ISSN 2319-5991 www.ijerst.com

Peer Reviewed, Referred & Indexed Journal

Research Paper

Systematic Assessment of Cyber Physical Security of Energy Management System for Connected and Automated Electric Vehicles

Shaik Sameer Ahmed
PG Scholar
Department of Information Technology
Shadan College of Engineering and Technology
Hyderabad, Telangana, India – 500086
sameerece15@gmail.com

Subramanian K.M
Professor
Department of of Computer Science and Engineering
Shadan College of Engineering and Technology
Hyderabad, Telangana, India – 500086
kmsubbu.phd@gmail.com

Imtiyaz Khan
Professor
Department of Information Technology
Shadan College of Engineering and Technology
Hyderabad, Telangana, India – 500086
imtiyaz.khan.7@gmail.com

***Abstract*— The rapid advancement of Connected and Automated Electric Vehicles (CAEVs) has increased reliance on Energy Management Systems (EMS), making them vulnerable to cyber-physical security threats that can compromise vehicle performance, safety, and energy efficiency. This paper presents a systematic assessment framework for evaluating the cyber-physical security of EMS in CAEVs. The proposed approach integrates multiple vehicle sensors and communication components to identify potential vulnerabilities within the control architecture. Various cyber-physical attack scenarios, including false data injection, sensor spoofing, and communication manipulation attacks, are modeled to analyze their impact on system operation. An EMS based on Model Predictive Control (MPC) is implemented to optimize energy utilization while maintaining vehicle performance under normal and attack conditions. Extensive simulations are conducted to collect operational data related to energy consumption, control actions, and vehicle dynamics. The collected data are analyzed using security-oriented performance metrics that evaluate system resilience, stability, comfort, and energy efficiency. The results provide a comprehensive understanding of how cyber-attacks influence EMS behavior and overall vehicle operation. The proposed assessment methodology enables the identification of critical vulnerabilities and supports the development of effective detection, mitigation, and recovery mechanisms, thereby enhancing the security, reliability, and sustainability of future connected and automated electric transportation systems.**

Keywords*— *Cyber-Physical Security, Connected and Automated Electric Vehicles, Energy Management System, Model Predictive Control, Sensor Integration, Vulnerability Assessment, Cyber-Attack Detection, Energy Consumption Analysis.

I. INTRODUCTION

Connected and Automated Electric Vehicles (CAEVs) are transforming modern transportation by integrating advanced sensing, communication, and intelligent control technologies to improve safety, mobility, and energy efficiency. The increasing deployment of vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and cloud-based communication systems enables vehicles to exchange real-time information and make autonomous driving decisions. However, the extensive connectivity of these systems introduces significant cybersecurity challenges that can threaten the reliability and safety of vehicle operations. Recent studies have highlighted the growing threat landscape associated with connected electric vehicles and autonomous transportation systems, emphasizing the need for comprehensive cybersecurity frameworks to address emerging vulnerabilities [1].

As electric vehicles become increasingly dependent on electronic control units, communication networks, and cloud-based services, they become attractive targets for cyber-attacks. Security risk assessment methodologies have been developed to evaluate potential threats and identify critical weaknesses within electric vehicle architectures [2]. The convergence of cyber and physical domains in intelligent transportation systems further increases the complexity of securing vehicle operations against malicious activities [3]. In particular, battery management systems and cloud-connected energy platforms have been identified as critical components requiring robust protection mechanisms due to their direct impact on vehicle performance and safety [4].

The integration of electric vehicles with smart grid infrastructures introduces additional cyber-physical security concerns related to power exchange and energy distribution networks [5]. Blockchain-based security mechanisms have been proposed to enhance trust and data integrity in vehicle-assisted smart grid ecosystems [6]. Furthermore, advanced cybersecurity strategies for connected and automated vehicles have demonstrated the importance of proactive threat modeling and vulnerability mitigation approaches [7].

Energy Management Systems (EMS) play a crucial role in optimizing battery utilization, energy consumption, and overall vehicle efficiency. Recent advancements in artificial intelligence have enhanced EMS capabilities through intelligent decision-making and adaptive control strategies [8]. AI-driven control techniques have also contributed to improved energy management and predictive maintenance in electric vehicle applications [9]. Intelligent EMS frameworks have been recognized as key enablers for future electric

transportation systems due to their ability to balance performance and energy efficiency [10]. However, vulnerabilities within battery management and energy control components continue to pose significant cybersecurity risks that require systematic analysis and mitigation [11].

