automotive digital twins are software-based systems, they are susceptible to various software attacks to its cyber systems. Attackers may use flaws in the VDT software to their advantage, such as lack of authentication procedures, unencrypted data storage, or improperly configured access controls, to obtain access to the system without authorization. This can result in altering the data kept in the VDT, such as faking diagnostic reports or forecasting the future incorrectly. Also, hackers can infect the VDT system with malware or viruses using software attacks, which might seriously impair vehicular operations [60]. In [61], the author examined the drawbacks of autonomous vehicles and suggests that by offering extra computational power and a wider range of perception, digital twin technology can aid in overcoming these constraints. The physical and digital layers, however, he explains security and privacy risks to the vehicular digital twin network. To address these concerns and threats to vehicular digital twin networks, the paper makes suggestions for potential defenses as well as open research questions for VDT from the angles of security and privacy.

Summarizing the incorporation of cyber technologies into contemporary vehicles has brought about several benefits in terms of safety and functionality, but it has also introduced new risks. To protect the protection and privacy of vehicle users, threat detection is essential, and [59] suggested that an asset-based approach is a suitable place to start. Although software-based assaults on automobile digital twins are a real possibility, hardware attacks like hardware Trojans (HTs) still pose a serious risk. The vulnerability of vehicular digital twins to software attacks necessitates the establishment of strong access controls, consistent software updates, and ongoing system monitoring. These techniques can help automotive digital twins reduce the dangers.

Table 8. Related automotive systems.

Vehicular Twin Systems	Sub-Systems	Attacks Possible
Cyber Systems	Vehicular Network Infotainment systems Telematics systems	Malware and Viruses, Dos Attacks Man-in-Middle attacks. Remote Exploits.
Electrical and Electronic Systems	Electronic Control Units (ECU'S) Sensors OBD systems	Software attacks Hardware attacks (EMI Attacks). Diagnostic access attacks.
Autonomous Systems	Lidar Radar Camera GPS	Spoofing attacks Sensor attacks

Table 9. Comparison of research papers.

Authors	Research Objective	Methodology	Outcome
Kyounggon Kim et al. [48]	Systematic investigation of autonomous vehicle attacks and defenses	Classification of attacks into three categories and defenses into three categories, focusing on AI/ML-based solutions	Identified vulnerabilities and proposed defense strategies for smart city integration
Viktor Engström et al. [6]	Unified baseline for cyberattack simulations in computer security	Systematic review of 11 key papers from 1999–2019	Highlighted commonalities and gaps in attack simulation research
Farhan Ahmad et al. [58]	Security and privacy of vehicular ad hoc networks (VANETs)	Asset-based approach with taxonomy of vulnerabilities, threats, and attacks	Proposes classification and mitigation strategies
Mehmet Bozdal et al. [59]	Demonstration of disruption via hardware Trojan on CAN bus	Simulates HT attack without physical access using untraceable faults	Highlights vulnerabilities in CAN communication
Aman Singh et al. [60]	Analyze cybersecurity vulnerabilities in automotive electronics	Focus on networked embedded systems and algorithms	Identified potential threats and proposed mitigation strategies
Chao He et al. [61]	Address security and privacy challenges in vehicular digital twin (VDT) networks	Analysis of VDT architecture and countermeasures for security	Identified open research challenges and proposed countermeasures
Mariana Segovia et al. [15]	Methodology for design and integration of digital twins (DTs)	Detailed phases from architecture planning to real-time data exchange	Outlined experimental platforms and standards for DTs
Pradeep Sharma Oruganti et al. [9]	Develop a testbed for automotive embedded systems' cybersecurity evaluation	Hardware-in-loop platform with network and mobility simulators	Demonstrates a GPS spoofing attack
Leonardo Presoto de Oliveira et al. [47]	Review of tools and methods in automotive diagnostics	Systematic literature review and surveys for extracting OBD data	Identified gaps in human–machine interface approaches
Chao He et al. [43]	Investigate security and privacy issues in vehicular digital twin networks	Proposes inter- and intra-twin communication models	Suggests countermeasures and discusses privacy-sensitive information

7.2.2. Electrical and Electronic Systems

Attacks on electrical and electronic systems provide a serious risk to the protection and safety of vehicular digital twins, and it is crucial to comprehend their function in such attacks to create efficient defenses. This review addresses the significance of electrical and electronic system intrusions in the context of vehicular digital twins and emphasizes the need for proactive defensive measures to reduce these dangers. Based on ECU development data and software flash pictures, the authors of [62] suggested an easily automated, quantitative, probabilistic method and measure for attack surface and weakness assessment automation. The technique is helpful for code reviews and made security inspections easier. The automotive attack surface consists of internal communication interfaces, external and user-accessible interfaces, and low-level hardware interfaces. Access restrictions, casing tamper-resistance, code size, previously discovered vulnerabilities, the strictness of compil-

ers, frameworks, and application binary interfaces, exploit mitigation techniques, security evaluations, and previously found vulnerabilities are some vulnerability indicators.

Communication between an automobile's electronic control units (modules) using in-vehicle communication protocols like the CAN bus is an essential component of the digital twin of the car. CAN lacks encryption and authentication, while being the most widely used protocol in automobiles, which might result in serious cybersecurity weaknesses [63]. The literature lists multiple CAN bus breaches, and as connected automobiles proliferate, additional attacks are predicted to occur. Securing CAN and modules is crucial to preventing major failure or accidents since they are high-priority targets for hackers. Another work explains CAN and OBDII-related vulnerabilities [64].

In conclusion, identifying and evaluating threats in digital twin electrical and electronic systems for modern automobiles is essential for ensuring their protection and security. Modules, sensors, and OBD systems are the three primary system categories under consideration, which are all possible targets for cyber intrusions and need to be continuously monitored and assessed in order to identify and stop risks. A useful method for locating weaknesses and testing prospective protection measures in a secure setting is the use of a digital twin perspective. Vehicle manufacturers may enhance the general protection and security of their vehicles and provide drivers and passengers more peace of mind by including threat assessment and mitigation techniques into the digital twin development process [62–64].

7.2.3. Autonomous Systems

Sensors like LiDAR, radar, cameras, and GPS are essential parts of autonomous systems. Autonomous vehicles can perceive their environment thanks to these sensors and base their decisions on that knowledge. These sensors are not impervious to dangers like cyberattacks, system failures, and physical damage, though, as with any technology. To ensure the secure and dependable functioning of autonomous vehicles, it is crucial to recognize and evaluate any potential risks to these sensors from the viewpoint of vehicular digital twin technology.

The author [8] discusses a novel method for spotting and dealing with sensor spoofing assaults on car radars, which are crucial for both assisted and autonomous driving. With a multi-input multi-output (MIMO) radar, expanded multiple beamforming is used as part of the method. Based on simulation analysis, it was concluded that the proposed technique performed better than advanced methods in terms of threat detection and distance measurement accuracy for adaptive cruise control. This improvement could help strengthen security at the software level of vehicular digital twins.

The attack technique suggested in work [65] used a fake radar to alter the speed and distance detected by an automotive FMCW mmWave radar that applies fast frequency modulation. The attacking radar changes its phase correction to hide its speed and modifies the delay to change its detected distance. The spoofing attack is demonstrated in two real-world situations using a hardware-based proof-of-concept system made with software-defined radio. The study also looks at defenses against this attack.

In-vehicle assault detection software that uses multi-source data from the CAV's onboard sensors is presented in this study [66]. On affordable embedded computing systems built into the CAV, the solution can be used. The experiment findings demonstrate the suggested solution's efficacy against various assault scenarios, and the study validates it using the real-time CARLA simulator.

In conclusion, there is a need for proactive response to threats to autonomous systems in vehicular digital twins. The primary components of autonomous systems are cameras, GPS, radar, and lidar, and it is essential to consider and evaluate potential threats to these

systems. Some of the most frequent dangers to autonomous systems are sensor spoofing and GPS location spoofing. In-vehicle attack detection solutions that combine data from multiple sources that are easily accessible through the vehicle's onboard sensors are just one example of the lightweight and affordable options for detecting such assaults that are becoming available with the evolution of technology.

