IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 18, 2020, accepted December 12, 2020, date of publication December 16, 2020,
date of current version December 31, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3045367

Cybersecurity of Onboard Charging Systems for Electric Vehicles–Review, Challenges and Countermeasures

ASHWIN CHANDWANI, (Student Member, IEEE), SAIKAT DEY, (Student Member, IEEE), AND AYAN MALLIK, (Member, IEEE)
Power Electronics and Control Engineering (PEACE) Laboratory, Arizona State University, Tempe, AZ 85281, USA
Ira A. Fulton School of Engineering, Arizona State University, Tempe, AZ 85281, USA

Corresponding author: Ayan Mallik (ayan.mallik@asu.edu)

ABSTRACT In this paper, the impacts of various data integrity attacks on the power electronic hardware present in an EV charger are comprehensively analyzed in order to provide necessary recommendations to defend against cyberattacks on electric vehicles and their onboard charging (OBC) systems. The adverse scenarios arising due to cyberattacks are carefully reviewed in this study, which includes (a) interfering with the main charger controller (FPGA) logic and its data, (b) establishing fake communication between the charging controller and other electronic control units (ECUs) connected over same controller area network (CAN) bus, and (c) interfering with the battery management system functionalities. A 6.6kW interleaved totem-pole PFC front-end followed by a high frequency DC-DC converter is used as our OBC representative system in this analysis. Possibilities and ways of potential cyberattacks on this model are investigated in detail. Effort is made towards providing software as well as hardware design-level protection mechanisms to mitigate the malicious effects of such cyberattacks on the OBC hardware. This system is simulated in MATLAB/Simulink to verify the fault occurrences under various data integrity attacks as well as to validate the effectiveness of our proposed countermeasure approaches. Quantitative analyses of the obtained results clearly demonstrate that if adequate precautionary measures are properly taken while designing the charging architecture (e.g., implementing intelligence to the main controller), any electrical hazard or deterioration of health of the components can be avoided to the maximum extent under the circumstances of a malicious cyberattack.

INDEX TERMS CAN, cybersecurity, electric vehicle, FPGA, onboard charger.

I. INTRODUCTION

Due to the numerous environmental threats pertaining to global warming and increased greenhouse gas emissions caused by the indispensable demand for fossil fuels, the electric vehicle (EV) industry has gained tremendous traction in the last decade. Several technologies to reduce fuel consumption or to use a combination of efficient fuels have been proposed and implemented in several countries. Various technologies like efficient Fuel-Cell Electric Vehicles [1], Hybrid Vehicles [2], and Battery based Electric Vehicles [3] have found their place in the EV market. However, with the evolution of EVs, the concept of "range anxiety" [4], [5] has become quite prevalent amongst the car buyers and owners. This has motivated the EV manufacturers to provide high energy density batteries [6] with high power density and efficient design of power electronics [7]. Along with the optimization in the battery design, the research and development related to the electronics involved in the battery charging infrastructure have also seen a major boost [8]. Various topologies like phase-shifted semi bridgeless rectifier, bridgeless rectifier, current doubler rectifier, boosting full-bridge rectifier/inverter [9] and the usage of wide band gap semiconductor devices in topologies like H-bridge LLC resonant converters [10] and inductance-double capacitances-series (LCC-S) [11] have been also proposed to achieve superior power conversion [12] for EV charging infrastructure.

Several interfacing devices also termed as Electric Vehicle Supply Equipments (EVSE), are also used widely that enable faster transfer of power with global compatibilities [13] like a standard J1772 connector for level 1 and 2 [14] and CHAdeMO for fast charging [15]. Also, with the advent of

The associate editor coordinating the review of this manuscript and approving it for publication was Zhilei Yao.

the Internet of Things (IoT), advanced communication protocols, cloud computing, and dependence on data analytics for enhanced predictability and efficient data transfer and control, the utility companies are able to efficiently control and modulate the power distribution [16]–[19]. However, due to the continuous monitoring and data transfer between the grid connected EV chargers and utility companies, using external devices, the system has become very vulnerable to cyberattacks [20]. For example, in 2019, a cyber-attack was reported by NERC affirming that a loophole in the web data-exchange interface of a vendor's firewall was exploited, thus allowing an attacker to cause unanticipated reboots of the devices. This led to Denial of Service (DoS) condition at a low-impact control center and several low-impact remote generation sites [21]. This problem is very relevant to EV charging stations and the EVSEs involved, due to their high accessibility and a large amount of power demand. These kinds of attacks are even more prevalent in level II EV chargers – typically the onboard chargers (OBC), where data privacy and cyber resiliency have not yet received enough maturity [22].

Typically, the initiation and stoppage of the charging cycle, along with the required power transfer is done through communication established between the vehicle/electronic system or battery side sensors and the controllers driving the various converters involved in a typical charger. Fig. 1 shows a generic onboard charging infrastructure and the physical connections among the major building blocks of the system: the power grid, charging station (EVSE), onboard charger, BMS and the battery. All the physical connections portray the flow of energy between the grid side and the EV battery. Apart from power transfer, these connections also serve the purpose of data exchange among the components through their communication channels. The battery management system (BMS) senses the real-time charging/discharging status of the battery by receiving information such as: terminal cell voltage, charging current, state of charge (SOC), state of health (SOH), cell temperature etc. of the battery. After processing the information, the BMS comes up with the desired charging profile and communicates with the OBC controller accordingly [23]. Under any circumstances if these communicated signals' data are altered, it can severely impact the charging parameters/profile of the battery, which can grow fatal as well. However, all the communication channels involved in the EV charging architecture make the system prone to the cyberattacks. An attacker can launch a cyber-attack on the system through various points of access, shown in the Fig. 1. As an example of data integrity attack, if the attacker gets a physical access to the communication channel established between the EVSE and the OBC, or the OBC and the BMS, then the sensitive data between the specific sub systems can be read as well as altered, and such alterations might cause serious impact on the safety of the vehicle and the interfacing grid [24]. On the other hand, if the attacker gets access to the FPGA controller present inside the onboard charger, a side channel attack can be launched on any of the residing logic blocks, as discussed in later sections. One similar scenario on the communication system can be infection of the charging main controller and ultimately, injection of undesired viruses and malware to the central management system, through the data communication lines. Such malicious codes can also be spread via various stations, leading to the number of infected EVs growing exponentially. Thus, it becomes very important to understand the corresponding cyber threats involved in any charging system and their impact on the grid. In addition to that, normal working of the internal structure of the OBC can also be easily disrupted by a malicious attack implemented on the main controller or the communication channels (CAN, WiFi, Bluetooth) connected to it. For example, by tweaking control parameters with a malevolent intent can cause over-voltage or over-current failures in the electronic components inside an OBC circuit [25].

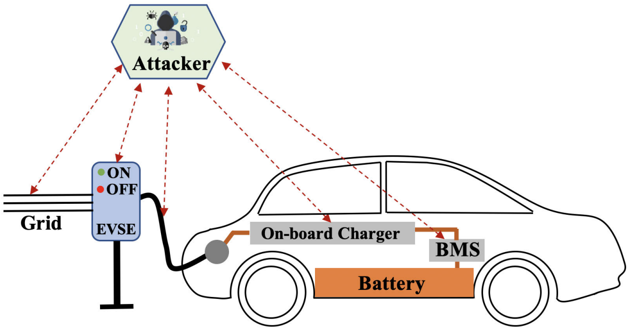


FIGURE 1. Conceptual configuration of an EV OBC based cyber-attack.

Recently, due to the advancements in the field of cybersecurity, several researchers have proposed numerous methods to prevent such cyberattacks by modeling the attacks precisely and finding passive countermeasures [26]–[28]. Although these countermeasures have been proved to be useful, they haven't been able to provide dynamic real-time response against the cyber-threats, which limit the systems to resume normal operation after the threats are cleared. Thus, with an overall perspective of cyber-resilient system, this paper elucidates the various kinds of hazard-causing cyber threats occurring in an OBC and puts effort to understand the specifics of the component failure modes related to cyber-attack by considering an example of a 6.6kW domestic OBC. Cyberattacks that affect the software logics and communication channels along with their effects on the hardware integrity of the charger are thoroughly investigated in this work. Threats pertaining to manipulation of CAN bus protocol and FPGA logic that are the direct source of attacks in an OBC system are also studied. The paper proposes and explains critical countermeasure approaches (in both software and hardware levels) that are implemented to ensure a cyber-resilient EV charging infrastructure. In addition to that, a novel real-time sensed data-based countermeasure scheme is proposed that ensures event-based detection of cyberattacks and provides protection against possible damages to the components involved in the circuit.

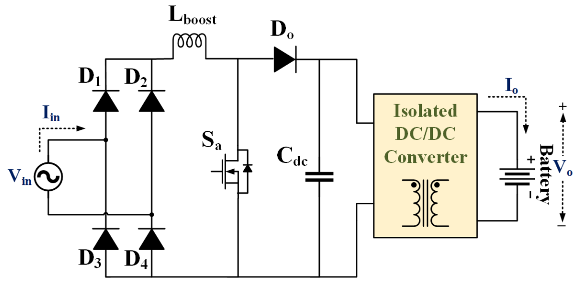


FIGURE 2. Conventional single-phase boost PFC with isolated DC/DC converter.

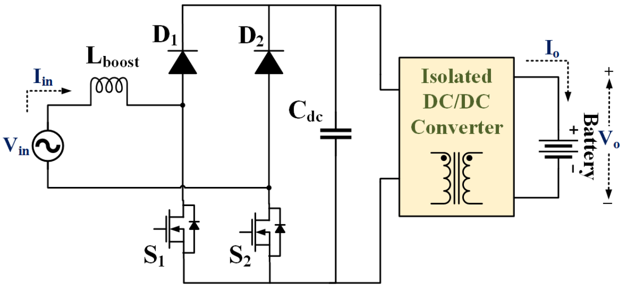


FIGURE 3. Bridgeless PFC topology with isolated DC/DC converter.

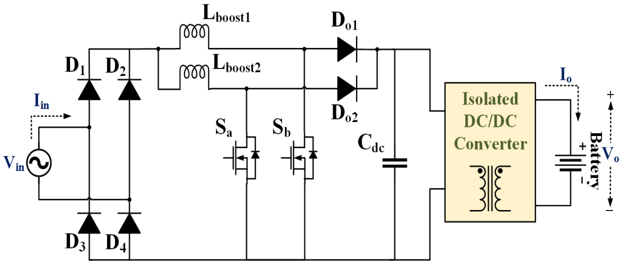


FIGURE 4. Interleaved boost PFC with isolated DC/DC converter.

The paper is organized as follows: Section II explains the various topologies used for OBC applications and then presents the design, control and simulation of a single-phase two-stage onboard charging topology. Section III provides the classification of the cyber-threats occurring in a typical OBC system. To understand the potential attack paths and logics used by the attacker, an illustrative modeling of various cyber-attacks is performed in Section IV and also, it is analytically shown how they can cause maximum damage to the system. Further on, to develop an attack responsive system, the critical countermeasures along with associated implementation results are thoroughly explicated and analyzed in Section V. Finally, Section VI puts forward conclusions with relevant discussions.

II. ONBOARD CHARGER TOPOLOGIES AND CONTROL SCHEME

There are several OBC topologies discussed in the literature [29], [30], each of them with some specific benefits as well as limitations: -

A. CONVENTIONAL SINGLE-PHASE BOOST PFC WITH ISOLATED DC/DC CONVERTER

The topology for conventional single-phase boost PFC with isolated DC/DC stage is described in Fig. 2. It is one of the most basic and commonly used topologies for OBC applications. The topology is relatively simple and provides an economically viable solution for most of the charging applications. Conventional single-phase PFC consists of a full bridge diode rectifier coupled to a single stage boost converter. The design and control scheme are targeted to get high (ideally unity) power factor. Additionally, the selected control scheme also maintains the output voltage to be constant, with least amount of input current ripple. The operational duty cycle is decided according to the desired output voltage and the rms value of input voltage. However, due to a large amount of diode conduction losses in the front-end stage, such a design is not suitable for load power above 1kW.

B. BRIDGELESS PFC TOPOLOGY WITH ISOLATED DC/DC CONVERTER

As shown in Fig. 3, the diode bridge at the input side is replaced with a combination of two fast recovery diodes and two MOSFETs, connected to the voltage source through a boost inductor. This is done so as to reduce the conduction losses of the diode bridge. The switches (S_1 and S_2) and diodes (D_1 and D_2) conduct, with the boost inductor to resemble a boost circuit in two half circuits (depending on the duty cycle). However, in this circuit, the input current ripple observed is still high. To resolve this issue, interleaving is introduced for boost PFC circuits.