The objective of this paper is to develop a systematic framework for assessing the cyber-physical security of Energy Management Systems in Connected and Automated Electric Vehicles. The major contributions of this work include sensor integration for security-aware monitoring, identification of critical vulnerabilities within EMS architectures, development of realistic cyber-physical attack scenarios, comprehensive energy consumption analysis under attack conditions, implementation of a Model Predictive Control (MPC)-based EMS, simulation-based data collection, and detailed performance evaluation using security and resilience metrics. The proposed framework provides valuable insights for enhancing the security, reliability, and energy efficiency of future connected electric transportation systems.

II. Related Work

Sifakis, Armyras, and Kanellos investigated real-time power management strategies for plug-in electric vehicles operating within virtual prosumer networks. Their work incorporated blockchain technology to provide integrated physical and network security while optimizing power exchange between electric vehicles and renewable energy resources. The study demonstrated that secure energy management mechanisms can improve system resilience while maintaining efficient power utilization in distributed energy environments [12].

Abreu, Branco, Reis, and Serôdio conducted a comprehensive review of cybersecurity challenges in connected and autonomous vehicles. Their study examined common attack vectors, vulnerabilities in communication networks, and security mechanisms employed in modern automotive systems. The authors emphasized the necessity of proactive security frameworks to protect vehicle functions from emerging cyber threats and ensure safe autonomous operation [13].

Elma, Cali, and Kuzlu presented an overview of bidirectional electric vehicle charging systems operating under Vehicle-to-Anything (V2X) environments. Their research highlighted the interaction between electric vehicles and cyber-physical power systems, discussing energy exchange mechanisms, communication architectures, and potential security concerns associated with bidirectional charging infrastructures [14].

Arsalan and colleagues proposed an enhanced real-time Artificial Transmission Management-based Model Predictive Control framework for electric vehicles with a strong focus on cyber-physical security. Their approach integrated predictive control techniques with security-aware operational constraints to improve vehicle performance while maintaining robustness against cyber disruptions. The study demonstrated the effectiveness of MPC in achieving secure and efficient energy management [15].

Guang and co-authors introduced a resilient cybersecurity management system designed specifically for connected and automated vehicles. Their framework combined threat monitoring, risk assessment, and adaptive defense mechanisms to improve vehicle security under dynamic operating conditions. The proposed architecture emphasized resilience as a critical factor for maintaining reliable vehicle operations during cyber-attacks [16].

Khan, Haider, Malik, Almasoudi, Alatawi, and Bhutta reviewed advanced microgrid energy management strategies involving electric vehicles, energy storage systems, and artificial intelligence techniques. Their work explored intelligent scheduling, optimization, and control approaches for efficient energy utilization. The study highlighted the importance of integrating smart energy management techniques with secure communication infrastructures to support future transportation systems [17].

Manias and collaborators analyzed current trends in smart grid cyber-physical security by examining system components, potential threats, and mitigation techniques. Their review identified vulnerabilities in communication networks, control systems, and distributed energy resources. The authors emphasized the significance of comprehensive security assessment methodologies for protecting interconnected cyber-physical energy infrastructures from sophisticated attacks [18].

Nuruzzaman investigated IoT-enabled condition monitoring systems in power distribution networks and discussed challenges related to SCADA-based automation, real-time analytics, and cyber-physical security. The study highlighted how increasing connectivity and data exchange create additional attack surfaces, necessitating robust monitoring and security mechanisms for critical energy infrastructures [19].

Rodríguez, Higuera, Higuera, Montalvo, and Crespo proposed a systematic methodology for assessing the security level of cyber-physical systems in the electricity sector. Their approach incorporated vulnerability identification, risk evaluation, and security metrics to quantify system resilience. The framework provided valuable insights into the development of structured security assessment procedures applicable to energy-related cyber-physical systems [20].

Mazumder and co-authors reviewed recent advancements in power-electronic innovations within cyber-physical systems. Their study discussed intelligent control architectures, power conversion technologies, communication frameworks, and system integration challenges. The authors emphasized the growing importance of cybersecurity considerations in power-electronic systems due to increasing levels of connectivity and automation [21].

