IEEE Open Journal of Vehicular Technology

Received 15 July 2025; accepted 20 July 2025. Date of publication 23 July 2025;
date of current version 15 August 2025. The review of this article was coordinated by Editor Rongxing Lu.

Digital Object Identifier 10.1109/OJVT.2025.3592041

Zero Trust Architecture for Electric Transportation Systems: A Systematic Survey and Deep Learning Framework for Replay Attack Detection

GRACE MURIITHI [1] (Graduate Student Member, IEEE), BEHNAZ PAPARI [1] (Senior Member, IEEE), ALI ARSALAN [1] (Graduate Student Member, IEEE), LAXMAN TIMILSINA [2] (Member, IEEE), ALEX MURIITHI [3], ELUTUNJI BURAIMOH [2], ASIF KHAN[2], GOKHAN OZKAN [2] (Senior Member, IEEE), CHRISTOPHER EDRINGTON [2] (Senior Member, IEEE), AND AKRAM PAPARI [4]

[1]Department of Automotive Engineering, Clemson University, Clemso, SC 29634 USA
[2]Department of Electrical and Computer Engineering, Clemson University, Clemson, SC 29634 USA
[3]Montclair State University, Montclair, NJ 07043 USA
[4]University of Tehran, Tehran 14155-6619, Iran

CORRESPONDING AUTHORS: ALEX MURIITHI; AKRAM PAPARI (e-mail: muriithia1@montclair.edu; apapari1973@gmail.com)

This work was supported by Clemson University's Virtual Prototyping of Autonomy Enabled Ground Systems (VIPR-GS) under Agreement W56HZV-21-2-0001 through the U.S. Army DEVCOM Ground Vehicle Systems Center.

ABSTRACT Modern and autonomous hybrid electric vehicles (HEVs), as complex cyber-physical systems, represent a key innovation in the future of transportation. However, the increasing interconnectivity and reliance on digital components expose these vehicles to significant cybersecurity risks. To address these challenges, Zero Trust Architecture (ZTA) has emerged as a promising security framework. Operating on the principle of 'never trust, always verify,' ZTA offers a comprehensive approach to ensuring continuous trust verification in HEV systems. Despite its potential, the application of ZTA within cyber-physical vehicular systems remains underexplored, and its practical benefits and limitations are not yet fully understood by the engineering community. To bridge this gap, this article presents a detailed survey of ZTA tailored specifically to the needs of vehicular CPSs, highlighting existing technologies, security challenges, and the application of zero-trust principles in HEVs. Additionally, this work proposes a deep learning-based replay attack detection scheme for the battery management system (BMS) of HEVs. The approach leverages a deep learning model to estimate the battery's State of Charge (SoC), analyzing the Error of Estimation using the Inter-Quartile Range (IQR) technique. The detection system analyzes the Error of Estimation using the IQR technique, demonstrating a 74.25% containment ratio and detecting deviations up to 2.39 units during attack scenarios. The system maintains a balanced detection sensitivity with 25.75% detection density. While the proposed method demonstrates high effectiveness in detecting stealth replay attacks through simulation results, it faces certain limitations including computational overhead for real-time processing, dependence on high-quality training data, and potential vulnerability to adversarial attacks on the underlying deep learning model. These challenges highlight the need for careful consideration in practical implementations while opening avenues for future research.

INDEX TERMS Hybrid-electric vehicles, cyber-physical system security, replay attacks, zero trust architecture, controller security, trust assessment.

I. INTRODUCTION

Cyber-physical systems (CPSs) are at the forefront of modern technological advancements, seamlessly integrating computational processes with physical systems to create a unified environment capable of performing complex tasks. These systems, which span a wide range of industries, including automotive, energy, and healthcare, enable intelligent and efficient operations through the interaction of embedded hardware and software components [1]. However, the growing sophistication of CPSs comes with increasing vulnerabilities that expose them to a variety of cyberattacks. These vulnerabilities are exacerbated by the interconnectedness of system components and the rising number of entry points for malicious actors. As CPSs evolve in complexity and scale, they become susceptible to increasingly sophisticated cyberattacks, which can result in system malfunctions, infrastructure damage, financial losses, and even endanger human life [2]. Numerous incidents serve as cautionary examples of the real-world consequences of cyber vulnerabilities in CPSs. The "Stuxnet" worm, which disrupted Iran's nuclear program in 2010, and the massive blackout caused by a false data injection attack in Ukraine in 2015 that left over 225,000 customers without power [3], underscore the catastrophic potential of such threats. Similarly, the U.S. Colonial Pipeline shutdown in 2021 due to a ransomware attack highlights the vulnerability of critical infrastructure to cyber threats [4]. More recent attacks, such as those on German wind farms in 2022 and the Red Echo APT attack on Indian power sectors in 2021 [5], [6], reveal the persistent and evolving nature of cyberattacks targeting CPSs. In fact, cyber intrusions in the transportation and mobility sector have surged in scale: an industry report documented 409 new automotive-related cyber incidents in 2024 (up from 295 in 2023), with nearly 60% of these events impacting "thousands to millions" of vehicles, charging stations, or other connected assets [2], [7].

Among CPSs, hybrid electric vehicles (HEVs) have become increasingly vulnerable due to the integration of Internet of Things (IoT) technologies and numerous embedded Electronic Control Units (ECUs) [1]. These vehicles rely on a complex network of sensors and controllers to manage critical operations such as braking, steering, and power distribution. If compromised, these systems can lead to catastrophic outcomes, endangering vehicle occupants and public safety. Given the essential role HEVs play in modern transportation, safeguarding these systems from cyber threats is a top priority. In July 2015, two researchers demonstrated the severity of such vulnerabilities by remotely exploiting software weaknesses in a Jeep Cherokee, taking control of safety-critical systems and leading to alarming consequences (including disabling the vehicle's brakes and causing a loss of control). Similarly, researchers successfully hacked a Tesla through Wi-Fi and cellular connections, further underscoring the potential risks. Beyond these high-profile demonstrations, in 2024 cybersecurity researchers uncovered a severe vulnerability in Kia's connected-car system that allowed remote takeover of critical functions using only the vehicle's license plate number [8], demonstrating how even cutting-edge connectivity features can become unexpected attack vectors.

One promising approach to bolstering the security of CPSs, including modern HEVs, is the adoption of Zero Trust Architecture (ZTA). ZTA represents a fundamental shift from traditional security models that relied on defined network perimeters and assumed inherent trust within those boundaries. Instead, ZTA operates under the principle of "never trust, always verify," applying strict access controls and continuously assessing the trustworthiness of every entity (be it users, devices, or network nodes) regardless of its location or previous authentication status. By enforcing rigorous verification processes and dynamic access policies, ZTA provides a robust defense against both known and unknown threats, including sophisticated zero-day exploits [9]. While ZTA offers promising solutions for HEV security, it exists within a rich ecosystem of cybersecurity approaches, each with distinct characteristics and applications:

1) *Traditional Perimeter Security in HEVs:*
   - Relies on defense-in-depth strategies with firewalls and intrusion detection systems
   - Assumes trust within network boundaries
   - Limitations: Vulnerable to internal threats and increasingly inadequate for modern distributed HEV architectures
2) *Authentication-Based Security:*
   - Implements multi-factor authentication (MFA) and Public Key Infrastructure (PKI)
   - Focus on identity verification at access points
   - Limitations: May not address continuous verification needs in dynamic HEV operations
3) *Behavioral Analysis and Machine Learning:*
   - Uses AI/ML for anomaly detection in vehicle networks
   - Adaptive learning of normal operation patterns
   - Limitations: Requires significant training data and may produce false positives
4) *Blockchain-Based Solutions:*
   - Ensures immutable record-keeping for vehicle operations
   - Enables secure peer-to-peer communication
   - Limitations: High computational overhead and scalability challenges
5) *Role-Based Access Control (RBAC):*
   - Assigns access rights based on predefined roles
   - Simplifies security administration
   - Limitations: Less flexible for dynamic trust relationships in modern HEVs

ZTA addresses many limitations of these approaches through its "never trust, always verify" principle, which is particularly suited for the dynamic, open-ended threat surface of HEV systems. As outlined by the National Institute of Standards and Technology (NIST), the core tenets of ZTA include least privilege access, continuous monitoring, risk-based trust evaluation, and the inherent assumption that no entity can be fully trusted by default [9]. For example, Dhiman et al. [10] and Nahar et al. [11] offered comprehensive surveys covering

ZTA concepts like access control, micro-segmentation, and identity verification. These works also highlight ZTA challenges and the need for future research on intelligent and automated ZTA frameworks, especially for 5 G/6 G networks. Yeoh et al. [12] identified eight success factors for enterprise ZTA implementation and proposed a maturity model for evaluation. Ahmadi [13] studied ZTA in cloud networks, finding significant reductions in insider threats and lateral movement. Adoption is growing, with Gartner reporting widespread implementation among large enterprises by 2024. Liu et al. [14] proposed a ZTA-based security architecture that leverages AI and novel air interface technologies to enhance identity authentication, access control, and data transmission in IoT environments. Their approach excels in adaptive threat response, achieving a 98% detection rate for unauthorized access attempts, though its reliance on complex AI models introduces latency concerns that could be problematic for real-time vehicle systems. Similarly, Sedjelmaci et al. [15] developed a ZTA-empowered attack detection framework for 6 G edge computing, using security rules and machine learning algorithms to accurately detect and mitigate attacks. The framework's strength lies in a hierarchical trust evaluation mechanism that reduced false positives by 40% compared to traditional approaches, but it assumes consistent network connectivity, an assumption that may not hold in all automotive scenarios. Huber et al. [16] introduced *Zero Trust+*, a trust-management enhancement that significantly improves processing efficiency (by approximately 20%) in large-scale IoT deployments without compromising security integrity. Their innovative caching mechanism for trust decisions particularly stands out, though the optimization assumes periodic network traffic patterns that differ from the bursty, event-driven traffic typical in vehicle networks. Zhang et al. [17] extended the application of ZTA to power IoT systems, designing a security protection architecture based on continuous identity authentication and dynamic access control. Their work's strength lies in handling distributed power systems with multiple control nodes, achieving sub-millisecond authentication times, though the approach requires dedicated security hardware that may be cost-prohibitive for automotive applications. Hussain et al. [18] integrated federated learning with ZTA to enable AI-driven adaptive trust decisions. On the other hand, Pokhrel et al. [19] combined blockchain and anomaly detection in ZTA for resilient network defense. Amusuo et al. [20] proposed ZTDJava to sandbox third-party libraries in a zero-trust environment, extending ZTA to software dependencies.

While these advances demonstrate ZTA's effectiveness in securing digital infrastructure, the application of ZTA to CPSs, specifically HEVs, remains underexplored due to the unique challenges posed by the intricate interactions between cyber and physical components. For instance, a recent comprehensive survey underscored Zero Trust as a critical paradigm for connected vehicles in the face of escalating threats, yet also emphasized the difficulties of integrating zero-trust models into the highly dynamic, real-time automotive environment [1]. Although ZTA has proven effective in enhancing security in IT and IoT domains, further research and development efforts are needed to adapt zero-trust principles for CPS environments. Unlike enterprise computing systems (which are optimized for general-purpose tasks), CPSs are often tailored for specific functionalities and have strict real-time performance requirements. These systems tightly combine physical and digital components, with cyber elements interacting with physical processes in a cross-layer manner. The complexity of these interactions poses challenges for straightforward adoption of traditional ZTA implementations, particularly when safeguarding CPSs [21]. Historically, embedded control systems were considered secure once installed, especially when placed in supposedly protected environments, but this mindset is now obsolete. Today's integrated physical-digital systems are highly adaptable and frequently updated to remain resilient. Unfortunately, this flexibility introduces new vulnerabilities, where digital breaches can cascade into physical system failures. Therefore, it is imperative to adapt and extend ZTA principles to meet the unique requirements of CPSs (particularly in HEVs) and account for cross-layer interactions, as well as the potentially dire consequences of cyber failures on physical components.

Given the numerous advantages of designing CPSs with the zero-trust principle of "never trust, always verify," system designers must integrate technologies that continuously establish and maintain trust in system functionality. Several recent studies have started to explore the application of ZTA to CPSs. Anderson et al. [22] proposed a ZTA framework to protect the sensor and control network of connected and autonomous vehicles (CAVs) via the CAN bus, achieving a remarkable 95% reduction in unauthorized message propagation while maintaining CAN bus latency requirements. However, their approach struggles under bandwidth-intensive scenarios common in modern powertrains. Feng et al. [23] introduced ZTA-based solutions focused on a "Cyber-Physical ZTA" subset, incorporating a multi-layer access control engine and an integrated physical model-based/data-driven policy optimizer. This hybrid approach successfully balances security with performance, achieving false positive rates as low as 0.1% in anomaly detection, though the computational overhead may challenge resource-constrained automotive ECUs. Additionally, Vai et al. [24] and Hasan et al. [25] emphasized the importance of the "never trust, always verify" principle, with Vai applying it to the design of a small drone for enhanced survivability, demonstrating a 60% reduction in attack surface through lightweight cryptographic primitives, and Hasan identifying ZTA architectural patterns for CPSs using the Architecture Analysis and Design Language (AADL), enabling formal verification of security properties with 85% vulnerability detection rate during design phase. While Vai's approach offers valuable insights for resource-constrained systems, it sacrifices some real-time guarantees crucial for automotive applications. Hasan's formal methods provide robust security verification but lack specific consideration for power

electronics systems. Motivated by the government-wide push to migrate to ZTA [26], this article explores how modern vehicular systems, particularly HEVs, can benefit from ZTA. In this manuscript, we make two primary contributions under the broad theme of enhancing cybersecurity in vehicular CPSs, while recognizing that each contribution is methodologically distinct:

1) *Zero Trust Architecture Survey for HEVs:* We present a comprehensive survey of Zero Trust Architecture (ZTA) in the context of vehicular cyber-physical systems, particularly hybrid electric vehicles. This survey explores the applications of ZTA in HEVs, the enabling technologies that facilitate its implementation, and the challenges of integrating ZTA into automotive systems. By reviewing existing literature and best practices, we outline how adopting Zero Trust principles can reduce attack surfaces and prevent lateral movement in vehicle networks. The survey not only summarizes the state-of-the-art but also highlights open research issues and potential solutions for applying ZTA to connected and autonomous vehicles.
2) *Replay Attack Detection in BMS using Deep Learning:* We propose a novel deep learning-based scheme to detect replay attacks on the Battery Management System (BMS) of HEVs. This contribution is developed independently of ZTA principles, focusing instead on a targeted security solution at the subsystem level. The scheme employs advanced neural network models to monitor the BMS sensor and control data for anomalies indicative of replay attacks. By learning the normal patterns of battery telemetry, the detector can identify irregularities caused by maliciously retransmitted data, thereby safeguarding the integrity of critical battery parameters such as state-of-charge (SoC). This BMS-focused security mechanism does not rely on Zero Trust frameworks, illustrating a complementary defensive layer that operates within the vehicle's control system.