7.2.4. Summary

At first, we classified automotive digital twin systems to identify threats. Secondly, subsystems of our taxonomy are derived. Then, we selected the most important sub systems to discuss the threat identification in context of automotive digital twin. Thirdly, we have conducted a detailed review of attacks and threats to or selected systems. Finally, we have explored different available researches in our areas to identify threats that may be harmful for vehicular digital twin.

7.3. Research Question 2: What Are the Current Methodologies Used for Threat Modeling in the Context of Digital Twins of Vehicles?

Cybersecurity experts and researchers can identify system weaknesses and security risks in different parts of digital twins, such as cyber, electrical, and electronic areas, through systematic threat modeling. Recognizing these threats early helps stakeholders reduce security risks that could affect the safety and protection of digital twin systems. This section gives an overview of threat modeling methods used for automotive digital twins and highlights important factors to consider when implementing security measures. It also provides recommended best practices for conducting threat modeling exercises. We categorize digital twin vehicles based on different threat modeling approaches and organize our review using the following methods:

- Data analysis approach
- System analysis approach
- Threat identification approach

7.3.1. Data Analysis Approach

A key component of digital twin technology in the automobile industry is data analysis. To identify any potential security threats or holes that could compromise data assets and flows, it includes continuously monitoring the data flow within a system. To assure the best performance, efficiency, and safety, data analysis is more crucial than ever due to the complexity of modern cars. In this situation, data analysis can assist automakers and service providers in making defensible choices based on information obtained from real-time data, improving outcomes for both clients and enterprises [67].

Risk assessment in automotive is performed using the SAHARA (Security and High-Assurance Research and Development for the Automotive industry) technique. The University of California, San Diego developed it for the security of automobile systems. This method uses both technological and non-technical controls, as well as several security controls and countermeasures. With this technique, possible vulnerabilities in vehicle systems are found and mitigated. The steps below must be taken for this strategy to be used effectively: Asset and threat identification, vulnerability discovery, risk assessment, countermeasure deployment, system monitoring, and system improvement [68].

Unified Safety and Security Scheme (USSS) is another automotive security framework which is developed by ENISA (European Union Agency for Cybersecurity). It is designed for connected automated vehicles. It includes guidelines for product life cycles. This framework is built of the following components: risk management, security development life cycle, incident response, supply chain security, and compliance and certification [69].

The US agency for highway safety developed the NHTSA automotive cybersecurity threat analysis approach to identify and counter possible threats to car cybersecurity. It is a strategy based on risk assessments. The steps in the NHTSA approach are as follows: identification of dangers, study of threats, selection of countermeasures, testing, validation, and oversight of countermeasures [70]. Microsoft also developed a threat analysis and modeling technique to find software application flaws and possible security threats. HEAVENS, the name of this tool, stands for the following:

- Hackers and attackers;
- Extensions and add-ons;
- Authorized users;
- Vendors and suppliers;
- End users;
- Network and connections;
- SDLC (Software design life cycle).

The systematic HEAVENS method for threat modeling the SDLC, this architecture takes security threats and vulnerabilities into account [71]. The steps are as follows: System boundaries must be defined, threats must be identified and analyzed, and countermeasures must be found and verified. A framework for threat analysis is called EVITA [72] (assessment of IT security threats to automotive systems). The BSI (Office of Information Security) created it. This methodology follows a similar three-phase framework. They include developing countermeasures and modeling threats and risks.

7.3.2. System Analysis Approach

A technique called fault tree analysis builds a logical diagram to examine the reasons why systems fail. Potential failures in the automotive digital twins can be found using this technique. For instance, FTA can be used to detect simulated vehicle brake system failure [73]. The FTA process involves the following steps: failures in the system are identified, creation of a logic diagram, often known as a "fault tree," that depicts the relationships between events; assessment of the fault tree is performed by estimating the likelihood that failure events will occur; followed by the identification of essential components and suggestions for preventing potential failures.

A method for analyzing the possible consequences of an event is event tree analysis (ETA). By using trees, this technique divides events. This technique can be used to evaluate the effects of potential failures within a digital twin of a physical counterpart. It entails identifying the relevant event and then creating a tree of potential outcomes. The top of the tree should be our goal, and its branches should stand in for potential outcomes. Following the development of the event tree, the analyst assigns probabilities to each branch depending on the likelihood that they will occur. Eventually, given the probabilities of each result, total risk associated will be computed [74].

A technique called CMA (common mode analysis) has been used to find probable system flaws or breakdowns. In the context of automotive digital twins, CMA is used to find issues that can impact both the replica and the real car. Identification of potential system-affecting common mode failures is a step in the process. Examples of these failures include sensor or actuator failures in hardware as well as software bugs. Calculations are made after failure assessment [75].

The severity of vulnerabilities in software and hardware systems is typically evaluated using the common vulnerability scoring system (CVSS). A general technique called CVSS is employed to assess and rank security flaws in in-vehicle software systems. A system's availability, confidentiality, and integrity are evaluated to determine the CVSS, which is a numerical indicator of vulnerability severity [76].

(Multi-agent functional safety analysis) In the automotive sector, FMVEA is used for safety and security analysis. It describes the various system module roles. Once discovered, OEMs can take preventative measures to ensure that the vehicle complies with safety standards and laws [77]. A technique for assessing vulnerability is called vulnerability and exposure research assessment (VERA). It is used to find and examine potential weaknesses in networks and information systems. This technique includes system characterization, threat and vulnerability detection, asset appraisal, risk and vulnerability assessment, risk reduction, and report production. In-vehicle Networks benefit greatly from the VERA approach [78].

7.3.3. Threat Identification Approach

By analyzing the interactions and components of the system, this approach can help identify any potential security risks or vulnerabilities that could jeopardize the system's functionality or safety. In the context of automotive digital twin technology, threat identification is an essential part of ensuring optimal performance, efficacy, and safety for drivers and passengers.

The security analysis and risk assessment (SARA) technique can be used to identify, assess, and manage the security risks associated with cyber physical systems. This approach may be useful for determining and evaluating the security risks associated with digital twins for automobiles [79]. A framework for evaluating security and risk to regulate information systems is called the security assurance method (SAM). The SAM technique is helpful in the automobile industry to assess security threats and put in place the required controls for vehicle information systems [80]. A sort of probabilistic model used for intrusion detection and protection is called a Bayesian defense graph (BDG). BDGs may be useful for modeling security threats related to digital twins of vehicles. This model can be useful to implement intrusion detection system and access controls [81,82].

A threat modeling technique called PASTA (Process for Attack Simulation and Threat Analysis) claims to be able to find and evaluate dangers in software systems. PASTA can be helpful in identifying dangers and weaknesses in the context of an automobile digital twin [83]. Similarly, VAST is an additional threat modeling approach (Visual, Agile, Simple Threat modeling) which is used to find and evaluate cybersecurity issues in software systems. Implementation of the VAST method entails a number of processes, including visual modeling to identify potential attack vectors using flowcharts, diagrams, and an agile process, which implies that the process is iterative and may update new vulnerabilities, threat analysis, and mitigation strategies [84].

The Bayesian network model (BNM), a probabilistic modeling tool, can be used to anticipate the likelihood of alternative events and explain the links between various system components. To understand how different digital twin system components interact with one another within the context of automotive digital twins, BNM can be utilized to analyze the behavior of the various digital twin system components. Consider a digital twin system for an automobile that uses a Bayesian network and variables to represent the system's many components, including the engine, gearbox, and brakes [76].

A risk assessment method called the attack tree method (ATM) is used to locate and evaluate potential security risks to the automotive digital replica system. This is a technique for creating attack scenarios that simulates attacks graphically. ATM can be performed to discover potential security flaws and evaluate the effects of various attack scenarios. This approach is based on breaking the system down into individual parts. Then, in order to identify the various dangers attached to them, several attack scenarios are depicted in tree-like structures. Nodes represent hypothetical assault scenarios, whereas branches indicate various phases or elements of an attack. The tree's leaves stand in for the probable

results of attacks (data theft). System simulation and design data are used in digital twin systems in the automotive industry. This information may pose a security risk. ATM can be used to identify security risks and weaknesses [85]. The threat modeling approaches are detailed in Table 10.

Table 10. Threat modeling approaches in automotive digital twins.