Minchala-Ávila, Arévalo, and Ochoa-Correa conducted a systematic review of Model Predictive Control techniques for electric vehicle integration and Vehicle-to-Grid applications. Their analysis demonstrated that MPC provides robust and efficient energy management capabilities through predictive optimization and adaptive control. The study highlighted MPC as a promising approach for balancing energy efficiency, operational reliability, and system robustness in advanced electric vehicle applications [22].

The reviewed literature demonstrates significant progress in cyber-physical security, resilient control systems, intelligent energy management, and secure communication

architectures for electric vehicles and related energy infrastructures. However, limited research has focused on a systematic assessment of cyber-physical attacks targeting Energy Management Systems in Connected and Automated Electric Vehicles while simultaneously evaluating their impact on energy consumption, control performance, and system resilience. This research gap motivates the development of a comprehensive framework that integrates vulnerability assessment, cyber-attack analysis, Model Predictive Control-based energy management, and security-oriented performance evaluation.

III. Materials And Methods

The proposed system presents a cyber-physical security assessment framework for Connected and Automated Electric Vehicles (CAEVs) with a focus on Energy Management System (EMS) protection and energy-efficient vehicle operation. The framework integrates multiple vehicle sensors, Electronic Control Units (ECUs), and communication modules to continuously monitor vehicle behavior and detect abnormal activities. Inspired by anomaly correlation techniques for electric vehicle security, the system evaluates sensor data and vehicle dynamics to identify malicious commands generated through cyber-attacks such as Denial-of-Service (DoS), replay attacks, and false command injection [23]. The proposed model incorporates an EMS that analyzes the impact of cyber-attacks on battery utilization, vehicle performance, and energy consumption. Security-aware monitoring mechanisms are employed to assess how abnormal control commands affect overall vehicle operation and travel efficiency. To strengthen system resilience, advanced cybersecurity assessment principles are utilized to evaluate vulnerabilities and attack severity within the vehicle ecosystem [24]. Furthermore, a Model Predictive Control (MPC)-based energy management strategy is implemented to optimize battery usage and maintain stable vehicle performance under both normal and attack conditions. The controller predicts future vehicle states using velocity and operational parameters, enabling early detection of suspicious behavior and preventing unnecessary energy expenditure. The proposed simulation framework records energy consumption, vehicle velocity, and attack impacts, providing a comprehensive evaluation of system security and efficiency. The design also considers intelligent autonomous vehicle architectures and energy subsystems to ensure realistic assessment of cyber-physical threats in modern connected electric vehicles [25].

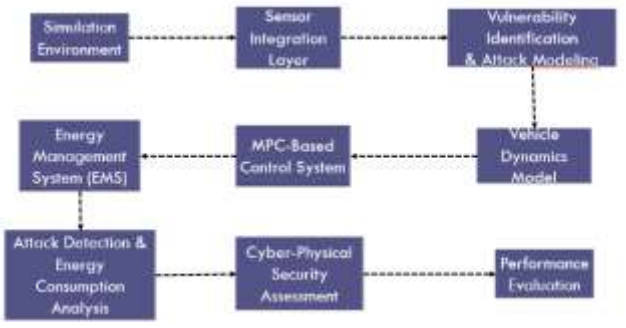

Fig.1 System Architecture

Figure 1 illustrates the sequential architecture of the proposed cyber-physical security evaluation framework for automated vehicles. The process begins with the Simulation Environment, which feeds operational scenarios into the Sensor Integration Layer to emulate real-time perception data. Potential vulnerabilities and adversarial behaviors are then simulated within the Vulnerability Identification & Attack Modeling block. This impacted data influences the Vehicle Dynamics Model, directly affecting the core driving behaviors regulated by the MPC-Based Control System. Consequently, these control alterations ripple into the Energy Management System (EMS). The framework captures these anomalies through the Attack Detection & Energy Consumption Analysis stage, which passes its metrics to the Cyber-Physical Security Assessment block. Finally, a comprehensive Performance Evaluation is executed to quantify the system's resilience and efficiency under adversarial conditions.

A) Sensor Integration and Vulnerability Identification:

The proposed framework utilizes multiple sensors embedded within Connected and Automated Electric Vehicles (CAEVs) to continuously monitor vehicle status and operating conditions. These sensors are assumed to be installed in critical vehicle subsystems such as braking systems, steering mechanisms, wheel assemblies, battery management units, and speed monitoring modules. The Electronic Control Unit (ECU) collects sensor measurements and issues control commands that regulate vehicle movement and operational behavior. During normal operation, sensors transmit real-time information regarding vehicle velocity, position, battery status, and environmental conditions. The collected data are used to maintain safe and efficient vehicle performance.