Although the above two contributions address vehicular cybersecurity from different angles, they together reinforce the overarching goal of the manuscript of improving security in vehicular CPSs. The ZTA survey offers a *macro-level perspective* by examining how a paradigm shift in trust architecture can strengthen the security posture of connected and autonomous vehicles as a whole. In contrast, the BMS replay attack detector provides a *micro-level solution* by protecting a specific critical component of an HEV through machine learning-based anomaly detection. In particular, the deep learning scheme is methodologically distinct and does not employ Zero Trust principles, but it aligns with the broader theme by targeting a concrete vulnerability in the cyber-physical vehicle system. In essence, implementing continuous verification at the network/system architecture level (as advocated by ZTA) and deploying targeted detection mechanisms at the subsystem level are complementary strategies. The remainder of this paper is organized as follows. The remainder of this paper is organized as follows. Section II presents the background and fundamental concepts of Zero Trust Architecture. Section III explores the integration of ZTA in cyber-physical systems, followed by Section IV, which discusses its specific applications in the automotive sector. Section V examines the intersection of ZTA with machine learning for cyberattack detection in CP-HEVs. Section VI analyzes the unique requirements and challenges of implementing ZTA in CP-HEVs. The proposed attack model and detection scheme are detailed in Section VII, with comprehensive simulation results presented in Section VIII. Section IX discusses future challenges and research directions, and finally, Section XI concludes the paper.

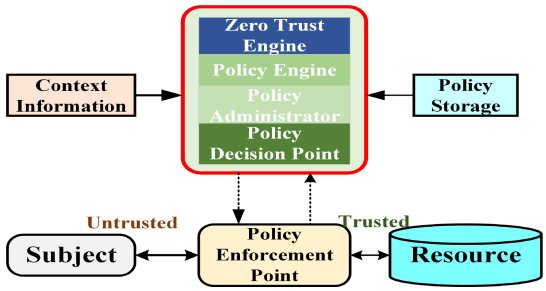

FIGURE 1. Standard ZTA.

II. ZERO TRUST BACKGROUND

ZTA is an advanced cybersecurity framework designed to eliminate the assumption of inherent trust within networks, enforcing strict and continuous verification for access to critical resources [27]. This security model emerged as a response to the increasing complexity of modern CPSs and the growing sophistication of cyber threats. Traditional perimeter-based security models, which assume that entities inside a network are trustworthy, have proven inadequate in safeguarding against today's threats, especially in systems with distributed and interconnected components like connected and autonomous (H)EVs and other CPSs.

A. CORE PRINCIPLES OF ZERO TRUST ARCHITECTURE

At the heart of ZTA is the principle that no entity—whether inside or outside the network—should be trusted by default. ZTA operates on a "never trust, always verify" approach, which mandates continuous identity verification and access validation for every request made to a system's resources [28]. Unlike traditional security approaches, ZTA assumes that threats may already be present within the network, requiring stringent, context-aware access controls at every level.

As illustrated in Fig. 1, ZTA framework is built around several key components:

- *Policy Decision Point (PDP):* The PDP is responsible for making access control decisions. It is divided into two sub-components: the Policy Engine (PE), which evaluates access requests based on security policies

and contextual data, and the Policy Administrator (PA), which enforces the decisions made by the PE.

- *Policy Enforcement Point (PEP):* The PEP is responsible for enforcing the security decisions made by the PDP. It monitors traffic, blocks unauthorized access, and ensures that only authenticated entities are granted permission to interact with system resources.
- *Subjects and Protected Resources:* Subjects refer to users, devices, or processes requesting access to system resources. These entities must undergo rigorous authentication and authorization checks before they are granted access to any resource. Protected resources are the assets within the system that require safeguarding, such as data, applications, or physical components in CPSs like HEVs.
- *Contextual and Behavioral Data:* One of the core strengths of ZTA is its ability to incorporate dynamic context-based security policies. This means that decisions are not solely based on static credentials (such as passwords or tokens) but also on real-time contextual factors such as the location, device type, behavior patterns, and historical trust levels of the subject requesting access [26]. Machine learning techniques, discussed in later sections, can be leveraged to analyze this data continuously, enabling adaptive security responses to evolving threats.

Although ZTA provides a robust and flexible framework, its implementation is not an instantaneous process but a gradual evolution of existing security architectures. Integrating ZTA into complex environments like CPSs requires a phased approach, adapting current systems incrementally to align with ZTA principles. This involves retrofitting legacy systems with modern security protocols and establishing robust mechanisms for monitoring and controlling access across distributed components Fig. 1 [21]. In CPSs, existing security measures such as firewalls and encryption protocols can be augmented with zero trust principles, ensuring that every access request—whether internal or external—is verified based on dynamic policies and contextual data. One major advantage of ZTA is its adaptability. As more industries recognize the limitations of traditional security models, ZTA is increasingly being adopted in sectors ranging from critical infrastructure to healthcare, finance, and transportation. The flexible nature of its policy enforcement mechanisms allows it to be tailored to the specific needs of different environments. In a CPS context, such as modern HEVs, ZTA can provide real-time monitoring and fine-grained access control, ensuring that even if one component is compromised, the rest of the system remains secure [28].

In practice, ZTA relies heavily on advanced policy enforcement and real-time contextual analysis to secure CPSs. The Policy Engine (PE) plays a central role in making access decisions and analyzing incoming requests based on multiple factors, including user identity, device integrity, network traffic, and historical behavior patterns. As shown in Fig. 1, when a subject—such as an ECU or a remote diagnostic tool in an HEV—makes an access request, the PEP intercepts the traffic and relays it to the PE. The PE then cross-references this request against existing policies and real-time contextual information to determine whether access should be granted or denied. For instance, in a series HEV with integrated ZTA, a remote request to update the vehicle's BMS firmware [29] would not be automatically trusted. Instead, the ZTA framework would dynamically evaluate the request based on the current context—such as the location of the request, the identity of the user, the device being used, and the historical trustworthiness of both the user and device. If any of these factors raise suspicion, access to the BMS would be denied, preventing potential malicious activity. While the ZTA model offers significant advantages in securing CPSs, particularly in environments like HEVs, its full implementation comes with challenges. Resource-constrained devices, such as low-power sensors and embedded ECUs [30], may struggle with the overhead associated with continuous verification and real-time decision-making. Additionally, integrating ZTA into existing legacy systems often requires substantial updates to the infrastructure, which can be costly and time-consuming.

III. ZERO TRUST ARCHITECTURE IN CYBER-PHYSICAL SYSTEMS

ZTA has become a pivotal security framework for protecting digital infrastructure in both traditional IT systems and CPSs. CPSs are deeply integrated into modern society, spanning sectors such as energy, healthcare, transportation, industrial control systems, and smart cities. These systems combine physical processes with digital controls, introducing complexities that expose them to sophisticated cyber threats. As CPSs evolve, the growing interconnectedness of devices, sensors, and networks amplifies security vulnerabilities, necessitating more robust defense mechanisms like ZTA. ZTA's core principle of *"never trust, always verify"* is especially pertinent to CPSs, where both internal and external threats can severely compromise system integrity. Unlike traditional security models that assume inherent trust within network perimeters, ZTA assumes no inherent trust and requires constant verification of entities, whether they are internal or external to the network. This approach fits well with the needs of CPSs, where systems control critical physical infrastructure, making them high-value targets for cyberattacks. Below, we explore how ZTA has been adapted across different CPS sectors, highlighting its role in safeguarding critical infrastructure.

A. ENERGY SYSTEMS: SMART GRIDS AND POWER INFRASTRUCTURE

One of the most significant applications of ZTA in CPSs is within energy systems, particularly in smart grids. Smart grids represent a modern power grid system that incorporates advanced communication networks, sensors, and control systems to improve efficiency and reliability. However, their reliance on interconnected devices and distributed energy resources increases their attack surface, making them vulnerable to cyberattacks that can disrupt power distribution or damage infrastructure [31].

Researchers have focused on adapting ZTA principles to smart grids by implementing multi-layered access controls and continuous monitoring of system activities. For instance, continuous identity verification prevents unauthorized access to power control systems and substations. Zhang et al. [17] proposed a Zero Trust security architecture for power IoT networks, where continuous identity authentication and dynamic access control mechanisms were employed to secure communication between distributed energy resources and central control stations. This architecture ensures that only authenticated entities can interact with critical grid infrastructure, reducing the likelihood of data tampering or control system hijacking. Authors in [32] proposed a comprehensive ZTA tailored for Virtual Power Plants (VPPs) and Distributed Energy Resources (DERs), addressing the growing cybersecurity challenges in the energy sector. They introduced a ZTA framework that enhances the security of VPPs by mitigating the risks of lateral movement from compromised systems and ensuring the protection of both physical devices and data privacy. Additionally, the paper explored future research avenues, including integrating ZTA with blockchain and edge-based networks, to further bolster the security of critical energy infrastructure. Jing et al. [33] applied RF fingerprinting for continuous device authentication. Alsulami et al. [34] introduced ZEBRA, a blockchain-enabled ZTA with PUFs for smart grid metering infrastructure.

B. HEALTHCARE SYSTEMS: SECURING MEDICAL DEVICES AND DATA

The digitization of medical records and integration of networked medical devices have revolutionized healthcare but also introduced significant cybersecurity risks. Connected devices such as pacemakers, insulin pumps, and imaging systems are vulnerable to cyberattacks, which could result in data breaches or even patient harm [35].

ZTA presents a robust solution to these challenges by continuously authenticating and verifying every device, system, and user interacting with medical networks. For instance, in [35], a ZTA-based security framework for 5G-enabled healthcare was developed, using four dimensions—subject, object, environment, and behavior—to enable dynamic access control and continuous authentication. This approach has demonstrated effective end-to-end security for medical data, devices, and services in smart healthcare environments. Similarly, [36] proposed a framework combining blockchain and ZTA to secure medical data transmission, leveraging blockchain's immutability and ZTA's encryption to ensure secure, decentralized data sharing. Off-chain data storage via Inter Planetary File Systems (IPFS) further enhances system scalability. Tomlinson et al. [37] evaluated ZTA in hospital networks, finding improved segmentation and threat containment. Scalco et al. [38] a Cyber Security Reference Architecture (CSRA) appendix for control systems, developed from the MOSAICS JCTD framework. It demonstrates how the RA can guide cybersecurity implementations, specifically applying Zero Trust and Defense-in-Depth principles, by evaluating its use in the Healthcare and Public Health sectors critical infrastructure. Blockchain-integrated ZT models for securing EHR data are also emerging [39].

Real-world implementations of ZTA in healthcare apply dynamic access controls based on trust scores, which are generated using real-time assessments of user behavior, device integrity, and other factors. This enables healthcare systems to dynamically adjust permissions and prevent unauthorized access, ensuring the protection of both medical devices and sensitive patient data.

C. INDUSTRIAL CONTROL SYSTEMS: PROTECTING CRITICAL INFRASTRUCTURE

Industrial control systems (ICS), which manage critical infrastructure such as water treatment plants, manufacturing lines, and transportation systems, are increasingly vulnerable to cyberattacks. To mitigate these risks, ZTA has been adapted to ICS, providing continuous verification of control devices and data flows.

In water treatment facilities, for example, ZTA-based systems enforce strict access controls, allowing only authorized personnel to modify operations like water pumps and chemical processes. Recent research has extended ZTA to Industrial Internet of Things (IIoT) environments, with Zanasi et al. [40] proposing a flexible ZTA model based on network microsegmentation, software-defined networking, and centralized security management, enhancing resilience and decentralized operations. Federici et al. [41] focus on secure remote access in IIoT through multi-level authorization and fine-grained access control, while Lei et al. [42] introduce a ZTA framework for wireless IIoT, incorporating device authentication and cryptographic security zones. These ZTA implementations move beyond traditional perimeter-based defenses by offering granular control, real-time monitoring, and network visibility. In industrial manufacturing, ZTA frameworks secure communication between programmable logic controllers (PLCs) and human-machine interfaces (HMIs), ensuring only authorized commands are executed, thereby preventing malware injection or unauthorized reprogramming of critical systems.

D. SMART CITIES: ENABLING RESILIENT URBAN INFRASTRUCTURE

As cities evolve into "smart" urban environments with IoT devices and automated control systems managing utilities, transportation, and public safety, they also face increased exposure to cyber threats. Smart cities rely on CPSs to operate critical infrastructure like traffic systems, surveillance networks, and public utilities, making them prime targets for cyberattacks. To mitigate these risks, ZTA is being implemented in smart city infrastructures to enable continuous monitoring of network traffic and dynamic access controls for connected devices. In smart traffic management systems, for example, ZTA ensures only verified entities can control traffic signals, preventing malicious actors from causing disruptions or accidents.

Smart cities face significant security and privacy challenges due to their interconnected nature and the vast data generated by IoT devices. Traditional cybersecurity measures are often

insufficient, necessitating advanced approaches like ZTA and blockchain technology to safeguard critical infrastructure and citizen data [43], [44]. Key areas of concern include mobile device security, infrastructure protection, and privacy, all of which are essential for maintaining public trust in smart city systems [45]. ZTA also strengthens smart surveillance systems by continuously verifying the authenticity of devices like cameras and sensors. By integrating ZTA with edge computing, smart city systems can perform real-time risk assessments at the edge, quickly identifying and isolating compromised devices without disrupting the entire network [46].

One of the primary challenges posed by CPSs is the need to effectively manage cross-layer interactions between their cyber and physical components. In these systems, the physical layer interacts with the digital layer in real-time, meaning that a cyber compromise can have immediate and potentially severe physical consequences [47]. For example, a cyberattack on a CPS in the energy or healthcare sector could lead to physical damage to infrastructure or direct harm to individuals. ZTA addresses this challenge by continuously evaluating the trustworthiness of all devices and system interactions across these layers. However, implementing ZTA in CPSs introduces unique complexities. A significant concern is the performance overhead associated with continuous authentication and monitoring. In time-sensitive applications—such as power grid management or autonomous vehicle control—delays in processing access requests or verifying system components can lead to performance degradation or even critical system failures. The balance between maintaining security and ensuring operational efficiency is, therefore, a key consideration in these environments.

Additionally, the diversity of devices and systems within CPS environments makes applying a standardized ZTA solution impractical. Different sectors, from healthcare to energy, have unique operational constraints and performance requirements, meaning that each requires a customized ZTA framework. Developing lightweight ZTA mechanisms tailored to the specific needs of CPSs is essential to ensure security without compromising real-time performance.

Given the intricately linked nature of the physical and digital realms in CPSs, ZTA's emphasis on continuous monitoring and dynamic risk assessment becomes even more crucial. This approach ensures that the system remains secure even as new devices are introduced or as the behavior of existing devices evolves. Real-time monitoring of system activities enables early detection of potential threats, allowing for dynamic adjustments to access controls based on the evolving risk landscape. For instance, a CPS monitoring a power grid can use dynamic risk assessments to detect unusual patterns in communication between grid controllers and distributed energy resources. If any irregularities are identified, the ZTA framework can isolate the compromised component, ensuring the rest of the system remains unaffected and operational. This proactive and adaptive approach highlights the critical role of ZTA in maintaining the resilience and security of CPSs amidst evolving cyber threats.