C. INTERLEAVED BOOST PFC WITH ISOLATED DC/DC CONVERTER

As seen in Fig. 4, the interleaved topology of boost PFC converter consists of a full bridge diode rectifier, connected to two parallel boost converters, operating at 180^0 phase shift. This is done so as to reduce the resultant input current ripple. Due to this, the required rating for the boost inductor is reduced by half, thus reducing the cost and volume.

D. THREE PHASE BOOST PFC WITH ISOLATED DC/DC CONVERTER

Fig. 5 shows the topology for a three-phase boost PFC with isolated DC/DC. Here, instead of a single-phase bridge as in the conventional 1-ph boost PFC, a six-pulse rectifier fed by a three-phase voltage source is coupled with the boost PFC circuit.

Additionally, the isolated DC/DC stage (as shown in Fig. 2-5) can be based on pulse width modulation (PWM) with a phase shifted secondary (Fig. 6) or can be based on pulse frequency modulation (PFM) with a resonant tank topology (Fig. 7). In either of the cases, the output voltage can be modulated by tuning the gain as per the requirement.

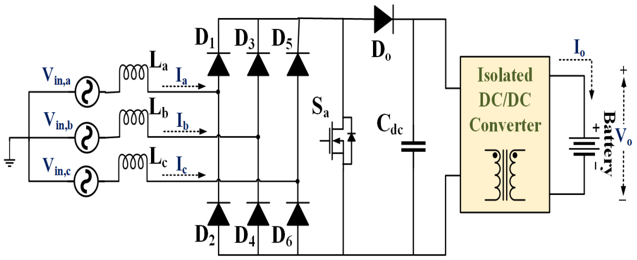


FIGURE 5. Three phase boost PFC with isolated DC/DC converter.

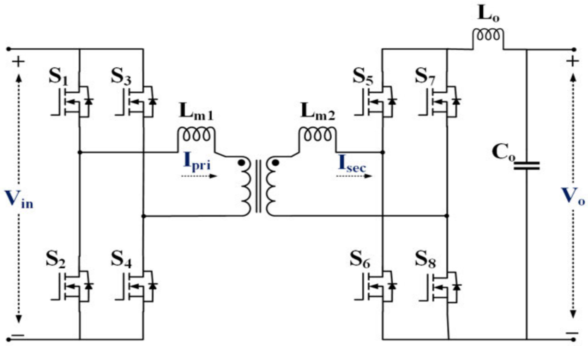


FIGURE 6. Dual active bridge DC/DC converter with shifted secondary.

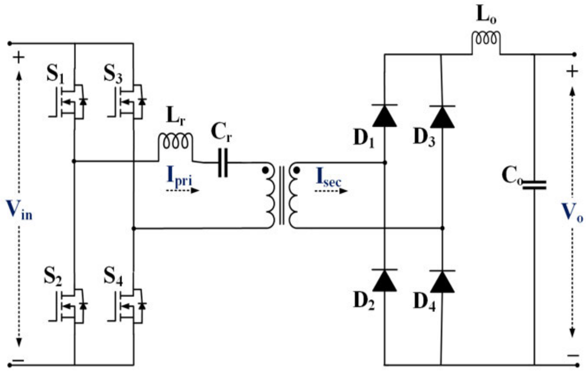


FIGURE 7. Resonant topology for DC/DC converter.

However, in this work, the threats pertaining to cybersecurity are discussed for a generic 6.6kW on-board charger. Thus, a more generalized single-phase topology that assimilates the positive features from the above-mentioned topologies is selected for detailed analysis.

The topology for a generic single-phase OBC that is selected as a candidate for cybersecurity analyses is shown in Fig. 8. It consists of an interleaved totem-pole boost power factor corrector (PFC) circuit [31], [32] followed by a dual active bridge (DAB) DC-DC stage. The PFC stage outputs a constant DC voltage (V_{dc}) that appears across the DC link capacitor (C_{dc}). A high frequency inverter is then used to convert the regulated DC link voltage to high frequency pulses that are magnetically induced to the terminal rectifier circuit using a high frequency transformer. The rectifier output is connected to the battery and the charging parameters (state of charge, state of health, cell temperature, cell voltages) are constantly monitored by a battery management system (BMS). As observed in the Fig. 8, the splitting of the input current intro inductor connected high frequency half bridges operating at 180 degrees phase difference helps in reducing the grid current ripple for enhanced power quality with lower THD [33], [34].

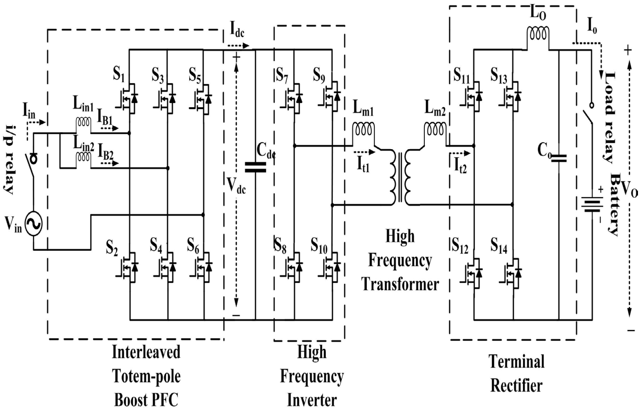


FIGURE 8. Single phase OBC circuit topology.

For driving the above-mentioned combination of converters, two specific control modules are required. Fig. 9 describes the control schematic for the interleaved boost PFC converter. As seen in the Fig. 9 (a), the reference DC link voltage (V_{dc}*) is compared with the actual DC link voltage (V_{dc}), to provide an error (ε) which is processed in a PI controller to generate peak reference current (I_{ref}). The sinusoidal component obtained by normalizing the input voltage (V_{in}) with respect to its peak ($V_{in,pk}$*) is multiplied with the obtained reference current amplitude to provide the reference input current (I_{ref} sin(θ)). The generated reference is then compared to the input currents (which are obtained by splitting input current (I_{in}) into two parts (I_{B1} and I_{B2}) as seen in Fig. 8), to generate corresponding error (ε_1 and ε_2)). These errors are processed through current loop PI controllers and saturation blocks to generate corresponding duty cycle signals (D_1* and D_2*) for each half bridge. Further on, as seen in Fig. 9(b), the generated duty cycle signals are processed and compared with a triangle wave to generate PWM based gate pulses (G_{PFC}).

Similarly, Fig. 10 shows the control schematic for the primary side high-frequency inverter and secondary side terminal rectifier. The control methodology tunes the phase angle difference between primary and secondary side full-bridges to control the power flow as well as to ensure zero voltage switching (ZVS) and thus reduces the switching loss incurred by the DC-DC conversion stage. As observed in the control block diagram, the reference output voltage (V_o*) is compared with the actual sensed voltage (V_o), to generate the error signal (ε), which is processed in a PI controller to produce reference phase shift (δ). The phase angle is further converted to time domain (t_o) by dividing the signal by a factor of 2πf. Gating pulses with 50% duty cycle at rated switching frequency (required to drive the high frequency

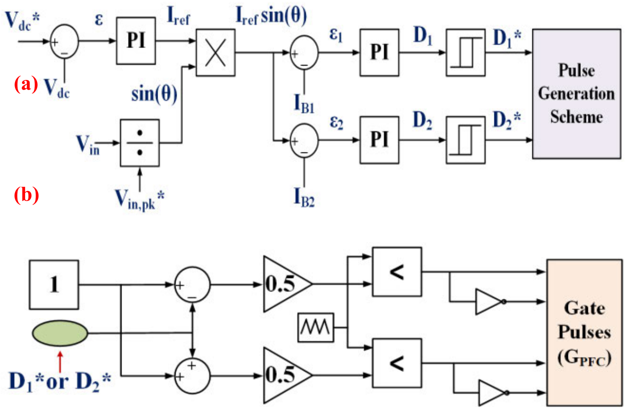


FIGURE 9. Control schematic for interleaved boost PFC converter: (a) Reference duty generation (b) Schematic for generation of gate pulses.

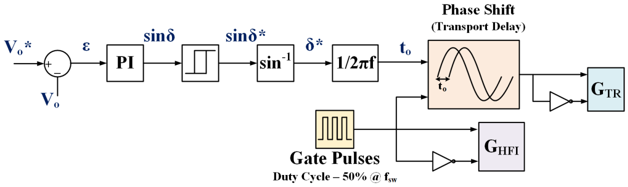


FIGURE 10. Control Schematic for high frequency inverter and terminal rectifier.

TABLE 1. Parameters for simulation study

Parameters	Values
Input Voltage	230Vac, 1-ph, 60Hz
Input side inductors (L_{in1} and L_{in2})	1.5mH
DC link capacitor (C_{dc})	2mF
Primary Inductance (L_{m1})	15μH
Transformer turns ratio	1:1
Output Inductor (L_o)	0.2 μH
Output Capacitor	150 μF
Output Voltage	450V
Sampling Time (T_s)	0.5 μs

inverter - G_{HFI}) are fed to the transport delay block along with the generated shift (t_o), to generate gating pulses for the terminal rectifier (G_{TR}).

Fig. 11. shows the simulated waveforms of the aforementioned OBC structure at 6.6kW load power. The parameters used for simulation are shown in Table 1. As per the measurement reports, it is observed that the DC link voltage and output voltage are held at 400V and 450V respectively, at an input power factor over 0.992 with an input current RMS of 14.67A.

A scaled-down hardware proof-of-concept (rated for 1kW) of the proposed OBC architecture is implemented and the results obtained are shown in Fig. 12. As observed, the input current waveform follows the phase of the input voltage waveform, thus achieving a power factor over 0.995 and an efficiency of 96.3% of the charger.

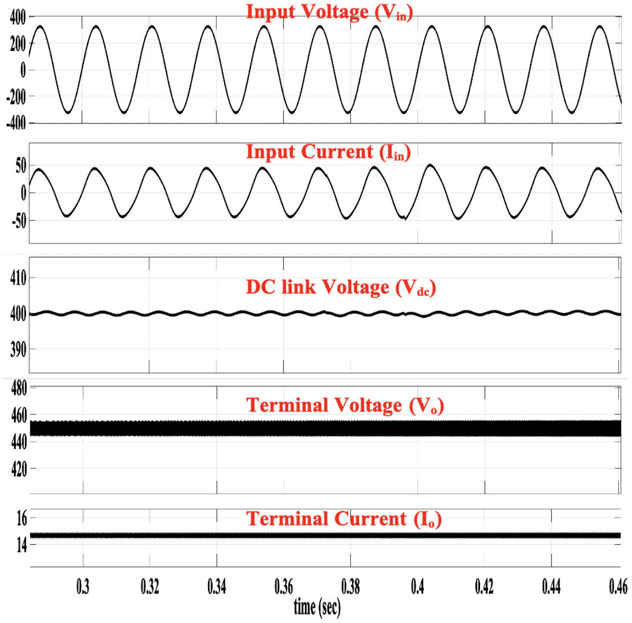
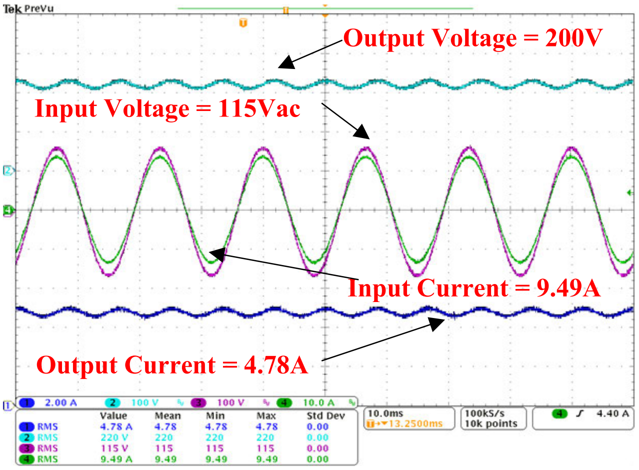


FIGURE 11. Simulation waveforms for OBC topology implementation (Y-axis: Input Voltage (V_{in}) – 200V/div, Input Current (I_{in}) – 50A/div, DC link voltage (V_{dc}) – 10V/div, Terminal Voltage (V_o) – 20V/div, Terminal Current (I_o) – 2A/div; X-axis: Time – 0.02sec/unit).



	Value	Mean	Min	Max	Std Dev
1 RMS	4.78 A	4.78	4.78	4.78	0.00
2 RMS	220 V	220	220	220	0.00
3 RMS	115 V	115	115	115	0.00
4 RMS	9.49 A	9.49	9.49	9.49	0.00

FIGURE 12. Hardware Implementation Results for 1kW rated OBC topology (Y-axis: Output Voltage (V_o) [Dark Green] – 100V/unit, Input Voltage (V_{in}) [Pink] – 100V/unit, Input Current (I_{in}) [Light Green] – 10A/unit, Output Current (I_o) [Dark Blue] – 2A/unit; X-axis: Time – 10ms/unit).

