World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

Enhancing Cybersecurity in Onboard Charging Systems of Electric Vehicles: A MATLAB-based Approach

Joseph Nnaemeka Chukwunweike [1,*], Abiodun Anuoluwapo Agosa [2], Uchechukwu Joy Mba [3], Oluwatobiloba Okusi [4], Nana Osei Safo [5] and Ozah Onosetale [6]

[1] *Automation and Process Control Engineer, Gist Limited, Bristol, United Kingdom.*
[2] *Electrical Engineer, University of South Wales, United Kingdom.*
[3] *Maritime Security Expert, Vega Solutions LLC, USA.*
[4] *IT & Cyber Security Analyst, Bristol Waste Company, Bristol, United Kingdom.*
[5] *Data Analyst, Emporia State University, United States.*
[6] *Electrical Engr. And Business Development/Relationship and Strategy Expert. LEE Engineering and Construction Company Limited, Lagos, Nigeria.*

World Journal of Advanced Research and Reviews, 2024, 23(01), 2661–2681

Publication history: Received on 13 June 2024; revised on 24 July 2024; accepted on 26 July 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.23.1.2259

Abstract

This research provides a comprehensive analysis of the impacts of various data integrity attacks on the power electronic hardware of electric vehicle (EV) chargers. The study aims to offer essential recommendations for defending against cyberattacks on electric vehicles and their onboard charging (OBC) systems. Adverse scenarios resulting from such cyberattacks are meticulously examined, and the system is simulated in MATLAB/Simulink to validate fault occurrences under different data integrity attacks. The quantitative analysis of the results clearly indicates that by incorporating adequate precautionary measures, such as integrating intelligent controls into the main controller during the design of the charging architecture, it is possible to significantly mitigate electrical hazards and prevent the degradation of component health, even in the event of a malicious cyberattack.

Keywords: Alternative current; Direct current; Diode bridge rectifier; Power factor; Controller; Charging efficiency; Volt-amperes; MATLAB.

1. Introduction

1.1. Background and Motivation

As the adoption of electric vehicles (EVs) accelerates globally, ensuring the security and integrity of their onboard charging systems becomes paramount. These systems are critical for powering EVs, and any vulnerabilities could have severe consequences. Cybersecurity in EV charging systems is essential for several reasons. Firstly, the increasing connectivity and complexity of these systems render them susceptible to cyber-attacks, which can compromise the safety and functionality of the vehicle. Secondly, ensuring the integrity of the charging process is vital for maintaining consumer trust and promoting the widespread adoption of EVs. Thirdly, the potential impact of a successful cyber-attack extends beyond individual vehicles, posing risks to the broader electric grid and public safety.

Data integrity attacks, in particular, present significant threats to EV charging systems. These attacks involve unauthorized manipulation or alteration of data within the system, leading to potentially catastrophic outcomes. For example, attackers could interfere with the charger controller logic, sending false signals that result in incorrect

* Corresponding author: Joseph chukwunweike

charging rates or even damage to the battery Khalid A et al (2019). Additionally, tampering with the battery management system (BMS) could cause improper battery cell balancing, reducing the battery's lifespan and posing serious safety hazards (Hamdare S et al. 2023).

One of the primary concerns is the controller area network (CAN) bus, which facilitates communication between various electronic control units (ECUs) within the vehicle. If compromised, an attacker could potentially send false signals to the charging controller, leading to unsafe charging conditions (Zhang & Zhang, 2022). Furthermore, advanced onboard charging systems equipped with sophisticated communication interfaces and control systems facilitate bidirectional communication with the charging infrastructure. These interfaces, if attacked, could disrupt the negotiation of charging parameters such as voltage and current, leading to suboptimal or unsafe charging performance (Li & Yu, 2021).

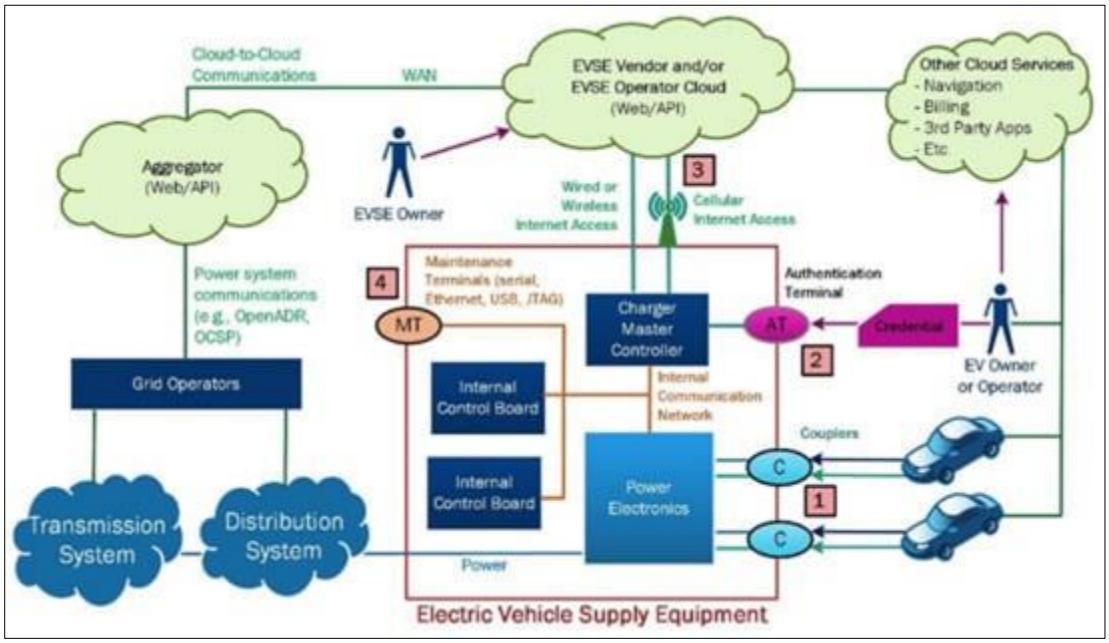

Figure 1 Theoretical design of a cyber-attack targeting an Electric Vehicle's On-Board Charger (OBC).

To mitigate these risks, it is crucial to integrate robust cybersecurity measures into the design and operation of EV charging systems. This includes implementing intelligent control mechanisms, secure communication protocols, and real-time monitoring systems to detect and respond to potential threats (Figure 1). By enhancing the security posture of these systems, we can ensure the integrity, reliability, and safety of the charging process, thereby instilling confidence in consumers and promoting the widespread adoption of EVs as a sustainable mode of transportation. In conclusion, cybersecurity in EV charging systems is not merely a technical challenge but a critical aspect of ensuring the safe and reliable operation of electric vehicles. As the adoption of EVs continues to grow, addressing the cybersecurity threats to their onboard charging systems will be essential for sustaining this growth and protecting both individual users and the broader power infrastructure.

1.2. Specific Challenges Addressed in the Research

The research addresses several specific challenges related to cybersecurity in onboard charging systems for electric vehicles (EVs). One major challenge is preventing unauthorized access to charging systems, which can protect against tampering with charging parameters and the injection of malicious code into control systems (Mbamalu IF et al., 2024). Another critical issue is safeguarding sensitive data transmitted between EVs and charging stations, such as user credentials and vehicle telemetry, through encryption and robust authentication protocols. Additionally, the research explores the need for standardized cybersecurity practices and guidelines developed by organizations like SAE and ISO. Challenges also include detecting anomalies and potential cyber-attacks using machine learning algorithms and hardware-based security measures, such as secure microcontrollers (Jones & Lee, 2024). Lastly, the study focuses on enhancing the resilience of charging infrastructure by deploying intrusion detection systems and real-time anomaly detection to ensure reliable and secure operations.

1.3. Objectives and Scope

- **Assess existing cybersecurity vulnerabilities** in onboard charging systems for electric vehicles (EVs).
- **Design and simulate a robust EV charging system** using MATLAB/Simulink software.
- **Implement effective cybersecurity measures** to mitigate identified threats.
- **Conduct comprehensive testing and validation** of the implemented cybersecurity solutions to ensure effectiveness and reliability.
- **Develop documentation and guidelines** for stakeholders, including EV manufacturers and charging infrastructure providers.
- **Boundaries Focus** is limited to onboard charging systems; broader EV or grid cybersecurity issues are not included.

2. Literature review

2.1. Overview of Cybersecurity Concerns in the Automotive Sector

Ensuring cybersecurity in the automotive sector requires developing standardized protocols that ensure security and interoperability across various technologies (Schmittner et al., 2019). However, existing standards often overlook the unique characteristics of electric vehicles (EVs) (Scalas et al., 2019). While some research has provided technical evaluations of the EV ecosystem, many studies, such as those by Bahrami (2020), fail to address critical security concerns. Specific components, like the Battery Management System (BMS), have been investigated by Khalid et al. (2019), but broader implications for EV components are often ignored. Recent studies highlight vulnerabilities in charging systems and protocols, including wired EV charging setups (Gottumukkala et al., 2020) and charging session negotiations (Antoun et al., 2020). Additionally, the Internet of Electric Vehicles introduces new security risks, with Ben Othmane L et al. (2020) focusing on communication networks and (Botsford C et al. (2020) analysing protocol vulnerabilities within the Vehicle-to-Grid framework. Despite these efforts, many systems lack dynamic real-time response capabilities to effectively address cyber threats.

2.2. Types of Data Integrity Attacks and Their Impact on Systems

Data integrity attacks pose significant threats to onboard charging systems for electric vehicles (EVs), jeopardizing the reliability and safety of these systems. Common types of data integrity attacks include data tampering, man-in-the-middle attacks, and spoofing.

- **Data Tampering**: This attack involves unauthorized modifications to the data exchanged between the EV and the charging station. Attackers may alter charging parameters, such as voltage and current levels, leading to incorrect charging rates or damage to the vehicle's battery (Brenna et al., 2020). Such tampering can result in battery degradation, increased wear, and potentially hazardous conditions (Acar et al., 2024).
- **Man-in-the-Middle (MitM) Attacks**: In this scenario, an attacker intercepts and potentially alters the communication between the EV and the charging station. This type of attack can lead to unauthorized data access and manipulation, impacting the charging process and causing data breaches involving sensitive user information (Chandwani et al., 2020).
- Spoofing: Spoofing attacks involve masquerading as a legitimate component of the charging system. Attackers may create fake charging stations or inject malicious code to deceive the vehicle's onboard systems. This can lead to incorrect charging behaviours or system malfunctions (W. Zeng and M. Y. Chow, 2012).

These attacks can compromise system performance, reduce battery lifespan, and pose safety risks. Robust cybersecurity measures and adherence to industry standards are essential to mitigate these threats and ensure the integrity of the charging infrastructure (M. Duvall, 2010).

2.3. Detailed Description of EV Onboard Charging Systems and Their Components

Electric vehicle (EV) onboard charging systems are critical for converting alternating current (AC) from the grid into direct current (DC) suitable for battery storage. These systems generally include several key components:

- **Onboard Charger**: Converts AC power from the grid to DC power for the battery. The onboard charger is integral to managing charging efficiency and compatibility (White et al., 2011).

- **Charging Port**: Interfaces between the EV and the charging infrastructure. Standardized connectors, such as the J1772 for Level 1 and Level 2, and CCS for Level 3, ensure proper connection and communication (De-Sousa et al., 2010; Morrowa et al., 2008).