To evaluate cybersecurity risks, the framework performs vulnerability identification on communication channels between sensors and the ECU. Potential weaknesses include unauthorized command injection, communication manipulation, spoofed sensor readings, and compromised control signals. Since sensors and ECUs exchange information automatically without direct human intervention, malicious entities may exploit communication vulnerabilities to alter vehicle behavior. The vulnerability assessment process identifies critical attack surfaces and determines how compromised sensor data can influence vehicle decisions. This analysis establishes the foundation for understanding cyber-physical risks and supports the development of monitoring mechanisms capable of detecting suspicious activities before they significantly impact vehicle safety, energy consumption, or operational reliability.

B) Cyber-Physical Attack Scenario Generation:

To evaluate the resilience of the Energy Management System (EMS), several cyber-physical attack scenarios are simulated within the vehicle environment. The attack generation process focuses on threats that target communication between sensors and the ECU. Common attack types include Denial-of-Service (DoS) attacks, replay attacks, and malicious command injection attacks. In a DoS attack scenario, excessive requests are transmitted to

communication resources, causing delays and reducing system availability. Replay attacks repeatedly transmit previously valid commands, forcing sensors to execute unnecessary actions and consume additional resources.

The simulation environment models vehicle movement on a road where vehicles receive continuous control instructions from the ECU. During attack execution, malicious commands are inserted into the communication process to emulate real-world cyber intrusions. These abnormal commands may cause sudden braking, unexpected acceleration, or irregular steering behavior. Such actions directly influence vehicle velocity and operational stability. Attack conditions are generated for predefined time intervals to observe both transient and long-term effects on system performance. By creating multiple attack scenarios, the framework enables a comprehensive assessment of how cyber threats influence vehicle behavior, control system reliability, and energy utilization. The generated scenarios serve as test cases for evaluating attack detection mechanisms and validating the effectiveness of the proposed security-aware EMS.

C) Energy Management System with Model Predictive Control:

The Energy Management System (EMS) is designed to monitor energy utilization and maintain efficient vehicle operation under both normal and attack conditions. The EMS employs Model Predictive Control (MPC), which predicts future vehicle states based on current operational data and control inputs. Vehicle velocity serves as a primary indicator for assessing system behavior. The controller continuously compares current vehicle speed with previous speed measurements to determine whether abnormal changes occur within a specific observation period.

When sudden deviations from expected velocity patterns are detected, the system interprets these anomalies as potential cyber-attacks. The MPC-based EMS responds by rejecting suspicious commands and preventing unnecessary execution of actions that could increase energy consumption or compromise safety. The controller dynamically adjusts operational decisions to maintain stable vehicle performance while minimizing battery usage. During attack periods, repeated or malicious commands often result in excessive actuator activity and increased power consumption. By identifying and suppressing such commands, the EMS reduces energy waste and improves battery efficiency. The predictive capability of MPC enables proactive decision-making, allowing the system to anticipate future operating conditions and implement corrective actions before severe performance degradation occurs. This approach enhances both cyber resilience and energy optimization in connected electric vehicles.

D) Simulation, Data Collection, and Performance Analysis:

The proposed framework is implemented as a simulation-based environment to evaluate cyber-physical security and energy management performance. Vehicles are represented as moving entities on a virtual roadway and operate according to commands received from the ECU. Throughout the simulation, sensor readings, vehicle velocity, command execution logs, and battery energy consumption values are continuously recorded. Both normal operational scenarios and cyber-attack scenarios are executed to generate comprehensive datasets for analysis.

The attack detection mechanism monitors vehicle velocity patterns and identifies abnormal behavior caused by malicious commands. Detected attack events are displayed within the simulation interface, allowing observation of system responses during intrusion attempts. After completing simulation runs, energy consumption data are visualized using time-based performance graphs. The x-axis represents simulation time, while the y-axis represents vehicle energy consumption. Comparative analysis is performed between normal operating conditions and attack conditions. The resulting performance metrics provide insights into battery utilization, attack impact severity, and system resilience. A reduction in energy consumption after attack mitigation demonstrates the effectiveness of the proposed EMS and MPC framework. The collected data are further analyzed to evaluate detection accuracy, operational stability, and energy-saving capabilities, providing a comprehensive assessment of cyber-physical security performance in connected and automated electric vehicles.