The combined comprehensive control scheme for the selected topology is shown in Fig. 13 and is implemented in a combined interface of Field Programmable Gate Array (FPGA) and Digital Signal Processor (DSP) [35], [36]. As seen in Fig. 13, a number of sensed inputs (DC link voltage (V_{dc}), Input Voltage (V_{in}), Input bridge currents (I_{B1}, I_{B2}), Output voltage (V_o), Output Current (I_o), Relay control signals – Input Relay (IR) and Load Relay (LR)) are given to the controller, and the corresponding control modules generate gating pulses for the various converters included in the topology (G^*_{PFC}, G^*_{HFI} and G^*_{TR}). Battery charging

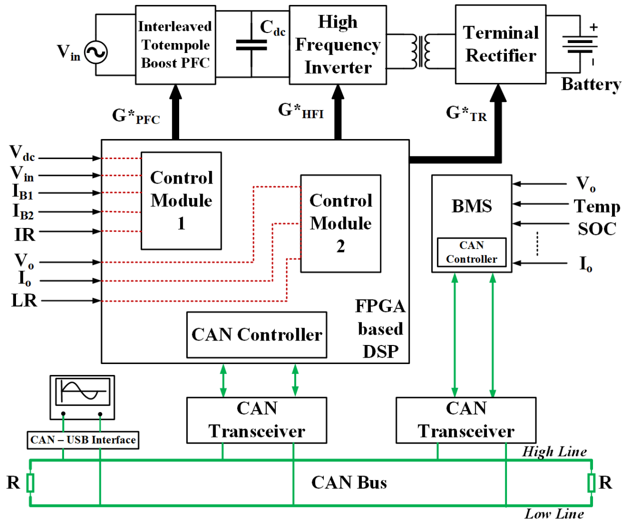


FIGURE 13. Comprehensive control scheme for OBC control.

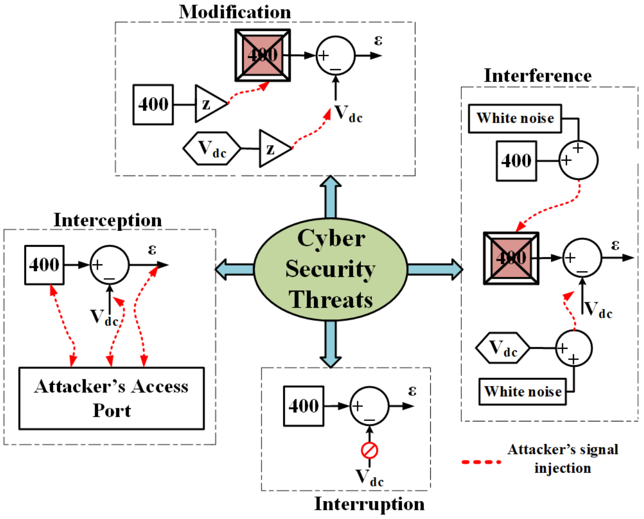


FIGURE 14. Major types of Cyber security threats.

profile and dynamics are handled by the BMS, which takes in sensed battery signals (V_O, Temperature data (Temp), State of Charge (SoC), State of Health (SoH), etc.). These signals (shown with black arrows) altogether form the physical layer of control, while the ones residing inside the power converter controller (FPGA and DSP) constitute the software layer. Additionally, the main controller communicates with other electronic control units (ECUs) through the Controller Area Network (CAN) [37] bus protocol. As seen in the Fig. 13, the CAN bus acts as the major communication protocol as it ties the main controller with the BMS and other ECUs via a programming port available through a CAN-USB interconvertible interface. In perspective of cybersecurity, the system topology is classified in terms of hardware (electronic circuit with stability and safety concerns) and software (FPGA logic and CAN communication) based cybersecurity.

III. CLASSIFICATION OF CYBER SECURITY THREATS TO THE OBC SYSTEM

The cyber-threats pertaining to an EV based OBC can be broadly classified into four major categories, which are illustrated in Fig. 14, that portrays the types of threats with respect to a particular DC link controller schematic inside an OBC.

Here, the controller senses the DC link voltage and compares it with a set control value (400V), and the corresponding error (ε) is processed to generate the required gating pulses for the converters. As observed in the Fig. 14, the aim of the attacker is to manipulate and change the control parameters of the circuit, making it vulnerable to variations and fluctuations in the system, thus affecting the system performance, health and safety. The various types of threats involved in an OBC based cyber-attack are presented as follows:

A. MODIFICATION

Modification refers to attacks targeting the information integrity of the system, which means an unauthorized party gains access to and tampers the sensed data. For instance, the attacker may try to alter the parameters of the controllers or sensors that might lead to degraded system performance and unwanted variation in the normal operation of the circuit [38]. There are two ways, the attacker can modify the system set parameters:

1) INCREASED SIGNAL

Modification of sensor signals by altering gains or other coefficients is a common manipulating method seen in such category of threats. For example, the output voltage sensed signal may be altered by multiplying with a gain factor, forcing the controller to track the increased voltage set point, resulting in overvoltage damage to the semiconductor switches or the battery.

2) DECREASED SIGNAL

Similar to the increased signal, in this kind of modification attack, the sensed control value is altered to a drastically reduced fraction of the actual control set value. These kinds of attacks make the system very precarious, as the controller, in an attempt to reduce the propagating error, will try to increase the sensed parameter, leading to permanent damage to the various components in the circuit.

If y is the actual sensed signal, then the modification attack parameter ($\hat{y}$) can be modified as shown in (1)

$$\hat{y} = \begin{cases} y & (t \notin T_{ATK}) \\ z * y & (t \in T_{ATK}) \end{cases} \tag{1}$$

where, if $z \in (0, 1)$, it can be addressed as a decreased attack and if $z \in (1, \infty)$, it portrays an increased attack.

B. INTERFERENCE

Interference here implies polluting the set control or sensed dataset, which ultimately affects the system dynamics. As a consequence of this attack, the controller, instead of processing the error for tracking the set value, will now try to track the polluted waveform, thus affecting the converter dynamic performance drastically [39].

1) WHITE NOISE

An attacker may try to inject unnecessary high frequency noise (greater than 1kHz) in the sensed signals, thus resulting in a distorted and disturbed performance of the controller.

$$\hat{y} = \begin{cases} y & (t \notin T_{ATK}) \\ y + white\ noise(f_N) & (t \in T_{ATK}) \end{cases} \tag{2}$$

2) COMBINATION OF WHITE NOISE AND MODIFICATION

The attack can also be a combination of a distorted waveform with alteration in the magnitude of the control parameters.

$$\hat{y} = \begin{cases} y & (t \notin T_{ATK}) \\ (z * y) + white\ noise & (t \in T_{ATK}) \end{cases} \tag{3}$$

C. INTERRUPTION

Interruption here refers to threats that target the availability of information. It includes instances where an attacker tries to destroy a cyber asset by making it unavailable for operation in a control system. For example, an attacker may try to block the control pulses from the DSP leading to voltage and current surges in the OBC circuit. Majorly, the Denial-of-Service (DoS) attacks fall under this category, where data extraction and processing are hampered by communication link jamming [38] and thus, the feedback loop seems to have been broken.

D. INTERCEPTION

Interception threats target the confidentiality of the information and allow the attacker to gain complete access to a cyber asset. Wiretapping, keystroke logging, fibber taping, etc. fall under this category of threats. Such threats make the OBC susceptible to dangers such as: overvoltage leading to semiconductor switch damage, loss of synchronization of the system, control system malfunction, etc. [38]

IV. MODELLING OF CYBERATTACKS ON THE OBC

The main aim of orchestrating a cyber-attack is to drastically affect the system performance or cause permanent damage to the various components involved in the circuit. Such attacks are typically executed by getting access to the physical or the remote layer of the EVSE. Some of the major classifications in terms of attacks for an EV OBC are modelled into two different categories: -

A. CONTROL BASED ATTACK

These kinds of attacks target the controller logic (FPGA) and the internal process structure (closed loop control) of the system. Moreover, the various communication protocols (CAN) used in the system are also vulnerable to such attacks.

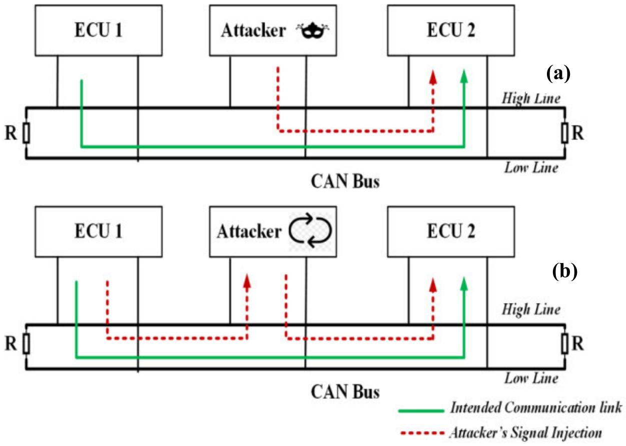


FIGURE 15. Manipulation of CAN bus: (a) Masquerade attack (b) Replay attack.

1) MANIPULATION OF CAN COMMUNICATION BUS

In CAN bus protocol, attacks like masquerade attacks [40], [41] followed by replay attacks [42]–[44] are likely to happen, where an ECU pretends to be another ECU by transmitting a message that the ECU is not entitled to send. In addition to this, the receiver is mostly unable to authenticate the identity of the sender of the message as an attacker could have pretended to be someone else (and thus sending a message with an ID the pretender was not configured to send it the first place). Fig. 15. gives an insight into how the masquerade and replay attacks are implemented. Such fraudulent messages that are broadcasted, might have malicious intent, so as to damage the system by affecting the communication between the various ECUs.

Considering the OBC control system shown in Fig. 13., the communication channel between the BMS and the main controller is implemented through a CAN bus. If the attacker gets access to either of the ECUs or the CAN-USB interface (which is typically used to monitor the system status), there is a chance of broadcasting false messages to these ECUs, leading to misguided set points and sensed signals. For example, the BMS captures data such as: SoC, battery voltage, individual cell voltages, temperature, etc. and sends them to the controller for further processing and control. In this scenario, if the data delivery is performed with an intent of disrupting the normal operation of the circuit, it may result in permanent battery damage (because of overvoltage, temperature derating, discharge rate imbalance, etc.)

2) INTRA-FPGA ATTACK

For this type of attack, the FPGA used is assumed to be shared amongst multiple control blocks for efficient usage [45]. As observed in Fig. 13. the main controller consists of an FPGA logic that implements two control modules separately for providing gate pulses to the converter circuits. A cyber-attack can be orchestrated by an attacker, who has access to another FPGA logic, which resides in the same control shell. Typically, a shared FPGA has basic security

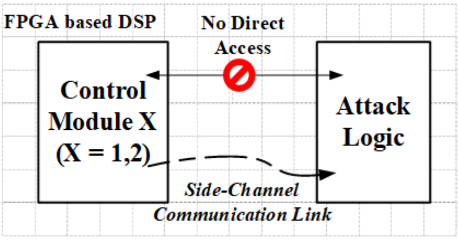


FIGURE 16. Intra FPGA attack.

measures implemented that ensure proper isolation between the two logics (physically portioned with a bunch of unused configurable logics). However, the attacker can try to implement an attack circuit on part of the FPGA with a goal to steal and alter victim's control logic residing on the same FPGA, through a side-channel communication link [46], which is termed as Intra-FPGA attack. Fig. 16. illustrates the above-mentioned scenario with its relevance to the aforementioned control topology. As the programmable logic of an FPGA is implemented to control the gating pulses as per the sensed inputs, it opens up a back gate for an attacker who can program the FPGA to alter the control logic running on the same System on Chip (SoC) [47], [48]. As FPGA can be programmed by loading a bitstream in software, an attacker who possesses the permission to program at least a part of FPGA, can orchestrate side-channel attacks remotely.

For example, a similar attack is considered on the terminal rectifier controller logic, that regulates the voltage appearing across the battery terminals. A decreased signal attack is mimicked on the sensed value of output voltage, by manipulating the FPGA logic and inserting a gain of 0.5 at t = 0.25 sec. Thus, so as to reduce the propagating error that is sent to the proportional integrator block, the control signals are inherently altered by the control system in a way, that the converter instead of tracking the set value of 450V, now tracks a voltage of 900V as seen in Fig. 17. This kind of high voltage appearing across the battery terminals is hazardous when the effective utilization of the battery is taken into consideration. Additionally, as the battery is the most important component in any electric vehicle, this kind of attack might be a potential reason for a severe safety hazard.