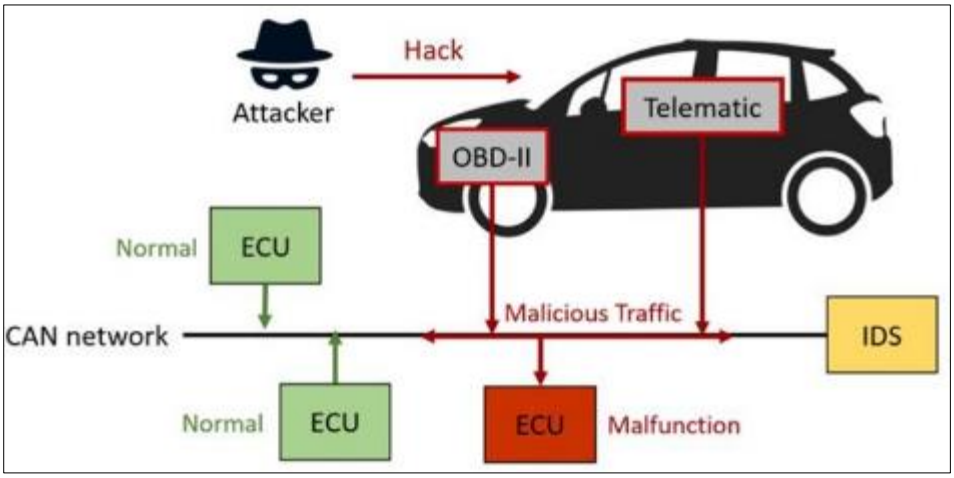

Figure 2 CAN bus-attack of automotive modules

- **Battery Management System (BMS)**: Monitors battery health, regulates charging rates, and ensures safety during the charging process (Acharya S et al., 2011).
- **Controller Area Network (CAN) Bus**: Facilitates communication between various electronic control units (ECUs) in the vehicle, including those responsible for the charging system (Acharya S et al., 2012).

2.4. Previous Studies on the Vulnerabilities of These Systems

Previous research has highlighted several vulnerabilities in onboard charging systems:

- **Data Integrity Attacks**: Studies have shown that attacks targeting data integrity can lead to incorrect charging rates or battery damage. For instance, machine learning algorithms have been proposed to detect anomalies in the charging process as a response to such threats (Mbamalu IF et al., 2024).
- **Hardware Vulnerabilities**: Research by Jones and Lee (2024) emphasizes the importance of hardware-based security measures, such as secure microcontrollers, to prevent firmware tampering and unauthorized access.

- **Cybersecurity Challenges**: Vulnerabilities in communication interfaces and control systems can be exploited, potentially compromising the vehicle's safety and the integrity of the charging process (Yilmaz et al., 2013; He et al., 202).

2.5. CAN Bus Security with Emphasis on Previous Studies on the Vulnerabilities of These Systems

The Controller Area Network (CAN) bus is critical in electric vehicles (EVs), facilitating communication among key components such as the powertrain control module and battery management system (Ning et al., 2019). Previous studies highlight severe vulnerabilities in CAN bus security, including unauthorized access and remote-control capabilities (Islam & Refat, 2020). Frequency-based intrusion detection systems have limitations in identifying complex attacks that alter data frame periodicity (Bi et al., 2022; Duan et al., 2021). The common attack phases involve interface identification, malicious node creation, and message injection (Hossain et al., 2020; Zhou et al., 2019). Effective countermeasures include encryption and establishing performance baselines (Ben Othmane et al., 2020; Hou et al., 2022). These studies underline the necessity for enhanced cybersecurity measures to protect the onboard charging systems of electric vehicles.

2.6. Electric vehicle (ev) charging methods and cybersecurity threats

Electric Vehicle (EV) charging systems can be categorized into three main types: conductive charging, inductive charging, and battery swapping systems. Each method has distinct characteristics and applications:

- 1. **Conductive Charging**:Conductive charging involves a direct connection between the charger and the vehicle's inlet (Habib et al., 2015). This method includes AC-DC power factor correction (PFC) converters and

DC-DC converters, making it highly effective and widely used in both off-board and on-board chargers (Khaligh & Dusmez, 2012). Charging levels range from Level 1 (AC, up to 1.92 kW) to Level 3 (DC, above 19.2 kW), catering to different power needs (Khaligh & Dusmez, 2012; Yilmaz & Krein, 2013). While convenient and reliable, the main drawback is the need for physical cable connections (Tashakor et al., 2017).

- 2. **Inductive Charging**: Inductive charging utilizes magnetic fields for contactless power transmission (Fahem et al., 2017). This method, supported by SAE recommendations, offers the benefit of no physical connectors but faces challenges like higher costs, lower efficiency, and complex manufacturing (Yilmaz & Krein, 2013). The technology, although advanced, suffers from issues related to magnetic coupling and power density.
- 3. **Battery Swapping Systems (BSS)**: Battery swapping allows for quick replacement of depleted batteries with fully charged ones (Habib et al., 2018). This method reduces charging time significantly and offers benefits such as extended battery life and lower management costs. Tesla's rapid battery replacement technology exemplifies this approach (Habib et al., 2018). However, challenges include the lack of standardization and potentially higher rental costs compared to traditional refuelling (Martínez-Lao et al., 2017).

2.7. Cybersecurity Threats to On-Board Chargers (OBC)

The cybersecurity threats to EV On-Board Chargers (OBCs) can be categorized into Four primary types:

- **Modification**: Unauthorized changes to charging parameters or firmware can disrupt the charging process or damage components.
- **Interception**: Interception threats compromise the confidentiality of information, enabling unauthorized access to sensitive data. Techniques such as wiretapping, keystroke logging, and fibre tapping pose risks to the On-Board Charger (OBC), potentially leading to overvoltage issues, loss of system synchronization, and control system failures (Ning J et al., 2019). Intercepting and tampering with communication between the vehicle and the charging station can lead to data breaches or incorrect charging rates.
- **Interruption**: Interruption involves actions that render a system non-functional, such as obstructing control signals or executing Denial-of-Service (DoS) attacks. These disruptions can lead to voltage and current spikes, affecting the OBC's functionality and feedback loop (Yang et al., 2019). Disruptions to the charging process can cause operational failures or safety hazards.
- **Interference attacks**: disrupt system performance by tampering with control or sensed data. Techniques include:
    - White Noise: Introducing high-frequency noise (over 1 kHz) causes irregular controller behaviour.
    - Combination of White Noise and Modification: Distorting waveforms and altering control parameters destabilize system performance (Richard L, Petit M., 2018). Understanding these threats is crucial for developing effective cybersecurity measures to protect EV charging infrastructure from potential attacks.

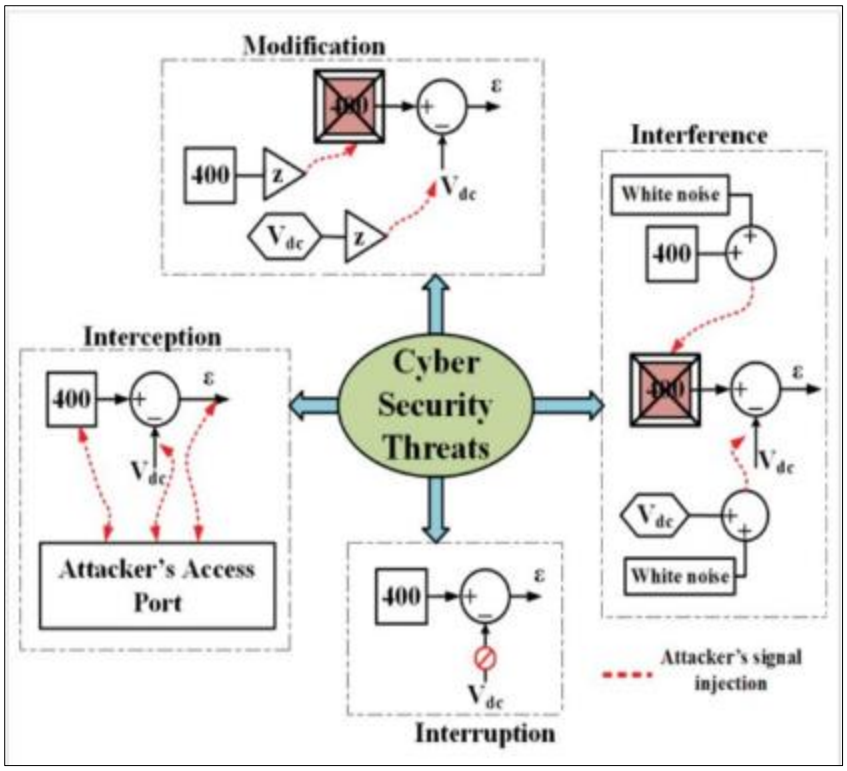

Figure 3 Categories of Cybersecurity Threats to EV On-Board Chargers (OBCs).

3. Methodology

3.1. System Design and Simulation Setup

The design of the onboard charging system (OBC) for electric vehicles (EVs) utilizes MATLAB/Simulink to create a detailed simulation model that replicates real-world charging processes. The primary goal is to develop a system capable of delivering 240V alternating current (AC) with power ratings up to 6KW to the vehicle's onboard charger.

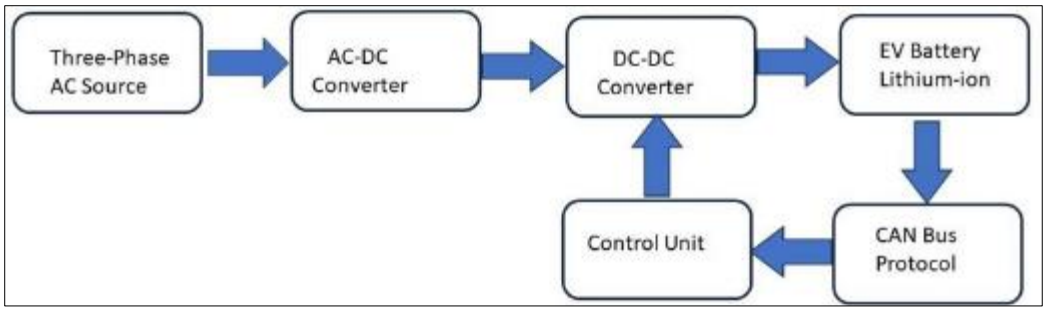

Figure 4 Diagram illustrating the proposed system's blocks.

3.1.1. Designing the Charging System Model

a. AC-DC Converter: Converts grid power (AC) into direct current (DC), necessary for charging the EV battery. The design incorporates a totem-pole boost converter, specifically an Interleaved Totem Pole Bridgeless Power Factor Correction (PFC) stage, as shown in Figure 5. This converter utilizes high-frequency MOSFET switches to efficiently convert AC mains voltage to regulated DC while ensuring a sine wave input current. The interleaved PFC circuits improve power factor by aligning input current with voltage, reduce current ripple, and enhance thermal performance by distributing the load across multiple circuits.