Approach	Description	Applicability/Use
STRIDE	Checklist-based model focusing on spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege.	Widely adopted in software-driven systems (e.g., ECUs); suitable for early design threat enumeration.
Attack Trees	Hierarchical representation of attack goals and sub-goals using tree structures.	Effective for structured multi-step attacks; referenced in ISO 21434-based modeling.
DFD + Threat Models	Combines data flow diagrams with methods like STRIDE to trace threats through system boundaries.	Applied during system architecture planning for identifying data-related threats and flows.
STPA-Sec	System-Theoretic Process Analysis adapted for security to identify unsafe control actions.	Used in cyber-physical systems; strong for hazard modeling in safety-critical environments.
Bayesian Networks	Probabilistic modeling of threat propagation and dependency using graph-based logic.	Supports scenario simulation and intrusion prediction; rarely adopted in industry.
HEAVENS	A structured automotive-focused framework integrating threat assessment with risk quantification.	Aligned with ISO 21434; focuses on lifecycle security for connected vehicles.

7.3.4. Summary

Ensuring the performance, efficiency, and safety of vehicular digital twins requires a structured and proactive approach to threat modeling. This includes continuous monitoring of system data flows to identify vulnerabilities, analyzing component interactions to detect structural weaknesses, and implementing detection strategies to uncover security risks. A systematic combination of these techniques strengthens the digital twin's resilience [86] and supports the development of robust automotive cybersecurity measures. Details of all used techniques are presented in Table 11.

While Section 7.3 provided a detailed textual review of various threat modeling approaches, Table 12 presents a comparative summary. This table evaluates each technique in terms of computational complexity, industry adoption, and their applicability to specific attack scenarios in automotive digital twins.

7.4. Research Question 3: What Are the Most Effective Methods for Validating Threat Models and Assessing Attacks on Digital Twins of Vehicles?

Validating the threat model and evaluating potential assaults are essential for assuring the security and resilience of an automotive digital twin against cyber threats. To do this, it is necessary to find any security flaws in the twin's architecture, design, or implementation, as well as to guarantee compliance with industry security standards and laws and to safeguard against changing cyber threats [87].

Table 11. Threat modeling tools and techniques from the literature.

Approach	Description	Methods
Data Analysis	Monitoring the system's data flow to find potential security threats and flaws involving data assets and flows.	SAHARA [41] USSS [69] NHTSA [43] EVITA [44] HEAVENS [46]
System Analysis	Examining the system's components and design to find any potential security holes and threats.	FTA [47] ETA [48] CMA [50] CVSS [52] FMVEA [53] VERA [54]
Threat Identification	Analyzing system interactions and components to find potential security threats and vulnerabilities.	SARA [55] SAM [56] BDG [57] PASTA [58] VAST [59] BNM [60] ATM [61]

Table 12. Comparison of threat modeling approaches for automotive DTs.

Approach	Computational Complexity	Industry Adoption	Attack Scenario Applicability	RQ Alignment
STRIDE	Low; simple rule-based	Moderate; used in software-focused automotive systems	Known attacks (e.g., ECU injection)	RQ1: Threat identification; RQ2: Structured modeling
PASTA	High; multi-stage process	High; adopted by BMW, aligns with UNECE R155	Structured attacks (e.g., CAN-Bus spoofing)	RQ2: Threat modeling; RQ3: Validation
MITRE ATT&CK	High; extensive database	Emerging in automotive; used in cybersecurity firms	Dynamic attacks (e.g., zero-day)	RQ1: Threat identification; RQ3: Attack simulation

A variety of strategies and methods are used to evaluate the quality and completeness of a threat model for vehicular digital twins. Some potential methods that are mentioned throughout literature are the following:

7.4.1. Penetration Testing

A penetration test is used to identify any vulnerabilities that the original threat model missed and to verify that the security measures in place are working. White-box pen testing (WBPT), conventional black-box pen testing (BBPT), and innovative gray-box pen testing (GBPT) are the three primary forms of pen testing. According to [88], the WBPT approach is a thorough knowledge test that grants the tester access to the system's internal data and source code. A technique for enhancing vehicle security testing is presented by the authors of this study [89], who combined safety and security. Through the use of safety analysis results as input for a threat analysis, they developed a new method for producing possible test cases. Test cases were created and run using the technique on an automotive electronic control unit (ECU) with safety-critical functionality. Because the authors were

able to take advantage of a test error, the airbags exploded. In general, this approach provides a systematic and effective way to identify and address security vulnerabilities in automotive systems.

This paper emphasizes how evolving technologies like connectivity and autonomy are driving a greater demand for more robust security measures and penetration testing in the car industry [90]. A threat model that includes safety and security considerations and a ranking of risk level is required to concentrate the tests on important vulnerabilities. The results of Microsoft's Threat Modeling Tool 2016 and Hazard Analysis and Risk Assessment (HARA) have been combined by the authors to form the CVSIL threat approach. The suggested solution assesses the overall CVSS [76] score as a risk level and derives the collateral damage potential statistic. Also, the authors have developed the Security-ASIL score for ranking, which incorporates security and safety analysis components. The approach was assessed using a fictitious adaptive cruise control (ACC) system [91].

The [92] seeks to develop the notions of how such an attacker might affect the behavior of the vehicle following that kind of attack. We specifically show how, on two distinct automobiles, we can sometimes manage the steering, braking, acceleration, and display. We also provide a method for identifying these kinds of assaults. We publish all technical data required to reproduce and comprehend the problems at hand, including the source code and a list of required hardware.

Penetration overall includes red teaming to simulate attacks on automotive digital twins. Red teaming is also used to identify potential security vulnerabilities in a threat model [93].

7.4.2. Attack Simulation

The threat model for an automobile digital twin needs to be tested in order to ensure that it is precise and comprehensive in identifying potential vulnerabilities and threats. Numerous techniques and processes, including penetration testing, which is covered in Section 7.4.1, are employed to assess the model's effectiveness. Using attack simulation tools is one such technique that can help discover possible attack scenarios and evaluate how well the security policies on the digital twin are preventing them [94]. Since the automotive sector still relies on digital twin technology for vehicle system analysis and simulation, it is imperative to evaluate the threat model in order to guarantee the safety and security of these systems.

VehicleLang is a domain-specific modeling language designed to simulate attack scenarios in automotive systems by modeling vehicle architectures and identifying vulnerabilities using known attack vectors [95]. It enables automated generation of attack graphs tailored to specific automotive digital twin models, making it useful for threat analysis and testing. However, its effectiveness is limited by its reliance on predefined libraries of known threats, reducing its ability to detect novel or zero-day attacks. Furthermore, its abstraction may not capture low-level hardware interactions, which restricts its utility in simulating hardware-based exploits or sensor-level attacks.

An embedded intrusion detection system (IDS) is introduced in [92] for the automotive industry. The IDS uses a two-step method that filters signals on the controller area network (CAN-Bus) and analyses possibly dangerous messages using a Bayesian network to detect potential cyberattacks. A test campaign was run to determine the method's effectiveness and efficiency, and the findings indicate good agreement in the presence of frequent cyberattacks with implementation characteristics outlined in Table 13.

Table 13. Implementation and limitations of VehicleLang and IDS approaches.

Tool/Method	Implementation and Limitations
VehicleLang	Implementation: - Domain-specific modeling language - Generates attack graphs from known threats - Validated via expert input and Feigenbaum testing [95] Limitations: - Cannot simulate hardware-level behavior - Limited to known attack patterns - Not suitable for zero-day vulnerabilities
IDS (CAN-Bus + Bayesian)	Implementation: - Filters CAN-Bus messages - Detects anomalies using Bayesian models - Evaluated in experimental setups [92] Limitations: - High false-positive rate in real use - Resource limits on ECUs - Incompatibility due to proprietary protocols

7.4.3. Summary

There is a lack of literature on digital twin attack modeling, despite the fact that cybersecurity is becoming more and more significant in the automotive sector. Attack simulations are a useful tool for assessing the cybersecurity of various systems, but little study has been performed specifically on digital twin systems. Attack simulations can evaluate how successfully security policies prevent potential attacks and replicate the actions an attacker would take to compromise sensitive system assets. Without such research, it is difficult to identify and address possible security vulnerabilities in digital twin systems.

7.5. Publication Trends

The volume of research on virtual twin systems in the automotive domain has grown steadily, reflecting their increasing relevance. Topics explored include their roles in design, testing, production, and system monitoring. Notably, many studies investigate how digital twins contribute to system safety, cost optimization, and performance enhancement, with a growing emphasis on cybersecurity validation.