B. HARDWARE BASED ATTACK

These kinds of attacks involve detrimental effects on the hardware circuitry of the OBC. Such attacks make the entire circuit vulnerable to permanent failure as these attacks may lead to pushing the hardware components to their maximum possible withstand limits.

1) SUDDEN LOSS OF LOAD

Such a threat is very commonly seen in a generic OBC. Here, an attacker attempts to send malicious signals to open the Load Relay (LR), even when the load is connected. This results in an immense voltage surge at the output side of the OBC. Under such attack scenario, if the semiconductor devices used in the synchronous rectifier are not rated for the adequate overvoltage, repeated occurrence of such overvoltage stress can permanently damage them. However, the battery along with the BMS are designed to withstand stress levels of 1.5-2 times the rated voltage for a short interval of time, such repeated occurrences lead to degraded performance of the battery, and premature end of life (EOF) of the battery. As seen in Fig. 18, the attacker toggles the LR signal at t = 0.25 sec, leading to the above-mentioned situation. As observed, the voltage across the output terminals reaches approx. 1.6 times its rated value at the attack instant.

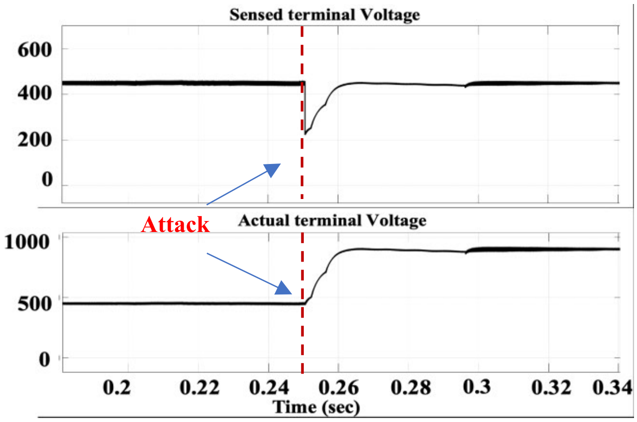


FIGURE 17. Intra FPGA attack (Y-axis: Sensed terminal voltage – 200V/unit; Actual terminal voltage (V_o) – 500V/unit, X-axis: Time – 0.02sec/unit).

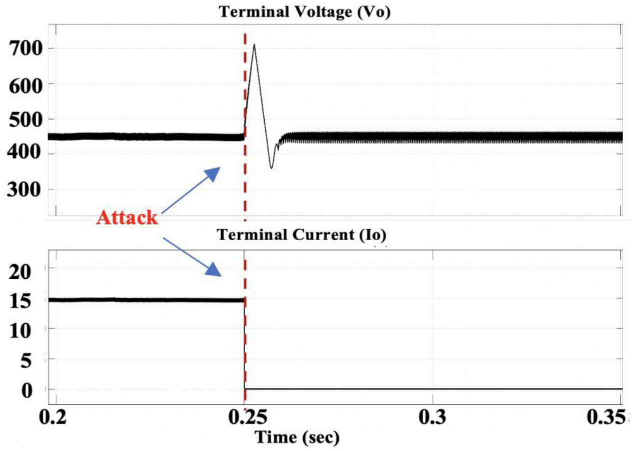


FIGURE 18. Sudden loss of load (Y-axis: Terminal voltage (V_o) – 100V/unit; Terminal current (I_o) – 5A/unit, X-axis: Time – 0.05sec/unit).

2) GRID SIDE SHORT CIRCUIT

In this kind of attack, as seen in Fig. 19, same set of gate pulses are fed to any two high/low side MOSFETs throughout, which leads to constantly charging the PFC inductors with the grid voltage across them and hence, (a) the input current will be 90^0 out of phase from the grid voltage and thus loses the PFC action; (b) the input current amplitude will go higher and may cross the device ratings, resulting in hitting

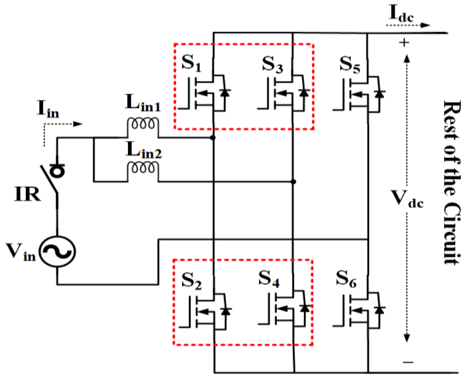


FIGURE 19. Grid side short circuit combination of switches.

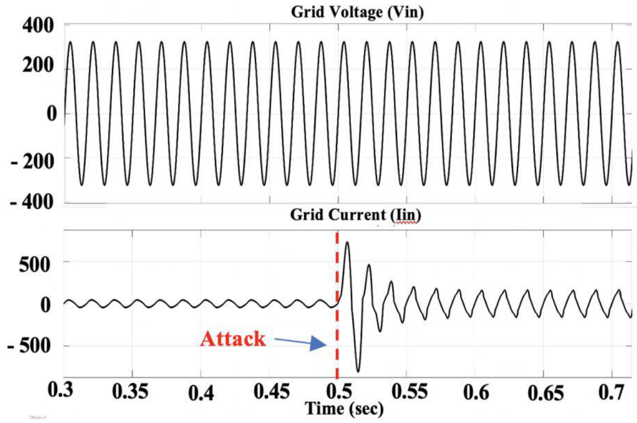


FIGURE 20. Grid side short circuit (Y-axis: grid voltage (V_{in}) – 200V/unit; grid current (I_{in}) – 500A/unit, X-axis: Time – 0.05sec/unit).

overcurrent protection [20]. Such repeated occurrences lead to permanent breakdown of the semiconductor devices and other passive components in the circuit.

As seen in Fig. 20., a similar situation is simulated, where the attacker tries to manipulate the gate pulses, leading to short circuit at the grid side. At t = 0.5 sec, S_1 and S_3 are on simultaneously, leading to gird current shooting up to 16 times its normal value. Also, after this instance, the system loses its equilibrium state, depicting an unstable behavior as a consequence of the attack.

3) SUDDEN LOSS OF INPUT

This kind of attack occurs when the Input Relay (IR) is toggled by an attacker by gaining access to the IR control signal. In such a case, an instantaneous surge appears across the IR, due to di/dt across the input inductors (L_{in1} and L_{in2}). Despite having high dielectric strength, such repeated attacks causing frequent voltage surges across the relay, eventually cause the relay to fail.

As observed in Fig. 21, the IR is opened suddenly by a malicious control signal for a period of 0.1 sec at t = 0.4 sec This causes a surge voltage (V_{pk} = 720V) across the IR for 0.1 sec, leading to detrimental effects in the dielectric material of the relay.

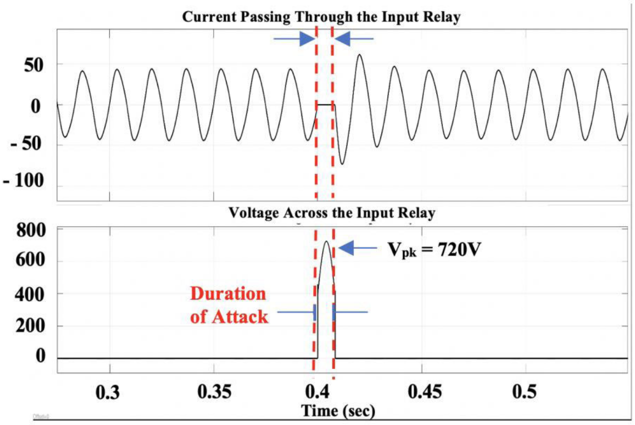


FIGURE 21. Sudden loss of input (Y-axis: current passing through the input relay – 50A/unit; voltage across the input relay – 200V/unit, X-axis: Time – 0.05sec/unit).

V. PROPOSED COUNTERMEASURES FOR CYBER-RESILIENT OBC AND VALIDATIONS

Possible ways of providing security to the cyber-physical power electronics system present in OBC & BMS of an EV include ensuring message authentication and data integrity. However, it is highly challenging to absolutely prevent all attack scenarios because attack methodologies have evolved together with protection schemes. Many researchers are trying to propose a modified security scheme for the CAN BUS protocol, which is the most used communication medium in any automobile specially in an EV infrastructure. CAN bus uses message authentication keys shared among the ECUs and uses counters for each sent/received message [49]–[53]. But applying message cryptography-based solutions incurs high overhead in terms of key decryption as it requires dealing with large keys and reduced communication speed of the CAN bus [49], [53]. This overhead is not suitable for power electronic controllers as they are resource-constrained in terms of both memory and computing capacity. Moreover, these network-based detection systems may not be effective for attacks that are launched within the system (e.g., FPGA attack), which, therefore, makes hardware design-level approaches to be more effective and suitable solutions for most types of cyberattacks for OBC applications. Several preventive measures have also been published, that correlate cybersecurity and attacks on EVSE [54]. These methods include third party management of control systems, higher level encryption of data exchange, firmware upgrades with improved security, etc. as shown in Fig. 22.

However, they still lack the feature of providing a dynamic response to the identified threat, leading to ineffective and sluggish isolation of the circuit. Consequently, new alternative ways to ensure cybersecurity for OBCs need to be introduced and validated. In that context, some of the preventive measures to safeguard the system against cyberattacks are reviewed in this paper and can be broadly classified into three major categories and discussed below. Fig. 23 summarizes the existing and proposed countermeasures in different

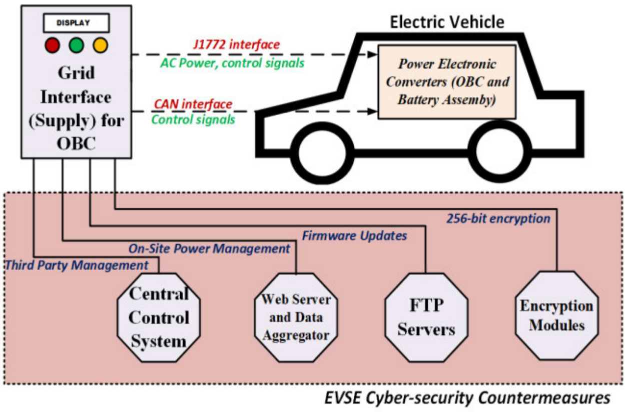


FIGURE 22. Counter measures for EVSE cyber security.

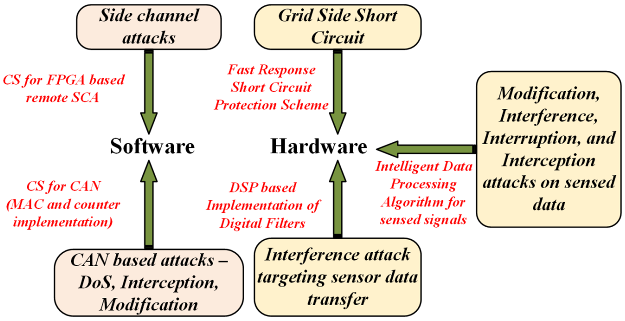

Side channel attacks
Grid Side Short Circuit
CS for FPGA based remote SCA
Fast Response Short Circuit Protection Scheme
Modification, Interference, Interruption, and Interception attacks on sensed data
Software
Hardware
Intelligent Data Processing Algorithm for sensed signals
CS for CAN (MAC and counter implementation)
DSP based Implementation of Digital Filters
CAN based attacks – DoS, Interception, Modification
Interference attack targeting sensor data transfer

FIGURE 23. Proposed Countermeasures for OBC system in categories.

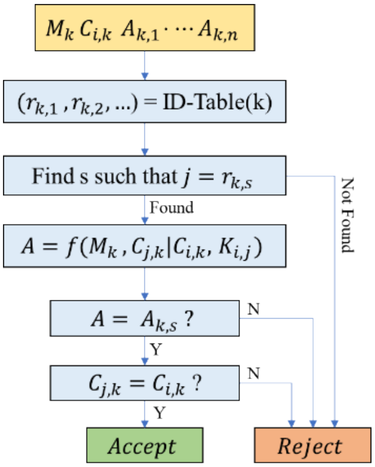

$M_k\, C_{i,k}\; A_{k,1} \cdots A_{k,n}$
$(r_{k,1}, r_{k,2}, \ldots) =$ ID-Table(k)
Find s such that $j = r_{k,s}$
Found
Not Found
$A = f(M_k, C_{j,k}|C_{i,k}, K_{i,j})$
$A = A_{k,s}$?
N
Y
$C_{j,k} = C_{i,k}$?
N
Y
Accept
Reject

FIGURE 24. Steps to perform by a receiving node N_j of a message M_k sent by a sending node N_i.

categories and shows the target sections of hardware and software-based attacks for each of such measures.