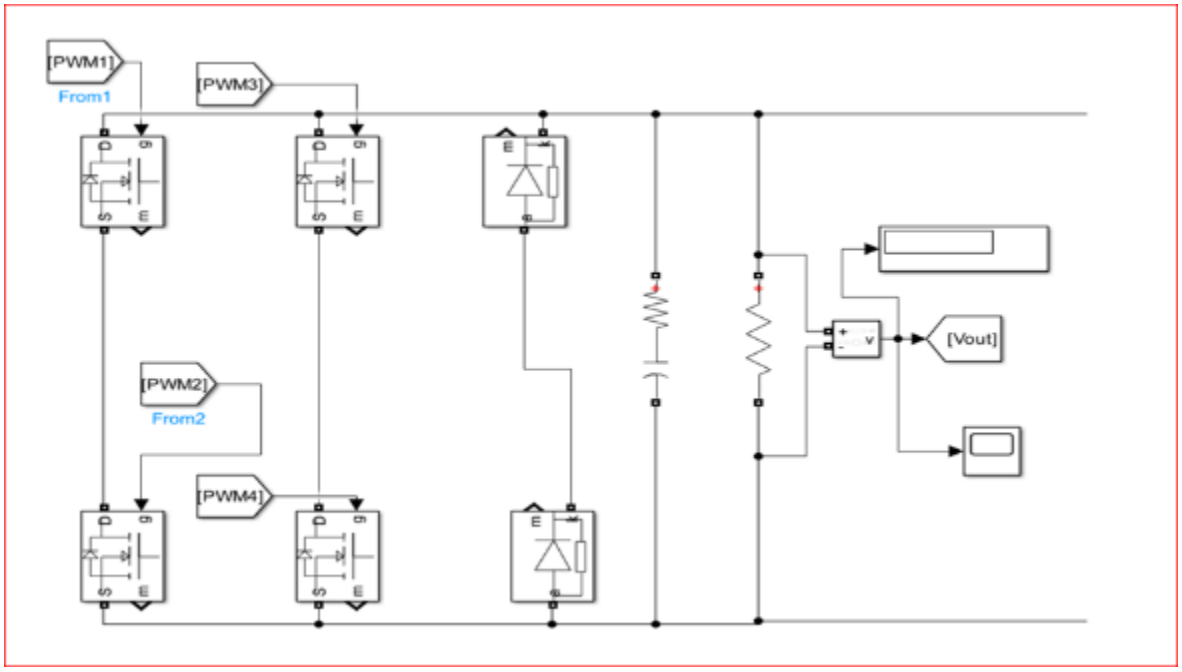

Figure 6 Block diagram of the AC-DC converter

b. DC-DC Converter: Adjusts the DC voltage to match the battery's requirements, ensuring efficient energy transfer.

$D = \frac{V_{out}}{V_{in}}$

Where:

(D) = is the duty ratio.

(V_ out) = is the output voltage of the converter. (V_ in) = is the input voltage of the converter.

In this design process the inductor, it is assumed that the buck converter operates continuously in conduction mode (CCM). A switching frequency of 10 kHz is selected for this purpose. Typically,

when working with CCM, the induction current ripple is taken to be approximately 10% of the output current (noted as $Iout$). Using Equation (3), the calculation for the required inductor value is determined.

$L = \frac{(Vd - V0)}{\Delta iL * fs}$ (3)

Where, fs = switching frequency in kHz and

ΔiL = inductor current ripple.

Equation (4) is used to calculate the capacitance value (C), which is essential in determining the output voltage ripple. Here, the output voltage ripple is set at a fixed 10%, ensuring a consistent 160V DC supply to the battery, which is recognized as the ideal charging voltage.

$\Delta V0 = \frac{Ts2\, V0}{8(LC1 - D)}$ (4)

The output capacitor value(C) is determined based on equation (5), considering the obtained output voltage ripple ($\Delta Vout$). (5)

$C = T^{s}2^{V0(1-D)}\,\Delta V08L$ (5)

c. Control Circuit: Manages the operation of the converters and monitors system performance to maintain safe and efficient charging.

d. Battery Model: Represents the vehicle's battery, simulating its response to varying charging conditions and states of charge. The battery management system (BMS) in the electric vehicle manages and safeguards the lithium-ion battery, which has a 160V nominal voltage and 20 Ah capacity, as shown in Figure 7. The BMS monitors essential parameters like state of charge, cell temperature, and voltages, protecting against overcharging, deep discharge, and overheating.

3.2. Components and Parameters

a AC Source: Provides the input voltage and current, typically set at 240V AC.

b AC-DC Converter: Includes parameters for power factor correction and efficiency.

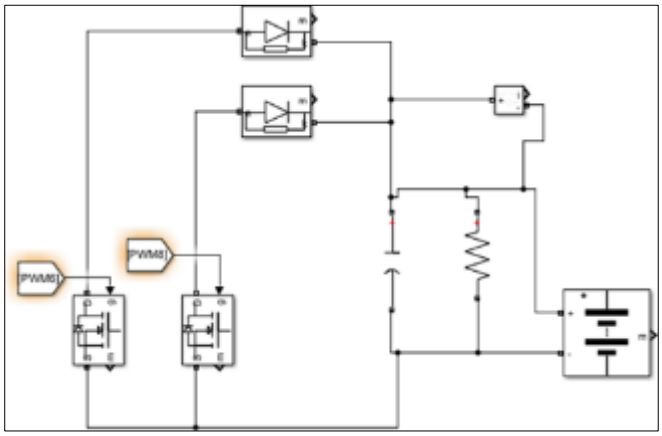

Figure 7 Block diagram of the DC-DC Converter

c DC-DC Converter: Configured with voltage regulation and control parameters.

d Control Circuit: Implements algorithms for pulse width modulation (PWM) and high-level communication (HLC) protocols, such as CAN, Qin H(2021). for advanced charging scenarios. The simulation setup involves integrating these components into a comprehensive model to analyse and optimize the charging system's performance under various conditions and potential cyberattack scenarios.

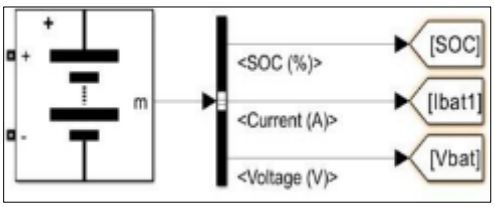

Figure 8 Block diagram of the Battery system

The control strategy for the battery charging system involves two key components: the interleaved boost PFC converter and the battery charging controller. **Figure 8** depicts the control circuit for the interleaved boost PFC converter. Here, the reference DC voltage (400V) is compared with the actual DC link voltage (Vout) to generate an error signal. This signal is processed by a PI controller to produce a peak reference current. This reference current, adjusted by the normalized sinusoidal input voltage (Vin), determines the reference input current. Errors are managed through current loop PI controllers and saturation blocks to generate duty cycle signals for each bridge.

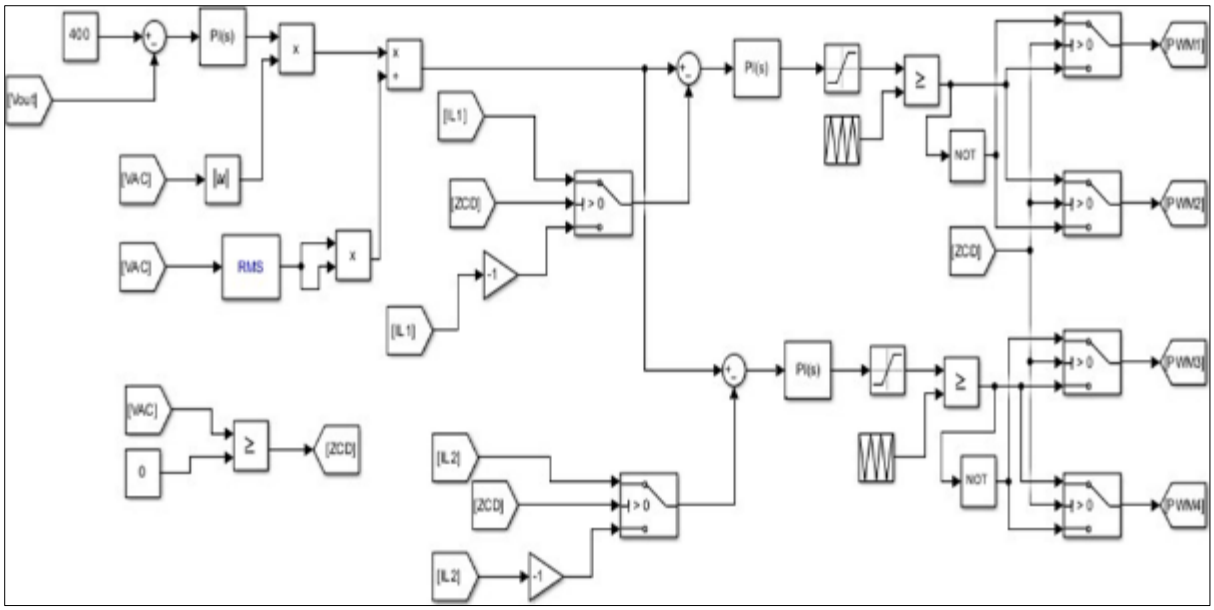

Figure 9 Control of Electric Vehicle Charging System

Figure 9 illustrates the control strategy for charging a lithium-ion battery using the constant current (CC) method. A PI controller generates a reference current (Iref) which is compared with the actual current (Iactual or Ibat). The error signal is minimized by the PI controller and then used to modulate the duty cycle of the converter via PWM. This ensures precise current regulation during the charging process. The next section will present simulation results, analysing the performance of the onboard charging system.

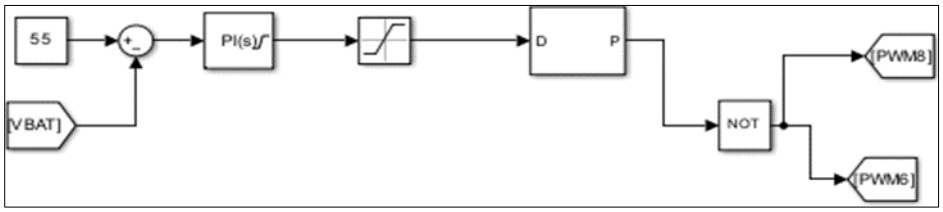

Figure 10 Block diagram of the Control system

The simulation was conducted using MATLAB/Simulink, focusing on the circuit depicted in Figure10.

Table 2 contains the design specifications for the EV charging system.