IV. Experimental Results

The proposed cyber-physical security assessment framework was evaluated using a simulation environment that models the operation of Connected and Automated Electric Vehicles (CAEVs) under normal and attack conditions. During simulation, vehicles moved continuously on a virtual roadway based on commands received from the Electronic Control Unit (ECU). The system monitored vehicle velocity, control commands, and energy consumption in real time. Under normal operating conditions, vehicles maintained stable movement patterns and consumed energy at an expected rate. The Energy Management System (EMS) recorded sensor information and continuously analyzed vehicle behavior to establish baseline operational characteristics.

To assess system resilience, Denial-of-Service (DoS) and replay attack scenarios were introduced into the communication network. These attacks generated abnormal commands that caused sudden variations in vehicle velocity. The proposed detection mechanism successfully identified suspicious behavior by comparing current velocity values with previously observed patterns. Whenever abnormal velocity changes persisted beyond the predefined threshold, the corresponding commands were classified as malicious and prevented from influencing vehicle operation.

The energy consumption analysis demonstrated a clear difference between normal and attack scenarios. The graphical results showed that attack conditions significantly increased energy usage due to repeated and unnecessary command execution. After activating the MPC-based EMS, malicious commands were effectively filtered, reducing excessive battery consumption. The green energy consumption curve representing protected operation remained considerably lower than the red attack curve, indicating improved energy efficiency, enhanced vehicle stability, and stronger cyber-physical resilience.

Table.1 Comparative Analysis of Vehicle Performance Under Normal and Cyber-Attack Conditions

Performance Metric	Normal Scenario	Attack Scenario
Vehicle Stability	High	Low
Abnormal Commands	Not Detected	Detected
Velocity Variation	Low	High
Energy Consumption	Low	High
Resource Utilization	Normal	Excessive
Battery Efficiency	High	Reduced
System Resilience	High	Moderate
Travel Time Performance	Improved	Degraded

Table 1 compares vehicle performance under normal and cyber-attack conditions, demonstrating that the proposed MPC-based EMS reduces energy consumption and improves stability.

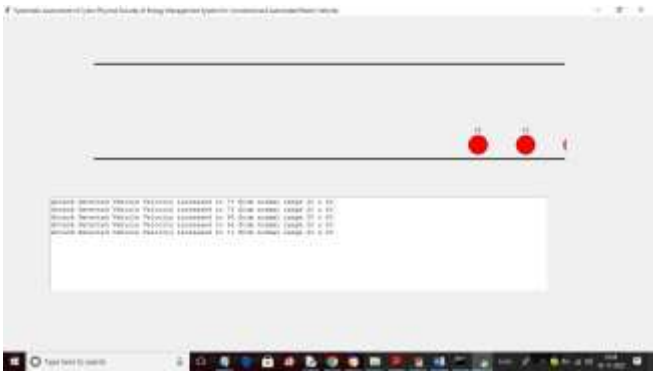

Fig.2 Real-Time Cyber-Attack Detection and Vehicle Simulation

Fig. 2 shows automated vehicle simulation with real-time attack detection, identifying abnormal velocity variations that impact energy consumption.

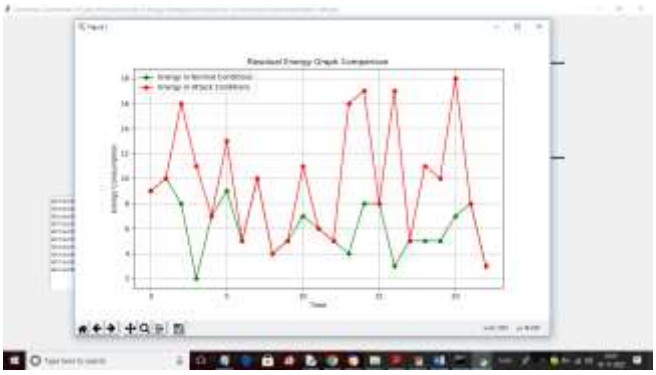

Fig.3 Residual Energy Graph Comparison

Fig. 3 compares energy consumption over time, demonstrating how mitigating DoS and replay attacks reduces vehicle energy consumption from the red malicious peaks to the green normal baseline.