A. CYBER SECURITY FOR CAN PROTOCOL IN OBC

As the structures of future electric vehicles are becoming more complex and more connected to the outside networks, the CAN bus becomes more vulnerable, and providing an improved security to this network is essential to protect the OBC and BMS from electrical hazards. A typical CAN bus being extremely vulnerable to different kinds of remote cyberattacks needs special security measures. The features that make the CAN bus prone to such cyberattacks are Multicast Messaging, lack of encryption, lack of message authentication by connected nodes, lack of addressing and presence of common point of entry such as: OBD-II [53] port, which allows access to all systems connected to the bus. The limited bandwidth (500 kbps) of the CAN bus [55] impose challenges on implementing robust authentication and encryption algorithms as they need much higher bandwidth and processing power. Efforts have been made to propose a security mechanism for the CAN protocol with a low communication overhead, which can provide security from masquerade and replay attacks [49]. This proposed security mechanism suggests each node will contain an identification table to compute MACs and each node will create a unique MAC for each receiver of its messages. This will also allow each node to manage how many MACs it needs to create and send in each message, authenticating each message with efficient use of bandwidth. Finally, this method implements a counter function. This is done by keeping a counter at the receiver node and sending nodes. In each message between nodes, the counter value will be sent in the payload which the receiving node will check if it matches the counter value in the node's memory. While receiving a message $\mathrm{M_k}$ sent by a sender $\mathrm{N_i}$, the receiver $\mathrm{N_j}$ will perform the step given in Fig. 24. Here f, C & A denotes the function to compute MAC, stored counter, computed MAC respectively.

The basic implementation techniques of countermeasures against the CAN based cyber-attacks are nearly identical in different applications where CAN is used as the primary communication medium between the nodes or ECUs, leading to a common hardware architecture. Thus, for most of the designs, software-based countermeasures are primarily independent of the nature of the application. However, any specific hardware-based countermeasure implementation can certainly depend on the hardware architecture of the system. As described earlier, the common port of entry to the CAN communication network in any motor vehicle including EVs is the OBD-II port. As it is commonly used by the attackers to launch the cyber-attacks on the system, a hardware-based protection scheme is proposed in [46], where it makes difficult for the attacker to gain physical access to this port. Realization of such countermeasures will require similar approach across the EVs if the physical hardware of the OBD-II port is same.

B. COUNTERMEASURES AGAINST FPGA BASED REMOTE SIDE-CHANNEL ATTACKS

Side-channel analysis (SCA) attacks have been known as a major threat to any unprotected cryptographic implementation in software and hardware, so as to the FPGA used as the main controller for our OBC application. In any SCA attack the attacker decodes the cryptographic keys of the FPGA logic block by examining the relation between the data/program processed and time/power/delay required for the same. Generic hardware countermeasures against Differential Power Analysis (DPA) attacks primarily need to decrease the relation between data processed by a major part of the cryptographic implementation and the actual power consumption or the time/delay required to process that function. Potential countermeasures to side channel-based attacks on FPGA system are one of these two categories: making the victim logic more resilient to side-channel attacks or making it more difficult for attackers to construct any power/delay monitoring circuits on an FPGA [56]. While it is a well-researched topic on how to make it difficult for any untrusted user to successfully launch a SCA attack, there are several options to achieve this goal:

- Reducing the Signal-to-Noise Ratio: This is a straightforward countermeasure where a specific part of the power traces is buried with lots of additive (Gaussian) noise making it complicated for an attacker to launch a practical DPA attack. One of the methods to inject noise in the power trace can be producing controlled short circuit on the FPGA for a very limited amount of time. This will increase the power consumption in the FPGA suddenly reducing the signal-to-noise ratio.
- Timing Disarrangement: DPA attacks operate on a high number of (key dependent) data points that are assumed to be sampled at exactly the same point of time. The attacker usually runs a series of alignment filters to overcome any intrinsic misalignment within the data processing, e.g., due to clock jitter or other operational variations. An effective countermeasure is to further randomize or shuffle the points in time when such attackable operations are processed. Of course, this method can also be overcome, requiring the attacker to use advanced filtering functions beyond simple peak alignment, such as complex integration and windowing methods.
- Signal Masking: An effective protection against DPA can only be when the attackable part of the signal stays completely hidden in the power trace. This can be done by applying random masks to the signal [57]

While it is a widely accepted fact that a single countermeasure cannot provide complete protection against the large variety of SCA attacks, a mix of all these countermeasures is typically required to provide the security against malicious SCA attacks on the FPGA used in the onboard charging (OBC) unit.

C. HARDWARE BASED DEFENSE MECHANISM

To protect the power electronic circuitry of the OBC system from any fatal cyberattack, we have proposed three major hardware-based countermeasures that can protect the hardware components of the system from getting damaged and to prevent the immediate risk associated with it. These measures are dynamic in nature and have very sharp response time, being effective to restrict the impact of the attack. Also, these are modelled in such a generic way that they can be used for any kind of OBC architecture as the possible modes of attacks/faults across the OBCs are very similar, which include sudden loss of load, loss of input, shoot-through or short circuit in a switching circuit etc. The implementation of the countermeasures does not depend on the circuit topology of the charger but still the designer can modify the response time of the countermeasures according to the nature of the sensors used, sensed data sampling rate of the main controller, and switching frequency of the converter, etc.

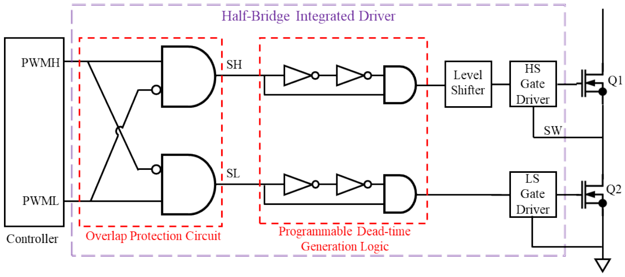

Half-Bridge Integrated Driver
PWMH
PWML
Controller
SH
SL
Overlap Protection Circuit
Programmable Dead-time Generation Logic
Level Shifter
HS Gate Driver
LS Gate Driver
SW
Q1
Q2

FIGURE 25. Additional digital logic circuit to prevent short circuit condition.

1) SHORT CIRCUIT/SHOOT THROUGH PROTECTION

Electrical short-circuit conditions can occur by either error in the control system or by interfering with the control system software to command the same phase-leg switches to turn on at the same time. The switch pairs that cause the DC or AC short-circuit conditions should not be turned on simultaneously at any time to protect the semiconductor switching devices and their related components of the PFC stage or DC-DC stage, as part of the OBC system. Generally, the non-overlapping switch operation is controlled and monitored by the DSP in software level, but this protection may not work if the DSP is overtaken by an attacker. The well-researched de-saturation protection scheme might be an effective solution for the overcurrent protection issue, but it has a limitation on the response time where high current switching devices are used, because of their shorter withstand time and high saturation current [20]. Therefore, to protect the devices in an OBC from a potential short circuit condition a more ground level, hardware-based protection circuit is proposed. It utilizes a simple external digital-logic gate circuitry shown in Fig. 25. between the controller and gate driver ICs which transfers gate signals to the switch pair of same leg while filtering out the overlapped portion. This circuit can be integrated inside the half-bridge gate driver as a part of its CMOS design while driving Si/SiC/GaN MOSFETs. In that case, a programmable dead time generation logic can also be implemented where the number of even inverter buffers (controlled by trimming) will provide the additional dead time between the high side and low side PWM signals.

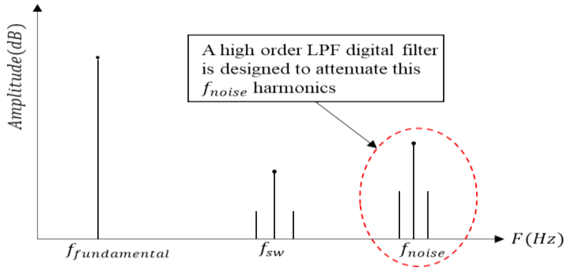


FIGURE 26. Harmonics in a sensed feedback signal under white noise attack.

The delay generated by one pair of inverter buffer inside the gate driver IC depends on the tunable RC parameters and can be made as small as 10 ns. Typically, in most of the applications, deadtime is kept between 1% and 3% of a complete switching cycle [58]. In our specific OBC application, a half-bridge gate driver from Silicon Labs (Si8271AB-IS1) is employed, which can generate a switching frequency up to 2MHz [59]. Therefore, while the logic circuit proposed in Fig. 25 can operate properly and safely upto 2MHz switching, the switching frequency in the design proposed in this work is set at 100kHz with a deadtime of 150ns (i.e., 1.5% of switching cycle).

2) DSP BASED IMPLEMENTATION OF DIGITAL FILTERS

Under the occurrence of noise attack, the voltage or current feedback signal of the OBC controller is injected with a white noise of high frequency with a certain amount of energy. In case of a high frequency noise injection, our proposed filtration scheme can retain the system stability under such an attack scenario. A harmonic distribution of a feedback sensor signal is shown in the Fig. 26.

For proper control operation of the DSP, the fundamental and switching frequency harmonics are to be retained in the processed signal. A lowpass filter (LPF) can be designed to mostly attenuate the f_{noise} frequency component and its harmonics. But such a filter design can be tricky if the f_{noise} and switching frequency (f_{sw}) are close by as we do not want to attenuate the f_{sw} harmonic component. That is the reason we need a higher-order (e.g. 4th to 6th) LPF to do this action with a higher roll-off rate and with minimal transition band. Designing an analog high order LPF will increase the circuit complexity as well as it is inefficient. Rather incorporating a digital IIR/FIR LPF inside the DSP will be helpful in this case as the implementation becomes easier and more flexible from a designer point of view. As an example of a casual discrete-time FIR filter of order N, the filtered signal is represented as follows:

$$y\,[n] = \sum\nolimits_{i=0}^{N} b_i \cdot x\,[\text{n-i}] \tag{4}$$

The cut-off frequency of the filter is to be decided depending on the converter switching frequency and the roll-off rate requirement. Such an approach will mitigate the effect of noise in the DSP feedback input signals and the control loop can work properly.

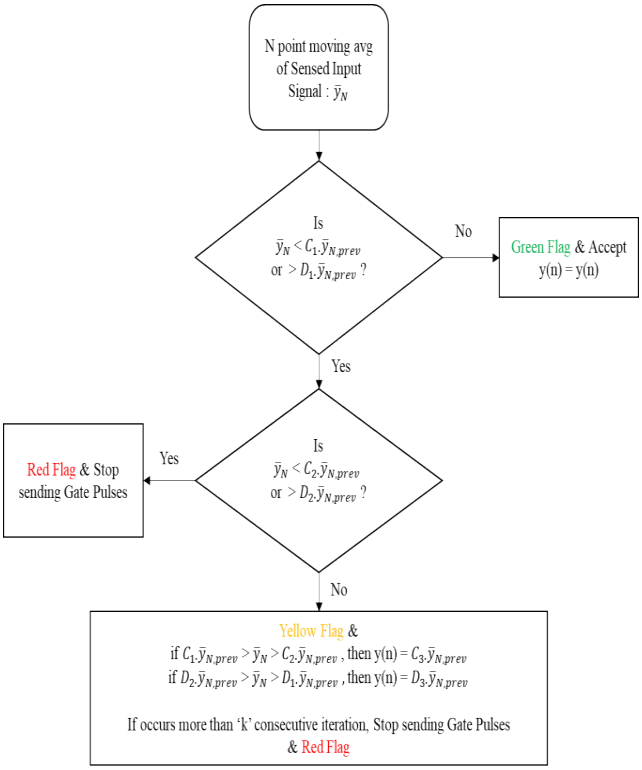

N point moving avg of Sensed Input Signal : $\bar{y}_N$
Is $\bar{y}_N < C_1.\bar{y}_{N,prev}$ or $> D_1.\bar{y}_{N,prev}$?
No
Green Flag & Accept y(n) = y(n)
Yes
Is $\bar{y}_N < C_2.\bar{y}_{N,prev}$ or $> D_2.\bar{y}_{N,prev}$?
Yes
Red Flag & Stop sending Gate Pulses
No
Yellow Flag &
if $C_1.\bar{y}_{N,prev} > \bar{y}_N > C_2.\bar{y}_{N,prev}$, then y(n) = $C_3.\bar{y}_{N,prev}$
if $D_2.\bar{y}_{N,prev} > \bar{y}_N > D_1.\bar{y}_{N,prev}$, then y(n) = $D_3.\bar{y}_{N,prev}$
If occurs more than ‘k’ consecutive iteration, Stop sending Gate Pulses & Red Flag

FIGURE 27. Flowchart of proposed algorithm to process sensed feedback signal in an OBC controller.

