A Deep Learning Based Cyber Attack Detection Scheme in DC Microgrid Systems

Koduru Sriranga SUPRABHATH, Machina Venkata Siva PRASAD, Sreedhar MADICHETTY, and Sukumar MISHRA

***Abstract*—In this article, a dual deep neural network (DDNN) based cyber-attack detection and correction method for direct current microgrids (DCMG) are proposed. DCMG are prone to cyber-attacks through their sensors and communication links. The injection of false data packets in the cyber layer can disrupt the control objectives, leading to voltage instability and load sharing patterns. Therefore, detection and correction of malicious data is essential for the DC microgrid stability. In this article, a DDNN is designed with prediction and correction networks. The prediction network composed with one input layer, two hidden layers and one output layer. This network predicts the converter's duty by considering the input features as DC bus voltage and the reference voltage. The correction network also composed with one input layer, two hidden layers and one output layer. This network provides the duty corresponding to the attack by considering the input features as DC bus voltage, battery voltage and reference voltage. The output from the prediction and correction network are implanted to detect and correct the false data injection (FDI) attacks. However, for the training purpose, the data is collected by performing the various attack scenarios who is able to inject the false data and disrupt the stable operation of the system. The data is then used to train a neural network to detect a larger set of FDI attacks. The proposed scheme's effectiveness is verified by conducting the real-time experiments for various attack scenarios and its results are explored.**

***Index Terms*—Cyber-attack, DC microgrid, deep learning, FDI attack mitigation, supervisory control.**

Nomenclature

Z_{trans} $(i-i_{\text{neighbour}})$	Line impedance between i^{th} node and its neighbor
V_{dc1}	DC bus voltage of converter 1
V_{dc2}	DC bus voltage of converter 2
V_{dc3}	DC bus voltage of converter 3
P_{dc1}	DC bus power of converter 1
P_{dc3}	DC bus power of converter 3
P_{L1}	Power at load 1
P_{L2}	Power at load 2
P_{L3}	Power at load 3
P_{G}	Generated power
P_{L}	Load power
$b_{\text{control}} = 0$	Battery charging control mode
$b_{\text{control}} = 1$	Battery discharging control mode
$r_{\text{L,b}}$	Parasitic inductive resistance of converter
$r_{\text{C,b}}$	Parasitic capacitive resistance of converter
R_1	Series line resistance of converter
C_{b}	Capacitance of converter
L_{b}	Inductance of converter
V_{b}	Energy source for converter
Q_1	N-MOSFET-1 of converter
D_1	Internal N-MOSFET-1 diode of converter
Q_2	N-MOSFET-2 of converter
D_2	Internal N-MOSFET-2 diode of converter
H^2	Hidden layer 2
H^K	K^{th} hidden layer
Z_0^K	Bias value for K^{th} hidden layer in neural network
Φ^1	Weight matrix between X_{P} and H^1 in neural network
Φ^2	Weight matrix between H^1 and H^2 in neural network
Φ^3	Weight matrix between H^2 and Y_{P}
Y_{P}	Output of neural network
$g(\cdot)$	Activation function of neural network
Z_0^1	Bias for 1^{st} hidden layer
h_n^K	Bias for n^{th} node of K^{th} hidden layer
X_{c}	Input for the correction network
ΔV_{C}	Difference between i^{th} DC bus voltage and battery voltage
V_{REF}	Reference voltage
Y_{C}	Output of the correction network
Y_{final}	Sum of prediction and correction network
P	Set of training examples
α	Learning rate
n_0	No. of input layer nodes
n_1 , n_2	No. of hidden layer nodes ($n_1 = n_2 = n$)
S_i	Linear Sum of inputs along with weights for i^{th} layer
O_i	Actual output of the output neural network
$\hat{o}_i$	predicted output of the output neural network
E	Cost function of neural network

I. Introduction

MICROGRIDS are gaining attention in recent days due to its ability to integrate various distributed energy resources (DER). The aim of sustainable energy generation can be achieved by the implementation of microgrids. Microgrids are classified as DCMG's, alternate current microgrids (ACMG) and hybrid microgrids (HMG) [1]. Absence of reactive power in DCMG, majority of the loads are DC in nature and more close to the generation and reduction in transmission losses all these factors make DCMG more preferable over others. The basic control strategies that are implemented in DCMG are decentralized control, centralized or supervisory control and distributed control. Among these control strategies supervisory control is implemented in this article, although this control suffers with single point

Manuscript received June 14, 2022; revised August 31, 2022; accepted October 4, 2022. Date of publication June 30, 2023; date of current version April 20, 2023. This work was supported by Science and Engineering Research Board under Startup Research Grant SERB/SRG/2020/000269t. *(Corresponding author: Sreedhar Madichetty.)*

K. S. Suprabath, M. V. S. Prasad, and S. Madichetty are with Mahindra University, Hyderabad 500043, India (e-mail: srirangakoduru@gmail.com; mvspchocdary@gmail.com; sreedhar.803@gmail.com).