Table 2 Design Parameters

S/n	Parameters	Values
1	Input Voltage	240V, AC
2	Frequency	50Hz
3	Series RLC Branch	0.02 ohms, 300e-6H, 2500e-6F
4	AC-DC Converter	0.1 ohms Ron, 0.01 ohms Rd, 1e5 ohms Rs
5	Inductance 1 and 2	L1 300e-6H, L2 300e-6h
6	Resistor	40 ohms
7	Switching Frequency	10KHz

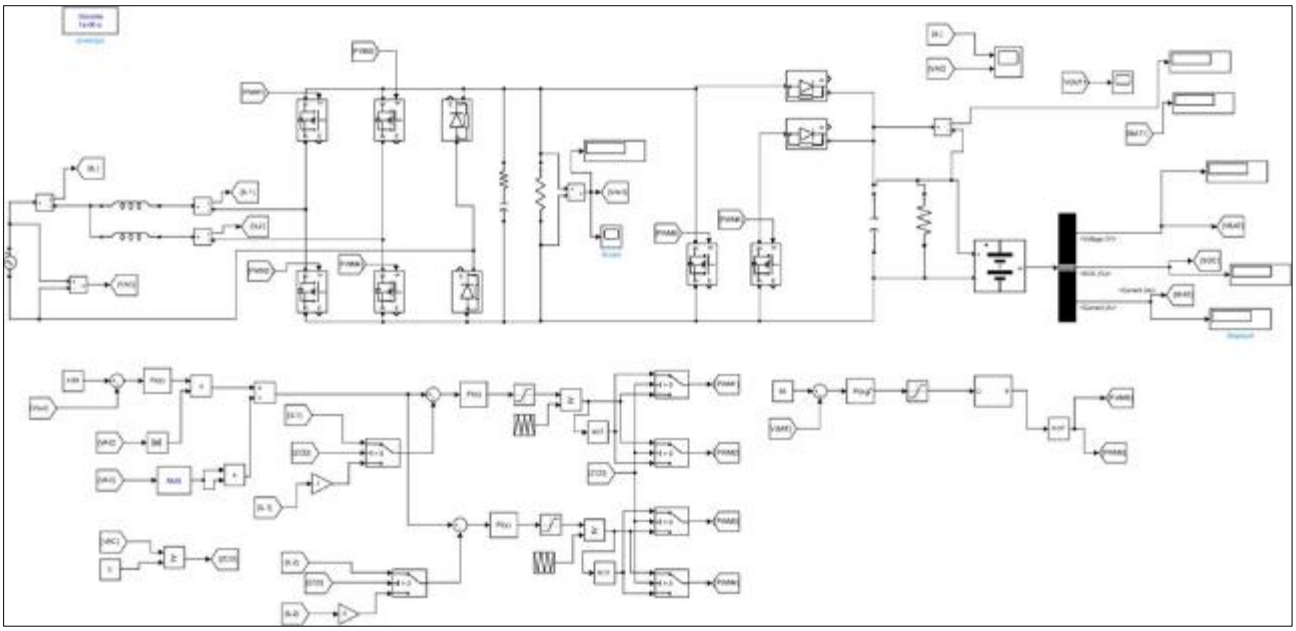

Figure 11 MATLAB/Simulink simulation of OBC circuit without Can Communication Bus

3.3. CAN Communication Protocol

The Controller Area Network (CAN) bus is integral to in-vehicle networking, linking the primary controller, Battery Management System (BMS), and other Electronic Control Units (ECUs). Known for its robustness and error resilience, CAN communication ensures efficient control signal transmission. It encompasses both hardware components and software elements, which include cybersecurity measures for CAN communications. Figure 12 illustrates the CAN bus's strategic connection with the system controller.

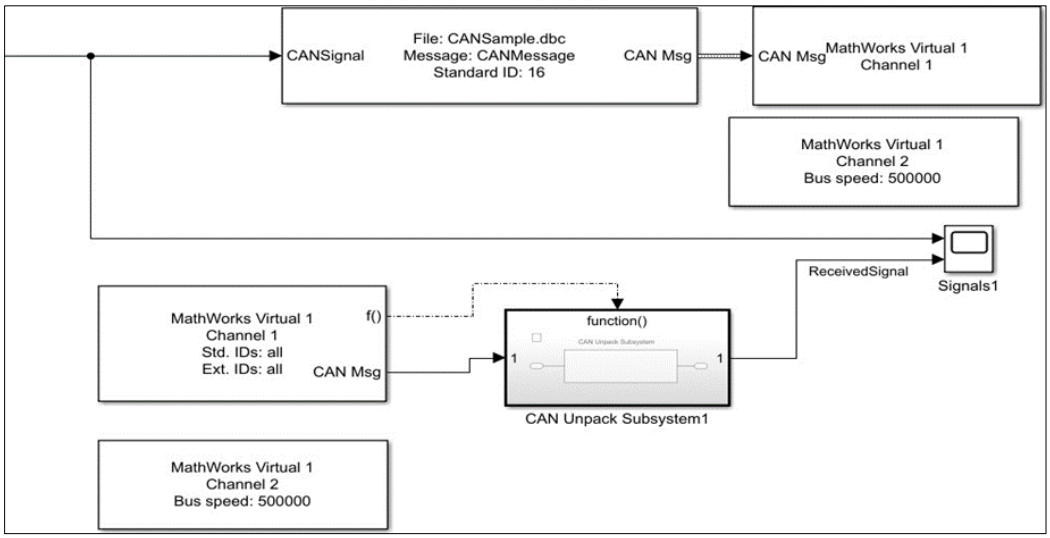

Figure 12 Can Communication Bus Protocol

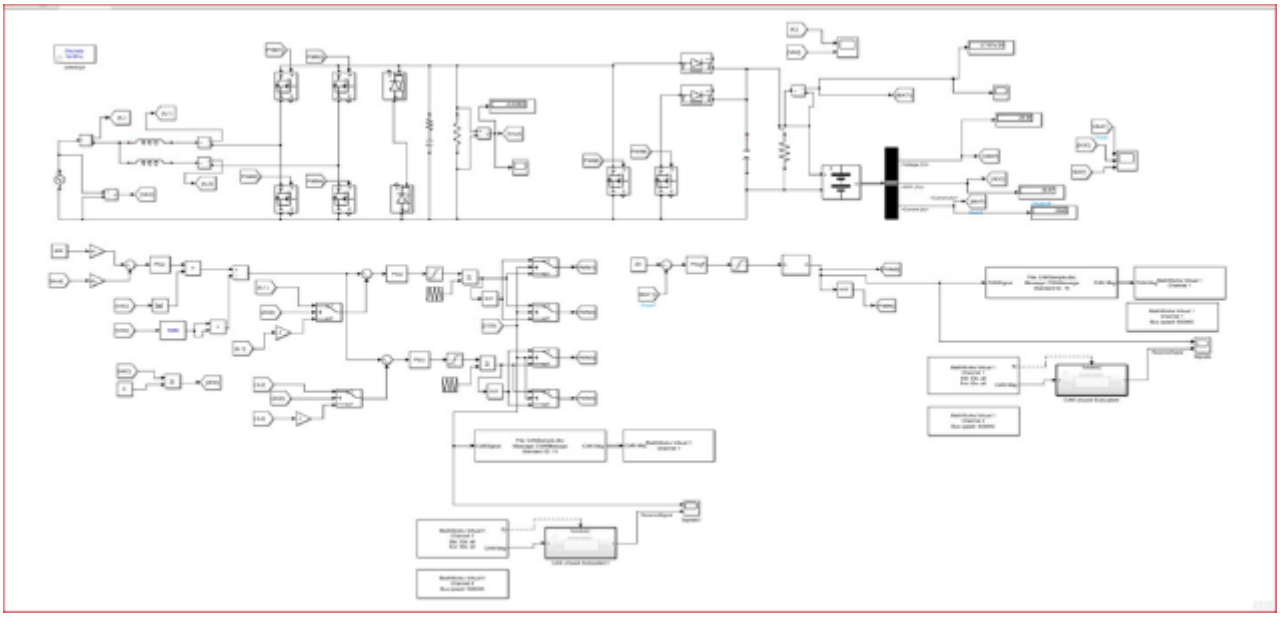

Figure 13 Simulation of Proposed system with Can Communication Bus

3.4. Modelling of Attacks on the Proposed System

In this section, a threat model is developed to identify potential security vulnerabilities within the On-Board Charger (OBC) system architecture. The model examines various cyber-attack scenarios such as firmware tampering, unauthorized access, and data breaches, aiming to impact system performance or cause damage to components. These attacks are typically executed by compromising either the physical or control layers of the Electric Vehicle Supply Equipment (EVSE).

3.5. Modification/Tampering Attacks

Modification attacks focus on the integrity of system information. In these scenarios, unauthorized parties' access and alter sensed data or control parameters, leading to degraded system performance. For example, an attacker might modify the settings of controllers or sensors, resulting in erroneous data readings or operational discrepancies that disrupt the normal functioning of the OBC system.

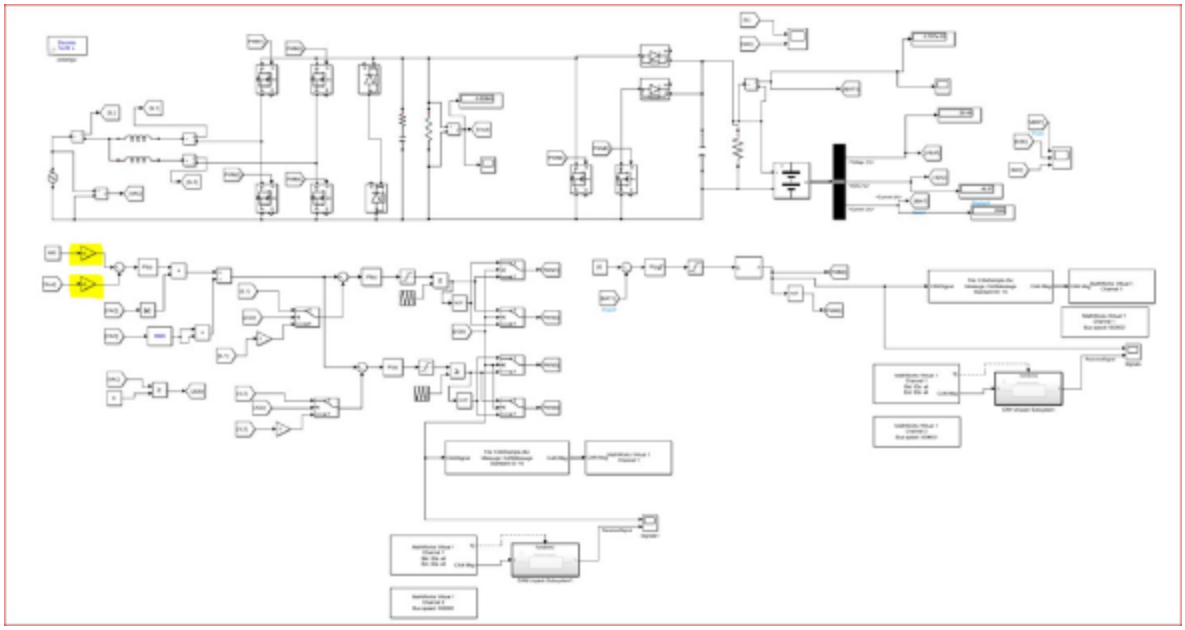

Figure 14 Simulation of the System by Tampering Attacks

3.6. Grid-Side Short Circuit Attacks

Figure 15 depicts a grid-side short circuit attack, where the same gate pulses are applied simultaneously to the high side MOSFETs. This causes both MOSFETs to turn on at the same time, leading to continuous charging of the PFC inductors with grid voltage. Consequently, the input current becomes out of phase with the grid voltage, disrupting the Power Factor Correction (PFC) action. This results in an increased input current amplitude, potentially exceeding device ratings and causing overcurrent conditions. Repeated occurrences of this issue can lead to permanent damage to semiconductor devices and other passive components in the circuit.