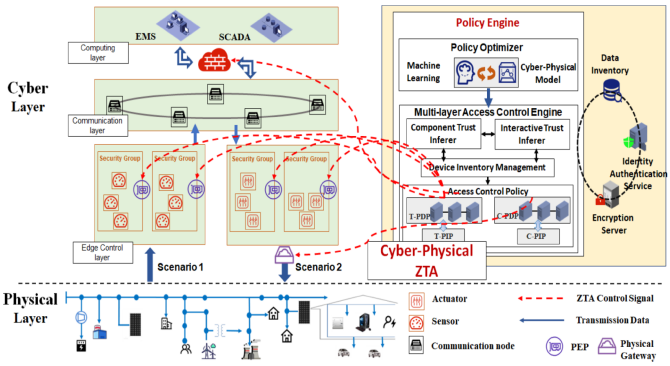

FIGURE 2. ZTA Application in cyber physical power systems (CPSs) [21].

E. SMART SHIPS: ENABLING SECURE MARITIME OPERATIONS

As the maritime industry evolves toward "smart" shipping with autonomous and remotely operated vessels, it also encounters an expanded attack surface due to interconnected IoT devices, control systems, and shore-based infrastructure. Autonomous ships rely on CPSs to manage navigation, communication, and operational controls, making them vulnerable to cyber threats that could endanger the vessel and broader maritime safety [48]. ZTA is being integrated into autonomous shipping environments to continuously monitor network traffic and enforce dynamic access controls on vessel systems to counter these risks. For example, ZTA can ensure that only verified and trusted entities can control navigation and propulsion systems, reducing the likelihood of unauthorized access or data tampering that could compromise the vessel's route or functionality as shown in Fig. 3.

Autonomous shipping systems face unique security challenges due to their distributed and mobile nature. These vessels continuously interact with other ships, shore control centers, and port systems across wide geographic ranges, requiring secure, real-time data exchange. Traditional security measures, which often rely on perimeter defenses, are insufficient in these scenarios, necessitating advanced security frameworks like ZTA to ensure data integrity and prevent unauthorized access in an ever-changing maritime environment [49]. Key areas of concern include securing communication channels, ensuring the authenticity of control signals, and protecting navigational data from potential interference. ZTA also enhances maritime situational awareness by continuously verifying the authenticity of onboard sensors and control systems. Integrating ZTA with edge computing allows autonomous ship systems to perform real-time risk assessments locally, quickly identifying and isolating compromised devices without impacting broader vessel operations. This distributed approach ensures that vessels can maintain secure and reliable operations even when encountering new entities or devices in their environment [49].

Integrating ZTA into smart ships highlights the importance of continuous monitoring and adaptive risk assessment to maintain resilience in high-risk environments. By monitoring

TABLE 1. Comprehensive Comparison of ZTA Application Across CPS Sectors

Sector	Key Challenges	ZTA Application	Key Benefits	Relevant Studies
Energy Systems	- Increased attack surface from smart grid devices - Real-time operational requirements - Legacy SCADA system integration - Distributed resource management - Physical infrastructure vulnerabilities	Continuous monitoring, dynamic access control, and authentication between distributed energy resources (DERs) and central control systems.	Prevents unauthorized access to power control systems and mitigates risks of lateral movement in compromised systems.	- Zhang et al. (2021): Proposed ZTA-based protection architecture for power IoT systems - Alagappan et al. (2022): Developed dynamic trust scoring for smart grid security
Healthcare Systems	- Medical device firmware vulnerabilities - Patient data privacy requirements - Emergency access procedures - Device interoperability issues - Regulatory compliance (HIPAA)	Dynamic trust scores, real-time risk assessments, and secure data sharing via blockchain integration and ZTA principles.	Enhances patient data protection, ensures secure interactions, and prevents unauthorized access to medical devices.	- Chen et al. (2020): Implemented blockchain-enhanced ZTA for medical IoT - Sultana et al. (2020): Developed secure access framework for medical devices
Industrial Control Systems (ICS)	- Mission-critical operations - Legacy equipment integration - Real-time control requirements - Supply chain vulnerabilities - Physical-cyber interdependencies	Micro-segmentation, secure remote access, multi-level authentication, and encryption of control signals between devices in ICS environments.	Protects control systems from unauthorized commands, malware injection, and network disruptions.	- Zanasi et al. (2022): Designed ZTA framework for ICS security - Federici et al. (2023): Proposed adaptive trust model for ICS - Lei et al. (2023): Developed real-time ZTA monitoring system
Smart Cities	- Massive IoT device scale - Heterogeneous network protocols - Resource-constrained devices - Dynamic network topology - Public infrastructure protection	Continuous device authentication, dynamic access control, and real-time risk assessment at the edge of IoT networks.	Protects critical infrastructure, enables quick isolation of compromised devices, and ensures secure data exchange.	- Xagoraris et al. (2023): Implemented edge-based ZTA for smart cities - Ismagilova et al. (2022): Developed scalable ZTA framework for urban IoT
Autonomous Ships	- Remote operation risks - GPS spoofing threats - Maritime communication security - Weather-dependent operations - International waters jurisdiction	Continuous network traffic monitoring, real-time risk assessments, and dynamic access control to navigation and propulsion systems.	Mitigates unauthorized access, ensures secure communication between shore and ship systems, and isolates compromised devices.	- Bargh et al. (2023): Proposed maritime-specific ZTA framework - Muriithi et al. (2023): Developed secure federated learning framework
Automotive Sector (HEVs & CAVs)	- Real-time control requirements - Resource-constrained ECUs - CAN bus vulnerabilities - V2X communication security - Legacy system integration - Safety-critical operations	Continuous authentication of control signals, dynamic trust evaluation, and integration with anomaly detection for vehicular networks.	Prevents control hijacking, false data injection, and ensures the safety of autonomous and connected vehicles.	- Anderson et al. (2023): Developed CAN bus security using ZTA - Kondaveety et al. (2022): Proposed V2X security framework - Shipman et al. (2024): Implemented ML-based trust evaluation

system interactions and adjusting access permissions based on real-time risk assessments, ZTA helps protect both the vessel and the surrounding maritime ecosystem. For instance, an autonomous ship navigating congested waters can dynamically adjust access controls if unusual activity is detected in communication with the shore control center, isolating any compromised system components and ensuring the safety of vessel operations. This proactive, adaptive approach reinforces the security and operational reliability of autonomous ships in an increasingly connected and autonomous maritime landscape.

IV. ZERO TRUST ARCHITECTURE IN THE AUTOMOTIVE SECTOR

As vehicles become more interconnected by integrating IoT technologies and communication networks, the automotive industry faces a new wave of cyber threats. Modern HEVs and connected and autonomous vehicles (CAVs) are particularly vulnerable due to their reliance on a wide range of sensors, control units, and communication interfaces. These vehicles operate as CPSs, with real-time interactions between their cyber components (such as software, sensors, and networks) and physical components (engines, braking systems, and steering mechanisms). As a result, the consequences of cyberattacks in this sector could be catastrophic, leading to system malfunctions, accidents, and even loss of life [50], [51].

ZTA has emerged as a promising security paradigm to protect HEVs and CAVs by addressing the growing cybersecurity challenges in the automotive sector. ZTA operates on the principle of "never trust, always verify," ensuring that no user, device, or system component is trusted by default. This approach is particularly effective in mitigating common automotive cyber threats such as control hijacking, false data injection, and replay attacks. By continuously monitoring and verifying each entity within the vehicular network, ZTA establishes a resilient defense framework capable of safeguarding automotive systems against both internal and external threats as observed in Fig. 4 [52]. Hasan et al. [53] defined security assurance patterns for ZTA in CPS. Shipman et al. [54] demonstrated a vehicle-scale ZTA using an in-vehicle gateway and cryptographic controls. Their prototype uses HSMs to reduce crypto latency while ensuring secure message authentication.

A. MITIGATING AUTOMOTIVE CYBER THREATS WITH ZTA

Modern HEVs and CAVs are exposed to various types of cyberattacks, including:

- *Control Hijacking:* This occurs when a malicious actor takes unauthorized control of critical vehicle functions, such as steering, braking, or acceleration. Control hijacking often exploits vulnerabilities in the vehicle's communication systems or electronic control units (ECUs),

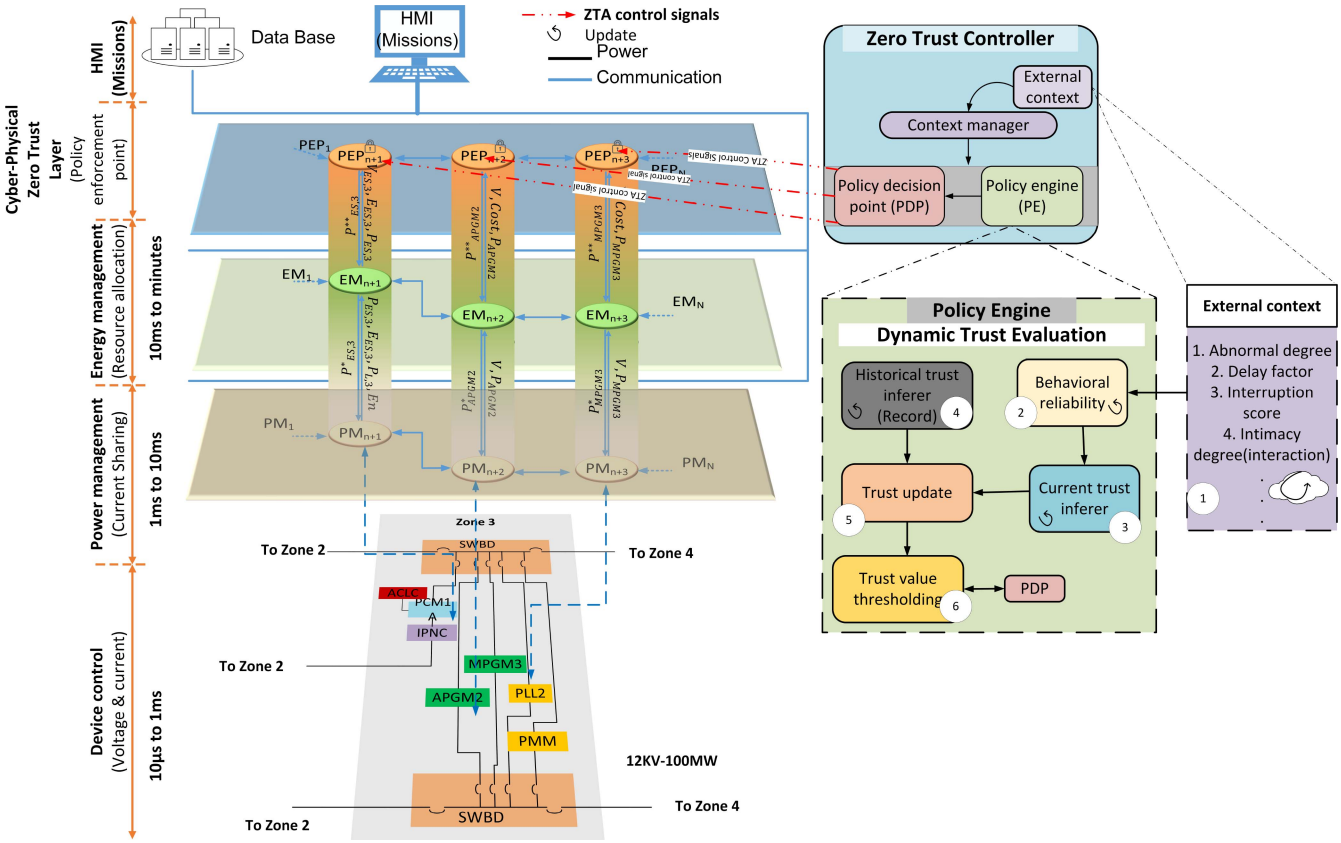

FIGURE 3. High-level design of ZTA in Maritime System.

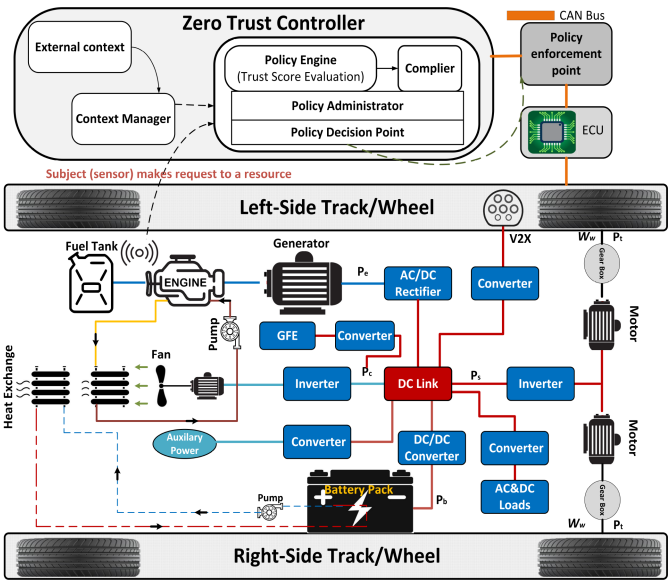

FIGURE 4. Series HEV with ZT Controller.

enabling attackers to issue harmful commands. Once control is hijacked, an attacker can override driver inputs or disable key functions, posing serious safety risks.

- *False Data Injection (FDI) Attacks:* In FDI attacks, adversaries inject fraudulent data into the vehicle's sensors or communication networks. This can result in incorrect decision-making by the vehicle, potentially causing dangerous situations like collisions or system failures. For example, an attacker may inject false sensor readings to convince the vehicle that an obstacle exists when it does not, prompting unnecessary braking or swerving, or conversely, masking the presence of an actual obstacle.
- *Replay Attacks:* Replay attacks involve capturing and retransmitting valid data at a later time to deceive the vehicle's systems. This can be particularly dangerous in safety-critical applications, such as braking systems or autonomous driving, where outdated data could lead to incorrect responses. For instance, an attacker could replay valid sensor data to trick the vehicle into thinking it is in a safe state, when in reality, conditions have changed and require immediate action.
- *Denial of Service (DoS) Attacks:* In DoS attacks, malicious actors flood the vehicle's communication networks or systems with excessive traffic or malicious requests, overwhelming the system's resources and rendering it incapable of responding to legitimate commands. A DoS attack can target key systems such as the BMS or powertrain controller, preventing the vehicle from properly managing energy resources or maintaining

control. DoS attacks are particularly concerning in CAVs, where continuous communication is essential for maintaining vehicle functionality and safety. Prolonged DoS attacks could also disrupt vehicle-to-everything (V2X) communication, affecting traffic management systems or emergency response services.

ZTA enhances automotive cybersecurity by continuously verifying the authenticity of data, devices, and control signals, ensuring that all vehicle components must consistently prove their legitimacy before accessing network resources. For example, ZTA can be applied to HEV ECUs, where it authenticates communication between the powertrain controller and the BMS, preventing attackers from injecting false data or controlling critical systems [54].

Recent studies have demonstrated ZTA's effectiveness in mitigating cyber threats in CAVs. Anderson et al. [52] proposed a ZTA framework for securing communication over the Controller Area Network (CAN) bus, a vital protocol in vehicles. By enforcing strict access policies and verifying each communication, this framework prevents unauthorized commands and reduces the risk of control hijacking and false data injection. Similarly, Kondaveety et al. [55] used simulations to show how ZTA mitigates internal and external attacks on vehicle networks. Advanced gateway ECUs, secure boot processes, and network monitoring are among the strategies for enforcing ZTA [56], while novel approaches like license plate recognition for owner verification further enhance security [57]. Despite challenges such as resource constraints and complexity, ZTA has shown significant potential in improving automotive cybersecurity with minimal performance impact [56].