Only a small number of articles were published on this subject in 2017, but by 2019, the quantity of articles had greatly increased. The number of publications on "automotive digital twin" increased significantly in 2020 compared to 2019. This pattern shows an increase in interest in the implementation of virtual twin technology within the automobile sector. Also, a wide range of topics, such as vehicle design, testing, production, and maintenance, are covered in the publications on this subject. The growing number of publications on digital twins reflects increasing academic and industrial interest, particularly in cybersecurity applications. Recent studies are increasingly focused on their use in security validation, rather than solely performance optimization.

Finally, publishing patterns indicate an increasing interest in using digital twin technology in the automotive sector, as well as more studies researching its potential applications and benefits.

8. Discussion

This section interprets the results of our systematic review, addresses the research questions, and reflects on the scope and limitations of the study.

The concept of vehicular digital twins (VDTs) is rapidly gaining traction in the automotive sector, with applications spanning software testing, hardware-in-the-loop (HIL) validation, and vehicular communication networks. Our review highlights the urgent need for a clear and universal taxonomy to guide research and development in this area. Without standardized definitions and classification schemes, meaningful synthesis and comparison of research findings would not be possible.

Through a systematic literature review, we identified recurring themes and elements in existing definitions and taxonomies of vehicular digital twins. This enabled us to construct a structured taxonomy, which underpins our subsequent analysis of threats, methodologies, and validation techniques.

RQ1: Threats to Automotive Digital Twins. Our review reveals a diverse array of threats targeting automotive digital twins, including unauthorized ECU access, sensor spoofing, and manipulation of in-vehicle networks [96]. The dynamic, interconnected nature of modern vehicles broadens the attack surface, necessitating proactive threat modeling and continuous security assessment [97,98].

RQ2: Threat Modeling Methodologies. We found that while several methodologies—such as STRIDE, attack trees, and ML-based simulations—are being applied to vehicle systems, there is no consensus on a universal approach. Table 11 in Section 2.2 summarizes their comparative strengths and limitations. The complexity of vehicular digital twins, which span software, hardware, and communication layers, complicates the development of comprehensive threat models [99,100].

RQ3: Validation and Simulation Gaps. There is a notable lack of research on grading attack simulations and validating threat models for vehicular digital twin systems. Most existing studies focus on identifying threats rather than systematically validating the effectiveness of proposed security mechanisms. Without validated models and robust attack simulations, it remains challenging to assess the completeness and real-world applicability of security solutions [101,102].

Research Trends and Gaps. Table 14 presents research trends in the automotive digital twin domain over the period covered by our review. Despite growing interest, significant knowledge gaps persist, particularly in the validation of threat models and attack simulations. This gap may result in overlooked vulnerabilities, potentially leading to severe consequences such as loss of vehicle control or compromised safety.

Table 14. Publication trends in automotive digital twins.

Year	Number of Publications
2012	1
2013	2
2014	4
2015	6
2016	9
2017	16
2018	40
2019	112
2020	267
2021	312

A broader distinction can be made by comparing the digital twins used in automotive and industrial environments with those applied in urban-scale systems, such as smart cities [103,104]. Unlike industrial digital twins typically confined to closed, well-regulated factory settings, urban scale and automotive digital twins must operate in dynamic, heterogeneous, and often publicly accessible environments. These systems face broader attack

surfaces due to their reliance on public networks, decentralized components, and real-time interactions with external systems. As discussed in [33], the security challenges in urban-scale digital twins are amplified by the need for interoperability, shared infrastructure, and the participation of multiple stakeholders. Consequently, threat modeling and simulation strategies used for industrial DTs may not be directly scaled to vehicular or smart city contexts without significant adaptation.

To further contextualize the challenges discussed in this review, Table 15 summarizes key differences in environment, security focus, and challenges [105] in industrial, vehicular, and urban digital twins.

Future Directions. To ensure the security and reliability of vehicular digital twin systems, future research should prioritize the development of standardized threat models, comprehensive attack simulation frameworks and methods for validating the effectiveness of security mechanisms. Such advances are essential for building safer and more resilient automotive systems [106,107].

Table 15. Comparison of Digital Twin Domains.

Domain	Environment	Security Focus	Key Challenges
Industrial DT	Closed, structured	Asset control, predictive failure	Low adaptability, proprietary systems, limited external interfaces
Vehicular DT	Semi-open, mobile	ECU threats, OTA updates	Real-time safety constraints, mobile networks, physical-cyber convergence
Smart City DT	Open, public	Network-layer threats, privacy, trust	Scale, heterogeneous data, shared infrastructure, multi-party governance

Smart city digital twins (DTs) [108] face unique cybersecurity challenges compared to industrial domains, addressing RQ1-RQ3. Unlike industrial internet of things (IIoT) DTs [109], which prioritize isolated [110] manufacturing systems, smart city DTs integrate heterogeneous IoT devices [111] (e.g., traffic sensors), increasing sensor spoofing risks, necessitating scalable threat identification (RQ1). Autonomous vehicle DTs focus on ECU-specific attacks (e.g., CAN-Bus spoofing), while smart city DTs require dynamic threat modeling (RQ2) for network-layer DDoS attacks on V2X systems. Smart grid [112,113] DTs emphasize power stability, contrasting with smart cities [86] focus on citizen safety validated through attack simulations (RQ3). Table 16 summarizes these distinctions, guiding tailored cybersecurity strategies for urban DTs.

Table 16. Comparison of DT cybersecurity aligned with suggested RQs across domains.

Domain	Key Challenge	Threat Example	Cybersecurity Focus	RQ Alignment
Smart Cities [114]	Heterogeneous IoT integration [115]	Sensor spoofing	Scalable threat detection	RQ1: Threat identification; RQ2: Dynamic modeling
IIoT	Isolated system integrity	Malware injection	Process continuity	RQ2: Structured modeling
Autonomous Vehicles	Real-time safety critical attacks	CAN-Bus spoofing	ECU protection	RQ1: Threat identification; RQ3: Validation
Smart Grids	Power system stability	Grid cyberattacks	Resilience measures	RQ3: Attack simulation

9. Conclusions

This systematic literature review highlights critical gaps in current cybersecurity measures for automotive digital twins particularly the lack of robust validation of threat modeling methodologies and systematic evaluation of attack simulations. By emphasizing proactive threat modeling and simulation-based testing, this review provides a structured foundation for the secure development of automotive digital twin (DT) systems. Without validated threat models and repeatable simulation strategies, it becomes difficult to assess the resilience of these systems under real-world threat conditions, potentially exposing them to severe vulnerabilities.

Future research should prioritize specific high-risk attack vectors such as CAN-Bus injection, GPS spoofing, and over-the-air (OTA) firmware tampering, which continue to challenge detection and emulation within DT environments. Integrating artificial intelligence (AI) and machine learning (ML) into DT testbeds presents an opportunity to enhance real-time anomaly detection, behavioral profiling, and autonomous cyber-response capabilities [116] .Recent studies have proposed deep learning for ECU behavior modeling [117], reinforcement learning for dynamic intrusion response [30], and federated learning for privacy-preserving analytics across vehicle fleets.

To address identified gaps, we propose prioritized research into DT-based trust chains and autonomous cyber-defensive DTs, grounded in recent advancements (RQ1–RQ3) as outlined in the Table 17. Trust chains, as piloted in Singapore's smart city initiative [118], leverage blockchain [119,120] to secure IoT data, enhancing threat identification (RQ1) for sensor spoofing. Autonomous DTs, driven by reinforcement learning adaptively mitigate DDoS attacks in urban traffic systems, bolstering attack simulation (RQ3). Integrated policy frameworks, inspired by a 2025 EU initiative [121], standardize threat modeling [122] (RQ2) for urban DTs. These directions, supported by pilots and literature, address standardization and dynamic risk surfaces, guiding secure smart city DTs.

Table 17. Grounded speculative concepts for future research.