3) INTELLIGENT DATA PROCESSING ALGORITHM FOR SENSOR SIGNALS

In a data integrity attack targeting the voltage/current sensors of an OBC architecture, the sensor signal is modified by increasing/decreasing the original value by some coefficients. Here we have proposed to provide intelligence to the main controller/DSP of an OBC while processing the sensed data so that the attack does not grow fatal. As can be seen from eq. (1-2), at the time of such attack, the sensor signal observes a sudden change in its value. Also, in case of attacks with a sudden loss of load and loss of input, as mentioned earlier, the output current and input current will see a drastic change in their values. Taking this feature into account, we proposed a modified algorithm (Fig. 27) to process the ADC inputs of the DSP.

Let us assume, $y\,(n)$ is the sensed input current of the PFC stage of the OBC at a sampling instant; $\bar{y}_N$ is the moving average of the same variable (of last **N** samples) at the same instant. Whereas $\bar{y}_{N,prev}$ is the moving average calculated at the previous sampling instant. While running in steady state or during start up, the input AC phase current of an EV charger cannot see a sudden sharp increase/ decrease in its value due to system limitation. So, in normal operating condition, $\bar{y}_N$ and $\bar{y}_{N,prev}$ will not be much different considering an AC line frequency of 60Hz and sampling frequency in tens of kHz range. But while the system comes under sudden loss of input attack, $\bar{y}_N$ will change drastically than $\bar{y}_{N,prev}$. In case of data integrity attacks also, the input current sensor data can get manipulated resulting in a large difference between $\bar{y}_N$ and $\bar{y}_{N,prev}$. Here we are making decisions based on **N** point moving average to omit the possibility of an unwanted system transient causing wrong decision taken by this algorithm. In the flowchart, C_1, C_2, C_3 and $D_1, D_2, D_3$are simple coefficients where $0 < C_2 < C_1 \leq C_3 \leq 1$, which relates to a decreased sensor signal attack and $1 \leq D_3 \leq D_1 < D_2 < \infty$, which portrays an increased attack.

If there is a small tolerable difference between $\bar{y}_N$ and $\bar{y}_{N,prev}$ values, as presented by: $D_1.\bar{y}_{N,prev} < \bar{y}_N < C_1.\bar{y}_{N,prev}$, the DSP will take the sample data $y(n)$ as it is. But if the difference is extremely huge which indicates towards a potential attack on the sensed data i.e., $\bar{y}_N < C_2.\bar{y}_{N,prev}$ or $\bar{y}_N > D_2.\bar{y}_{N,prev}$, then the DSP will immediately go into a fault mode and will stop sending the pulses to the gate drivers. After certain time delay the converter can resume its operation again.

The last case where the difference is moderately huge and it cannot be confirmed if there is any attack, then the DSP will put up a yellow flag to that and will take the decision in following fashion: if $C_1.\bar{y}_{N,prev} > \bar{y}_N > C_2.\bar{y}_{N,prev}$, then y(n) $= C_3.\bar{y}_{N,prev}$, and if $D_2.\bar{y}_{N,prev} > \bar{y}_N > D_1.\bar{y}_{N,prev}$, then y(n) $= D_3.\bar{y}_{N,prev}$. If the algorithm results in this condition for 'k' consecutive iterations, then the DSP will hold a red flag and stop sending any PWM signal. Here 'k' can be decided based on the noise immunity and sampling time of the system. 'k' can be kept higher for a system with high sampling frequency and high degree of noise proneness and vice-versa holds. The values of C_3 and D_3 are to be decided so that the control loop does not lose its stability and a situation of overcurrent or overvoltage does not occur.

In this algorithm, the values of N, C_1, C_2, D_1, D_2 are to be decided by the designer keeping in mind the nature of the sensed signal that will be processed by the DSP. The values of C_1, C_2, D_1, D_2 will decide the sensitivity of the proposed algorithm. The response time will be more if N increases; at the same time, error magnitude will be less. In case of a loss of load attack, the response time should be very minimal, which can be achieved if we increase the output current sampling frequency and also, minimize the program execution time in the DSP, which is achieved by splitting the program into two parts: attack-check portion followed by the Main loop, as shown in Fig. 28.

In case of any cyber-attack detection by the proposed intelligence method, the main loop is completely bypassed and hence not executed, which blanks all the PWM signals within a fraction of loop execution time and thus expedites the shutdown process of the system.

Fig. 29 shows the simulation schematic for implementation of the proposed countermeasure scheme. The control modules as explained in Section II take in the sensed signals as inputs and provide gating pulses to the converters. The proposed algorithm is also implemented as a separate control module, which takes in all the sensed signals and provides a control decision signal (g*) for stopping the gate pulses. In principle, it acts as an enable/disable signal for the control modules. When a cyberattack is detected by the proposed algorithm, g∗ goes from high to low, thus blanking the gate pulses required to drive the converters.

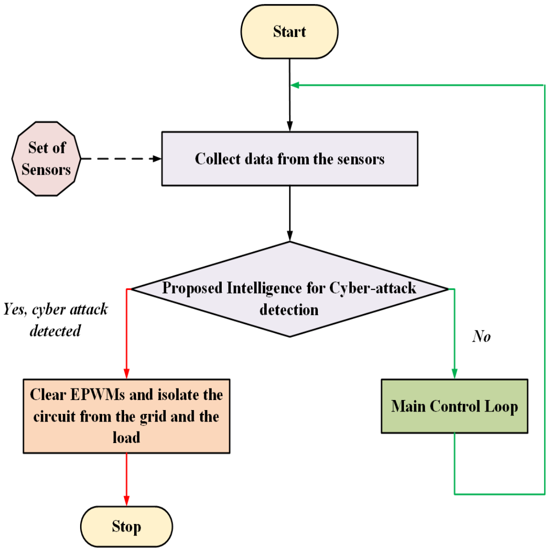

Start
Set of Sensors
Collect data from the sensors
Proposed Intelligence for Cyber-attack detection
Yes, cyber attack detected
No
Clear EPWMs and isolate the circuit from the grid and the load
Main Control Loop
Stop

FIGURE 28. Minimizing response time under attack condition.

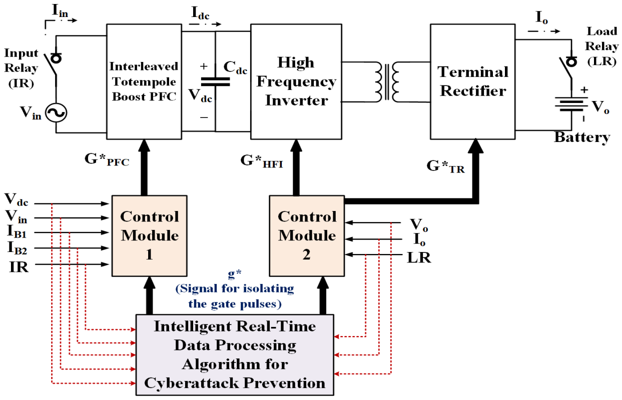


FIGURE 29. Simulation Schematic of the proposed cyberattack protection scheme.

The results from the implementation of this proposed algorithm under individual cyberattacks are shown in Fig. 30 and Fig. 31, where it protects the OBC from a loss of load attack and manipulation of output terminal voltage reference attack, respectively. As seen earlier in Fig. 18, under a loss of load attack the voltage across the output terminals of the OBC suddenly increases from its nominal value. While implementing our algorithm in the DSP we took C_1, C_2, D_1, D_2, k as 0.95, 0.8, 1.05, 1.2, 5 respectively. Once the loss of load attack takes place, the sensed output voltage tries to overshoot, and the algorithm ends up holding the Yellow Flag condition for consecutively 5 times. As a result, the controller stops sending the gate pulses to the converter switches and the output voltage drops down causing no over-voltage stress to the rectifier side semiconductor devices as well as the battery. Our prevention scheme is also verified (Fig. 31) under an Intra FPGA attack

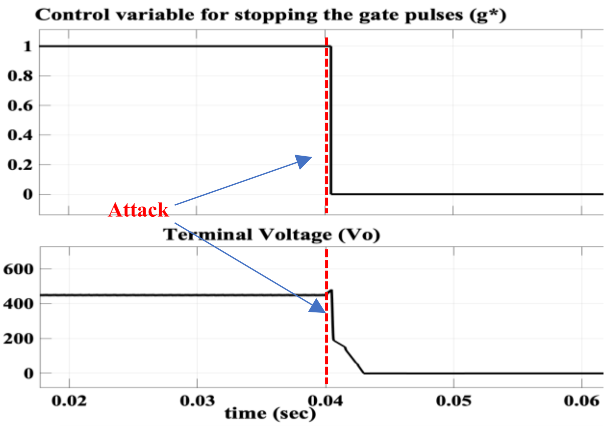


FIGURE 30. Prevention from a loss of Load attack: (Y-axis: Control Signal to stop PWMs (g*) – 0.5V/unit; Terminal Voltage (V_o) – 200V/unit, X-axis: Time – 0.01sec/unit).

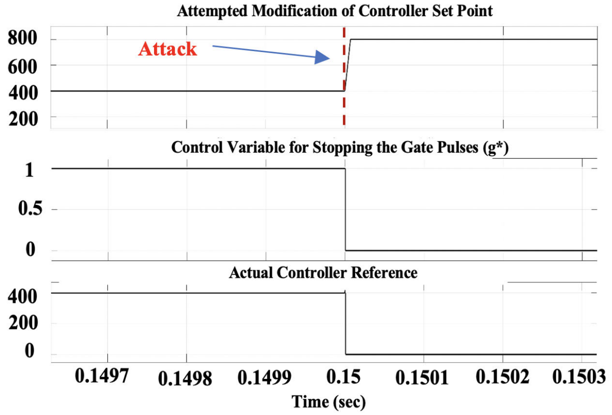


FIGURE 31. Prevention from attack based on manipulation of output terminal DC voltage reference (Y-axis: Terminal Voltage Reference (V_{ref}) – 200V/unit; Control Signal to Stop all PWMs (g*) – 1V/unit; Actual DC Terminal Voltage (V_o) – 200V/unit, X-axis: Time – 0.1ms/unit).

where the attacker intentionally changed the output voltage reference from 400 to 800V while the converter is running in normal condition. In this case, we implement our algorithm taking the output voltage reference as an input variable which increases suddenly leading an overshoot in actual OBC output voltage. Here also the algorithm detects the sudden increment in the output voltage reference and stops providing the PWMs to the switches. Thus, the converter components stay under their safe limit of operation.

Simultaneous pair of attacks on the OBC system impose challenge on any preventive measure as it needs a faster response time to keep the system under its safe operating limits. The performance of the proposed countermeasure is validated under two simultaneous cyberattacks on the OBC where it protects the system from the loss of load and output voltage reference manipulation attacks, as shown in Fig. 32. Fig. 32 suggests as the load is removed and the output DC voltage reference is maliciously changed from 400V to 800V at the same time, the actual terminal output voltage tries to shoot up. This voltage overshoot is detected as a sign of attack on the system by the algorithm and hence the OBC controller is directed to stop sending the gate pulses.

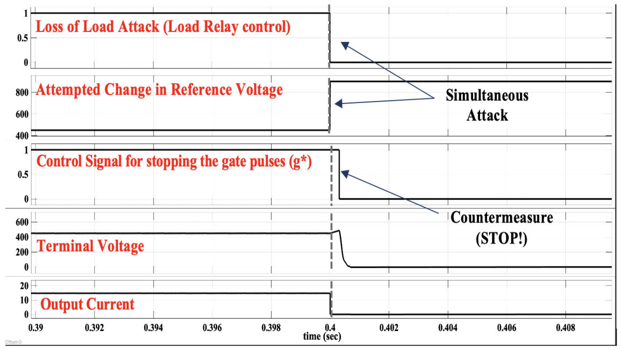


FIGURE 32. Prevention from simultaneous attacks: sudden loss of load & manipulation of output dc voltage reference (Y-axis: load relay control signal (attack) – 0.5V/unit; voltage control reference signal – 200V/unit; control signal to stop all PWMs (g*) – 0.5V/unit; terminal voltage– 200V/unit; output current – 10A/unit, X-axis: Time – 0.002s/unit).