S. Mishra is with Indian Institute of Technology Delhi, Delhi 110016, India (e-mail: sukumarmiitdelhi@gmail.com).

Digital Object Identifier 10.24295/CPSSTPEA.2023.00012

failure it has high observability and controllability compared to other strategies. Supervisory control consists of central controller that control all the local controllers at each node.

A. Motivation

Cyber security is the most overseen parameter in the microgrid, but the ignorance on this aspect leads to substantial damage not only in physical aspects but also economic aspects as well. The possibility of cyber-attack is largely in the communication links and near the sensor. As the sensor data is taken as feedback and given to the control algorithm to process and the processed values are again sent back to the nodes as set points or reference values. In this entire closed loop control, communication layer is key through which all the data is being transmitted. Some of the most common cyber-attacks that attacker is likely to perform by intruding into the network layer are denial of service (DoS) attack [2], false data injection (FDI) attack [3], man in the middle attack (MITM) [4]. Among the various cyber-attacks, FDI attack is preferred attack by the attackers, as this attack can be performed both in network and physical layer [5]. The continuous monitoring of any malicious activities in the hardware converter level of the DCMG would be critical. FDI attack happens when an attacker tries to access the sensor information to falsify the data received at the controller end. To carry out a successful attack, the attacker should be able to intrude into the network or should be able to gain unauthorised access to the controller's arena; in either of these cases, the operation of the DCMG is disrupted.

B. Literature Review

In literature, various methodologies are proposed using various techniques to detect and mitigate the cyber-attacks in DCMG. Among those, state estimation (SE) techniques are commonly used techniques. In [6] authors has proposed distributed SE (DSE) algorithms, which mainly rely on the weighted least-square (WLS) approaches. Here, every time step estimation has to be performed with WLS, for which this topology can detect the false/bad data only within that time frame acquired. DSE technique suffers with inaccurate estimations and observability issues when the number of nodes and distribution networks increases in the system [7]. Apart from DSE, other attack detection and mitigation techniques in the literature are also discussed. FDI attack (FDIA) detection and quantification are implemented in [8] using signal temporal logic. This article monitors voltage and current signals within the predefined boundaries. A software-defined networking (SDN) architecture with limited numbers of nodes is investigated, the threat issues [9] and recovery from the threats is observed. However, the design of the SDN architecture for cyber-attack detection is very complex. Load curtailment mechanism is implemented in [10] to detect and mitigate the unconventional FDI attacks, having a considerably good impact on the economy. The game theory approach is discussed in [11], [12] to provide cyber security analysis for FDI attacks. Distributed control approach and the effect of the denial of service attack on the microgrids are discussed in [13].

C. System Configuration

As the industrial 4.0 evolution has made to integrate a lot of sensors and IOT devices into the system, the availability of data is humongous. If the available data is utilised in an effective way, there is a huge scope in improving the control and operation of the DCMG. Artificial Intelligence (AI) is the domain that uses data driven techniques for prediction and classification. In [14] the authors has discussed the applications of AI in power electronics and design of intelligent controllers. Machine learning and deep learning algorithms are used for attack detection and mitigation. Probabilistic neural network [15], K-nearest neighbors search [16], supervisory learning [17] etc., have been recently implemented for cyber-attack detection. Despite these promising and motivating solutions, the machine learning (ML) approaches lack accuracy and reliability and maloperate during sudden transients. On the other hand, the ability of the deep learning techniques to handle the system complexity improves the system reliability in transient conditions. In [18] authors implemented the artificial neural network (ANN) to implement the voltage control of DC-DC converter, in which training data is collected from model predictive controller for offline training and trained model is implemented in the voltage control of DC-DC converter. FDIA detection and mitigation is performed in [19], fault data is injected in DC bus voltage measured. ANN is used to estimate the fault injected and by considering the converter output voltage and output current as features and the predicted fault data as the output of ANN. The estimated fault value is negated from the faulty DC bus voltage. Therefore, in this article it implemented a dual deep network which predicts and corrects the false data independently and efficiently.