Concept	Description	Citation/Example	RQ Alignment
DT-Based Trust Chains	Secure IoT data exchanges	El-Hajj (2024) [123]; Singapore pilot	RQ1: Threat identification
Autonomous Cyber-Defensive DTs	Adaptive attack mitigation	Ozkan-Okay et al. (2024) [124]; traffic system	RQ3: Attack simulation
Integrated Policy Frameworks	Standardized security protocols	2024 EU initiative [121]	RQ2: Threat modeling

Moreover, there is a growing need for standardized AI-enhanced digital twin frameworks that align with automotive cybersecurity regulations such as ISO/SAE 21434 and UNECE R155. These frameworks should support trust-driven DT ecosystems by enabling data integrity validation, auditability, and adaptive threat mitigation. Strengthening these foundations will not only improve the scalability and reliability of DT-based security testing [125] but also inform global policy and standards for connected vehicle ecosystems.

To address critical gaps in automotive DT security, we prioritize three attack vectors and AI/ML-driven solutions, aligning with RQ1–RQ3. CAN-Bus injection, a safety-critical threat, demands advanced threat identification (RQ1) and modeling with STRIDE (RQ2) to prevent vehicle control breaches. GPS spoofing, disrupting autonomous navigation, requires robust attack simulations (RQ3) using tools like VehicleLang. OTA firmware tampering, exploiting software updates, necessitates lifecycle security testing per UNECE R155. Federated learning enables distributed anomaly detection for real-time threat identification (RQ1), while reinforcement learning optimizes adaptive attack simulations (RQ3). These

priorities address scalability and zero-day attack gaps, guiding the development of resilient DT frameworks and are summarized in Table 18.

Table 18. Prioritized future research directions.

Priority Area	Description	AI/ML Solution	RQ Alignment
CAN-Bus Injection	Safety-critical vehicle control breach	Federated learning	RQ1: Threat identification; RQ2: Modeling
GPS Spoofing	Disruption of autonomous navigation	Reinforcement learning	RQ3: Attack simulation
OTA Firmware Tampering	Exploitation of software updates	Explainable AI for modeling	RQ2: Threat modeling; RQ3: Validation

Ultimately, this review emphasizes that future advancements must go beyond theoretical models and move toward empirically validated, scalable, and standards-aligned solutions capable of addressing the evolving threat landscape in automotive and smart transportation domains.

Author Contributions: Conceptualization, U.M.S. and D.M.M.; methodology, U.M.S.; software, K.A.S.; validation, K.K., G.F. and D.M.M.; formal analysis, U.M.S.; investigation, D.M.M. and G.F.; resources, K.A.S.; data curation, K.A.S.; writing—original draft preparation, U.M.S.; writing—review and editing, D.M.M.; visualization, U.M.S.; supervision, K.K.; project administration, K.K.; funding acquisition, G.F. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding and the APC was funded by Saarland University, Germany.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. El-Rewini, Z.; Sadatsharan, K.; Selvaraj, D.F.; Plathottam, S.J.; Ranganathan, P. Cybersecurity challenges in vehicular communications. *Veh. Commun.* **2020**, *23*, 100214. [CrossRef]
2. Grieves, M.; Vickers, J. *Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems*; Springer: Cham, Switzerland, 2017; pp. 85–113.
3. da Silva, A.C.F.; Wagner, S.; Lazebnik, E.; Traitel, E. Using a cyber digital twin for continuous automotive security requirements verification. *arXiv* **2021**, arXiv:2102.00790. [CrossRef]
4. Tao, F.; Qi, Q.; Wang, L.; Nee, A. Digital twins and cyber–physical systems toward smart manufacturing and industry 4.0: Correlation and comparison. *Engineering* **2019**, *5*, 653–661. [CrossRef]
5. Hu, W.; Zhang, T.; Deng, X.; Liu, Z.; Tan, J. Digital twin: A state-of-the-art review of its enabling technologies, applications and challenges. *J. Intell. Manuf. Spec. Equip.* **2021**, *2*, 1–34. [CrossRef]
6. Engström, V.; Lagerström, R. Two decades of cyberattack simulations: A systematic literature review. *Comput. Secur.* **2022**, *116*, 102681. [CrossRef]
7. Faleiro, R.; Pan, L.; Pokhrel, S.R.; Doss, R. Digital twin for cybersecurity: Towards enhancing cyber resilience. In Proceedings of the Broadband Communications, Networks, and Systems: 12th EAI International Conference, BROADNETS 2021, Virtual Event, 28–29 October 2021; Proceedings 12; Springer: Berlin/Heidelberg, Germany, 2022; pp. 57–76.
8. Kapoor, P.; Vora, A.; Kang, K.D. Detecting and mitigating spoofing attack against an automotive radar. In Proceedings of the 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall), Chicago, IL, USA, 27–30 August 2018 ; pp. 1–6.
9. Oruganti, P.S.; Appel, M.; Ahmed, Q. Hardware-in-loop based automotive embedded systems cybersecurity evaluation testbed. In Proceedings of the ACM Workshop on Automotive Cybersecurity, Dallas, TX, USA, 27 March 2019; pp. 41–44.
10. Berkovich, S.; Avdoshin, S. Enhancing the Security of Digital Twins in Cyber-Physical Systems. *Int. J. Netw. Secur.* **2020**, *22*, 41–50.
11. Chhetri, S.; Zheng, Z.; Leshem, G.; Al Faruque, M. Security of IoT Cyber-Physical Systems: Digital Twin-based Approach. In Proceedings of the IEEE International Conference on Hardware/Software Codesign and System Synthesis, Seoul, Republic of Korea, 1–6 October 2017; pp. 1–10.