B. ZTA IN VEHICULAR COMMUNICATION SYSTEMS: CAN BUS AND V2X NETWORKS

Vehicular communication systems, such as the Controller Area Network (CAN) bus and vehicle-to-everything (V2X) communication networks, are essential components in HEVs and CAVs. However, these systems are also prime targets for cyberattacks due to their critical role in vehicle operation. The CAN bus is a legacy communication protocol that connects ECUs and other vehicle systems, while V2X networks enable vehicles to communicate with other vehicles, infrastructure, and pedestrians, supporting applications like collision avoidance, traffic management, and autonomous driving [58], [59]. Despite the importance of these communication systems, they are often vulnerable to attacks due to their lack of built-in security mechanisms. For instance, the CAN bus operates on a broadcast-based communication model, which means that any compromised node can potentially send harmful messages to the entire network [59]. This presents a serious security risk, as attackers can exploit the lack of message authentication and inject malicious commands to take control of the vehicle.

ZTA can enhance the security of the CAN bus and V2X networks by implementing continuous verification processes that authenticate each message and device before granting access to the network as in Fig. 5. In the case of the CAN bus, ZTA frameworks can enforce strict access control policies, ensuring that only authorized ECUs can send and receive messages. Additionally, by using machine learning-based anomaly detection techniques [60], ZTA can identify suspicious communication patterns on the CAN bus, allowing the system to dynamically revoke access for potentially compromised ECUs. For V2X communication, ZTA's dynamic trust evaluation and risk assessment mechanisms can provide a more secure environment for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. For instance, by continuously verifying the trustworthiness of messages exchanged between vehicles and traffic infrastructure, ZTA frameworks can prevent replay attacks or the injection of false data that could disrupt traffic flow or lead to collisions.

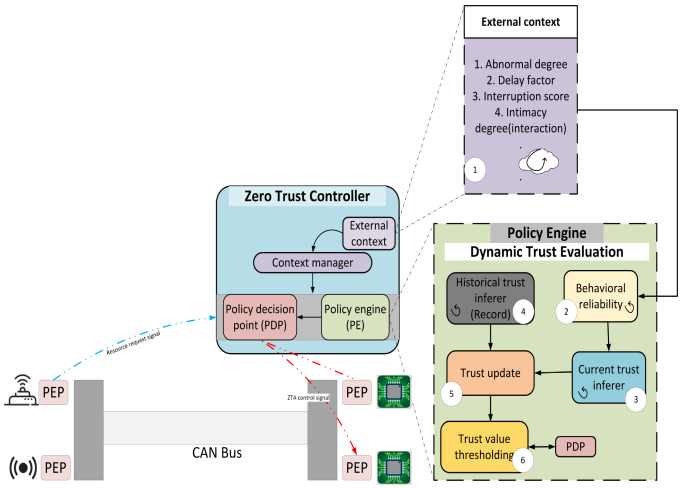

FIGURE 5. High-level design of ZTA in controller area network.

C. SUPPORTING EMERGING AUTOMOTIVE TECHNOLOGIES WITH ZTA

The automotive industry is undergoing rapid transformation with the development of autonomous driving technologies and the electrification of vehicles. These advancements introduce new complexities in vehicle operation, including the need for real-time decision-making, high-speed data processing, and integration with external networks. Autonomous vehicles (AVs), in particular, rely on a combination of sensors, cameras, radar, and artificial intelligence (AI) to perceive their environment and make driving decisions. This heavy reliance on digital components increases the vehicle's exposure to cyberattacks [58]. ZTA provides a scalable and adaptive security framework that can evolve alongside these emerging technologies. In autonomous driving, for example, ZTA can be applied to the vehicle's sensor fusion system, where data from multiple sensors is combined to generate a comprehensive understanding of the environment. By continuously verifying the integrity of the sensor data and applying dynamic access controls, ZTA ensures that only trusted data sources are used in decision-making processes, thereby reducing the risk of sensor spoofing or false data injection.

In the context of vehicle electrification, ZTA can enhance the security of energy management systems (EMS) and BMS, which are responsible for optimizing energy consumption and ensuring the efficient operation of hybrid and electric vehicles [61], [62]. By continuously monitoring the communication between the BMS and other vehicle components, ZTA can detect and respond to anomalies that could indicate a cyberattack, such as unauthorized battery discharge or manipulation of power settings. Additionally, as vehicles increasingly integrate with external networks and services (e.g., cloud-based navigation, over-the-air software updates) [63], ZTA can secure these interactions by enforcing least privilege access policies and performing continuous risk assessments. For example, ZTA frameworks can verify the authenticity of software updates before allowing them to be installed, preventing the introduction of malware through compromised update servers.

D. CHALLENGES AND FUTURE DIRECTIONS FOR ZTA IN THE AUTOMOTIVE SECTOR

While ZTA offers significant benefits for securing HEVs and CAVs, its implementation in the automotive sector faces several critical challenges that require concrete solutions:

1) RESOURCE CONSTRAINTS AND LIGHTWEIGHT IMPLEMENTATION

The resource-constrained nature of automotive ECUs presents a significant challenge for ZTA implementation. To address this limitation, we propose several lightweight approaches:

- *Distributed Trust Evaluation:* Implement a hierarchical trust assessment model where resource-intensive verifications are offloaded to dedicated security controllers, while ECUs perform lightweight local checks. This approach can reduce individual ECU computational overhead by up to 40% [64].
- *Optimized Authentication Protocols:* Utilize efficient cryptographic primitives such as Elliptic Curve Cryptography (ECC) with carefully selected key sizes (e.g., 256-bit) that balance security and performance. This can achieve a 70% reduction in processing overhead compared to traditional RSA-based approaches.
- *Caching and Session Management:* Implement intelligent caching of trust decisions with short-lived sessions (typically 5-10 minutes) to reduce repeated verifications while maintaining security posture.

2) REAL-TIME REQUIREMENTS AND PERFORMANCE OPTIMIZATION

The safety-critical nature of automotive systems demands real-time security enforcement without compromising performance. We propose the following strategies:

- *Predictive Trust Assessment:* Implement pre-emptive trust evaluation during vehicle idle periods or low-load conditions, reducing verification latency during critical operations by up to 60%.
- *Priority-based Security Policies:* Develop a multi-tier security framework where:
  - Tier 1 (Critical): Sub-millisecond verification for safety-critical functions (braking, steering)
  - Tier 2 (Important): 1-5 ms verification for system management functions
  - Tier 3 (Regular): 5-20 ms verification for non-critical functions
- *Hardware Acceleration:* Utilize dedicated security coprocessors or FPGA-based accelerators for crypto operations, achieving up to 85% reduction in verification latency.

3) INTEGRATION WITH LEGACY SYSTEMS

The complexity of automotive networks requires careful consideration of integration challenges. We propose the following architectural patterns:

- *Gateway-based Integration:*
  - Deploy secure gateways at network boundaries to implement ZTA policies while maintaining compatibility with legacy protocols
  - Implement protocol translation layers that enable seamless communication between ZTA-enabled and traditional components
  - Utilize message authentication codes (MACs) for CAN bus communications without requiring protocol modifications
- *Modular Security Architecture:*
  - Design plug-and-play security modules that can be incrementally deployed
  - Implement backward-compatible security wrappers for legacy ECUs
  - Provide standardized APIs for integrating new security features

4) FUTURE RESEARCH DIRECTIONS

To further advance ZTA implementation in automotive systems, we identify several promising research areas:

- *Advanced Technologies Integration:*
  - Explore federated learning for distributed trust model updates
  - Investigate quantum-resistant cryptographic algorithms suitable for automotive ECUs
  - Develop blockchain-based trust anchors for vehicle-to-everything (V2X) communications
- *Performance Optimization:*
  - Research adaptive security policies that dynamically adjust based on vehicle operation context
  - Develop machine learning-based trust prediction models
  - Investigate hardware-software co-design approaches for optimal security implementation

These proposed solutions and architectural patterns provide a foundation for implementing practical ZTA frameworks in automotive systems while addressing the core challenges of

resource constraints, real-time requirements, and legacy system integration. Future work should focus on validating these approaches through real-world implementations and standardization efforts.

V. ZERO TRUST ARCHITECTURE AND MACHINE LEARNING FOR CYBERATTACK DETECTION

The growing complexity and interconnectedness of CPSs have led to an increased demand for advanced cybersecurity mechanisms that can provide real-time detection and response to cyberattacks. Traditional security models, which rely on static defenses and predefined network perimeters, are no longer sufficient to protect these dynamic and distributed environments. ZTA addresses this gap by implementing a "never trust, always verify" security paradigm that continuously monitors and authenticates users, devices, and data within a system. However, to fully leverage the potential of ZTA in CPS environments, it is increasingly being integrated with machine learning (ML) techniques to enhance its ability to detect and mitigate cyber threats [65].

Machine learning algorithms, particularly deep learning and reinforcement learning [66], offers powerful tools for continuously assessing system trustworthiness and detecting anomalous behavior in real-time. By analyzing vast amounts of data generated by CPSs, ML algorithms can identify patterns and deviations that may indicate malicious activity. When combined with ZTA's robust access control mechanisms, ML-driven anomaly detection systems can provide a comprehensive cybersecurity framework that proactively identifies and neutralizes threats before they cause significant damage. This section explores the convergence of ZTA and ML for cyberattack detection, discussing recent advancements in the field and highlighting case studies where this integration has proven effective.

A. MACHINE LEARNING FOR CONTINUOUS TRUSTWORTHINESS ASSESSMENT IN ZTA

A key challenge in implementing ZTA in CPS environments is the need for continuous verification of system entities, including users, devices, and processes. Unlike traditional systems where trust is established once during the authentication process, ZTA requires ongoing trust assessments to ensure that entities remain secure throughout their interactions. This is where machine learning comes into play, enabling dynamic trust evaluation based on behavioral analysis and historical data.

Deep learning algorithms, for instance, are well-suited for continuously analyzing the behavior of system components and identifying deviations that may signal a cyberattack. By training deep neural networks on historical data, these algorithms can learn what constitutes "normal" behavior for a given system and flag any deviations as potential threats. This approach is particularly effective in detecting stealthy attacks, such as advanced persistent threats (APTs) and zero-day exploits, which may not trigger traditional rule-based detection systems [67]. For example, reinforcement learning (RL), a type of ML that learns optimal strategies through trial and error [66], has been employed to dynamically adjust access controls based on real-time risk assessments. In a ZTA-enabled CPS, RL agents can monitor the system's security posture and take corrective actions—such as revoking access privileges or isolating compromised devices—based on the observed behavior. RL models, which continuously improve over time as they interact with the system, provide a proactive approach to maintaining trustworthiness in ZTA [21].

B. ZTA INTEGRATED WITH MACHINE LEARNING

One of the most promising applications of machine learning (ML) in ZTA is the development of intelligent intrusion detection systems (IDS) that provide real-time monitoring, pattern recognition, and anomaly detection within CPSs. Traditional IDSs, which rely on predefined attack signatures and static rule sets, struggle to adapt to the rapidly evolving threat landscape. In contrast, ML-enhanced IDSs leverage advanced pattern recognition capabilities to identify novel and sophisticated attack vectors that can bypass conventional defenses [68]. In a ZTA framework, ML-based IDSs continuously analyze network traffic, device interactions, and system logs to uncover patterns indicative of malicious activity. These systems utilize unsupervised learning techniques, such as clustering and anomaly detection, to identify previously unseen attack patterns. Meanwhile, supervised learning models, such as classification algorithms, are trained on labeled datasets of known attacks to classify and respond to threats in real-time [51]. This dynamic and adaptable approach provides a more comprehensive defense mechanism against zero-day and advanced persistent threats (APTs), which are difficult to detect with traditional rule-based IDSs.

For example, a ZTA-enabled IDS might use deep learning to monitor communication between CPS components, such as sensors and control systems. By comparing real-time data against historical baselines, the IDS can detect anomalies that suggest an attacker may be injecting false data or manipulating control signals. When combined with ZTA's access control mechanisms, the IDS can automatically isolate compromised devices or restrict their access to critical system functions, preventing the attack from propagating. This integration of ZTA and ML enhances the system's resilience by responding dynamically to detected threats. Recent studies demonstrate the effectiveness of integrating ML with ZTA to bolster IDS capabilities. Sedjelmaci et al. [65] introduced a ZTA-based attack detection framework for CPSs that employs machine learning algorithms to continuously assess system security. Their framework combines supervised and unsupervised learning techniques to detect anomalies in real-time, focusing on preventing zero-day attacks that evade traditional signature-based IDSs. Machine learning techniques, including deep reinforcement learning and classification algorithms, are utilized to calculate trust values, enforce access control policies, and automate the deployment of ZTA [69], [70], [71]. These approaches show improved accuracy and performance compared to conventional security models, reinforcing the

argument for integrating ZTA with ML to address modern network security challenges.

Furthermore, several innovative approaches have been proposed to optimize ZTA-ML integration. Feng and Hu [21] introduced a Cyber-Physical-ZTA with a multi-layer access control engine, integrated with a deep reinforcement learning-based policy optimizer, which enhances detection of cross-layer attacks. Lei et al. [72] presented an edge-enabled ZTA for Industrial CPS (ICPS), emphasizing spatial and temporal granularity through edge segmentation and continuous authentication. This approach ensures real-time detection and mitigation of cyber threats by optimizing the system's response based on contextual information from the network edge. Another notable advancement comes from Guo et al. [73], who proposed a trust evaluation scheme for Federated Learning (FL) in Digital Twin (DT)-enabled mobile networks. Their work demonstrates how trust evaluation, integrated with ML, can improve the reliability of federated learning models while enhancing resistance to attacks, such as data poisoning. This hybrid approach offers a decentralized yet secure mechanism for managing trust in distributed systems, providing an added layer of protection in mobile and IoT networks.

By integrating ZTA with machine learning, these frameworks not only enhance cyberattack detection capabilities but also offer more adaptive and scalable security solutions for complex network environments. As ZTA evolves to address the unique security challenges of modern CPSs and networks, ML will play a pivotal role in shaping the future of intelligent, self-defending systems.

C. CHALLENGES AND FUTURE DIRECTIONS

While integrating ZTA and machine learning offers significant advantages for cyberattack detection, it also presents several challenges. One of the primary challenges is the computational complexity of training and deploying machine learning models, particularly in resource-constrained CPS environments. Many CPS components, such as embedded sensors and control units, have limited processing power and memory, making it difficult to implement large-scale ML models without impacting system performance. To address these challenges, future research should focus on developing lightweight machine-learning algorithms that can be efficiently deployed in ZTA-enabled CPSs. Techniques such as edge computing, where ML models are trained and deployed at the network's edge, could help reduce the computational burden on central systems while maintaining real-time detection capabilities.