V. Conclusion

This work presented a systematic cyber-physical security assessment framework for Connected and Automated Electric Vehicles (CAEVs) with a focus on Energy Management Systems (EMS). The study investigated how cyber-attacks targeting sensors, communication channels, and Electronic Control Units (ECUs) can influence vehicle performance, operational stability, and battery energy consumption. A simulation environment was developed to model normal and attack scenarios, including Denial-of-Service (DoS) and replay attacks, enabling detailed analysis of their impact on vehicle behavior. An Energy Management System based on Model Predictive Control (MPC) was implemented to monitor vehicle dynamics and identify abnormal operating conditions through velocity-based anomaly detection. The experimental results demonstrated that malicious commands can significantly increase energy consumption, create unstable vehicle responses, and reduce overall system efficiency. By detecting and filtering suspicious commands, the MPC-based EMS effectively minimized unnecessary battery usage and improved operational reliability. The developed framework provides valuable insights into vulnerability identification, attack impact analysis, and energy-aware security management for modern electric vehicles. The results confirm that integrating cyber-physical security mechanisms with intelligent energy management can enhance vehicle resilience and maintain stable performance under adverse conditions. Future work can focus on implementing advanced machine learning-based attack detection techniques, real-time deployment in connected vehicle platforms, and evaluation of additional cyber-physical attack scenarios to further strengthen the security and efficiency of autonomous electric transportation systems.

VI. Future Work

Future research can extend the proposed framework by integrating real-time deployment in hardware-in-the-loop (HIL) and connected vehicle testbeds. Advanced machine learning techniques such as federated learning, reinforcement learning, and graph neural networks can be explored to improve adaptive cyber-attack detection in Energy Management Systems (EMS). Additionally, the incorporation of digital twin technology can enable continuous monitoring and predictive security analysis of CAEV systems under dynamic operating conditions. Future work may also focus on optimizing lightweight security algorithms for edge-based ECUs to ensure low-latency decision-making in resource-constrained automotive environments. Furthermore, large-scale validation using real vehicular datasets and smart transportation infrastructures will enhance the practical applicability, robustness, and scalability of the proposed cyber-physical security framework.

References

[1] Arachchige, K. G., Alkaabi, G., Murtaza, M., Haq, Q. E. U., Abualkishik, A. Z., & Lee, C. C. (2025). Threat landscape and integrated cybersecurity framework for v2v and autonomous electric vehicles. *World Electric Vehicle Journal*, *16*(8), 469.

[2] Shirvani, S., Baseri, Y., & Ghorbani, A. (2023). Evaluation framework for electric vehicle security risk assessment. *IEEE transactions on intelligent transportation systems*, *25*(1), 33-56.

[3] He, C., Xu, X., Jiang, H., Jiang, J., Liang, C., & Chen, T. (2025). A Review of Cyber-Physical Security for Intelligent Connected Vehicles. *Chinese Journal of Mechanical Engineering*, 100178.

[4] Naseri, F., Kazemi, Z., Larsen, P. G., Arefi, M. M., & Schaltz, E. (2023). Cyber-physical cloud battery management systems: Review of security aspects. *Batteries*, *9*(7), 382.

[5] Khalaf, M., Ayad, A., Tushar, M. H. K., Kassouf, M., & Kundur, D. (2024). A survey on cyber-physical security of active distribution networks in smart grids. *IEEe Access*, *12*, 29414-29444.

[6] Kaur, K., Kaddoum, G., & Zeadally, S. (2021). Blockchain-based cyber-physical security for electrical vehicle aided smart grid ecosystem. *IEEE transactions on intelligent transportation systems*, *22*(8), 5178-5189.

[7] Girdhar, M. (2025). *Advanced Cybersecurity Strategies for Cyber-Physical Systems: Case Studies in EV Charging Stations, Connected & Automated Vehicles, and Digital Substations* (Doctoral dissertation).

[8] Arévalo, P., Ochoa-Correa, D., & Villa-Ávila, E. (2024). A systematic review on the integration of artificial intelligence into energy management systems for electric vehicles: Recent advances and future perspectives. *World Electric Vehicle Journal*, *15*(8), 364.

[9] Ricciardi Celsi, L., & Valli, A. (2023). Applied control and artificial intelligence for energy management: An overview of trends in EV charging, cyber-physical security and predictive maintenance. *Energies*, *16*(12), 4678.