D. Key Contributions

The foremost contributions of the present paper are

1) Designing supervisory control architecture of three bus DCMG with DDNN controller in the primary control.
2) Developing AI enabled controller to control the operation of bi-directional converter.
3) Developing an neural network based algorithm to detect and mitigate the effect of FDIA on the sensors of DCMG.
4) Demonstrating the effectiveness of the algorithm for intermittent generations and dynamic loading in real time hardware setup.

E. Organization

The rest of this article is organized as follows: Section II analyses the modeling and working of the proposed system and explains, in detail, the control architecture of DCMG. The proposed dual deep learning technique and its algorithm is discussed in Section III. Section IV discusses results of the proposed methodology and the behaviour of the system is

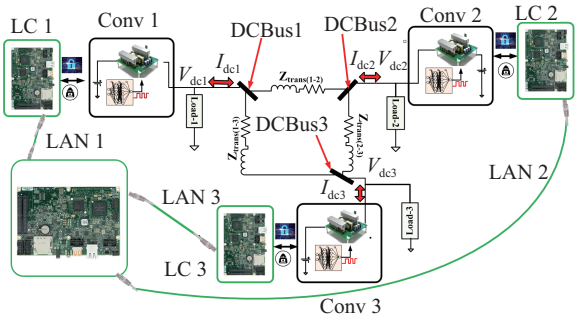

Fig. 1. Basic architecture of DDNN controlled supervisory control of DC microgrid system.

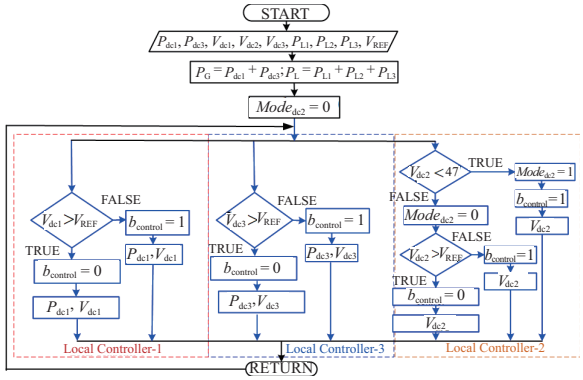

Fig. 2. Proposed control architecture for three bus DC microgrid system.

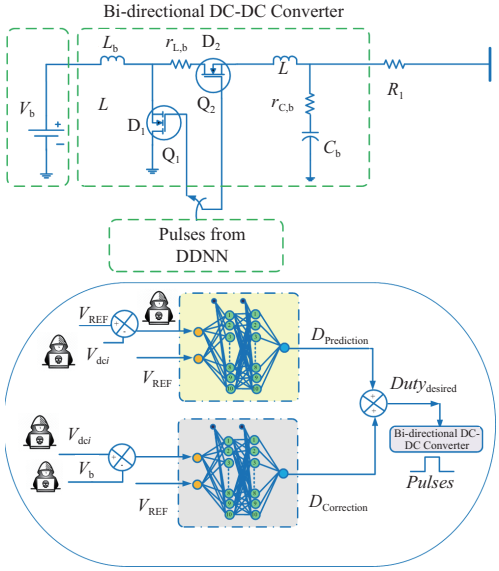

Fig. 3. DDNN controlled Bi-directional DC-DC converter.

analysed under various test conditions. Section V concludes summarizing the article and discussing the future scope for the proposed method.