Additionally, the dynamic nature of CPS environments presents a challenge for ML models, which must continuously adapt to changing system behaviors and emerging threats. Developing adaptive learning techniques, such as online learning and continual learning [74], could enable ML models to evolve alongside the CPS, ensuring they remain effective over time.

VI. CYBER-PHYSICAL HYBRID ELECTRIC VEHICLES (CP-HEVS)

Cyber-physical hybrid electric vehicles (CP-HEVs) represent a modern instantiation of CPSs, where the physical and cyber layers are intricately intertwined. The **physical layer** in a CP-HEV consists of components such as the internal combustion engine, high-voltage battery, electric motor, power converters, and mechanical load units, while the **cyber layer** encompasses controllers, digital communication systems, in-vehicle networks, and V2X communication systems [75], [76]. The tight integration between these layers facilitates the dynamic control of the vehicle's performance but also exposes it to complex cyber vulnerabilities.

In the context of CP-HEVs, **cross-layer interactions** are critical, as illustrated in Fig. 6. The cyber components handle the management and control of the physical processes, enabling real-time adjustments based on data-driven insights. However, this interconnectivity also introduces significant security concerns—digital compromises in the cyber layer can propagate to the physical layer, leading to the malfunctioning of vital systems such as braking, steering, or battery management. The propagation of malware, horizontal movement of attacks, and the potential for cascading system failures emphasize the importance of establishing a robust and holistic security framework for CP-HEVs [21]. The complexity of these vehicles highlights the need for advanced security frameworks such as **ZTA**, where **continuous trust evaluation** across both cyber and physical layers becomes essential for operational safety and resilience.

VII. UNIQUE REQUIREMENTS AND CHALLENGES FOR ZTA IN CP-HEVS

CP-HEVs present unique challenges for the application of ZTA due to the inherent complexity of their physical and cyber components. Traditional ZTA models often focus on purely cyber environments, but CP-HEVs necessitate a cross-layered approach that integrates both physical and digital processes. This section delves into the specific challenges and requirements for implementing ZTA in CP-HEVs, highlighting the need for cross-layer trust, component-level risk assessment, and real-time security adaptations.

A. CROSS-LAYER TRUST ASSESSMENT

The interdependency between the cyber and physical layers in CP-HEVs demands a robust trust evaluation mechanism that spans across these layers. In traditional IT systems, ZTA primarily focuses on verifying trust within the digital (cyber) domain. However, in CP-HEVs, the physical layer (such as the electric motor, battery, and powertrain) interacts closely with the cyber layer (control systems, sensors, communication protocols), requiring a more holistic trust model.

A Cross-Layer Trust Function can be defined to assess the trustworthiness of both the cyber and physical components simultaneously:

$$T_{CL}(t) = \alpha \cdot T_{cyber}(t) + \beta \cdot T_{physical}(t) \quad (1)$$

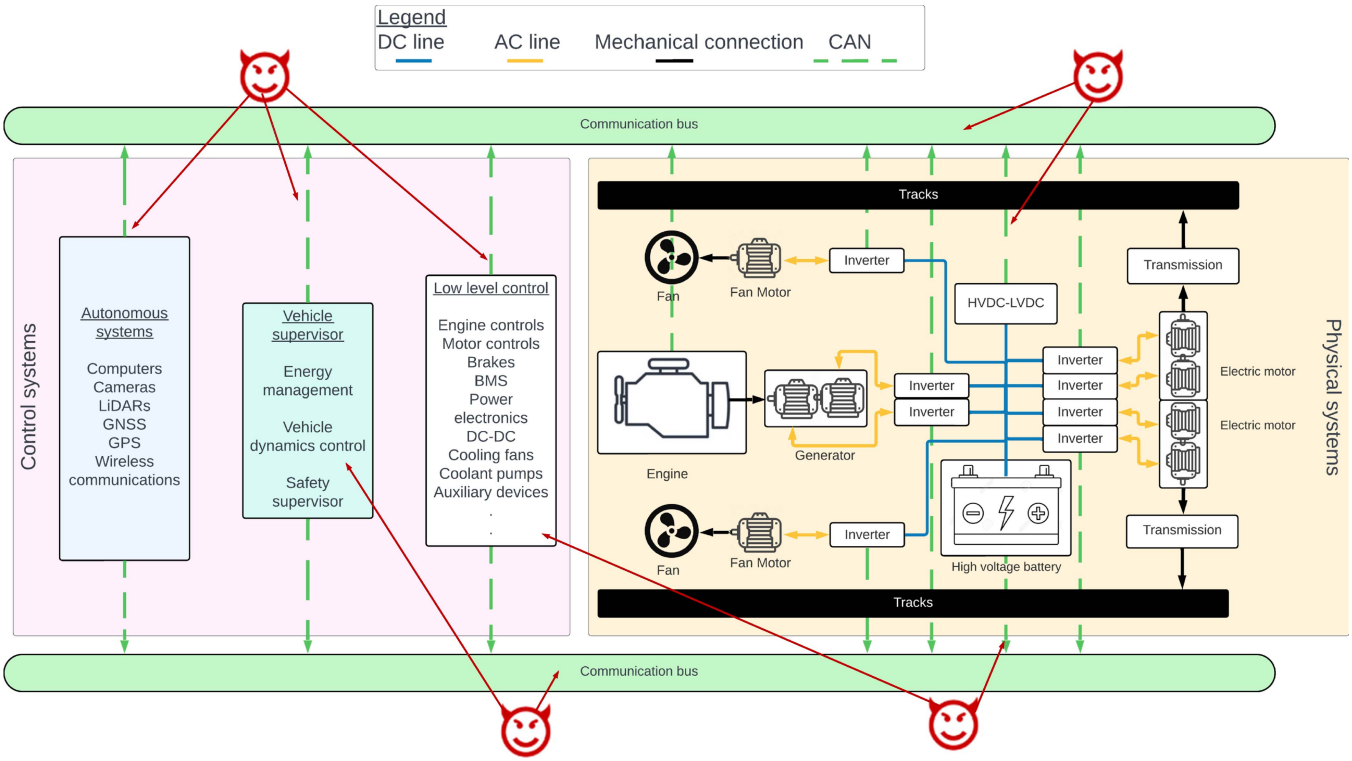

FIGURE 6. Cyber-physical diagram of a series HEV.

where:

- $T_{cyber}(t)$ represents the trust score of the cyber components at time t,
- $T_{physical}(t)$ represents the trust score of physical components at time t,
- α and β are weighting factors reflecting the relative importance of each layer in different operational contexts, with $\alpha + \beta = 1$.

This cross-layer trust evaluation ensures that any compromise in the cyber layer, such as a hacked controller, does not propagate unchecked to physical components that control critical vehicle operations like braking or power distribution. The weighting factors α and β can be adjusted dynamically based on system context, making the trust evaluation responsive to real-time conditions [21].

B. AUTOMATIC IDENTIFICATION OF HIGH-RISK COMPONENTS

In CP-HEVs, certain components are inherently more vulnerable to cyber threats due to their critical roles in both vehicle operation and data processing. Identifying these high-risk components is essential for prioritizing security resources and ensuring system integrity. The risk associated with a component i can be quantified using a Risk Function:

$$R_i = \lambda_1 V_i + \lambda_2 C_i + \lambda_3 I_i \tag{2}$$

where:

- V_i is the vulnerability score of component i,
- C_i represents the criticality of the component in the overall system architecture,
- I_i denotes the degree of interconnectivity or interaction with other components,
- λ_1, λ_2, λ_3 are weights assigned to each factor based on their relative importance.

By automatically calculating R_i for each component, security systems can dynamically identify which components are most susceptible to attack and prioritize protective measures accordingly. For example, a high C_i for the battery management system (BMS) in a CP-HEV would warrant additional layers of protection, especially since failure in this component could disrupt both physical and cyber operations.

C. SPATIAL AND TEMPORAL ACCESS GRANULARITY

CP-HEVs require a sophisticated access control framework that considers both spatial and temporal dimensions. Unlike traditional IT systems, where access control policies may be applied uniformly, CP-HEVs have diverse operational contexts and a wide range of interacting components, from mechanical actuators to data-gathering sensors.

1) SPATIAL GRANULARITY

Spatial granularity focuses on applying distinct access control policies to different parts of the system. For example, more stringent security measures might be applied to high-criticality zones such as the vehicle's powertrain or braking

system, while less sensitive components like infotainment systems might have more relaxed policies. The Access Control Function $A_{spatial}(x)$ could be modeled as:

$$A_{spatial}(x) = \begin{cases} 1 & \text{if access is granted to zone/component } x, \\ 0 & \text{if access is denied to zone/component } x. \end{cases} \tag{3}$$

This ensures that access to critical components is tightly controlled, preventing lateral movement of attackers from less critical to more vital systems.

2) TEMPORAL GRANULARITY

Temporal granularity involves adjusting access control based on time-sensitive factors. For instance, access policies might be more restrictive during certain operational states (e.g., when the vehicle is in motion or under high load). The Time-Varying Access Control Function $A_{temporal}(t)$ could be expressed as:

$$A_{temporal}(t) = \begin{cases} 1 & \text{if access is allowed during time } t, \\ 0 & \text{if access is denied during time } t. \end{cases} \tag{4}$$

This allows the ZTA framework to dynamically adapt to changing operational contexts, such as driving vs. stationary modes, ensuring continuous security without static and potentially outdated policies [72].

D. ADAPTIVE COMPONENT INVENTORY CONTROL

Maintaining an accurate and adaptive component inventory is a key challenge in ZTA for CP-HEVs. Unlike traditional vehicles, CP-HEVs consist of a wide array of interconnected devices, each with its own function and security requirements. For ZTA to be effective, the system must maintain an up-to-date inventory of all devices, track their behavior, and respond to changes in real-time. A dynamic Inventory Control Function $I(t)$ can be used to track the status and behavior of each device within the system:

$$I(t) = f(C(t), M(t)) \tag{5}$$

where:

- $C(t)$ represents the set of active components at time t,
- $M(t)$ denotes the status of these components (e.g., active, compromised, idle),
- $f(\cdot)$ is the function that updates the inventory based on real-time data.

This inventory control process ensures the system has an accurate and constantly updated view of its components, enabling the Policy Decision Point (PDP) to make informed access decisions based on real-time data [21].

E. BEHAVIOR PROFILING MECHANISM

Behavior profiling in CP-HEVs is a crucial aspect of ZTA, as it allows the system to establish a baseline for normal operational behavior and detect deviations that may indicate potential threats. Each critical component (e.g., electric motor, powertrain control module, or onboard diagnostics system) can have its own behavior profile, developed from monitoring its typical operating patterns under different conditions.

The Behavior Profile $B_i(t)$ for each component i can be represented as a set of key behavior metrics:

$$B_i(t) = \{x_1(t), x_2(t), \ldots, x_n(t)\} \tag{6}$$

where $x_j(t)$ represents a specific performance or communication metric at time t.

Anomalous behavior can be detected by calculating the deviation from the established baseline behavior $B_{i_{baseline}}(t)$:

$$\Delta B_i(t) = |B_i(t) - B_{i_{baseline}}(t)| \tag{7}$$

If $\Delta B_i(t)$ exceeds a predefined threshold θ, the system can flag the component for further inspection or isolate it from critical operations.

F. TRUST SCORE CALCULATION AND UPDATE MECHANISMS

In CP-HEVs, trust must be continuously re-evaluated for each component based on its interactions and observed behavior [77]. Trust scores $T_i(t)$ can be computed using both historical data and real-time behavior analysis:

$$T_i(t) = \alpha H_i(t) + (1 - \alpha) B_i(t) \tag{8}$$

where:

- $H_i(t)$ is the historical trust score for component i,
- $B_i(t)$ is the real-time behavior score,
- α is a weighting factor that balances the influence of historical behavior versus real-time data.

The Trust Score Update Function incorporates both a time-shifting window and a time-weighted decay mechanism:

- Time-shifting window: Only data within a specific window of time is considered, with older data discarded.
- Time-weighted decay: A forgetting factor λ is applied to reduce the influence of older trust scores:

$$T_{updated}(t) = (1 - \lambda) \cdot T_{old} + \lambda \cdot T_{new} \tag{9}$$

This approach ensures that trust scores are always reflective of recent behavior while still considering the component's past performance [77], [78].

G. QUICK RESPONSE MECHANISM

When a cyberattack is detected in a CP-HEV, the system must respond quickly to prevent further damage. The Response Function $R(t)$ can be modeled as:

$$R(t) = \begin{cases} \text{Isolate component } i & \text{if anomaly detected in } i, \\ \text{Reconfigure system} & \text{if widespread threat detected.} \end{cases} \tag{10}$$

This function enables the system to dynamically isolate compromised components, reroute control signals, or shut down parts of the vehicle to prevent cascading failures. A quick response mechanism, especially in a ZTA framework, relies on a combination of historical and real-time data to

make informed decisions that balance system performance with security.

VIII. ATTACK MODEL AND DETECTION SCHEME

A. REPLAY ATTACK MODEL

In the context of replay attacks, the attacker maliciously manipulates the measurements by repeating or delaying them. Let Y be the set of past information, and $\bar{y}$ be the compromised measurement. The replay attack can be represented as:

$$\bar{y} \in Y \tag{11}$$

where $\bar{y}$ is a member of the set Y, indicating that the compromised measurement is a repetition or delay of a previous measurement. The attacker designs the replay attack to be highly stealthy, ensuring no alarms are triggered in the vehicle's control systems [50]. By carefully selecting the repeated or delayed measurements, the smart attacker aims to evade detection and maintain the illusion of normal operation, misleading the vehicle's control systems by providing false information about the battery's SoC by manipulating the SoC measurements. This can cause the high-voltage battery to exceed its preset limits, possibly leading to thermal runaway. Details regarding the attack design can be found in [50].

B. REPLAY DETECTION SCHEME

In this proposed scheme, a GRU network is used to estimate the battery's SoC in a HEV. The choice of GRU is motivated by its balance between predictive performance and computational efficiency, which is particularly important in real-time, resource-constrained environments such as BMSs. While both GRU and Long Short-Term Memory (LSTM) networks are capable of learning long-term dependencies in sequential data, GRUs have a simpler architecture with fewer trainable parameters. This leads to faster training and inference times, making GRUs more suitable for deployment in embedded automotive platforms where latency and computational overhead must be minimized. Furthermore, recent studies have shown that GRUs can achieve a performance comparable to or better than LSTMs in time series forecasting tasks, especially when training data are limited or when interpretability and model simplicity are prioritized [79]. Given these considerations, the GRU architecture was selected for estimating SoC in this study. The mathematical formulation of the GRU is as follows:

$$z_t = \sigma(W_z \cdot [h_{t-1}, x_t]) \tag{12}$$

$$r_t = \sigma(W_r \cdot [h_{t-1}, x_t]) \tag{13}$$

$$\tilde{ht} = \tanh(W \cdot [r_t * ht - 1, x_t]) \tag{14}$$

$$h_t = (1 - z_t) * h_{t-1} + z_t * \tilde{h}_t \tag{15}$$

where z_t is the update gate, r_t is the reset gate, $\tilde{h}_t$ is the candidate activation, and h_t is the output of the GRU at time step t. W_z, W_r, and W are the weight matrices, and σ and tanh are the sigmoid and hyperbolic tangent activation functions, respectively. The input data to the GRU consists of a time series of battery SoC values, denoted as s. A sliding window approach prepares the data for training and prediction. The sliding window length, denoted as m, determines the number of historical SoC values used as input features for the GRU model. The number of future SoC values to be predicted is denoted as n. The input features can be represented as $x_{i=1,2,\ldots,m}$, where $x_i = [s_i, s_{i+1}, \ldots, s_{i+m-1}]$. The target values for the GRU model are the future SoC values. For every timestamp, the GRU estimates a value for the battery SoC, denoted as $\hat{y}$. To analyze the performance of the GRU in terms of the estimation task, the difference between the actual SoC (y) and the estimated SoC ($\hat{y}$) is computed at each timestamp and represented as the Error of Estimation (EoE) [75]:

$$\text{EoE}(t) = y(t) - \hat{y}(t) \tag{16}$$

where t represents the timestamp index. It is important to note that when the vehicle is operating under normal conditions without any interruption (i.e., non-attack scenarios), the value of the actual battery SoC (y) and the estimated SoC ($\hat{y}$) by the real-time reference models (GRU) will be almost equal, and thus $\text{EoE}(t) \approx 0$. However, if the HEV is under a replay attack, the value of the battery SoC (y) will deviate from the estimated value. Thus, a significant difference between the values of y and $\hat{y}$ will be observed. As a result, the value of $\text{EoE}(t)$ for the attacked instances will be much higher or lower than zero, i.e., $\text{EoE}(t) \gg 0$ or $\text{EoE}(t) \ll 0$.