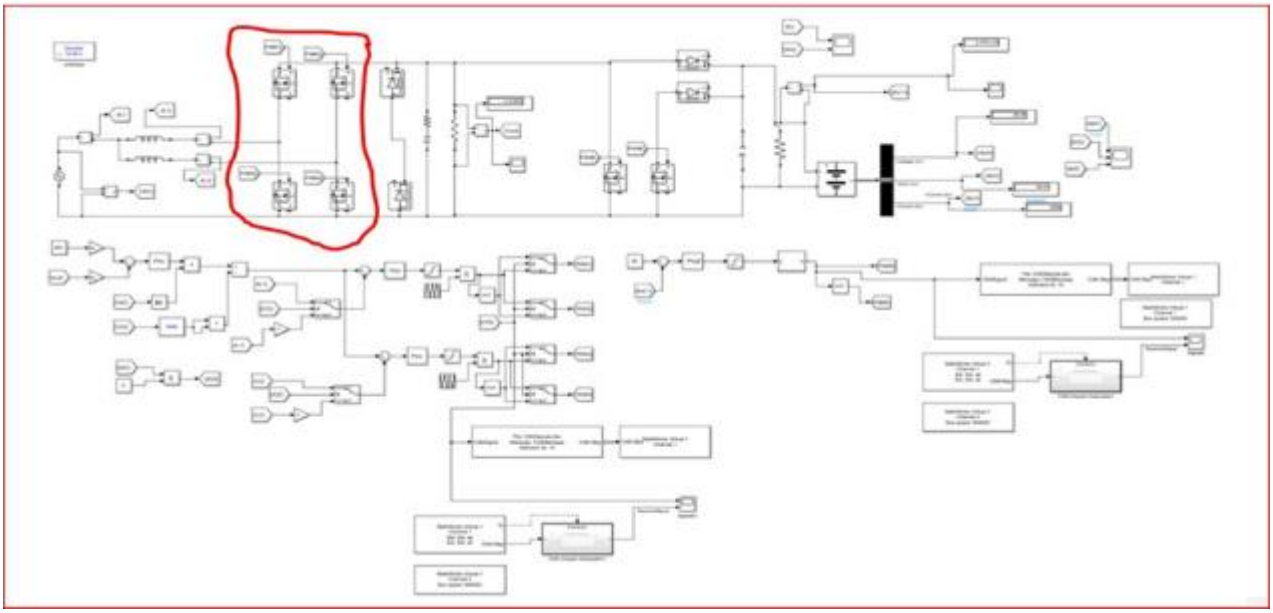

Figure 15 Simulation of the Proposed System Short Circuit Attacks**.**

3.7. Sudden Loss of Input

In the context of an electric vehicle (EV) charging system, a Sudden Loss of Input attack involves an abrupt and unexpected disruption or complete cessation of the power supply or input signals to the onboard charger (OBC). This scenario can simulate the sudden cut-off of power, potentially causing significant harm to the system's stability and operation. Such interruptions might lead to incomplete charging cycles, damage to the OBC components, or a loss of critical system data, impacting the overall performance and reliability of the EV charging system

3.8. Attacks Related to the Battery and the BMS

*3.8.1. Denial of Service (DoS)***

A Denial of Service (DoS) attack targets the Battery Management System (BMS) by overwhelming it with false messages, disrupting its ability to process legitimate data and manage energy distribution. This can block vital responses, such as temperature monitoring, potentially leading to overheating and damage to the battery. DoS attacks can also obstruct user access to battery status information, compromising operational safety.

3.8.2. Tampering Attack

Tampering attacks involve physical interference with the battery or BMS, potentially causing short circuits or fires. Such attacks may also degrade the BMS's interaction with the battery, reducing its efficiency. Countermeasures include anomaly detection systems to cut off power to tampered components and tamper-proof technologies to safeguard critical parts.

3.8.3. Spoofing, Replaying, and Man-in-the-Middle (MitM)

Spoofing and MitM attacks deceive the system by impersonating the BMS or tampering with communication data, potentially damaging the battery or disrupting energy flow. Attackers may alter current demands, causing overcharging or excessive discharge, thus shortening battery life. To counter these threats, strong identification protocols, source

authentication, and integrity protection for communications are essential. An intrusion detection system and redundant controllers can further protect against such attacks and ensure robust operation of the BMS and charging syste

4. Simulation results

4.1. Analysing the Electric Vehicle Charging Simulation

Figure 16 presents the simulation waveforms for the onboard charger (OBC) before any attacks are introduced. The input voltage is measured at 300.2V, while the current is maintained at 50A. The waveform shows that the current is sinusoidal and in phase with the voltage, indicating a stable and efficient charging process. This alignment is crucial for optimal performance and power factor correction in the OBC system.

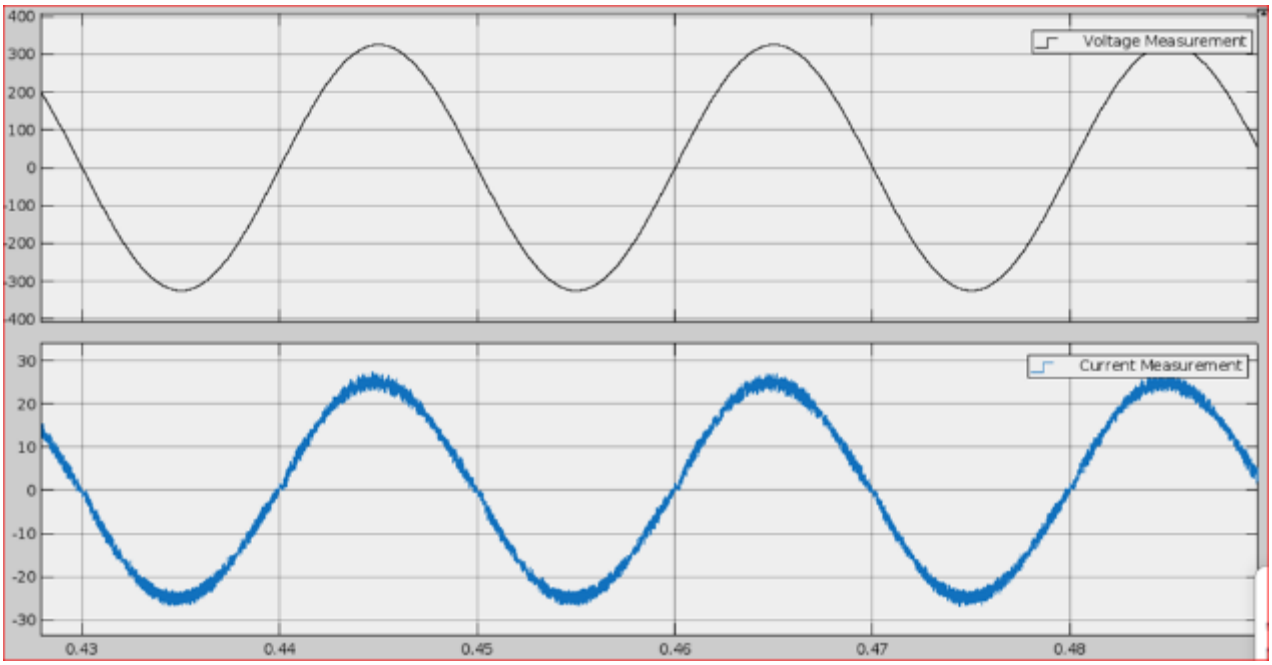

Figure 16 Input Voltage and Current Waveform of the Charging System Before Attacks

Figure 17: Display the wave form of the output voltage The output voltage measurement Simulation waveforms of the charging system without attacks are illustrated in Figure 17. It is worth mentioning that the output voltage is regulated and constant at the reference value of 400A.

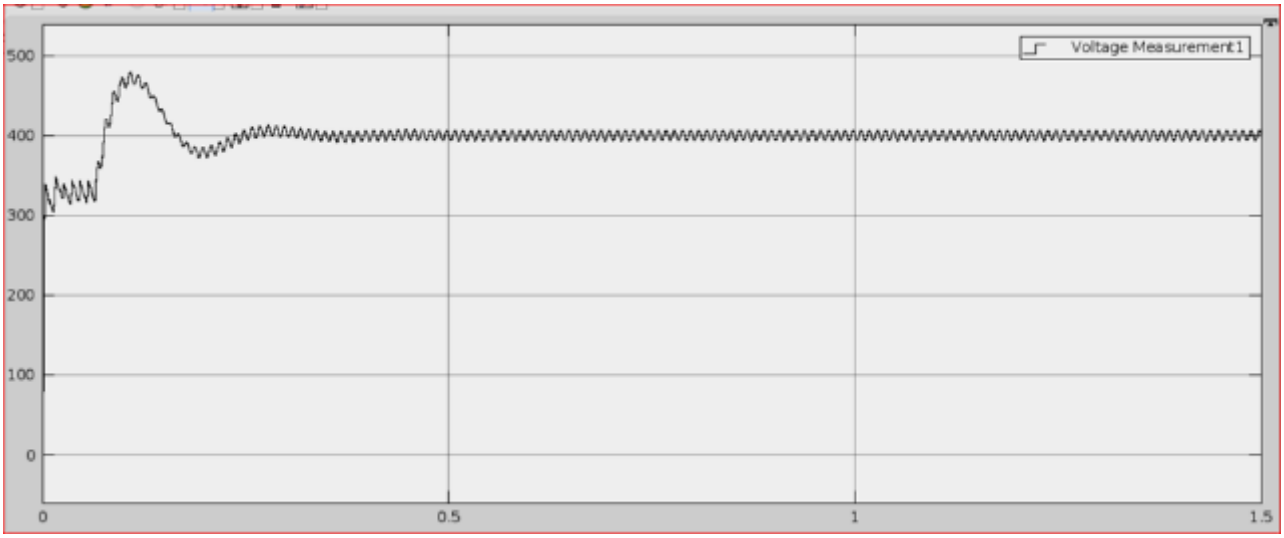

Figure 17 Output Voltage Waveform of The Charging System.

As shown in figure 18 the waveforms for the state of charge, charging voltage, and charging current in the Electric Vehicle (EV) charging system. It shows the charging cycle of the battery Notably, the state of charge was measured at 50.05%. Simultaneously, the charging current was recorded at-9.98A, and the battery voltage during the charging process was measured at 51.79V.

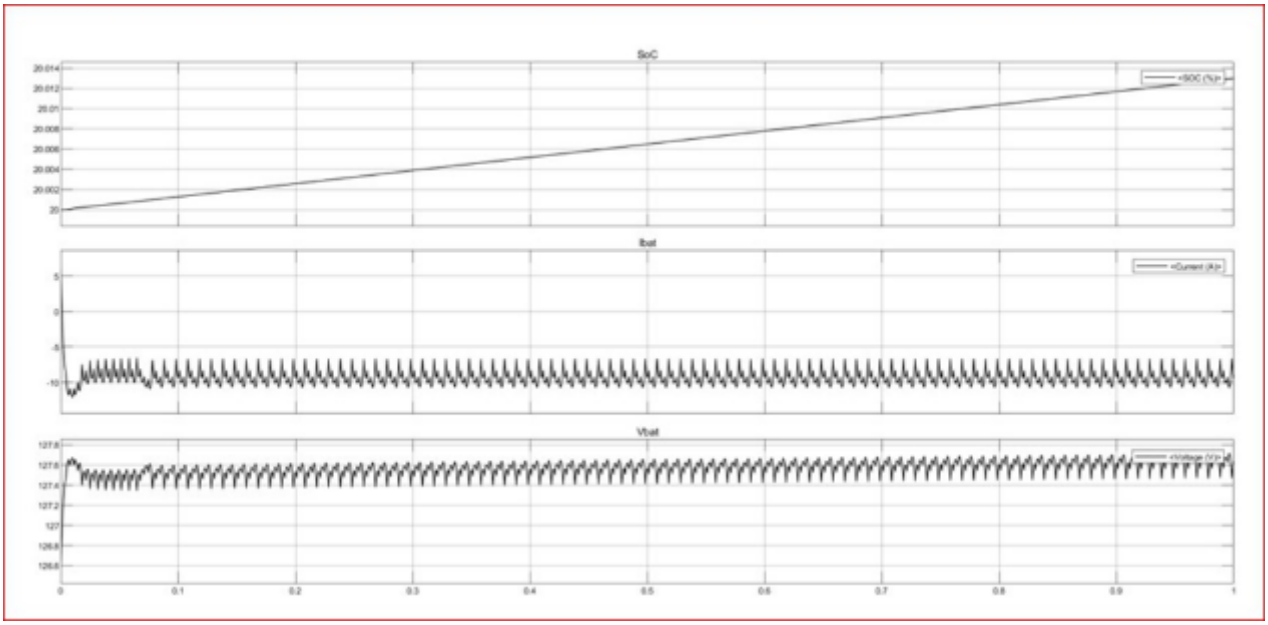

Figure 18 Battery charging voltage and current waveform.