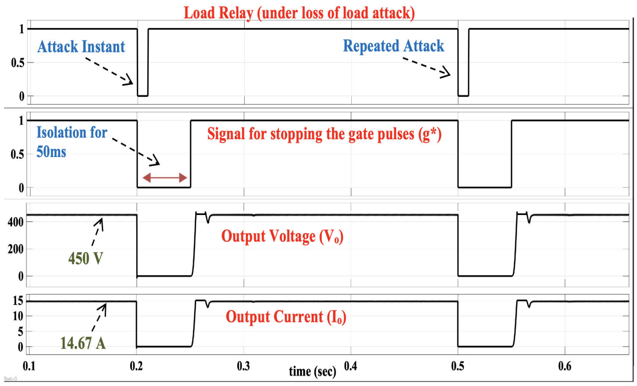


FIGURE 33. Prevention from repeated attacks: consecutive sudden loss of load attacks (y-axis: load relay control signal (attack) – 0.5V/unit; control signal to stop all PWMs (g*) – 0.5V/unit; terminal voltage (V_o) – 200V/unit; output current– 5A/unit, X-axis: Time – 0.1s/unit).

As observed in the results shown in Fig. 30-32, the proposed data processing algorithm protects the system by turning it completely off. However, it is also important for the system to come back to its initial operating state once the attack is mitigated. Thus, a similar scenario is also presented in Fig. 33 where repeated attacks (consecutive loss of load attacks) are mimicked on the system. Here, at t = 0.2sec, the first loss of load attack occurs (for a duration of 10ms), and proposed control scheme isolates the system by forcing both the output voltage and load current to zero. A delay of 50ms is then given for the DC link capacitor to discharge and the entire circuit to de-energize. Correspondingly, the system regains its initial state at t = 0.25 sec. Another loss of load attack occurs at t = 0.5 sec, and as observed in Fig. 33, the controller is able to isolate the system and is able to get it back to its normal operating condition.

This proposed intelligent data processing algorithm is thus verified and its usefulness is validated using our on-board charger model through simulation. The generic nature of the algorithm makes it applicable to any kind of OBC architecture as well as useful against across the range of the cyberattacks as the generalized structure of the algorithm only takes in the ADC inputs or the predefined control references (generated by supervisory control unit) as its input variables. The main program logic stores a wide variety of signatures of signal distortions under various types of attacks, and hence applies different analytical checks on the signal functions continuously to search for attacks (if any) at each sampling cycle. For different power electronic topologies, the converter operation or the control can be different in nature, but this proposed attack detection and countermeasure algorithm only looks for the signatures of cyber-attacks in its computational variables and does not interfere with the implemented control logic of the OBC system as a whole. Also, casual system faults caused due to other reasons than cyberattacks can be smartly distinguished by carefully choosing the algorithm coefficients i.e., N, C_1, C_2, D_1, D_2. In case of real EVs, the countermeasure can be implemented in the main control unit (DSP or FPGA) of the OBC. For the OBCs with different operating frequency and different numbers of sensed or control variables, the designer can tune the algorithm implemented in the controller differently as per the required response time and the nature of the working variables. Furthermore, prior to implementing such smart algorithms in any real EV's OBC, various computational and experimental trials have to be done to ensure safety as the top priority. This is because an EV has a vast number of sensed variables that can come under cyberattack and the algorithm coefficients need to be tuned for each of them.

VI. CONCLUSION

The scope of severe data integrity attacks on an EV onboard charger hardware from various loopholes present in its architectural design such as the vulnerable communication link - CAN, the decryptable FPGA logic blocks, etc. are carefully investigated and analyzed. Their adverse impacts on the various subsystems of the OBC i.e. the power electronic hardware including the semiconductor devices and their drivers, the passive components, and the battery have been analyzed through simulating a 6.6kW OBC test bench under the attack scenarios. To protect this system from such malicious attacks, three effective countermeasures have been proposed in this paper along with discussing the applicability of the existing countermeasures to protect the CAN bus from cyberattacks and FPGAs from SCA attacks. The short circuit protection circuitry can eliminate any possibility of the severe DC-link short-circuit failure. The noise injection-based attacks that are very common in any cyber-physical system can be taken care of by the implementation of high roll-off digital filters inside the controller. Lastly, the effectiveness of our proposed intelligence algorithm, which is implemented inside the converter controller to detect a data integrity attack on the OBC, is validated through results, where it successfully detects attacks such as loss of load and manipulation of voltage reference and immediately stops the converter operation. While the adoption of any one countermeasure cannot mitigate all the attacks but a combination of the existing and the proposed measures can protect the OBC system from a wide variety of potential cyberattacks. It is shown in our work that the adoption of advanced countermeasures to detect attacks early enough can prevent the attacks leading to hazardous failures, if not completely eliminate the possibility of such attacks.

REFERENCES

[1] R. Jurgesn, "Fuel-cell hybrid Evs," in *Electric Hybrid-Electric Vehicles: Fuel Cell Hybrid EVs*. Warrendale, PA, USA: SAE, 2011, p. 9.

[2] K. S. Grewal and P. M. Darnell, "Model-based EV range prediction for electric hybrid vehicles," in *Proc. Hybrid Electr. Vehicles Conf. (HEVC)*, London, U.K., 2013, pp. 1–6, doi: 10.1049/cp.2013.1895.

[3] Y. Zhang, J. He, and D. M. Ionel, "Modeling and control of a multiport converter based EV charging station with PV and battery," in *Proc. IEEE Transp. Electrific. Conf. Expo. (ITEC)*, Detroit, MI, USA, Jun. 2019, pp. 1–5, doi: 10.1109/ITEC.2019.8790632.

[4] K. Fahem, D. E. Chariag, and L. Sbita, "On-board bidirectional battery chargers topologies for plug-in hybrid electric vehicles," in *Proc. Int. Conf. Green Energy Convers. Syst. (GECS)*, Hammamet, Tunisia, Mar. 2017, pp. 1–6, doi: 10.1109/GECS.2017.8066189.

[5] A. Alsabbagh, X. Wu, and C. Ma, "Distributed electric vehicles charging management considering time anxiety and customer behaviors," *IEEE Trans. Ind. Informat.*, early access, Jun. 19, 2020, doi: 10.1109/TII.2020.3003669.

[6] H. H. Wu, A. Gilchrist, K. D. Sealy, and D. Bronson, "A high efficiency 5 kW inductive charger for EVs using dual side control," *IEEE Trans. Ind. Informat.*, vol. 8, no. 3, pp. 585–595, Aug. 2012, doi: 10.1109/TII.2012.2192283.

[7] B. Eberleh, F. von Borck, and S. Raiser, "A highly integrated, mass produced battery module as basis for various EV and HEV systems.," in *Proc. Electr. Power Train*, Leipzig, Germany, Nov. 2010, pp. 1–6, doi: 10.1109/EMOBILITY.2010.5668073.

[8] N. Trivedi, N. S. Gujar, S. Sarkar, and S. P. S. Pundir, "Different fast charging methods and topologies for EV charging," in *Proc. IEEMA Eng. Infinite Conf. (eTechNxT)*, New Delhi, India, Mar. 2018, pp. 1–5, doi: 10.1109/ETECHNXT.2018.8385313.

[9] T. Jalakas, I. Roasto, and D. Vinnikov, "Analysis of battery charger topologies for an electric vehicle," in *Proc. 13th Biennial Baltic Electron. Conf.*, Tallinn, Estonia, Oct. 2012, pp. 223–226, doi: 10.1109/BEC.2012.6376857.

[10] Z. Li, X. Yang, Y. Li, J. Li, B. Zhang, and T. Lei, "Design and implementation of a high-efficiency DC/DC converter for EVs charging basing on LLC resonant topology and silicon-carbide devices," in *Proc. IEEE Int. Power Electron. Appl. Conf. Exposit. (PEAC)*, Shenzhen, China, Nov. 2018, pp. 1–6, doi: 10.1109/PEAC.2018.8590636.

[11] Y. Chen, H. Zhang, C.-S. Shin, K.-H. Seo, S.-J. Park, and D.-H. Kim, "A comparative study of S-S and LCC-S compensation topology of inductive power transfer systems for EV chargers," in *Proc. IEEE 10th Int. Symp. Power Electron. Distrib. Gener. Syst. (PEDG)*, Xi'an, China, Jun. 2019, pp. 99–104, doi: 10.1109/PEDG.2019.8807684.

[12] V. Monteiro, J. G. Pinto, and J. L. Afonso, "Experimental validation of a three-port integrated topology to interface electric vehicles and renewables with the electrical grid," *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2364–2374, Jun. 2018, doi: 10.1109/TII.2018.2818174.

[13] S. Mousavian, M. Erol-Kantarci, L. Wu, and T. Ortmeyer, "A risk-based optimization model for electric vehicle infrastructure response to cyber attacks," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6160–6169, Nov. 2018, doi: 10.1109/TSG.2017.2705188.

[14] A. Zahedmanesh, D. Sutanto, and K. M. Muttaqi, "Analyzing the impacts of charging plug-in electric vehicles in low voltage distribution networks: A case study of utilization of droop charging control system based on the SAE J1772 standard," in *Proc. Australas. Universities Power Eng. Conf. (AUPEC)*, Melbourne, VIC, Australia, Nov. 2017, pp. 1–6, doi: 10.1109/AUPEC.2017.8282409.

[15] S. Rumale, H. A. Ashkar, T. Kerner, F. Koya, and M. Eitzenberger, "Design and implementation of an on-board vehicle CHAdeMO interface for Vehicle-to-Grid applications," in *Proc. IEEE Int. Conf. Power Electron., Smart Grid Renew. Energy (PESGRE)*, Cochin, India, Jan. 2020, pp. 1–6, doi: 10.1109/PESGRE45664.2020.9070445.

[16] E. Akakabota, G. Pillai, and M. Allison, "Supporting LV distribution network voltage using PV inverters under high EV penetration," in *Proc. 54th Int. Universities Power Eng. Conf. (UPEC)*, Bucharest, Romania, Sep. 2019, pp. 1–6, doi: 10.1109/UPEC.2019.8893498.

[17] C.-C. Lin, D.-J. Deng, C.-C. Kuo, and Y.-L. Liang, "Optimal charging control of energy storage and electric vehicle of an individual in the Internet of energy with energy trading," *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2570–2578, Jun. 2018, doi: 10.1109/TII.2017.2782845.

[18] L. Guo, B. Yang, J. Ye, H. Chen, F. Li, W.-Z. Song, L. Du, and L. Guan, "Systematic assessment of cyber-physical security of energy management system for connected and automated electric vehicles," *IEEE Trans. Ind. Informat.*, early access, Jul. 24, 2020, doi: 10.1109/TII.2020.3011821.

[19] M. S. Islam, M. Nadarajah, and K. Y. Lee, "Characterization of charging load for a large number of EV units in distribution grids," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Chicago, IL, USA, Jul. 2017, pp. 1–5, doi: 10.1109/PESGM.2017.8274570.

[20] Y. Park, O. C. Onar, and B. Ozpineci, "Potential Cybersecurity Issues of Fast Charging Stations with Quantitative Severity Analysis," in *Proc. IEEE CyberPELS (CyberPELS)*, Knoxville, TN, USA, 2019, pp. 1–7, doi: 10.1109/CyberPELS.2019.8925069.

[21] NERC. (Sep. 2019). *Lesson Learned—Risks Posed by Firewall Firmware Vulnerabilities*. Accessed: Aug. 8, 2020, from. [Online]. Available: https://www.eenews.net/assets/2019/09/06/document_ew_02.pdf

[22] R. Walton. (Aug. 15, 2019). *Simultaneous Hack of EV Chargers Could Cause Manhattan Blackout, NYU Researchers Find*. Accessed: Aug. 8, 2020, from. [Online]. Available: https://www.utilitydive.com/news/simultaneous-hack-of-ev-chargers-could-cause-manhattan-blackout-nyu-resear/560974/

[23] V. Monteiro, J. G. Pinto, and J. L. Afonso, "Operation modes for the electric vehicle in smart grids and smart homes: Present and proposed modes," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1007–1020, Mar. 2016, doi: 10.1109/TVT.2015.2481005.

[24] Z.-Y. Hou, P.-Y. Lou, and C.-C. Wang, "State of charge, state of health, and state of function monitoring for EV BMS," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Las Vegas, NV, USA, Aug. 2017, pp. 310–311, doi: 10.1109/ICCE.2017.7889332.

[25] D. Reeh, F. Cruz Tapia, Y.-W. Chung, B. Khaki, C. Chu, and R. Gadh, "Vulnerability analysis and risk assessment of EV charging system under cyber-physical threats," in *Proc. IEEE Transp. Electrific. Conf. Expo. (ITEC)*, Detroit, MI, USA, Jun. 2019, pp. 1–6, doi: 10.1109/ITEC.2019.8790593.

[26] P. Nespoli, D. Papamartzivanos, F. Gomez Marmol, and G. Kambourakis, "Optimal countermeasures selection against cyber attacks: A comprehensive survey on reaction frameworks," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 2, pp. 1361–1396, 2nd Quart., 2018, doi: 10.1109/COMST.2017.2781126.