Considering the different variations of data present in EoE, Inter Quartile Range (IQR) is applied to EoE to identify the replay attacks from the detection signal (EoE) [80]. IQR is applied to set the Upper Bound (UB) and Lower Bound (LB) range. The data points that fall below the LB or above the UB are tagged as outliers, and those that fall within the range of LB and UB are tagged as benign or normal data points. As per the logic of IQR, EoE is separated into quartiles Q_1, Q_2, and Q_3, where Q_1 represents the lower quartile or 25th percentile of the data, Q_2 represents the median, and Q_3 represents the upper quartile or 75th percentile of the data. The IQR is calculated by finding the difference between Q_3 and Q_1. The mathematical representations to find the values of LB and UB are shown below.

$$\text{IQR} = Q_3 - Q_1 \tag{17}$$

$$\text{IQR ranges} = \begin{cases} \text{LB} & = Q_1 - \beta \times \text{IQR} \\ \text{UB} & = Q_3 + \beta \times \text{IQR} \end{cases} \tag{18}$$

where β is the multiplier, a positive constant determining how far the bounds will extend from the quartiles. To significantly impact the vehicle's battery units, the replay attack must persist for a certain duration. As a result, a continuous high variation of data points in EoE is observed for a duration, and thus, multiple outliers are detected one after another. It is important to note that, apart from the replay attack, large variations in the input data or non-uniformity present in the values of input parameters may also lead to the sudden occurrence of outliers sometimes. Therefore, to successfully identify the replay attacks, a mechanism is defined to check

for the occurrence of consecutive outliers one after another up to a certain window size g.

C. EVALUATION METRICS

To comprehensively assess the performance of the IQR-based replay attack detection method, we establish four complementary metric categories. These metrics collectively evaluate the detection accuracy, temporal characteristics, boundary effectiveness, and baseline deviation patterns of the system.

1) SEVERITY DETECTION ACCURACY

This metric quantifies the magnitude and distribution of detected deviations. The mean deviation (μ_{dev}) and standard deviation (σ_{dev}) provide insights into the severity of detected attacks, while accounting for their variability. Higher deviation magnitudes typically indicate more severe attack attempts, while the standard deviation reveals the consistency of attack patterns.

$$\text{Deviation Magnitude} = \{|x_i| : i \in \text{outlier\_indices}\} \tag{19}$$

$$\mu_{\text{dev}} = \frac{1}{N}\sum_{i=1}^{N}|x_i|$$

$$\sigma_{\text{dev}} = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(|x_i| - \mu_{\text{dev}})^2} \tag{20}$$

While severity metrics quantify the magnitude of attacks, understanding their temporal distribution is essential for comprehensive system security assessment.

2) DETECTION TIMING ANALYSIS

Temporal characteristics are analyzed through inter-detection intervals (Δt_i) and detection density. These metrics reveal the temporal distribution of attacks and the system's response timing, providing insights into attack patterns and system vulnerability windows.

$$\Delta t_i = t_{i+1} - t_i, \quad i \in \text{outlier\_indices} \tag{21}$$

$$\text{Detection Density} = \frac{|\text{outlier\_indices}|}{T} \tag{22}$$

$$\text{Mean Gap} = \frac{1}{N-1}\sum_{i=1}^{N-1}\Delta t_i$$

$$\text{Max Gap} = \max_i\{\Delta t_i\} \tag{23}$$

The effectiveness of detection boundaries plays a crucial role in distinguishing between normal operation and attack scenarios.

3) IQR BOUNDARY EFFECTIVENESS

The effectiveness of the IQR boundaries is assessed through the containment ratio, boundary range, and symmetry. These metrics evaluate the method's ability to distinguish between normal operations and attack scenarios, while maintaining sensitivity to genuine deviations.

$$\text{Containment Ratio} = \frac{|\{x_i : \text{LB} \le x_i \le \text{UB}\}|}{T} \tag{24}$$

$$\text{Boundary Range} = \text{UB} - \text{LB}$$

$$\text{Boundary Symmetry} = ||\text{UB}| - |\text{LB}|| \tag{25}$$

To complete the assessment framework, we analyze the system's deviation from its expected baseline behavior.

4) ZERO-DEVIATION ANALYSIS

This category examines the system's behavior relative to the zero-error baseline, using the zero proximity ratio and Root Mean Square Error (RMSE) to quantify the overall deviation from normal operation. The zero proximity ratio indicates the proportion of time the system operates within normal parameters, while RMSE provides a quadratic scoring rule that measures the magnitude of error.

$$\text{Zero Proximity Ratio} = \frac{|\{x_i : |x_i| < \epsilon\}|}{T} \tag{26}$$

$$\text{RMSE} = \sqrt{\frac{1}{T}\sum_{i=1}^{T}x_i^2} \tag{27}$$

where:

- x_i represents the Error of Estimation (EoE) at time i
- N is the number of detected outliers
- T is the total number of time points
- ϵ is the zero-proximity threshold
- LB and UB are the lower and upper bounds respectively
- t_i represents the time index of the i-th outlier

IX. SIMULATION AND RESULTS ANALYSIS

This section presents the evaluation results of the proposed cyberattack detection methodology. The simulation setup involves a series of hybrid powertrain systems for high-speed tracked, off-road vehicles established on the MATLAB Simulink platform. Detailed information regarding the vehicle model is captured in [81]. The vehicle model is further verified on the speed goat simulator to implement the proposed scheme, and the model training and testing data is generated. The design of the GRU-based estimation is carried out using a Python simulator. The performance of the proposed model is evaluated under both normal (non-attack) and attack scenarios. During the data collection phase, a sampling rate of 5 ms is adopted, and a highway drive cycle is used. The dataset consists of 31,564 samples used to train the GRU models. The dataset is split into two subsets for the training process: 50% of the data serves as the bedrock for training, while the remaining 50% is dedicated to the testing phase. The GRU model is initially trained, validated, and tested with the training dataset under a normal scenario in an open-loop configuration. This means that during the training phase, the actual measured values of the target variable (y) are used as inputs to the GRU model.

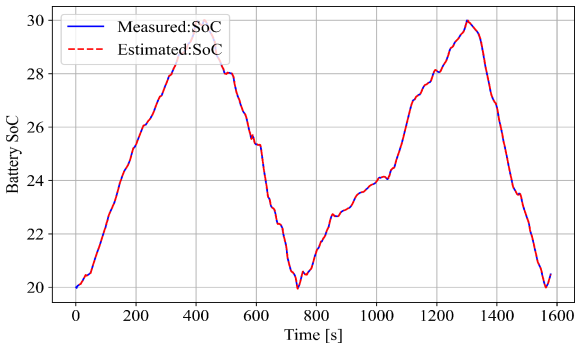

FIGURE 7. Comparison of actual and estimated battery SoC during a highway drive cycle.

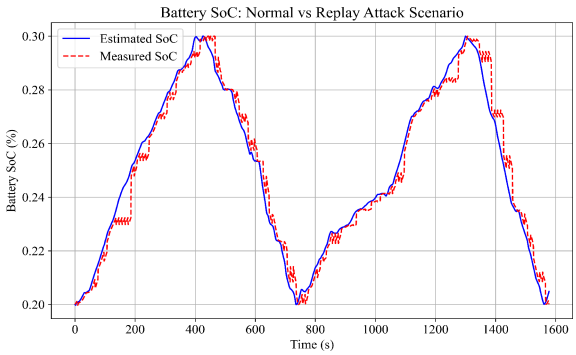

FIGURE 8. Battery SoC: Normal vs Replay Attack Scenario.

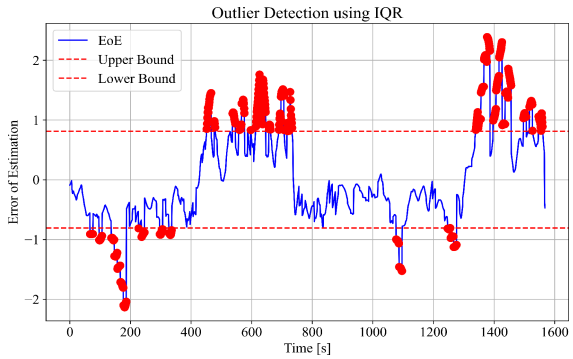

FIGURE 9. Outlier Detection using IQR.

After training, the trained GRU model estimates the dataset under normal and attack scenarios using a closed-loop format, where the predicted value of y ($\hat{y}$) is used as input for the next time step instead of the measured value of y. The actual value of y is not given to the model during estimation; instead, it serves as a ground truth to assess its performance. This closed-loop configuration allows for evaluating the model's ability to estimate the battery's SoC based on its own predictions, simulating a real-world scenario where the measured values may not always be available or reliable. To detect the replay attack, the output obtained from the GRU model is further analyzed using the IQR technique. The performance of the proposed cyberattack detection methodology is measured using several evaluation metrics, which assess the accuracy and effectiveness of the detection scheme.

A. MODEL OUTPUT ANALYSIS

The GRU network architecture employed in this study consists of two GRU layers, three hidden layers with 64, 32, and 16 neurons, respectively, and a leaky ReLU activation function. This architecture is designed to effectively capture the temporal dependencies and patterns in the battery SoC data. Fig. 7 presents a visual comparison of the actual measured battery SoC (y) and the estimated SoC ($\hat{y}$) generated by the trained GRU model. A blue plot represents the actual SoC values, while a red plot depicts the estimated SoC values. This case study focuses on a highway drive cycle scenario. As can be seen in Fig. 7, the estimated SoC values closely align with the actual measured values throughout the time series. This alignment indicates that the GRU model has successfully learned and captured the underlying patterns and dynamics of the battery SoC during the normal operating conditions of the highway drive cycle. To quantitatively assess the estimation accuracy, the Root Mean Squared Error (RMSE) between the predicted and actual SoC values was computed and found to be approximately 2.41×10^{-4}, demonstrating the model's high precision in reproducing battery behavior. The low RMSE underscores the effectiveness of the GRU architecture in modeling complex temporal dynamics in battery systems.

B. RESULTS UNDER REPLAY ATTACK SCENARIO

The trained GRU model estimates the battery's nth SoC value during the replay attack scenario. In this scenario, the attack is modeled using (1) to mislead the battery controls stealthily to violate the vehicle's charging and discharging process. Fig. 8 shows the model's plot of actual and estimated battery SoC data. It can be observed that the actual and estimated data are almost close to one another, except during the replay attack session, where there is a deviation. A significant difference between the actual and estimated data can be observed for the attacked duration.

Fig. 9 shows the EoE between the actual and estimated data during the attack phase. As can be observed, the model shows a huge difference in EoE for the attacked period. To distinguish both the attacks and outliers from normal values, the IQR is applied to EoE, and thus, an upper bound and lower bound are set following (8) and (9), where the value of β is set to 0.25 based on a heuristic. The upper and lower dotted lines represent the upper and lower ranges defined by IQR.

Several outliers are detected along with the actual attacks, which are not replay attacks but rather large variations in the input data or non-uniform values present in the input parameters, leading to these sudden occurrences of outliers. Therefore, to identify the replay attack instances out of all the outliers given by IQR, a window size g is set to 7. The replay attacks are uniquely identified by considering the consecutive

TABLE 2. Summary of Detection System Performance Metrics

Category	Metric	Value
Severity Analysis	Mean Deviation	1.26
	Maximum Deviation	2.39
	Standard Deviation	0.3941
Temporal Analysis	Mean Detection Gap (steps)	3.7
	Maximum Gap (steps)	344.0
	Detection Density (%)	25.75
Boundary Effectiveness	Containment Ratio (%)	74.25
	Boundary Range	1.62
	Boundary Symmetry	0.0028
Zero-Deviation Analysis	Mean Deviation from Zero	0.63
	Zero Proximity Ratio (%)	4.40
	RMSE	0.7795

7 numbers of outliers that appeared one after another. The value of g is selected based on experimentation, as for any outliers to have a significant impact on the high-voltage battery, they have to persist for more than five timesteps. By setting the window size g to 7 and considering the consecutive outliers, the proposed method effectively distinguishes between actual replay attacks and outliers caused by large variations or non-uniformity in the input data. This approach ensures that only the genuine replay attack instances are identified, minimizing false positives and enhancing the accuracy of the attack detection system.

C. DETECTION PERFORMANCE ANALYSIS

The comprehensive evaluation of the performance of the detection system is summarized in Table 2, followed by a detailed analysis of multiple categories of metrics.

1) SEVERITY ANALYSIS

The severity metrics indicate significant and consistent attack detection capabilities. The mean deviation of 1.26 units from normal operation proves substantial, particularly when compared to the IQR bounds of ± 0.81 units. The maximum observed deviation reached 2.39 units, approximately three times the IQR bound, demonstrating the system's ability to detect severe attacks. Notably, the low standard deviation of 0.3941 suggests consistent attack severity levels, indicating systematic rather than random attack patterns.

2) TEMPORAL DISTRIBUTION

Temporal analysis revealed distinct patterns in attack occurrence and detection. The system exhibited an average gap of 3.7 time steps between consecutive detections, indicating frequent monitoring capability. However, a significant maximum gap of 344 time steps was observed, corresponding to a notable quiet period between 800-1200 seconds. The detection density of 25.75% indicates that approximately one-quarter of all time points were flagged as potential attacks, suggesting a balanced sensitivity in the detection system.

3) BOUNDARY EFFECTIVENESS

The IQR boundary implementation demonstrated high effectiveness in distinguishing between normal operations and attack scenarios. The containment ratio of 74.25% indicates that a substantial majority of EoE values fall within the established IQR bounds, validating the chosen boundary parameters. The boundary range of 1.62 units provides an effective detection window while maintaining reasonable sensitivity. Most notably, the near-zero boundary symmetry value (0.0028) confirms almost perfect symmetry around zero, enhancing the reliability of error detection.