The charging efficiency of the EV is shown below. The charging efficiency is the percentage of the ratio of the amount of energy stored in the battery during charging to the energy consumed from the charging source.

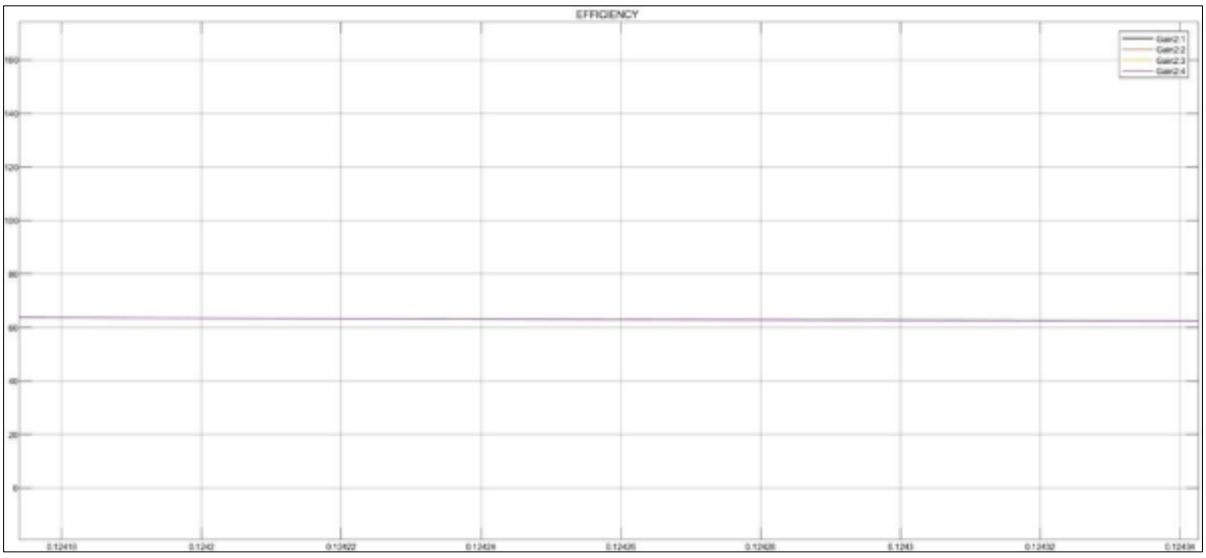

Figure 18a Charging Efficiency Waveform**.**

4.2. Attacks on the Grid Side

Figure 19 illustrates a scenario where an attacker manipulates the gate pulses, resulting in a short circuit on the grid side. At t = 1.5 seconds, this manipulation causes the grid current to surge from its normal 50A to 400A. Following this disturbance, the system fails to maintain its equilibrium, leading to unstable behaviour. Additionally, Figure 18 highlights a noticeable phase difference between the voltage and current before and after the attack, as observed in Figures 18a and 18b.

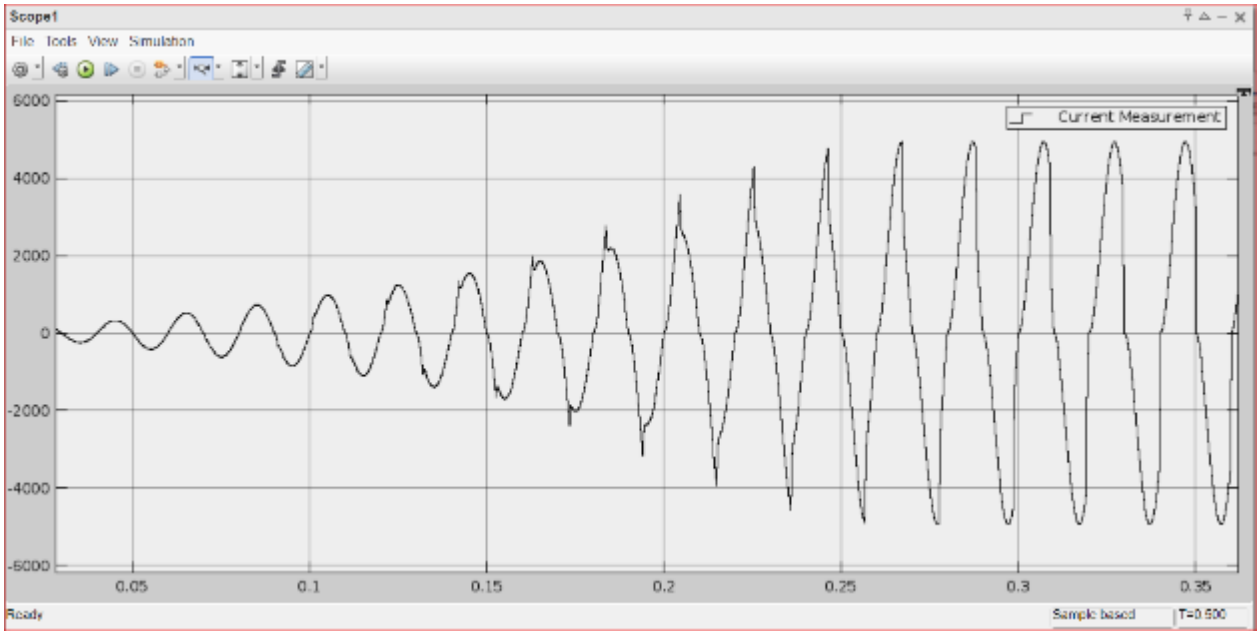

Figure 18b Current Waveform of The Charging System with Short Circuit Attacks

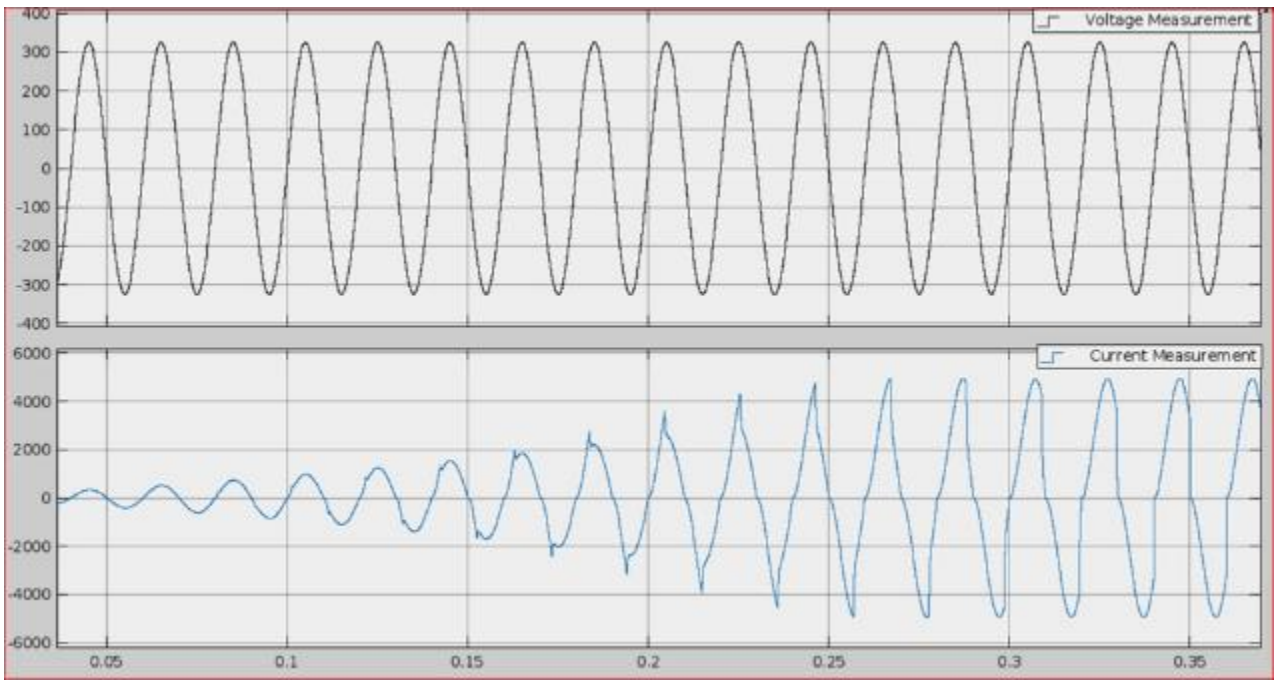

Figure 19a Input Voltage and Current Waveform of the Charging System with Attacks.

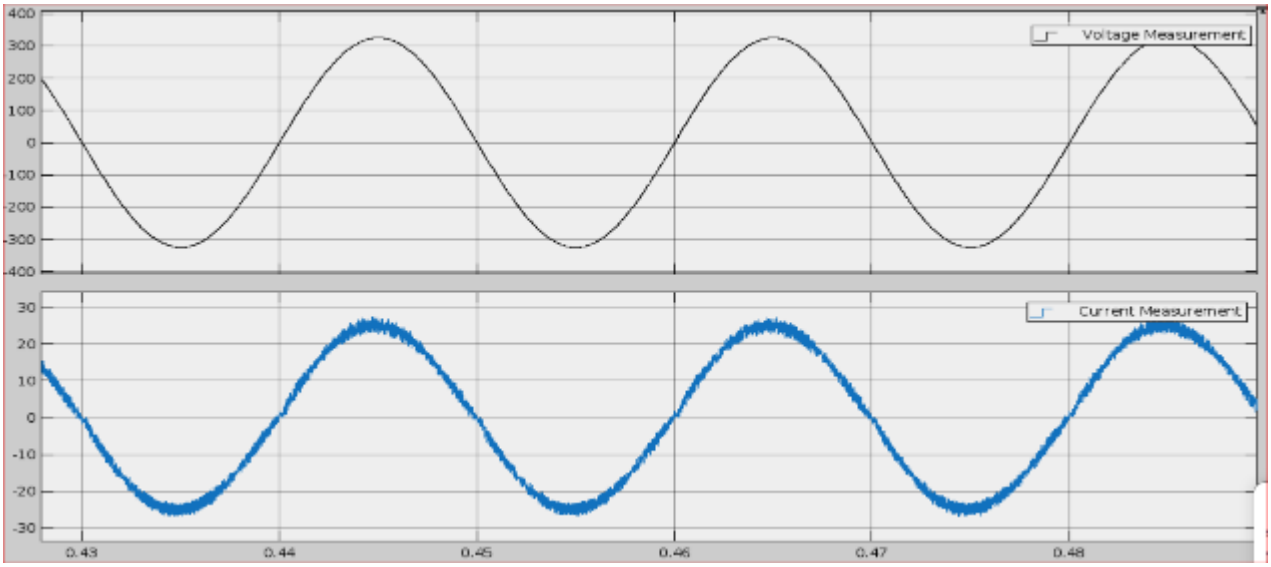

Figure 19b Input Voltage and Current Waveform of the Charging System Without the Attacks**.**

4.2.1. Attacks by tampering

tampering with the control parameters of the circuit by adding a higher gain factor to the control value(400v) decreasing the values of voltage from 300v to -200v, as depicted in Figure 19, typically results in a increase in the current measurement from 50A to 4000A. thus affecting the system performance, health and safety.