[10] Teimoori, Z., & Yassine, A. (2022). A review on intelligent energy management systems for future electric vehicle transportation. *Sustainability*, *14*(21), 14100.

[11] Murlidharan, S., Ravulakole, V., Karnati, J., & Malik, H. (2025). Battery management system: Threat modeling, vulnerability analysis, and cybersecurity strategy. *IEEE Access*.

[12] Sifakis, N., Armyras, K., & Kanellos, F. (2025). Real-time power management of plug-in electric vehicles and renewable energy sources in virtual prosumer networks with integrated physical and network security using blockchain. *Energies*, *18*(3), 613.

[13] Abreu, R., Branco, F., Reis, M. J., & Serôdio, C. (2025). Cybersecurity in connected and autonomous vehicles: A systematic review of automotive security. *IEEE Access*.

[14] Elma, O., Cali, U., & Kuzlu, M. (2022). An overview of bidirectional electric vehicles charging system as a Vehicle to Anything (V2X) under Cyber–Physical Power System (CPPS). *Energy Reports*, *8*, 25-32.

[15] Arsalan, A., Papari, B., Timilsina, L., Muriithi, G., Moghassemi, A., Rahman, S. I., ... & Edrington, C. S. (2024). Enhanced Real-Time ATM-Based MPC for Electric Vehicles With Cyber–Physical Security Aspect. *IEEE Transactions on Transportation Electrification*, *11*(1), 4698-4716.

[16] Guang, H., He, Y., Zheng, B., Gong, W., Shi, Y., Wu, H., ... & Karimi, H. R. (2025). Perspective: A Novel Resilient Cybersecurity Management System for Connected and Automated Vehicles. *Automotive Innovation*, *8*(2), 335-367.

[17] Khan, M. R., Haider, Z. M., Malik, F. H., Almasoudi, F. M., Alatawi, K. S. S., & Bhutta, M. S. (2024). A comprehensive review of microgrid energy management strategies considering electric vehicles, energy storage systems, and AI techniques. *Processes*, *12*(2), 270.

[18] Manias, D. M., Saber, A. M., Radaideh, M. I., Gaber, A. T., Maniatakos, M., Zeineldin, H., ... & El-Saadany, E. F. (2024). Trends in smart grid cyber-physical security: components, threats, and solutions. *IEEE Access*, *12*, 161329-161356.

[19] Nuruzzaman, M. (2025). IoT-enabled condition monitoring in power distribution systems: a review of scada-based automation, real-time data analytics, and cyber-physical security challenges. *Journal of Sustainable Development and Policy*.

[20] Rodríguez, M. Á. S., Higuera, J. B., Higuera, J. R. B., Montalvo, J. A. S., & Crespo, R. G. (2021). A systematic approach to analysis for assessing the security level of cyber-physical systems in the electricity sector. *Microprocessors and Microsystems*, *87*, 104352.

[21] Mazumder, S. K., Kulkarni, A., Sahoo, S., Blaabjerg, F., Mantooth, H. A., Balda, J. C., ... & De La Fuente, E. P. (2021). A review of current research trends in power-electronic innovations in cyber–physical systems. *IEEE Journal of Emerging and Selected Topics in Power Electronics*, *9*(5), 5146-5163.

[22] Minchala-Ávila, C., Arévalo, P., & Ochoa-Correa, D. (2025). A systematic review of model predictive control for robust and efficient energy management in electric vehicle integration and V2G applications. *Modelling*, *6*(1), 20.

[23] Girdhar, M., Hong, J., Lee, H., & Song, T. J. (2021). Hidden markov models-based anomaly correlations for the cyber-physical security of ev charging stations. *IEEE Transactions on Smart Grid*, *13*(5), 3903-3914.

[24] Olasehinde, D. O., Bamisile, O., Ejiyi, C. J., Zhang, G., Cai, D., Li, J., ... & Huang, Q. (2026). Cybersecurity in cyber-physical power systems: analyzing vulnerabilities, threats, and control structures. *Cluster Computing*, *29*(3), 133.

[25] Raeispour, M., Yan, S., Meegahapola, L., & Yu, X. (2026). Cyber-physical security of virtual power plants: A survey. *IEEE Open Journal of the Industrial Electronics Society*.