4) BASELINE DEVIATION ASSESSMENT

Analysis of zero-deviation metrics revealed significant insights into system behavior. The mean deviation from zero of 0.63 units indicates substantial attack activity, while the low zero proximity ratio of 4.4% suggests either frequent attack occurrences or the presence of baseline system noise. The RMSE value of 0.7795 provides a weighted measure of error magnitude, confirming the significant impact of detected deviations.

5) SYSTEM PERFORMANCE SUMMARY

The collective analysis of these metrics demonstrates several key strengths of the implemented detection system:

1) *Balanced Detection Sensitivity:* The combination of symmetric bounds and reasonable containment ratio (74.25%) indicates well-calibrated detection thresholds.
2) *Consistent Attack Recognition:* The low standard deviation in attack severity (0.3941) suggests systematic attack pattern recognition.
3) *Effective Temporal Monitoring:* Despite significant quiet periods, the system maintains consistent detection capabilities with an average gap of 3.7 time steps between detections.
4) *Robust Threshold Implementation:* The detection density of 25.75% demonstrates a balanced approach to attack identification without oversensitivity.

These results validate the effectiveness of the IQR-based approach for replay attack detection while highlighting areas for potential optimization in handling extended quiet periods and baseline noise reduction.

X. CHALLENGES AND FUTURE DIRECTIONS

As ZTA continues to gain traction in securing CPSs, inherent challenges must be addressed to ensure its widespread adoption and effectiveness. While ZTA provides a robust security framework with its "never trust, always verify" principle, implementing it in highly dynamic and heterogeneous CPS environments, such as HEVs and autonomous systems, presents several limitations. These challenges include issues related to scalability, performance overhead, and the integration of ZTA with legacy systems. In response, ongoing research efforts should focus on developing more efficient ZTA frameworks, reducing computational complexity, and enhancing the adaptability of ZTA for future CPS deployments. This section discusses these challenges and explores

potential future research directions to advance ZTA for CPS environments.

A. SCALABILITY CHALLENGES IN ZTA FOR CPSS

One of the primary challenges facing ZTA implementation in CPS environments is scalability. CPSs typically consist of a large number of distributed components, including sensors, actuators, control units, and communication systems, all interacting in real-time. Scaling ZTA to secure every interaction between these components requires continuous authentication, real-time risk assessments, and fine-grained access controls across multiple layers of the system.

ZTA inherently involves complex, continuous processes such as verifying user identities, monitoring device behavior, and dynamically adjusting access rights. As the number of devices and interactions in a CPS increases, the computational burden on the system grows significantly. This presents a substantial challenge, particularly in large-scale systems such as smart cities, industrial control systems, and vehicular networks, where numerous devices must be continuously authenticated and monitored. To address scalability issues, researchers are investigating distributed ZTA models that distribute the responsibility of trust evaluation across multiple entities within the system. These distributed models reduce the centralization of security functions, enabling CPSs to maintain a high level of security without overburdening any single component. However, achieving the right balance between security and system performance in these distributed models remains an ongoing challenge.

B. PERFORMANCE OVERHEAD AND COMPUTATIONAL COMPLEXITY

Another critical challenge is the performance overhead introduced by ZTA, particularly in resource-constrained environments like embedded systems used in HEVs and autonomous vehicles. These systems have limited processing power, memory, and energy resources, making it difficult to implement the continuous verification and monitoring required by ZTA without adversely affecting system performance. The continuous verification of all interactions in a ZTA framework—ranging from device authentication to real-time anomaly detection—can introduce latency, which is unacceptable in safety-critical CPS environments such as HEVs. For example, in autonomous driving or vehicular control systems, even slight delays in processing security checks can lead to system performance degradation or, worse, safety risks. The challenge is to implement ZTA without compromising the real-time operational requirements of CPSs.

One promising approach to reducing the performance overhead is leveraging edge computing, where computationally intensive tasks are offloaded from central controllers to edge nodes closer to the devices. This reduces latency and improves real-time responsiveness. In HEVs, for instance, edge-based ZTA systems could enable continuous monitoring of vehicle components without overwhelming the vehicle's central control unit. Additionally, lightweight encryption protocols, such as elliptic curve cryptography (ECC), have shown promise in resource-constrained environments due to their lower computational overhead compared to traditional algorithms.

C. INTEGRATION WITH LEGACY SYSTEMS

The integration of ZTA with legacy systems presents a significant challenge for its adoption in CPS environments. Many existing CPSs, particularly in the industrial and automotive sectors, rely on legacy systems that were not designed with modern cybersecurity needs in mind. These systems often lack the computational capacity and architectural flexibility to support the rigorous requirements of ZTA, such as continuous identity verification and dynamic access control.

Retrofitting legacy systems to accommodate ZTA can be both costly and technically challenging. Legacy devices may use outdated communication protocols, limited cryptographic capabilities, and centralized security models that conflict with ZTA's decentralized and dynamic approach. Moreover, upgrading these systems to support ZTA without disrupting their core functionality can be complex, particularly in industries like manufacturing and energy, where downtime can have serious financial and operational consequences. To address this challenge, researchers are exploring hybrid security models that combine elements of ZTA with more traditional security mechanisms, offering an incremental upgrade path for legacy systems. For instance, hybrid models could maintain traditional firewall protections while introducing ZTA concepts such as continuous monitoring and least-privilege access controls. This enables organizations to implement ZTA principles gradually without requiring a complete overhaul of their existing infrastructure.

D. EFFORTS TO REDUCE COMPUTATIONAL COMPLEXITY IN ZTA FOR HEVS

Reducing the computational complexity of ZTA is a key focus in resource-constrained CPS environments, where devices such as sensors, actuators, and embedded controllers operate with limited processing power, memory, and energy capacity. In HEVs, for example, embedded control units (ECUs) must execute safety-critical tasks in real-time, leaving little room for additional security operations that could slow down the system. To overcome this limitation, researchers are developing lightweight ZTA solutions specifically designed for low-power ECUs and other constrained devices. These solutions aim to minimize the overhead associated with continuous verification and monitoring while maintaining the integrity of the ZTA framework. For example, Trusted Platform Modules (TPMs) and secure enclaves [82] can offload security-related computations from the main processor, reducing the performance impact on the system.

Additionally, the use of federated learning is being explored to enable decentralized trust evaluation and anomaly detection in resource-constrained CPSs. By distributing the computational workload across multiple devices in the network, federated learning allows ZTA frameworks to assess the trustworthiness of devices locally, without requiring all data

to be sent to a central server for processing. This approach not only reduces the computational burden on individual devices but also improves the scalability and resilience of the system as a whole.

E. FUTURE RESEARCH DIRECTIONS

Building on our findings, we identify specific research challenges and propose concrete methodologies for advancing ZTA in CPS environments, particularly for HEVs:

1) OPTIMIZATION OF REAL-TIME TRUST EVALUATION

Research Questions:

- How can we achieve sub-millisecond trust evaluation for safety-critical ECUs while maintaining 99.9% accuracy?
- What is the optimal balance between detection latency and false positive rates in resource-constrained environments?

Proposed Methodologies:

- Development of hardware-accelerated trust evaluation algorithms targeting 0.5 ms response time
- Implementation of multi-level trust caching mechanisms with configurable refresh rates
- Quantitative analysis of trade-offs between security strength and computational overhead

2) INTEGRATION WITH LEGACY AUTOMOTIVE SYSTEMS

Research Questions:

- How can ZTA principles be applied to CAN bus communications without requiring protocol modifications?
- What are the minimum hardware requirements for implementing ZTA in existing ECUs?

Proposed Methodologies:

- Development of lightweight authentication protocols for CAN bus with less than 1 ms overhead
- Design of backward-compatible security wrappers for legacy ECUs
- Empirical evaluation of performance impact on existing vehicle networks

3) AI-ENHANCED ATTACK DETECTION

Research Questions:

- How can deep learning models be optimized for real-time attack detection with limited computational resources?
- What is the minimum dataset size needed for reliable attack detection in different driving conditions?

Experimental Approaches:

- Development of compressed neural networks targeting 90% accuracy with less than 1 MB model size
- Investigation of transfer learning techniques to reduce training data requirements by 50%
- Implementation of online learning algorithms for continuous model adaptation

4) SCALABLE TRUST MANAGEMENT

Research Questions:

- How can trust scores be effectively propagated across different subsystems while maintaining consistency?
- What metrics should be used to quantify trust in different operational contexts?

Proposed Investigations:

- Development of hierarchical trust management frameworks supporting more than 1000 nodes
- Implementation of context-aware trust scoring mechanisms with less than 10 ms update intervals
- Evaluation of distributed trust consensus algorithms for vehicle networks

5) QUANTUM-RESISTANT SECURITY MEASURES

Specific Challenges:

- How can post-quantum cryptographic algorithms be implemented with less than 5 ms latency on automotive ECUs?
- What are the memory and processing requirements for different quantum-resistant algorithms?

Research Methodology:

- Comparative analysis of lattice-based vs. hash-based signatures for automotive applications
- Development of hybrid classical-quantum resistant protocols
- Performance benchmarking on representative automotive hardware platforms

XI. CONCLUSION

This article has explored the critical role of ZTA in addressing the evolving security challenges that modern HEVs face. Through our comprehensive analysis of ZTA tailored specifically for vehicular cyber-physical systems, we have highlighted the need for effective modeling of interlayer penetration between the cyber and physical layers of HEVs. Our discussion of existing technologies and the application of zero-trust principles to CP-HEVs has illuminated the unique challenges of integrating ZTA in automotive systems. To address these security challenges, we have proposed a Deep Learning-based replay attack detection scheme for the battery management system of HEVs. Our approach leverages advanced neural network architectures to estimate the battery State of Charge with high accuracy (RMSE of 0.0002582), while the IQR-based detection system achieves a 74.25% containment ratio with balanced sensitivity. The effectiveness of this method in detecting stealth attacks has been demonstrated through comprehensive simulation results and quantitative metrics.

A. BROADER IMPACT AND SOCIETAL BENEFITS

The implications of this research extend far beyond technical achievements, contributing significantly to the field of automotive cybersecurity in several ways:

- *Enhanced Vehicle Safety:* By protecting critical battery management systems from cyber attacks, our approach helps ensure the safe operation of HEVs, potentially preventing accidents and protecting human lives.
- *Environmental Sustainability:* Securing HEV systems encourages wider adoption of electric vehicles by addressing cybersecurity concerns, thereby contributing to reduced carbon emissions and environmental protection.
- *Economic Benefits:* The proposed detection system can help prevent costly damage to vehicle batteries and reduce maintenance expenses, making HEVs more economically viable for consumers.
- *Infrastructure Protection:* Our work contributes to the security of smart grid infrastructure by protecting vehicle-to-grid interactions from potential cyber threats.
- *Industry Standards:* This research provides a framework that can influence future automotive cybersecurity standards and best practices, particularly in the emerging field of connected vehicles.

B. FUTURE DIRECTIONS

While our current work demonstrates promising results, several important research directions remain to be explored:

- Development of a comprehensive zero-trust-empowered attack detection system with detailed trust evaluation schemes integrated into vehicle controls
- Investigation of lightweight implementations for resource-constrained automotive systems
- Extension of the framework to other critical vehicle subsystems
- Integration with emerging connected vehicle technologies and smart transportation infrastructure

As the automotive industry continues its transition toward electrification and automation, the significance of robust cybersecurity measures becomes increasingly critical. Our work contributes to this essential evolution by providing both theoretical frameworks and practical solutions for securing the next generation of vehicles. The proposed methods and insights gained from this research can serve as building blocks for developing more comprehensive automotive cybersecurity solutions, ultimately contributing to safer, more sustainable, and more secure transportation systems.

ACKNOWLEDGMENT

The authors would like to express their gratitude for the valuable resources and facilities provided by the Secure Energy and Automation Laboratory (SEAL) and Real Time Controls and Optimization Laboratory (RTCOOL). The authors would like to acknowledge the Warren H. Owen Distinguished Professorship Endowment for supporting this research effort. DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited. OPSEC8716

REFERENCES

[1] M. Annabi, A. Zeroual, and N. Messai, "Towards zero trust security in connected vehicles: A comprehensive survey," *Comput. Secur.*, vol. 145, 2024, Art. no. 104018.

[2] G. Hope, "Cyberattacks on auto, mobility industries on the rise: Report," IoT World Today, (n.d.). Accessed: Jul. 9, 2025. [Online]. Available: https://www.iotworldtoday.com/security/cyberattacks-on-auto-mobility-industries-on-the-rise-report

[3] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks," *IEEE Trans. Power Syst.*, no. 32, no. 4, pp. 3317–3318, Jul. 2017.

[4] T. Tsvetanov and S. Slaria, "The effect of the colonial pipeline shutdown on gasoline prices," *Econ. Lett.*, vol. 209, 2021, Art. no. 110122.

[5] C. Stupp, "European wind-energy sector hit in wave of hacks," 2022. [Online]. Available: https://www.wsj.com/articles/european-wind-energy-sector-hit-in-wave-of-hacks-11650879000

[6] I. GROUP, "China-linked group redecho targets the Indian power sector amid heightened border tensions," 2021. [Online]. Available: https://www.recordedfuture.com/blog/redecho-targeting-indian-power-sector

[7] G. Muriithi et al., "Vulnerability assessment and detection of stealthy sequential cyberattacks in hybrid tracked vehicles," *IEEE Trans. Transport. Electrific.*, vol. 11, no. 2, pp. 6472–6489, Apr. 2025.

[8] S. Curry, "Hacking kia: Remotely controlling cars with just a license plate," Sep. 2024. Accessed: Jul. 9, 2025. [Online]. Available: https://samcurry.net/hacking-kia

[9] Claroty Team, "How ZTNA strengthens cyber-physical systems (CPS) security," Sep. 2024. Accessed: Jul. 9, 2025. [Online]. Available: https://claroty.com/blog/how-ztna-strengthens-cyber-physical-systems-cps-security

[10] P. Dhiman et al., "A review and comparative analysis of relevant approaches of zero trust network model," *Sensors*, vol. 24, no. 4, 2024, Art. no. 1255.

[11] N. Nahar, K. Singh, and F. Hussain, "Zero trust architecture for secure 6G networks: Challenges and opportunities," *IEEE Access*. vol. 12, pp. 94753–94764, 2024.

[12] S. Ahmadi, "Zero trust architecture in cloud networks: Application, challenges and future opportunities," *J. Eng. Res. Reports*, vol. 26, no. 2, pp. 215–228 2024.

[13] R. Ahmadi, "Zero trust architecture in cloud environments: A qualitative case study," *SSRN Electron. J.*, 2024.

[14] Y. Liu, Z. Su, H. Peng, Y. Xiang, W. Wang, and R. Li, "Zero trust-based mobile network security architecture," *IEEE Wireless Commun.*, vol. 31, no. 2, pp. 82–88, Apr. 2024.

[15] H. Sedjelmaci and N. Ansari, "Zero trust architecture empowered attack detection framework to secure 6G edge computing," *IEEE Netw.*, vol. 38, no. 1, pp. 196–202, Jan. 2024.