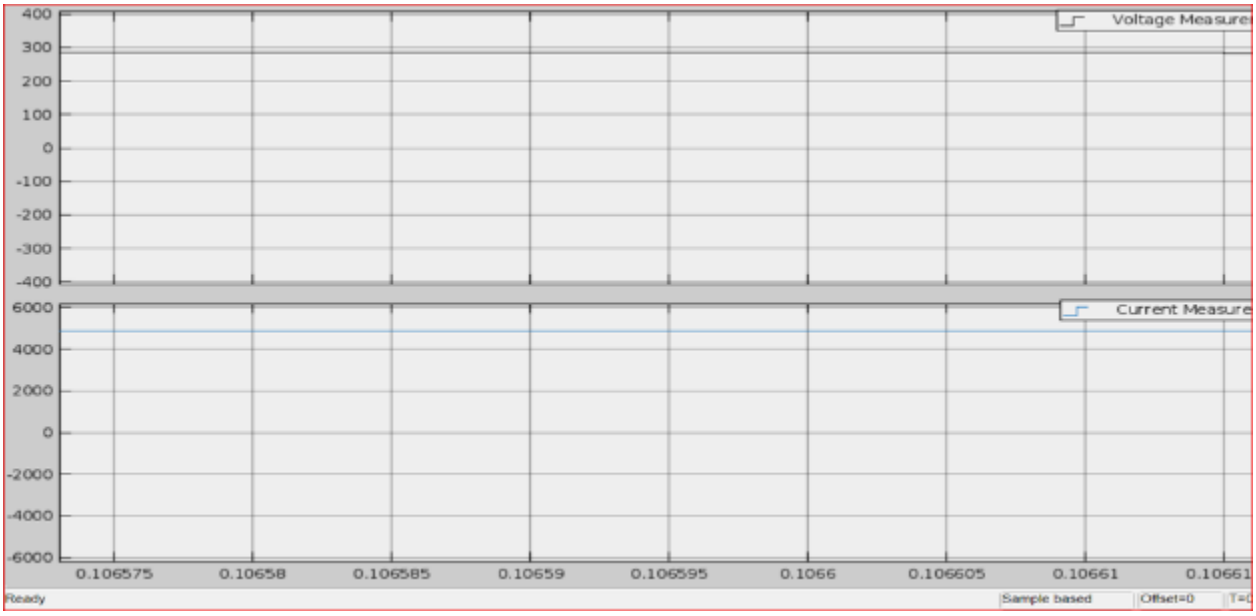

Figure 20 Input Voltage and Current with an Increase in Value

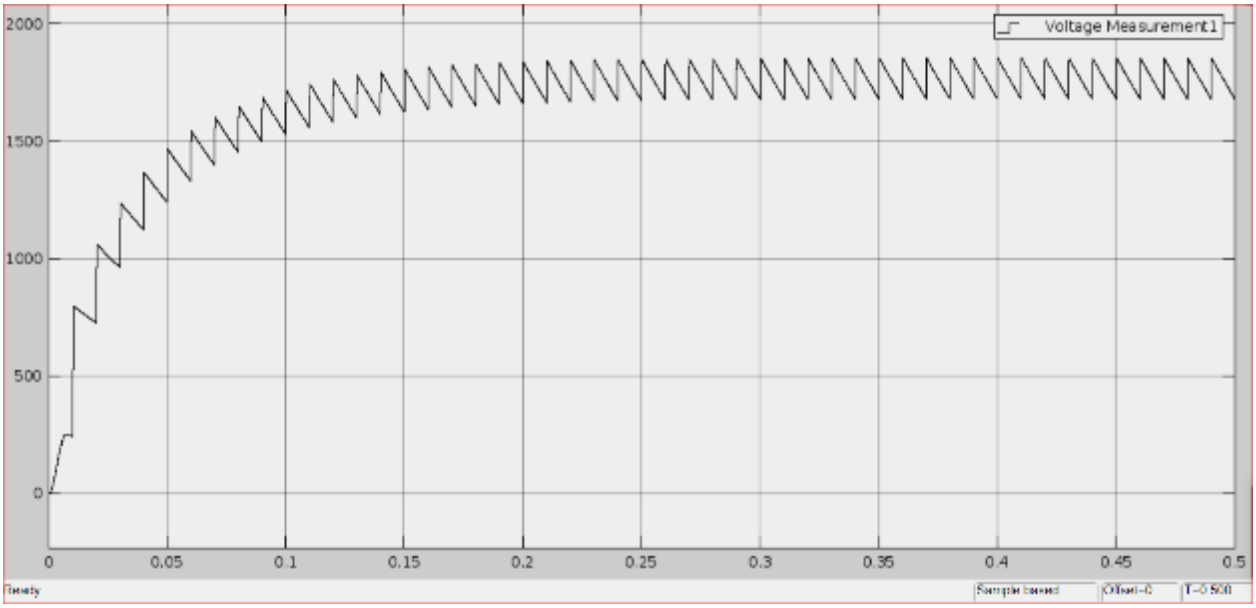

Figure 21 Output Voltage with an Increase in Value

4.2.2. Sudden Loss of Input Attacks

As observed in Figure 22 a and b, the input relay is opened suddenly by a malicious control signal for a period of 0.17 This causes a surge current across the input relay for 0.17 sec, leading to detrimental effects in the dielectric material of the relay.

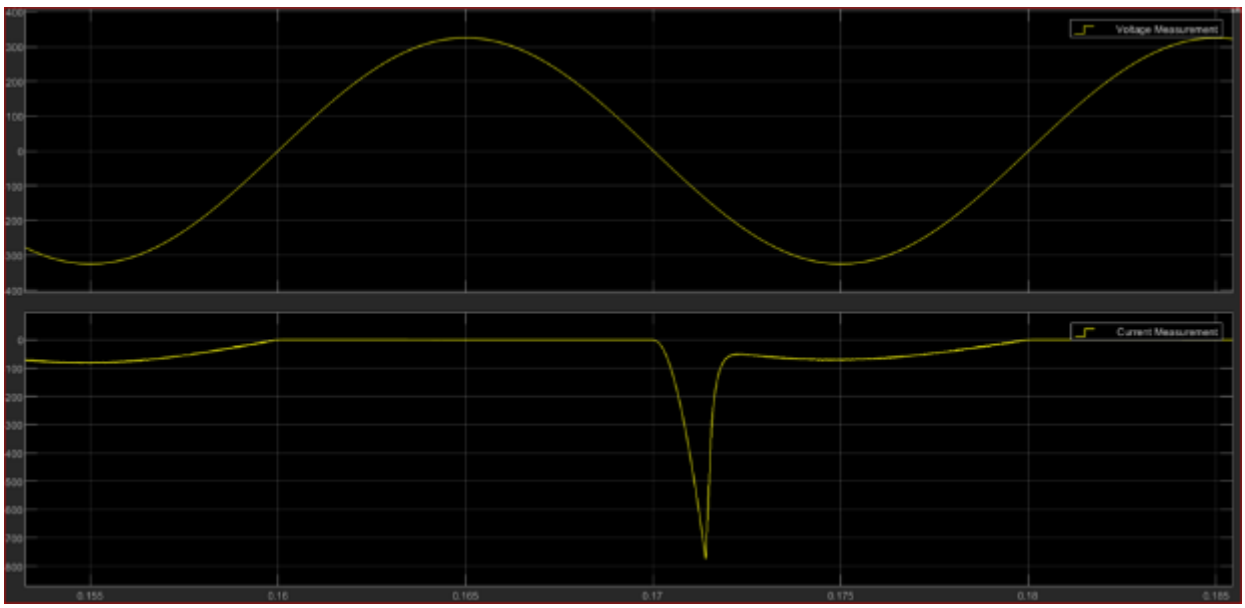

Figure 22a Sudden Loss of Input Attacks

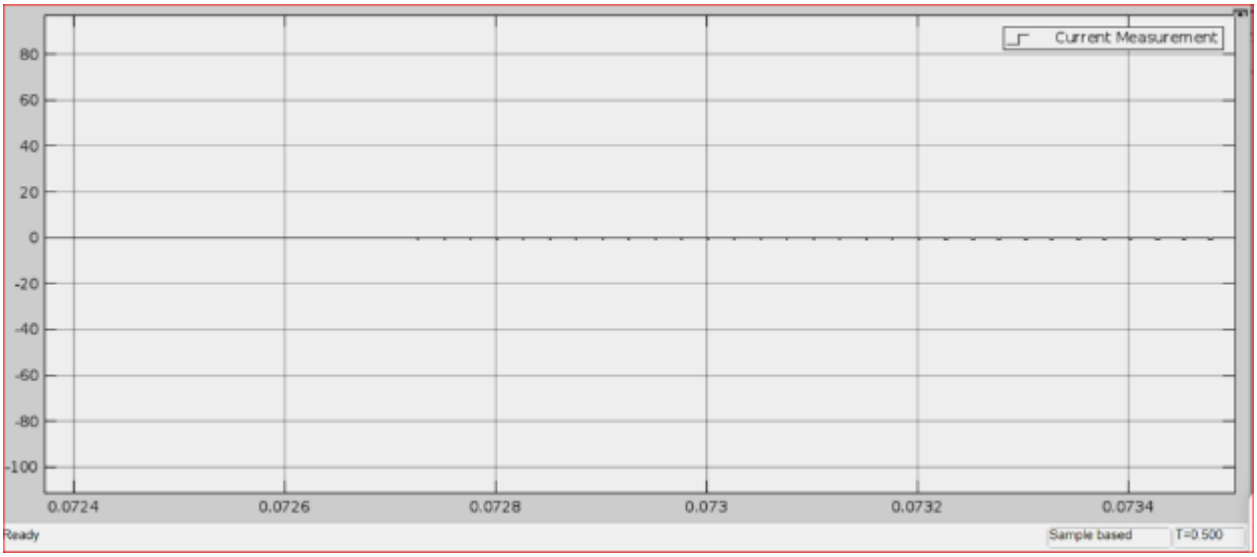

Figure 22 b Sudden Loss of Input Attacks

4.2.3. Proposed Hardware-Based Countermeasures for EV Security

Securing the physical power electronics in an On-Board Charger (OBC) and Battery Management System (BMS) is crucial. Ensuring message authentication and data integrity can mitigate many risks, though it's challenging to prevent all possible attacks due to evolving methodologies. Several preventive measures have been suggested, including third-party management of control systems, advanced encryption, and regular firmware upgrades (Rawson M et al., 1998). Here, we propose three major hardware-based countermeasures to protect EV systems from damage and mitigate immediate risks:

4.2.4. Short Circuit Protection

Short circuits in Electric Vehicles can lead to overheating, fires, or significant damage to batteries and other components. These can result from control system errors or malicious interference causing phase-leg switches to turn on simultaneously. To prevent such conditions, ensure that switch pairs do not turn on simultaneously. Implementing smart fuses and circuit breakers can provide rapid disconnection during faults, enhancing protection for semiconductor devices and related components in the PFC and DC-DC stages.