[27] B. Yang, L. Guo, F. Li, J. Ye, and W. Song, "Vulnerability assessments of electric drive systems due to sensor data integrity attacks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 5, pp. 3301–3310, May 2020, doi: 10.1109/TII.2019.2948056.

[28] C. Tu, X. He, X. Liu, and P. Li, "Cyber-attacks in PMU-based power network and countermeasures," *IEEE Access*, vol. 6, pp. 65594–65603, 2018, doi: 10.1109/ACCESS.2018.2878436.

[29] M. Y. Metwly, M. S. Abdel-Majeed, A. S. Abdel-Khalik, R. A. Hamdy, M. S. Hamad, and S. Ahmed, "A review of integrated on-board EV battery chargers: Advanced topologies, recent developments and optimal selection of FSCW Slot/Pole combination," *IEEE Access*, vol. 8, pp. 85216–85242, 2020, doi: 10.1109/ACCESS.2020.2992741.

[30] M. Yilmaz and P. T. Krein, "Review of battery charger topologies, charging power levels, and infrastructure for plug-in electric and hybrid vehicles," *IEEE Trans. Power Electron.*, vol. 28, no. 5, pp. 2151–2169, May 2013, doi: 10.1109/TPEL.2012.2212917.

[31] Y.-F. Yao and Y.-R. Chen, "Analysis and design of One-Cycle-Controlled dual-boost power factor corrector," in *Proc. CES/IEEE 5th Int. Power Electron. Motion Control Conf.*, Shanghai, China, Aug. 2006, pp. 1–4, doi: 10.1109/IPEMC.2006.4778219.

[32] E. Sehirli and M. Altinay, "Input-output linearization control of single-phase buck-boost power factor corrector," in *Proc. 47th Int. Univ. Power Eng. Conf. (UPEC)*, London, U.K., Sep. 2012, pp. 1–6, doi: 10.1109/UPEC.2012.6398557.

[33] C.-C. Hua, L.-K. Chou, C.-W. Chuang, and C.-C. Chuang, "Interleaved voltage-doubler boost PFC with coupled inductor," in *Proc. 2nd Int. Conf. High Voltage Eng. Power Syst. (ICHVEPS)*, Bali, IN, USA, Oct. 2019, pp. 1–6, doi: 10.1109/ICHVEPS47643.2019.9011042.

[34] M.-H. Park, C.-O. Yeon, J.-I. Baek, Y. Jeong, G.-W. Moon, and J.-S. Park, "An improved current compensation method for high PF and low THD in digital boost power factor corrector," in *Proc. IEEE 3rd Int. Future Energy Electron. Conf.*, Kaohsiung, Taiwan, Jun. 2017, pp. 1065–1070, doi: 10.1109/IFEEC.2017.7992189.

[35] W. Yin, Z. Kai, and D. Jinping, "FPGA-based expanded circuit design for DSP signal processing," in *Proc. 5th Int. Conf. Intell. Syst. Design Eng. Appl.*, Hunan, China, Jun. 2014, pp. 511–516, doi: 10.1109/ISDEA.2014.121.

[36] M. Xie, Y. Jiang, J. Huang, and C. Wang, "Design and implementation of a seeker signal processor based on FPGA and DSP," in *Proc. 8th Int. Congr. Image Signal Process. (CISP)*, Shenyang, China, Oct. 2015, pp. 1411–1416, doi: 10.1109/CISP.2015.7408104.

[37] D. Jang, S. Han, S. Kang, and J.-W. Choi, "Communication channel modeling of controller area network (CAN)," in *Proc. 7th Int. Conf. Ubiquitous Future Netw.*, Sapporo, Japan, Jul. 2015, pp. 86–88, doi: 10.1109/ICUFN.2015.7182505.

[38] B. Yang, L. Guo, F. Li, J. Ye, and W. Song, "Impact analysis of data integrity attacks on power electronics and electric drives," in *Proc. IEEE Transp. Electrific. Conf. Expo (ITEC)*, Detroit, MI, USA, Jun. 2019, pp. 1–6, doi: 10.1109/ITEC.2019.8790574.

[39] E. Axell, P. Eliardsson, S. Tengstrand, and K. Wiklundh, "Power Control in Interference Channels with Class A Impulse Noise," in *IEEE Wireless Commun. Lett.*, vol. 6, no. 1, pp. 102–105, Feb. 2017, doi: 10.1109/LWC.2016.2634529.

[40] H. J. Jo, J. H. Kim, H.-Y. Choi, W. Choi, D. H. Lee, and I. Lee, "MAuth-CAN: Masquerade-Attack-Proof authentication for in-vehicle networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 2, pp. 2204–2218, Feb. 2020, doi: 10.1109/TVT.2019.2961765.

[41] Z. Xiang, H. Guangyu, and W. Zhigong, "Masquerade detection using support vector machines in the smart grid," in *Proc. 7th Int. Joint Conf. Comput. Sci. Optim.*, Beijing, China, Jul. 2014, pp. 30–34, doi: 10.1109/CSO.2014.15.

[42] K. M. Malik, H. Malik, and R. Baumann, "Towards vulnerability analysis of voice-driven interfaces and countermeasures for replay attacks," in *Proc. IEEE Conf. Multimedia Inf. Process. Retr. (MIPR)*, San Jose, CA, USA, Mar. 2019, pp. 523–528, doi: 10.1109/MIPR.2019.00106.

[43] K. Murakami, H. Suemitsu, and T. Matsuo, "Classification of repeated replay-attacks and its detection monitor," in *Proc. IEEE 6th Global Conf. Consum. Electron. (GCCE)*, Nagoya, Angola, Oct. 2017, pp. 1–2, doi: 10.1109/GCCE.2017.8229303.

[44] J. Zhao, J. Wang, and L. Yin, "Detection and control against replay attacks in smart grid," in *Proc. 12th Int. Conf. Comput. Intell. Secur. (CIS)*, Wuxi, China, Dec. 2016, pp. 624–627, doi: 10.1109/CIS.2016.0151.

[45] E. Strollo and A. Trifiletti, "A shared memory, parameterized and configurable in FPGA, for use in multiprocessor systems," in *Proc. 23rd Int. Conf. Mixed Des. Integr. Circuits Syst.*, Lodz, Poland, Jun. 2016, pp. 443–447, doi: 10.1109/MIXDES.2016.7529783.

[46] M. Zhao and G. E. Suh, "FPGA-based remote power side-channel attacks," in *Proc. IEEE Symp. Secur. Privacy (SP)*, San Francisco, CA, USA, May 2018, pp. 229–244, doi: 10.1109/SP.2018.00049.

[47] S. Gehrer and G. Sigl, "Reconfigurable PUFs for FPGA-based SoCs," in *Proc. Int. Symp. Integr. Circuits (ISIC)*, Singapore, Dec. 2014, pp. 140–143, doi: 10.1109/ISICIR.2014.7029535.

[48] N. Agrawal and S. Samanta, "Development of system-on-chip based digital control for power converter application," in *Proc. IEEE Int. Conf. Power Electron., Drives Energy Syst. (PEDES)*, Chennai, India, Dec. 2018, pp. 1–4, doi: 10.1109/PEDES.2018.8707515.

[49] C. Lin and A. Sangiovanni-Vincentelli, "Cyber-security for the controller area network (CAN) communication protocol," in *Proc. Int. Conf. Cyber Secur.*, Washington, DC, USA, 2012, pp. 1–7, doi: 10.1109/CyberSecurity.2012.7.

[50] H. M. Song, H. R. Kim, and H. K. Kim, "Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Kota Kinabalu, Malaysia, 2016, pp. 63–68, doi: 10.1109/ICOIN.2016.7427089.

[51] A. Groll and C. Ruland, "Secure and authentic communication on existing in-vehicle networks," in *Proc. IEEE Intell. Vehicles Symp.*, Xi'an, China, 2009, pp. 1093–1097, doi: 10.1109/IVS.2009.5164434.

[52] U. E. Larson, D. K. Nilsson, and E. Jonsson, "An approach to specification-based attack detection for in-vehicle networks," in *Proc. IEEE Intell. Vehicles Symp.*, Eindhoven, The Netherlands, 2008, pp. 220–225, doi: 10.1109/IVS.2008.4621263.

[53] S. Hartzell and C. Stubel, "Automobile CAN bus network security and vulnerabilities," Univ. Washington, Seattle, WA, USA, Tech. Rep., 2017. Accessed: Dec. 15, 2020. [Online]. Available: https://canvas.uw.edu/files/47669787/download

[54] *Federal Fleet Cybersecurity*. Accessed: Aug. 26, 2020. [Online]. Available: https://www.energy.gov/eere/femp/federal-fleet-cybersecurity

[55] S. Corrigan, "Introduction to the controller area network," Texas Instrum., Dallas, TX, USA, Appl. Rep. SLOA101A, Jul. 2008.

[56] M. C. Kisacikoglu, M. A. Rahman, K. Akkaya, and B. Akin, "Emerging cyber-pyhsical power electronics attacks in autonomous electric vehicles," in *Proc. IEEE CyberPELS (CyberPELS)*, Knoxville, TN, USA, 2019. Accessed: Dec. 15, 2020. [Online]. Available: http://mck.people.ua.edu/uploads/8/7/7/8/87787552/power_electronics_cyber_security_final1.pdf, doi: 10.1109/CyberPELS.2019.8925069.

[57] S. Ghandali, T. Moos, A. Moradi, and C. Paar, "Side-channel hardware trojan for provably-secure SCA-protected implementations," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 28, no. 6, pp. 1435–1448, Jun. 2020, doi: 10.1109/TVLSI.2020.2982473.

[58] R. Beiranvand, B. Rashidian, M. R. Zolghadri, and S. M. H. Alavi, "Optimizing the normalized dead-time and maximum switching frequency of a Wide-Adjustable-Range LLC resonant converter," *IEEE Trans. Power Electron.*, vol. 26, no. 2, pp. 462–472, Feb. 2011, doi: 10.1109/TPEL.2010.2068563.

[59] (Dec. 5, 2019). *Si8271AB-IS*. Accessed: Nov. 11, 2020. [Online]. Available: https://www.silabs.com/isolation/isolated-gate-drivers/si827x-isolated-gate-drivers/device.si8271ab-is

ASHWIN CHANDWANI (Student Member, IEEE) received the bachelor's degree in electrical engineering from Nirma University, Ahmedabad, India, in 2017. He is currently pursuing the Ph.D. degree with the Electrical Engineering Department, Arizona State University. He has two years of professional experience, working at ABB India Ltd., in the Solar and Electric Vehicle Infrastructure (EPPE) Department. He has served the project lead position for a product localization project of 100kW solar string inverter (PVS-100-TL). His current research interests include power electronic converters, advanced switching and modulation techniques, renewables energy resources, power quality compensation, distributed energy resources (DERs) integration to smart grid, and applications of machine learning in power systems.

SAIKAT DEY (Student Member, IEEE) received the B.Tech. degree in electrical engineering from the Indian Institute of Engineering Science and Technology (IIEST), Shibpur, India, in 2018. He is currently pursuing the Ph.D. degree in systems engineering with the Arizona State University–Polytechnic. From 2018 to 2020, he worked as a Power Electronics Design Engineer with Tagore Technology, India, where he developed some highly efficient and compact power electronic converter solutions with Tagore's GaN power products. His research interests include the design, control, and optimization of power electronic converters; and highly efficient and high-power density power converter solutions using wide bandgap (WBG) semiconductors.

AYAN MALLIK (Member, IEEE) received the B.Tech. degree in electrical engineering from the Indian Institute of Technology (IIT) Kharagpur, India, in 2014, and the M.S. and Ph.D. degrees in electrical engineering from the University of Maryland (UMD), College Park, MD, USA, in 2018. He is currently an Assistant Professor with Arizona State University. His current research interests include the design, modeling, control, and optimization of power electronic converters, characterizations and applications of wide bandgap (WBG) semiconductors, highly efficient and high-power density solutions for power conversions in the applications of more-electric-aircrafts, electric vehicles, wireless charging, and data centers. He has worked on research, development, and testing of regulated transformer rectifier units for more-electric-aircrafts, integrated bidirectional onboard charger design for electric vehicles, high density DC/DC conversion for data centers, and among many other projects dealing with power conversion in a wide range of power between mW and kW levels. He was a recipient of various awards and recognitions, including first place in Dean's Doctoral Student Research Award at UMD in 2019, the Distinguished Dissertation Award in the Department of Electrical and Computer Engineering (ECE) in 2019, the UMD's Invention of the Year Award in 2018, the Jimmy H. C. Lin Invention Award in 2018 in the ECE Department, the Best presentation Award in Applied Power Electronics Conference and Exposition (APEC) in 2018, the UMD's Outstanding Graduate Student Award in 2016, and among many others.