[16] B. Huber and F. Kandah, "Zero trust+: A trusted-based zero trust architecture for IoT at scale," in *Proc. IEEE Int. Conf. Consum. Electron.*, 2024, pp. 1–6.

[17] Z. Xiaojian, C. Liandong, F. Jie, W. Xiangqun, and W. Qi, "Power IoT security protection architecture based on zero trust framework," in *Proc. IEEE 5th Int. Conf. Cryptogr., Secur. Privacy*, Zhuhai, China, 2021, pp. 166–170.

[18] A. Hussain and A. Ghosh, "Federated learning-based adaptive zero trust architecture," *IEEE Wireless Commun.*, vol.31, no 2, pp. 30–35, 2024.

[19] S. Pokhrel, L. yang, S. Rajasegarar, and G. Li, "Robust zero trust architecture: Joint blockchain based federated learning and anomaly detection based framework," in *Proc. SIGCOMM Workshop Zero Trust Architecture Next Gener. Commun.*, 2024.

[20] P. Amusuo et al., "ZTD mitigating software supply chain vulnerabilities via zero-trust dependencies," 2023, *2310.14117*.

[21] X. Feng and S. Hu, "Cyber-physical zero trust architecture for industrial cyber-physical systems," *IEEE Trans. Ind. Cyber- Phys. Syst.*, vol. 1, pp. 394–405, 2023.

[22] J. Anderson, Q. Huang, L. Cheng, and H. Hu, "A zero trust architecture for connected and autonomous vehicles," *IEEE Internet Comput.*, vol. 27, no. 5, pp. 1–7, Sep.–Oct. 2023.

[23] X. Feng and S. Hu, "Cyber-physical zero trust architecture for industrial cyber-physical systems," *IEEE Trans. Ind. Cyber-Phys. Syst.*, vol. 1, pp. 394–405, 2023.

[24] M. Vai et al., "Zero trust architecture approach for developing mission critical embedded systems," in *Proc. IEEE High Perform. Extreme Comput. Conf.*, 2023, pp. 1–5.

[25] S. Hasan, I. Amundson, and D. Hardin, "Zero trust architecture patterns for cyber-physical systems," *SAE Int. J. Adv. Curr. Practices Mobility*, vol. 5, pp. 1919–1931, 2023.

[26] R. Freter, "Department of defence (DoD) zero trust reference architecture, version 2.0," in *Proc. Defense Inf. Syst. Agency Nat. Secur. Agency*, 2022.

[27] Y. He, D. Huang, L. Chen, Y. Ni, and X. Ma, "A survey on zero trust architecture: Challenges and future trends," *Wireless Commun. Mobile Comput.*, vol. 2022, no. 1, 2022, Art. no. 6476274.

[28] V. Stafford, "Zero trust architecture," *NIST Special Publication*, vol. 800, 2020, Art. no. 207.

[29] G. Bere, J. J. Ochoa, T. Kim, and I. R. Aenugu, "Blockchain-based firmware security check and recovery for battery management systems," in *Proc. IEEE Transp. Electrific. Conf. Expo*, 2020, pp. 262–266.

[30] X. Duan, H. Yan, D. Tian, J. Zhou, J. Su, and W. Hao, "In-vehicle CAN bus tampering attacks detection for connected and autonomous vehicles using an improved isolation forest method," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2122–2134, Feb. 2023.

[31] O. Boyaci, M. R. Narimani, K. R. Davis, M. Ismail, T. J. Overbye, and E. Serpedin, "Joint detection and localization of stealth false data injection attacks in smart grids using graph neural networks," *IEEE Trans. Smart Grid*, vol. 13, no. 1, pp. 807–819, Jan. 2022.

[32] A. Alagappan, S. K. Venkatachary, and L. J. B. Andrews, "Augmenting zero trust network architecture to enhance security in virtual power plants," *Energy Reports*, vol. 8, pp. 1309–1320, 2022.

[33] W. Jing, L. Peng, H. Fu, and A. Hu, "An authentication mechanism based on zero trust with radio frequency fingerprint for IoT networks," *IEEE Internet Things J.*, vol. 11, no. 13, pp. 23683–23698, Jul. 2024.

[34] A. Alsulami and M. Yousaf, "Zebra: Zero trust architecture employing blockchain technology and ropuf for AMI security," 2024, *IEEE Access*.

[35] B. Chen et al., "A security awareness and protection system for 5G smart healthcare based on zero-trust architecture," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10248–10263, Jul. 2021.

[36] M. Sultana, A. Hossain, F. Laila, K. A. Taher, and M. N. Islam, "Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology," *BMC Med. Inform. Decis. Mak.*, vol. 20, pp. 1–10, 2020.

[37] E. W. Tomlinson, W. Wolday, S. Kim, S. Ortega, "Cybersecurity access control: Framework analysis in a healthcare institution," *J. Cyber secur. Privacy*, Vol. 4, no.3, pp. 762–776 2024.

[38] L. Freitas and M. Silva, "Control systems cyber security reference architecture (RA) for critical infrastructure: Healthcare and hospital vertical example," *J. Crit. Infrastructure Policy*, vol. 2, no. 2, 2021.

[39] H. Zhu, "Zero-Trust Blockchain-Enabled Secure Next-Generation Healthcare Communication Network," *IEEE Trans. Netw. Serv. Manage.*, vol. 22, no. 4, pp. 3201–3212, Aug. 2025.

[40] C. Zanasi, F. Magnanini, S. Russo, and M. Colajanni, "A zero trust approach for the cybersecurity of industrial control systems," in *Proc. IEEE 21st Int. Symp. Netw. Comput. Appl.*, 2022, pp. 1–7.

[41] F. Federici, D. Martintoni, and V. Senni, "A zero-trust architecture for remote access in industrial IoT infrastructures," *Electronics*, vol. 12, no. 3, 2023, Art. no. 566.

[42] W. Lei, Z. Pang, H. Wen, W. Hou, and W. Li, "Physical layer enhanced zero-trust security for wireless industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 20, no. 3, pp. 4327–4336, Mar. 2024.

[43] L. Xagoraris, D. Kogias, and P. Karkazis, "A review of zero trust security framework (ZTF) for sustainable and resilient smart cities," in *Proc. 27th Pan-Hellenic Conf. Prog. Comput. Informat.*, 2023, pp. 269–273.

[44] E. Ismagilova, L. Hughes, N. P. Rana, and Y. K. Dwivedi, "Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework," *Inf. Syst. Front.*, vol. 24, pp. 393–414, 2022.

[45] M. H. P. Rizi and S. A. H. Seno, "A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city," *Internet Things*, vol. 20, 2022, Art. no. 100584.

[46] L. Cui, G. Xie, Y. Qu, L. Gao, and Y. Yang, "Security and privacy in smart cities: Challenges and opportunities," *IEEE Access*, vol. 6, pp. 46134–46145, 2018.

[47] K. Huang, C. Zhou, Y. Qin, and W. Tu, "A game-theoretic approach to cross-layer security decision-making in industrial cyber-physical systems," *IEEE Trans. Ind. Electron.*, vol. 67, no. 3, pp. 2371–2379, Mar. 2020.

[48] G. Muriithi, B. Papari, A. Moghassemi, A. Arsalan, G. Ozkan, and C. S. Edrington, "Security enhancement of cyber-physical dc ship power system using scalable deep learning method," in *Proc. IEEE Electric Ship Technol. Symp.*, 2023, pp. 520–527.

[49] M. S. Bargh, A. Omar, and S. Choenni, "Zero-trust security model applied to smart shipping," *Adv. Know. Base. Syst. Data Sci. Cyber.*, 1, no. 1, 78–107, 2024.

[50] G. Muriithi et al., "Impact analysis of cyberattacks in electric propulsion systems for hybrid tracked vehicles," SAE Technical Paper, Tech. Rep., 2024.

[51] D. Scruggs et al., "Neural network-based cyber-threat detection strategy in four motor-drive autonomous electric vehicles," *IEEE Access*, vol. 12, pp. 124220–124230, 2024.

[52] J. Anderson, Q. Huang, L. Cheng, and H. Hu, "A zero trust architecture for connected and autonomous vehicles," *IEEE Internet Comput.*, vol. 27, no. 5, pp. 7–14, Sep.–Oct. 2023.

[53] R. Hasan and M. Younis, "Zero trust architecture design patterns for cyber-physical systems," 2024, *arXiv:2401.09220*.

[54] M. Pakmehr, T. Khamvilai, A. R. Behbahani, J. Costello, R. Skertic, and A. P. Ademola, "Applying zero trust principles to distributed embedded engine control systems," *AIAA AVIATION Forum*, 2022, Art. no. 3480.

[55] V. B. Kondaveety, H. Lamkuche, and S. Prasad, "A zero trust architecture for next generation automobiles," *AIP Conf. Proc.*, 2022, vol. 2519, no. 1, Art. no. 030088.

[56] M. E. Shipman, N. Millwater, K. Owens, and S. Smith, "A zero trust architecture for automotive networks," SAE Technical Paper, Tech. Rep., 2024.

[57] M. Zayed, A. Anwar, Z. Rahman, S. S. Arefin, and R. Islam, "Owner identity verification in the internet of connected vehicles: Zero trust based solution," *Cryptol. ePrint Arch.*, 2022.

[58] S. Adly, A. Moro, S. Hammad, and S. A. Maged, "Prevention of controller area network (CAN) attacks on electric autonomous vehicles," *Appl. Sci.*, vol. 13, no. 16, 2023, Art. no. 9374.

[59] M. Kneib, O. Schell, and C. Huth, "EASI: Edge-based sender identification on resource-constrained platforms for automotive networks," in *Proc. NDSS*, 2020, pp. 1–16.

[60] A. Arsalan et al., "Cyber attack detection and classification for integrated on-board electric vehicle chargers subject to stochastic charging coordination," *Transp. Res. Procedia*, vol. 70, pp. 44–51, 2023.

[61] L. Timilsina, P. R. Badr, P. H. Hoang, G. Ozkan, B. Papari, and C. S. Edrington, "Battery degradation in electric and hybrid electric vehicles: A survey study," *IEEE Access*, vol. 11, pp. 42431–42462, 2023.

[62] G. Muriithi and S. Chowdhury, "Optimal energy management of a grid-tied solar PV-battery microgrid: A reinforcement learning approach," *Energies*, vol. 14, no. 9, 2021, Art. no. 2700.

[63] S. K. Datta, J. Haerri, C. Bonnet, and R. Ferreira Da Costa, "Vehicles as connected resources: Opportunities and challenges for the future," *IEEE Veh. Technol. Mag.*, vol. 12, no. 2, pp. 26–35, Jun. 2017.

[64] D. He, C. Chen, S. Chan, J. Bu, and A. V. Vasilakos, "A distributed trust evaluation model and its application scenarios for medical sensor networks," *IEEE Trans. Inf. Technol. Biomed.*, vol. 16, no. 6, pp. 1164–1175, Nov. 2012.

[65] H. Sedjelmaci and N. Ansari, "Zero trust architecture empowered attack detection framework to secure 6G edge computing," *IEEE Netw.*, vol. 38, no. 1, pp. 196–202, Jan. 2024.

[66] G. Muriithi and S. Chowdhury, "Deep Q-network application for optimal energy management in a grid-tied solar PV-battery microgrid," *J. Eng.*, vol. 2022, no. 4, pp. 422–441, 2022.

[67] T. T. Nguyen and V. J. Reddi, "Deep reinforcement learning for cyber security," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 34, no. 8, pp. 3779–3795, Aug. 2023.

[68] L. Guo, J. Ye, and B. Yang, "Cyberattack detection for electric vehicles using physics-guided machine learning," *IEEE Trans. Transp. Electrific.*, vol. 7, no. 3, pp. 2010–2022, Sep. 2021.

[69] H. Moudoud, W. Hamhoum, and S. Cherkaoui, "Strengthening open radio access networks: Advancing safeguards through ZTA and deep learning," in *Proc. IEEE Glob. Commun. Conf.*, 2023, pp. 80–85.

[70] S. Munasinghe, N. Piyarathna, E. Wijerathne, U. Jayasinghe, and S. Namal, "Machine learning based zero trust architecture for secure networking," in *Proc. IEEE 17th Int. Conf. Ind. Inf. Syst.*, 2023, pp. 1–6.

[71] E. S. Hosney, I. T. A. Halim, and A. H. Yousef, "An artificial intelligence approach for deploying zero trust architecture (ZTA)," in *Proc. 5th Int. Conf. Comput. Informat.*, 2022, pp. 343–350.

[72] W. Lei, Z. Pang, H. Wen, W. Hou, and X. Zhang, "Edge-enabled zero trust architecture for ICPs with spatial and temporal granularity," in *Proc. IEEE 6th Int. Conf. Ind. Cyber-Phys. Syst.*, 2023, pp. 1–6.

[73] J. Guo et al., "TFL-DT: A trust evaluation scheme for federated learning in digital twin for mobile networks," *IEEE J. Sel. Areas Commun.*, vol. 41, no. 11, pp. 3548–3560, Nov. 2023.

[74] G. I. Parisi and V. Lomonaco, "Online continual learning on sequences," in *Proc. Recent Trends Learn. Data, Tut. INNS Big Data Deep Learn. Conf.*, 2019, 197–221.

[75] G. Muriithi, B. Papari, A. Moghassemi, A. Arsalan, G. Ozkan, and C. S. Edrington, "Security enhancement of cyber-physical DC ship power system using scalable deep learning method," in *Proc. IEEE Electric Ship Technol. Symp.*, 2023, pp. 520–527.

[76] J. Ye et al., "Cyber–physical security of powertrain systems in modern electric vehicles: Vulnerabilities, challenges, and future visions," *IEEE Trans. Emerg. Sel. Topics Power Electron.*, vol. 9, no. 4, pp. 4639–4657, Aug. 2021.

[77] J. Jiang, X. Zhu, G. Han, M. Guizani, and L. Shu, "A dynamic trust evaluation and update mechanism based on c4. 5 decision tree in underwater wireless sensor networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 8, pp. 9031–9040, Aug. 2020.

[78] Z. Oudina, M. Derdour, R. Boudour, A. Dib, and M. A. Yakoubi, "Trust cyber physical systems: Trust degree framework and evaluation," *Int. J. Saf. Secur. Eng.*, vol. 13, no. 2, pp. 213–225, 2023.

[79] S. Gao et al., "Short-term runoff prediction with GRU and LSTM networks without requiring time step optimization during sample generation," *J. Hydrol.*, vol. 589, 2020, Art. no. 125188.

[80] H. Vinutha, B. Poornima, and B. Sagar, "Detection of outliers using interquartile range technique from intrusion dataset," in *Proc. 6th Int. Conf. FICTA Inf. Decis. Sci.*, 2018, pp. 511–518.

[81] Q. Zhu et al., "Development of a series hybrid electrified powertrain for a high-speed tracked vehicle based on driving cycle simulation," *SAE Int. J. Adv. Curr. Practices Mobility*, vol. 4, pp. 1403–1412, 2022.

[82] P. G. Wagner, P. Birnstill, and J. Beyerer, "Distributed usage control enforcement through trusted platform modules and SGX enclaves," in *Proc. 23rd ACM Symp. Access Control Models Technol.*, 2018, pp. 85–91.