12. Alcaraz, C.; Zeadally, S. Cybersecurity and Privacy in Smart Cities. In *Smart Cities: Cybersecurity and Privacy*; Domingo-Ferrer, J., Sánchez, D., Eds.; Routledge: Abingdon, UK, 2018.
13. Lu, Y.; Liu, C.; Wang, K.; Huang, H.; Xu, X. Digital Twin-Based Cyber-Physical Production System: A 5C Architecture Perspective. *IEEE Access* **2020**, *8*, 2168–2175.
14. UNECE. UNECE Regulation No.155: Cyber Security and Cyber Security Management System; United Nations Economic Commission for Europe: Geneva, Switzerland, 2021. Available online: https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security (accessed on 17 June 2025).
15. Segovia, M.; Garcia-Alfaro, J. Design, modeling and implementation of digital twins. *Sensors* **2022**, *22*, 5396. [CrossRef]
16. Ferreira, A.; Pacheco, F.; Goncalves, J. Digital Twins in Smart Cities for Cybersecurity Monitoring. *IEEE Access* **2021**, *9*, 17576–17588.
17. Chen, J.; Li, Z.; Zhang, Y.; Zheng, L. Digital Twin in Industrial Cybersecurity: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 2061–2085.
18. Boyes, H.; Watson, T. Digital twins: An analysis framework and open issues. *Comput. Ind.* **2022**, *143*, 103763. [CrossRef]
19. Unity Technologies. Digital Twin Definition. Available online: https://unity.com/solutions/digital-twin-definition (accessed on 27 March 2025).
20. Sharifi, A.; Yamagata, Y.; Kono, T.; Yokohari, M. (Eds.) *Security and Privacy Applications for Smart City Development*; CRC Press: Boca Raton, FL, USA, 2021.
21. Fuller, A.; Fan, Z.; Day, C.; Barlow, C. Digital twin: Enabling technologies, challenges and open research. *IEEE Access* **2020**, *8*, 108952–108971. [CrossRef]
22. Liu, Z.; Qin, Y.; Yang, Y.; Feng, Y. Cybersecurity and the Digital Twin: Recent Advancements and Future Trends. *J. Netw. Comput. Appl.* **2020**, *160*, 102642.
23. Jones, C.; Silva, J.; Sundaram, R. Exploring the Security Implications of Digital Twin in Critical Infrastructures. *J. Inf. Secur. Appl.* **2018**, *40*, 58–64.
24. Ma, Z.; Zhang, H.; Wang, P. Digital Twin-Driven Cyber-Physical Production System: Framework and Implementation. *J. Manuf. Syst.* **2019**, *58*, 36–45.
25. Smith, A.; Brown, C.; Johnson, D. Blockchain for Digital Twin Security in Industrial IoT: A Survey. *IEEE Internet Things J.* **2020**, *7*, 13212–13225.
26. Park, J.; Kim, H.; Lee, D. Digital Twin for Cybersecurity in Autonomous Vehicles: A Survey. In Proceedings of the 2021 IEEE International Conference on Autonomous Systems (ICAS), Montréal, QC, Canada, 11–13 August 2021; pp. 98–105.
27. Homaei, M.; Mogollon Gutierrez, O.; Sancho Nunez, J.C.; Avila Vegas, M.; Caro Lindo, A. A Review of Digital Twins and Their Application in Cybersecurity Based on Artificial Intelligence. *arXiv* **2023**, arXiv:2311.01154. [CrossRef]
28. Wang, Y.; Su, Z.; Guo, S.; Dai, M.; Luan, T.H.; Liu, Y. A Survey on Digital Twins: Architecture, Enabling Technologies, Security and Privacy, and Future Prospects. *arXiv* **2023**, arXiv:2301.13350. [CrossRef]
29. Liu, S.; Leng, J.; Zhang, H. Digital Twin for Cyber-Physical System in Industry 4.0: A Comprehensive Review. In Proceedings of the 2019 IEEE International Conference on Systems, Man and Cybernetics (SMC), Bari, Italy, 6–9 October 2019; pp. 1897–1902.
30. Buchholz, M.; Suri, N.; Hensley, B. Cyber Resilience and Autonomous Digital Twins. In *Lecture Notes in Computer Science*; Springer: Berlin/Heidelberg, Germany, 2023. [CrossRef]
31. Yoon, J.; Kim, Y.; Seo, J. Secure Communication in Digital Twin Systems with Blockchain Integration. *Sensors* **2020**, *20*, 6458.
32. Marksteiner, S.; Bronfman, S.; Wolf, M.; Lazebnik, E. Using Cyber Digital Twins for Automated Automotive Cybersecurity Testing. In Proceedings of the 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Vienna, Austria, 7–11 September 2021; pp. 123–128.
33. Elayan, H.; Shrestha, R.; Tang, J. Digital Twin in Smart Cities: Cybersecurity and Privacy Challenges. In Proceedings of the 2020 IEEE International Smart Cities Conference (ISC2), Virtually, 28 September–1 October 2020; pp. 1–7.
34. de Hoz Diego, J.D.; Temperekidis, A.; Katsaros, P.; Konstantinou, C. An iot digital twin for cyber-security defence based on runtime verification. In Proceedings of the Leveraging Applications of Formal Methods, Verification and Validation. Verification Principles: 11th International Symposium, ISoLA 2022, Rhodes, Greece, 22–30 October 2022; Proceedings, Part I; Springer: Berlin/Heidelberg, Germany, 2022; pp. 556–574.
35. Tan, L.; Li, W.; Wang, X.; Huang, X. Security in Cyber-Physical Systems: The Role of Digital Twins. *IEEE Internet Things J.* **2020**, *7*, 4438–4446.
36. Bonney, M.; de Angelis, M.; Dal Borgo, M.; Andrade, L.; Beregi, S.; Jamia, N.; Wagg, D. Development of a digital twin operational platform using Python Flask. *Data-Centric Eng.* **2022**, *3*, e1. [CrossRef]
37. Zhang, P.; Cui, M.; Li, X. Digital Twins for Cybersecurity in Smart Manufacturing: A Framework. *IEEE Access* **2020**, *8*, 57902–57911.
38. Damjanovic-Behrendt, V.; Hofmann, C. A privacy-aware digital twin for smart grid operations. *Energy Procedia* **2017**, *114*, 389–394.
39. Damjanovic-Behrendt, V. A digital twin-based privacy enhancement mechanism for the automotive industry. In Proceedings of the 2018 International Conference on Intelligent Systems (IS), Funchal, Portugal, 25–27 September 2018; pp. 272–279.

40. Uslar, M.; Rosinger, C.; Schlegel, S. Security by design for the smart grid: Combining SGAM and NISTIR 7628. *IEEE Trans. Smart Grid* **2021**, *10*, 123–130.
41. Lee, J.; Bagheri, B.; Kao, H. Security of Digital Twins for Cyber-Physical Systems in Smart Manufacturing. *Comput. Ind.* **2020**, *109*, 76–83.
42. Jiang, Y.; Wang, S.; Feng, X. Digital Twins for Cybersecurity in Healthcare Systems: A Survey. *IEEE Access* **2020**, *8*, 69013–69022.
43. He, Y.; Sun, J.; Liu, Z. Digital Twin and Its Cybersecurity Challenges. *IEEE Trans. Ind. Inform.* **2021**, *17*, 1420–1430.
44. Henry, P.; Radcliffe, M.; Freeman, S. Cybersecurity for Digital Twins in Smart Grids: A Comprehensive Review. *IEEE Access* **2019**, *7*, 35958–35977.
45. Wolf, M. Threat Modeling Tool extension for Penetration Tester (TMTe4PT). Master Thesis, Deggendorf Institute of Technology, Deggendorf, Germany, 2019.
46. Fernandez de Arroyabe, I.; Watson, T.; Angelopoulou, O. Cybersecurity in the Automotive Industry: A Systematic Literature Review (SLR). *J. Comput. Inf. Syst.* **2023**, *63*, 716–734. [CrossRef]
47. de Oliveira, L.P.; Wehrmeister, M.A.; de Oliveira, A. Systematic literature review on automotive diagnostics. In Proceedings of the 2017 VII Brazilian Symposium on Computing Systems Engineering (SBESC), Curitiba, PR, Brazil, 6–10 November 2017; pp. 1–8.
48. Kim, K.; Kim, J.S.; Jeong, S.; Park, J.H.; Kim, H.K. Cybersecurity for autonomous vehicles: Review of attacks and defense. *Comput. Secur.* **2021**, *103*, 102150. [CrossRef]
49. Bhatti, G.; Mohan, H.; Singh, R.R. Towards the future of smart electric vehicles: Digital twin technology. *Renew. Sustain. Energy Rev.* **2021**, *141*, 110801. [CrossRef]
50. Jones, D.; Snider, C.; Nassehi, A.; Yon, J.; Hicks, B. Characterising the Digital Twin: A systematic literature review. *Cirp J. Manuf. Sci. Technol.* **2020**, *29*, 36–52. [CrossRef]
51. El-Sayed, M.; Sankar, S.; Prasad, M.; Badr, Y. Edge of Things: The Big Picture on the Integration of Edge, IoT and the Digital Twin. *J. Parallel Distrib. Comput.* **2021**, *144*, 171–185.
52. Schwarz, C.; Wang, Z. The role of digital twins in connected and automated vehicles. *IEEE Intell. Transp. Syst. Mag.* **2022**, *14*, 41–51. [CrossRef]
53. Semeraro, C.; Lezoche, M.; Panetto, H.; Dassisti, M. Digital twin paradigm: A systematic literature review. *Comput. Ind.* **2021**, *130*, 103469. [CrossRef]
54. Kitchenham, B.A.; Charters, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*; Technical Report EBSE 2007-001; Software Engineering Group, School of Computer Science and Mathematics, Keele University: Keele, Staffordshire, UK; Department of Computer Science, University of Durham: Durham, UK, 2007.
55. Altair. One Total Twin. Available online: https://altair.com/one-total-twin/ (accessed on 17 June 2025).
56. Autodesk. Digital Twin: Unlock the Value of the Physical and Digital Worlds. Available online: https://www.autodesk.eu/campaigns/digital-twin (accessed on 17 June 2025).
57. Amazon Web Services, Inc. AWS IoT TwinMaker. Available online: https://aws.amazon.com/iot-twinmaker/ (accessed on 17 June 2025).
58. Ahmad, F.; Adnane, A.; Franqueira, V.N. A systematic approach for cyber security in vehicular networks. *J. Comput. Commun.* **2016**, *4*, 38–62. [CrossRef]
59. Bozdal, M.; Randa, M.; Samie, M.; Jennions, I. Hardware trojan enabled denial of service attack on can bus. *Procedia Manuf.* **2018**, *16*, 47–52. [CrossRef]
60. Singh, A.; Singh, M. An empirical study on automotive cyber attacks. In Proceedings of the 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 5–8 February 2018; pp. 47–50.
61. He, C.; Luan, T.H.; Lu, R.; Su, Z.; Dong, M. Security and Privacy in Vehicular Digital Twin Networks: Challenges and Solutions. *IEEE Wirel. Commun.* **2022**, *30*, 154–160. [CrossRef]
62. Salfer, M.; Eckert, C. Attack surface and vulnerability assessment of automotive electronic control units. In Proceedings of the 2015 12th International Joint Conference on e-Business and Telecommunications (ICETE), Colmar, France, 20–22 July 2015; Volume 4, pp. 317–326.
63. Bozdal, M.; Samie, M.; Jennions, I. A survey on can bus protocol: Attacks, challenges, and potential solutions. In Proceedings of the 2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE), Southend, UK, 16–17 August 2018; pp. 201–205.
64. Kang, T.U.; Song, H.M.; Jeong, S.; Kim, H.K. Automated reverse engineering and attack for CAN using OBD-II. In Proceedings of the 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall), Chicago, IL, USA, 27–30 August 2018; pp. 1–7.
65. Komissarov, R.; Wool, A. Spoofing attacks against vehicular FMCW radar. In Proceedings of the 5th Workshop on Attacks and Solutions in Hardware Security, Virtual, 19 November 2021; pp. 91–97.