5. Conclusion

The design and evaluation of the Electric Vehicle (EV) charging system using MATLAB Simulink have provided valuable insights into the impact of various attacks on system performance. As the automotive industry shifts towards electrification, integrating advanced technologies in EVs brings significant benefits but also exposes new vulnerabilities. The onboard charging system, which acts as a crucial interface between the electric grid and the vehicle's battery, plays a key role in ensuring efficient energy transfer and uninterrupted operation. However, this integration introduces cybersecurity risks, including Denial of Service (DoS), spoofing, and physical tampering, which can compromise the vehicle's safety, reliability, and privacy.

To mitigate these threats, a multi-layered cybersecurity strategy is essential. This includes implementing robust authentication mechanisms, encrypting communication channels, deploying intrusion detection systems, and regularly updating software to address vulnerabilities. Collaboration among automotive manufacturers, regulatory bodies, cybersecurity experts, and academia is crucial to establishing industry standards and guidelines for securing EV charging systems. By fostering such collaboration, stakeholders can share knowledge, exchange threat intelligence, and develop innovative solutions to address emerging cybersecurity challenges.

In conclusion, as the transportation ecosystem becomes increasingly connected and electrified, prioritizing cybersecurity in onboard charging systems is critical. A proactive, holistic approach to cybersecurity will help build trust, enhance safety, and support the widespread adoption of electric vehicles, driving towards a cleaner and more sustainable future.

Way Forward

To strengthen the security of onboard charging systems for electric vehicles (EVs), two key recommendations are proposed:

- **Comprehensive Security Analysis**: Conduct a thorough assessment of the system's security and resilience. This includes identifying potential cyber threats, vulnerabilities, and attack vectors that could compromise data integrity and confidentiality during charging operations. By evaluating the system's security posture, stakeholders can implement robust defences and improve protection against cyber-attacks.
- **Dynamic Threat Response Mechanisms**: Develop adaptive security measures capable of detecting and responding to evolving threats in real-time. This should include the implementation of intrusion detection systems, anomaly detection algorithms, and proactive risk mitigation strategies to ensure the continuous, secure operation of onboard charging systems.

These measures aim to enhance the efficiency, reliability, and environmental sustainability of EV charging systems by addressing current limitations and preparing for future cybersecurity challenges.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

Reference

[1] Brighente A, Conti M, Donadel D, Poovendran R, Turrin F, Zhou J. Electric Vehicles Security and Privacy: Challenges, Solutions, and Future Needs. arXiv preprint arXiv:2301.04587. Available from: https://arxiv.org/abs/2301.04587

[2] Hamdare S, Kaiwartya O, Aljaidi M, Jugran M, Cao Y, Kumar S, Mahmud M, Brown D, Lloret J. Cybersecurity Risk Analysis of Electric Vehicles Charging Stations. Sensors. 2023;23(15):6716. Available from: https://doi.org/10.3390/s23156716

[3] Review of Electric Vehicle Charger Cybersecurity Vulnerabilities: Potential Impacts and Defenses. Available from: ResearchGate.

[4] Haghbin S, Khan K, Lundmark S, Alakla M, Carlson O, Leksell M, et al. Integrated chargers for EVs and PHEVs: Examples and new solutions. In: Proceedings of the International Conference on Electrical Machines; 2010; 2010. p. 1-6.

[5] Kim JS, Choe GY, Jung HM, Lee BK, Cho YJ, Han KB. Design and implementation of a high-efficiency on-board battery charger for electric vehicles with frequency control strategy. In: Proceedings of the IEEE Vehicle Power and Propulsion Conference; 2010 Sep; 2010. p. 1-6.

[6] Lacroix S, Laboure E, Hilairet M. An integrated fast battery charger for electric vehicle. In: Proceedings of the IEEE Vehicle Power and Propulsion Conference; 2010 Sep; 2010. p. 1-6.

[7] Su W, Eichi H, Zeng W, Chow MY. A survey on the electrification of transportation in a smart grid environment. IEEE Transactions on Industrial Informatics. 2012;8(1):1-10.

[8] Duvall M. Charging infrastructure update. In: Proceedings of the Electric Power Research Institute (EPRI) CPUC Electric Vehicle Workshop; 2010 Mar.

[9] Botsford C, Szczepanek A. Fast charging vs. slow charging: Pros and cons for the new age of electric vehicles. In: 24th Electric Vehicle Symposium; 2009 May.

[10] De-Sousa L, Silvestre B, Bouchez B. A combined multiphase electric drive and fast battery charger for electric vehicles. In: Proceedings of the IEEE Vehicle Power and Propulsion Conference; 2010 Sep; 2010. p. 1-6.

[11] Morrowa K, Karnerb D, Francfort J. Plug-in hybrid electric vehicle charging infrastructure review. U.S. Department of Energy Vehicle Technologies Program Final Report 58517; 2008 Nov.

[12] Rawson M, Kateley S. Electric vehicle charging equipment design and health and safety codes. California Energy Commission Report; 1998 Aug 31.

[13] Schmittner C, Macher G. Automotive cybersecurity standards-relation and overview. In: International Conference on Computer Safety, Reliability, and Security; 2019; Springer; 2019. p. 153-165.

[14] Scalas M, Giacinto G. Automotive cybersecurity: Foundations for next-generation vehicles. In: 2019 2nd International Conference on New Trends in Computing Sciences (ICTCS); 2019. p. 1-6.

[15] Bahrami. EV charging definitions, modes, levels, communication protocols and applied standards. Changes. 2020;1:10-01.

[16] Khalid A, Sundararajan A, Hernandez A, Sarwat AI. Facts approach to address cybersecurity issues in electric vehicle battery systems. In: 2019 IEEE Technology & Engineering Management Conference (TEMSCON); 2019. p. 1-6.

[17] Chandwani S, Dey S, Mallik A. Cybersecurity of onboard charging systems for electric vehicles—review, challenges and countermeasures. IEEE Access. 2020;8:226982-226998. Available from: https://ieeexplore.ieee.org/abstract/document/9296573

[18] Acharya S, Dvorkin Y, Pandziˇ c H, Karri R. Cybersecurity of smart electric vehicle charging: A power grid perspective. IEEE Access. 2020;8:214434-214453.

[19] Ye J, Guo L, Yang B, Li F, Du L, Guan L, Song W. Cyber–physical security of powertrain systems in modern electric vehicles: Vulnerabilities, challenges, and future visions. IEEE Journal of Emerging and Selected Topics in Power Electronics. 2020;9(4):4639-4657.

[20] Chandwani A, Dey S, Mallik A. Cybersecurity of Onboard Charging Systems for Electric Vehicles—Review, Challenges and Countermeasures. IEEE Access. 2020;8:226982-226998. Available from: https://ieeexplore.ieee.org/abstract/document/9296573 (accessed April 20, 2023).

[21] Ning J, Wang J, Liu J, Kato N. Attacker identification and intrusion detection for in-vehicle networks. IEEE Communications Letters. 2019;23(11):1927-1930. https://doi.org/10.1109/LCOMM.2019.2937097

[22] Islam R, Refat RUD. Improving CAN bus security by assigning dynamic arbitration IDs. Journal of Transportation Security. 2020;13(1-2):19-31. https://doi.org/10.1007/s12198-020-00208-0

[23] Bi Z, Xu G, Xu G, Tian M, Jiang R, Zhang S. Intrusion detection method for in-vehicle CAN bus based on message and time transfer matrix. Security and Communication Networks. 2022. https://doi.org/10.1155/2022/2554280

[24] Duan X, Yan H, Tian D, Zhou J, Su J, Hao W. In-vehicle CAN bus tampering attacks detection for connected and autonomous vehicles using an improved isolation forest method. IEEE Transactions on Intelligent Transportation Systems. 2021. https://doi.org/10.1109/TITS.2021.3128634

[25] Qin H, Yan M, Ji H. Application of controller area network (CAN) bus anomaly detection based on time series prediction. Vehicular Communications. 2021;27:100291. https://doi.org/10.1016/j.vehcom.2020.100291

[26] Hossain MD, Inoue H, Ochiai H, Fall D, Kadobayashi Y. LSTM-based intrusion detection system for in-vehicle CAN bus communications. IEEE Access. 2020;8:185489-185502. https://doi.org/10.1109/ACCESS.2020.3029307

[27] Zhou A, Li Z, Shen Y. Anomaly detection of CAN bus messages using a deep neural network for autonomous vehicles. Applied Sciences. 2019;9(15):3174. https://doi.org/10.3390/app9153174

[28] Ben Othmane L, Dhulipala L, Abdelkhalek M, Multari N, Govindarasu M. On the performance of detecting injection of fabricated messages into the CAN bus. IEEE Transactions on Dependable and Secure Computing. 2020;19(1):468-481. https://doi.org/10.1109/TDSC.2020.2990192

[29] Hou S, Chen X, Ma J, Zhou Z, Yu H. An ontology-based dynamic attack graph generation approach for the internet of vehicles. Frontiers in Energy Research. 2022;10:928919. https://doi.org/10.3389/fenrg.2022.928919

[30] D'Angelo G, Castiglione A, Palmieri F. A cluster-based multidimensional approach for detecting attacks on connected vehicles. IEEE Internet of Things Journal. 2020;8(16):12518-12527. https://doi.org/10.1109/JIOT.2020.3032935

[31] Boumiza S, Braham R. An anomaly detector for CAN bus networks in autonomous cars based on neural networks. In: 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob); 2019 Oct; IEEE; 2019. p. 1-6. https://doi.org/10.1109/WiMOB.2019.8923315

[32] D'Angelo G, Castiglione A, Palmieri F. A cluster-based multidimensional approach for detecting attacks on connected vehicles. IEEE Internet of Things Journal. 2020;8(16):12518-12527. https://doi.org/10.1109/JIOT.2020.3032935

[33] Yilmaz M, Krein PT. Review of battery charger topologies, charging power levels, and infrastructure for plug-in electric and hybrid vehicles. IEEE Transactions on Power Electronics. 2013;28(5):2151-2169.

[34] Richard L, Petit M. Fast charging station with battery storage system for EV: grid services and battery degradation. In: Proceedings of the 2018 IEEE International Energy Conference (ENERGYCON); 2018

[35] Chukwunweike JN, Michael S, Mbamalu IF, Emeh C. Artificial Intelligence and Electrocardiography: A Modern Approach to Heart Rate Monitoring. World J Adv Res Rev. 2024;23(01):1385-1414. Available from: https://doi.org/10.30574/wjarr.2024.23.1.