66. Kamal, M.; Barua, A.; Vitale, C.; Laoudias, C.; Ellinas, G. GPS location spoofing attack detection for enhancing the security of autonomous vehicles. In Proceedings of the 2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall), Virtually, 27–30 September 2021; pp. 1–7.
67. Franke, U.; Cohen, M.; Sigholm, J. What can we learn from enterprise architecture models? An experiment comparing models and documents for capability development. *Softw. Syst. Model.* **2018**, *17*, 695–711. [CrossRef]
68. Macher, G.; Sporer, H.; Berlach, R.; Armengaud, E.; Kreiner, C. Sahara: A security-aware hazard and risk analysis method. In Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition (DATE), Grenoble, France, 9–13 March 2015; pp. 621–624.
69. Cui, J.; Sabaliauskaite, G. Us 2: An unified safety and security analysis method for autonomous vehicles. In Proceedings of the Advances in Information and Communication Networks: Proceedings of the 2018 Future of Information and Communication Conference (FICC), Singapore, 5–6 April 2018; Springer: Berlin/Heidelberg, Germany, 2018; Volume 1, pp. 600–611.
70. Martin, J.; Carter, A. Nhtsa cybersecurity research. In Proceedings of the 25th International Technical Conference on the Enhanced Safety of Vehicles (ESV). National Highway Traffic Safety Administration, Detroit, MI, USA, 5–8 June 2017.
71. Knight, A. The Hitchhiker's Guide To Hacking Connected Cars: Methodology and Jump Kit Readiness. Available online: https://alissaknight.medium.com/the-hitchhikers-guide-to-hacking-connected-cars-methodology-and-jump-kit-readiness-3efcab428210 (accessed on 4 November 2017).
72. Ruddle, A.R.; Weyl, B.; Idrees, S.; Roudier, Y.; Friedewald, M.; Leimbach, T.; Fuchs, A.; Gürgens, S.; Henninger, O.; Rieke, R.; et al. *Security Requirements for Automotive On-Board Networks Based on Dark-Side Scenarios. Deliverable D2.3: EVITA—E-Safety Vehicle Intrusion Protected Applications*; Technical Report, Project No. 224275, Seventh Framework Programme (FP7); Fraunhofer Institute for Secure Information Technology SIT: Darmstadt, Germany, 2009. Available online: https://www.evita-project.org/Publications/EVITA_D2.3.pdf (accessed on 17 June 2025).
73. Ruijters, E.; Stoelinga, M. Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools. *Comput. Sci. Rev.* **2015**, *15*, 29–62. [CrossRef]
74. Izosimov, V.; Asvestopoulos, A.; Blomkvist, O.; Törngren, M. Security-aware development of cyber-physical systems illustrated with automotive case study. In Proceedings of the 2016 Design, Automation & Test in Europe Conference & Exhibition (DATE), Dresden, Germany, 14–18 March 2016; pp. 818–821.
75. Hillenbrand, P.; Tenbohlen, S.; Keller, C.; Spanos, K. Understanding conducted emissions from an automotive inverter using a common-mode model. In Proceedings of the 2015 IEEE International Symposium on Electromagnetic Compatibility (EMC), Dresden, Germany, 16–22 August 2015; pp. 685–690.
76. Wang, Y.; Yu, B.; Yu, H.; Xiao, L.; Ji, H.; Zhao, Y. Automotive cybersecurity vulnerability assessment using the common vulnerability scoring system and bayesian network model. *IEEE Syst. J.* **2022**, *17*, 2880–2891. [CrossRef]
77. Schmittner, C.; Ma, Z.; Schoitsch, E.; Gruber, T. A case study of fmvea and chassis as safety and security co-analysis method for automotive cyber-physical systems. In Proceedings of the 1st ACM Workshop on Cyber-Physical System Security, Singapore, 14–17 April 2015; ACM: New York, NY, USA, 2015; pp. 69–80.
78. Park, S.; Park, H. Pier: Cyber-resilient Risk Assessment Model for Connected and Autonomous Vehicles. *Wirel. Netw.* **2024**, *30*, 4591–4605. [CrossRef]
79. Monteuuis, J.P.; Boudguiga, A.; Zhang, J.; Labiod, H.; Servel, A.; Urien, P. Sara: Security automotive risk analysis method. In Proceedings of the 4th ACM Workshop on Cyber-Physical System Security, Incheon, Republic of Korea, 4 June 2018; pp. 3–14.
80. Zhang, Y.; Chu, L.; Ou, Y.; Guo, C.; Liu, Y.; Tang, X. A cyberphysical system-based velocity-profile prediction method and case study of application in plug-in hybrid electric vehicle. *IEEE Trans. Cybern.* **2019**, *51*, 40–51. [CrossRef]
81. Fang, W.; Zhang, W.; Chen, W.; Pan, T.; Ni, Y.; Yang, Y. Trust-based attack and defense in wireless sensor networks: A survey. *Wirel. Commun. Mob. Comput.* **2020**, *2020*, 1–20. [CrossRef]
82. Dietz, M.; Vielberth, M.; Pernul, G. Integrating digital twin security simulations in the security operations center. In Proceedings of the 15th International Conference on Availability, Reliability and Security, Virtually, 25–28 August 2020; pp. 1–9.
83. Toyama, T.; Yoshida, T.; Oguma, H.; Matsumoto, T. Pasta: Portable automotive security testbed with adaptability. In Proceedings of the Black Hat Europe, London, UK, 3–6 December 2018.
84. Shevchenko, N.; Chick, T.A.; O'Riordan, P.; Scanlon, T.P.; Woody, C. *Threat Modeling: A Summary of Available Methods*; Technical Report; Carnegie Mellon University Software Engineering Institute: Pittsburgh, PA, USA, 2018.
85. Fraile, M.; Ford, M.; Gadyatskaya, O.; Kumar, R.; Stoelinga, M.; Trujillo-Rasua, R. Using attack-defense trees to analyze threats and countermeasures in an ATM: A case study. In Proceedings of the Practice of Enterprise Modeling: 9th IFIP WG 8.1. Working Conference, PoEM 2016, Skövde, Sweden, 8–10 November 2016; Proceedings; Springer: Berlin/Heidelberg, Germany, 2016; Volume 9, pp. 326–334.
86. Do, Q.; Mirakhorli, M. Cyber Resilience of Digital Twin Systems in Critical Infrastructures. *IEEE Trans. Dependable Secur. Comput.* **2019**, *17*, 123–132.
87. Smith, C. *The Car Hacker's Handbook: A Guide for the Penetration Tester*; No Starch Press: San Francisco, CA, USA, 2016.

88. Ebert, C.; Ray, R. Penetration Testing for Automotive Cybersecurity. *ATZelectronics Worldw.* **2021**, *16*, 16–22. [CrossRef]
89. Dürrwang, J.; Braun, J.; Rumez, M.; Kriesten, R.; Pretschner, A. Enhancement of automotive penetration testing with threat analyses results. *SAE Int. J. Transp. Cybersecur. Priv.* **2018**, *1*, 91–112. [CrossRef]
90. Garikapati, D.; Shetiya, S.S. Autonomous Vehicles: Evolution of Artificial Intelligence and the Current Industry Landscape. *Big Data Cogn. Comput.* **2024**, *8*, 42. [CrossRef]
91. Wang, Z.; Gupta, R.; Han, K.; Wang, H.; Ganlath, A.; Ammar, N.; Tiwari, P. Mobility digital twin: Concept, architecture, case study, and future challenges. *IEEE Internet Things J.* **2022**, *9*, 17452–17467. [CrossRef]
92. Pascale, F.; Adinolfi, E.A.; Coppola, S.; Santonicola, E. Cybersecurity in automotive: An intrusion detection system in connected vehicles. *Electronics* **2021**, *10*, 1765. [CrossRef]
93. Dietz, M.; Putz, B.; Pernul, G. A distributed ledger approach to digital twin secure data sharing. In Proceedings of the IFIP Annual Conference on Data and Applications Security and Privacy, Charleston, SC, USA, 15–17 July 2019; Springer International Publishing: Cham, Switzerland, 2019; Volume 11559, pp. 281–300.
94. Eckhart, M.; Ekelhart, A. Towards security-aware virtual environments for digital twins. In Proceedings of the 4th ACM Workshop on Cyber-Physical System Security, Incheon, Republic of Korea, 4 June 2018; pp. 61–72.
95. Katsikeas, S.; Johnsson, P.; Hacks, S.; Lagerström, R. VehicleLang: A probabilistic modeling and simulation language for modern vehicle IT infrastructures. *Comput. Secur.* **2022**, *117*, 102705. [CrossRef]
96. Laaki, H.; Miche, Y.; Tammi, K. Prototyping a digital twin for real-time remote control over mobile networks. *IEEE Access* **2020**, *8*, 5823–5832.
97. Oka, D.K. Trends of Automotive Threats and Attacks. Technical Report; In Proceedings of the GlobalPlatform Cybersecurity Vehicle Forum, Tokyo, Japan, 22 May 2025.
98. Harbor, B. Digital Twins in Automotive Cybersecurity: A Smarter Way for TARA, 2025. Published on Block Harbor Insights. Available online: https://www.blockharbor.io/blog/digital-twins-in-automotive-cybersecurity-a-smarter-way-for-tara (accessed on 16 June 2025).
99. Das, P.; Al Asif, M.R.; Jahan, S.; Ahmed, K.; Bui, F.M.; Khondoker, R. STRIDE-Based Cybersecurity Threat Modeling, Risk Assessment and Treatment of an In-Vehicle Infotainment System. *Vehicles* **2024**, *6*, 1140–1163. [CrossRef]
100. AbdulGhaffar, A.; Matrawy, A. LLMs' Suitability for Network Security: A Case Study of STRIDE Threat Modeling. *arXiv* **2025**, arXiv:2505.04101. [CrossRef]
101. Kang, Y.; Wen, J.; Kang, J.; Zhang, T.; Du, H.; Niyato, D.; Yu, R.; Xie, S. Hybrid-Generative Diffusion Models for Attack-Oriented Twin Migration in Vehicular Metaverses. *arXiv* **2024**, arXiv:2407.11036. [CrossRef]
102. Voas, J.; Mell, P.; Laplante, P.; Piroumian, V. *Security and Trust Considerations for Digital Twin Technology*; Technical Report NIST IR 8356; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2025. [CrossRef]
103. Farsi, M.; Daneshkhah, A.; Hosseinian-Far, A.; Jahankhani, H. (Eds.) *Digital Twin Technologies and Smart Cities*; Springer: Berlin/Heidelberg, Germany, 2020.
104. Sivarethinamohan, R.; Reddy, R.S. Digital Twin for Smart City Resilience and Solutions. In *Digital Twin and Blockchain for Smart Cities*; Wiley: Hoboken, NJ, USA, 2024. [CrossRef]
105. Korman, M.; Välja, M.; Björkman, G.; Ekstedt, M.; Vernotte, A.; Lagerström, R. Analyzing the effectiveness of attack countermeasures in a SCADA system. In Proceedings of the 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids, SPSR-SG@CPSWeek, Pittsburgh, PA, USA, 21 April 2017; pp. 73–78.
106. Ross, J.W. Enterprise architecture: Driving business benefits from it. *Ssrn Electron. J.* **2006**, 1–15. [CrossRef]
107. Iacob, M.E.; Meertens, L.; Jonkers, H.; Quartel, D. From enterprise architecture to business models and back. *Softw. Syst. Model.* **2014**, *13*, 1059–1083. [CrossRef]
108. Dodge, M.; Kitchin, R. The challenges of cybersecurity for smart cities. In *Creating Smart Cities*; Coletta, C., Evans, L., Heaphy, L., Kitchin, R., Eds.; Routledge: London, UK, 2018. [CrossRef]
109. Al-Issa, Y.; Soltanisehat, L.; Bertino, E. Cybersecurity in Digital Twin for Industrial IoT: Challenges and Solutions. *IEEE Trans. Ind. Electron.* **2018**, *65*, 1533–1544.
110. Yu, S.; Zhou, Y.; Xu, J. Cybersecurity Framework for Digital Twins in Industrial IoT Environments. *Future Gener. Comput. Syst.* **2019**, *94*, 451–466.
111. Hearn, M.; Rix, S. Cybersecurity considerations for digital twin implementations. *IIC J. Innov.* **2019**, *10*, 107–113.
112. Wei, X.; Zhang, W.; Lu, R. Digital Twin for Smart Grid Security: Architecture and Applications. *J. Grid Comput.* **2018**, *16*, 479–497.
113. Zhang, J.; Yang, G.; Jiang, L. A Digital Twin-Based Approach for Improving the Cybersecurity of Industrial Control Systems. In Proceedings of the 2019 IEEE International Conference on Cyber-Physical Systems (ICCPS), Montreal, QC, Canada, 16–18 April 2019; pp. 347–350.
114. Coletta, C.; Evans, L.; Heaphy, L.; Kitchin, R. (Eds.) *Creating Smart Cities*; Routledge: London, UK, 2019.
115. Groshev, O.; Shishkov, B.; Qiao, Y. Towards Secure Digital Twins for IoT-Enabled Smart Manufacturing. *Int. J. Secur. Netw.* **2019**, *14*, 191–201.

116. Kaur, M.; Mishra, V.; Maheshwari, P. The convergence of digital twin, IoT, and machine learning: Transforming data into action. In *Digital Twin Technologies and Smart Cities*; Springer International Publishing: Cham, Switzerland, 2020; pp. 3–17.
117. Raza, M.; Saeed, M.J.; Riaz, M.B.; Sattar, M.A. Federated Learning for Privacy-Preserving Intrusion Detection in Software-Defined Networks. *IEEE Access* **2024**, *12*, 69551–69567. [CrossRef]
118. Smart Nation and Digital Government Office. Singapore's Smart City Initiatives: A Sustainable Future. Smart Nation Singapore, 2025. Available online: https://www.smartnation.gov.sg/initiatives/smart-city-solutions/ (accessed on 16 March 2025).
119. Li, Y.; Peng, P.; Xu, Y.; Huang, H. Blockchain-Enabled Digital Twins: Secure and Efficient Cyber-Physical Systems. *IEEE Access* **2021**, *9*, 3488–3501.
120. Gheisari, M.; Ali, S. Blockchain for Digital Twin Management and Security in Internet of Things. In Proceedings of the 2020 IEEE International Conference on Blockchain, Rhodes Island, Greece, 2–6 November 2020; pp. 43–50.
121. European Commission. Rolling Plan for ICT Standardisation 2025. Available online: https://interoperable-europe.ec.europa.eu/collection/rolling-plan-ict-standardisation/rolling-plan-2025 (accessed on 27 April 2024).
122. Eckhart, M.; Ekelhart, A. A specification-based state replication approach for digital twins. In Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and Privacy, Toronto, ON, Canada, 15–19 October 2019; pp. 36–47.
123. El-Hajj, M. Systematic literature review: Digital twins' role in enhancing security for Industry 4.0 applications. *Secur. Priv.* **2024**, *7*, e396. [CrossRef]
124. Ozkan-Okay, M.; Akin, E.; Aslan, Ö.; Kosunalp, S.; Iliev, T.; Stoyanov, I.; Beloev, I. A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cybersecurity solutions. *IEEE Access* **2024**, *12*, 12229–12256. [CrossRef]
125. Karafili, E.; Bales, K.; Lupu, E. A Formal Approach for Digital Twins of Critical Infrastructures. *Int. J. Crit. Infrastruct. Prot.* **2018**, *22*, 32–43.