II. Proposed Methodology

Model of three bus DCMG with a communication network is shown in Fig. 1. It consists of two primary energy sources with solar photovoltaic (SPV) system, and one hybrid energy storage system connected in ring main topology with three buses, i.e., DCbus1, DCbus2, and DCbus3, which can be extended to DCbus*n*. DCbus1 and DCbus2 are equipped with SPV panels and battery energy storage system (BESS). DCbus3 is connected with hybrid energy storage system (HESS); it is a combination of a battery and supercapacitor system. Supercapacitors are used to improve the battery life under sudden charge/discharge conditions. Their fast charge and discharge rates enable the DCMG to regain the DC bus voltage in very less time. Battery storage systems are equipped with bidirectional DC-DC converters, and their control is performed through DDNN. A bidirectional converter with DDNN control ensures the system's safety towards FDIA's. All the energy sources are connected with line impedance of 0.242 Ω and 0.21 µH per kilometre. The distance between DCbus1 to DCbus2 is 1 km, DCbus2 to DCbus3 is 2 km, and DCbus3 to DCbus1 is 3 km. V_{dci}, I_{dci}, Load–i are the DC bus voltage, DC bus current, and load at the ith bus, where i^{th} bus, where $i \in 1, 2, ..., n$. Furthermore, $Z_{trans(i-i_{neighbor})}$ is the line impedance between i^{th} system and its neighbor. Where LAN 1, LAN 2 and LAN 3 are the ethernet connections from supervisory control to local controller (LC) 1, local controller 2 and local controller 3 respectively. All these converters exchange information with supervisory control through local controllers. Local controller at i^{th} bus collects the information of the bus parameters such as bus voltage, bus current, power generated, state of charge (SOC) of the battery and load power. The collected information is sent to the supervisory controller, which decides the mode of operation. The detailed workflow of the developed control architecture is shown in Fig. 2. Initially the information of three buses, i.e., DC bus voltage (V_{dc1}, V_{dc2}, V_{dc3}), DC bus power (P_{dc1}, P_{dc3}) and load power (P_{L1}, P_{L2}, P_{L3}) are measured and stored. In the next step, it will check for the power balance between generated power (P_G) and load power (P_L), later it will start with mode initialization of dc bus-2 with default value '0'. When the modes are initialized, the information will be communicated to local controllers-1, 2 and, 3 simultaneously. In the local controllers 1 and 3, it will compare the bus voltage and reference voltage. If the dc bus voltage is greater than the specified reference voltage, the battery starts charging and else the battery will enter in to discharge mode and it is specifi by $b_{control}$. Where $b_{control}$ indicates the operation of the battery storage element in BESS and HESS. In local controller 2, initially it will compare the bus voltage with the critical grid voltage 47 V in this case. If bus voltage is less than the critical grid voltage then mode of the DCbus2 is made 1 (i.e., $Mode_{dc2} = 1$), super capacitor and battery combination acts in this case to compensate the bus voltage. Once V_{dc2} is greater then 47 V super capacitor is isolated, V_{dc2} is compared to V_{REF} and the battery operation is decided.

A. Bi-Directional DC-DC Converter Design With Dual Deep Neural Network Controller

DDNN controlled bi-directional DC-DC converter is shown in Fig. 3. A bi-directional converter facilitates to operate in

buck mode and boost mode. If the DC bus voltage is greater than the reference value, it operates in buck mode in which switch Q_2 is ON and power flows from grid to battery. If bus voltage is less than the reference value, it operates in boost mode in which switch Q_1 is ON and battery discharges to maintain the grid voltage to the reference value.

The switching of the bidirectional converter depends on the information received from the various voltage sensors of DCMG. Launching FDIA is the most convenient way for the attacker to disturb the system's harmony by modifying the sensor information. A dual deep neural network control mechanism is proposed to maintain the authenticity and safeguarding of sensor information.

A dual deep neural network mechanism is the combination of a prediction network and a correction network. The prediction network predicts the duty cycle of the switch by considering the input features as voltage sensor values received from the DC bus voltage sensor and reference voltages, respectively. The proposed prediction network contains an input layer, two hidden layers and an output layer. The input of the prediction network is shown in (1), where X_P is the input vector. ΔV_P is the difference between the reference voltage and i^{th} bus DC voltage, Z_b is the input layer bias initialized by the network.

$$X_P = \begin{bmatrix} Z_b \\ \Delta V_P \\ V_{REF} \end{bmatrix} \tag{1}$$

$$H^K = \begin{bmatrix} Z_0^K \\ h_1^K \\ h_2^K \\ \vdots \\ h_n^K \end{bmatrix} \tag{2}$$

$$\Phi^{(1)} = \begin{bmatrix} \Phi_{10}^1 & \Phi_{11}^1 & \Phi_{12}^1 \\ \Phi_{20}^1 & \Phi_{21}^1 & \Phi_{22}^1 \\ \vdots & \vdots & \vdots \\ \Phi_{n0}^1 & \Phi_{n1}^1 & \Phi_{n2}^1 \end{bmatrix} \tag{3}$$

$$\Phi^{(2)} = \begin{bmatrix} \Phi_{10}^2 & \Phi_{11}^2 & \Phi_{12}^2 & \cdots & \Phi_{1n}^2 \\ \Phi_{20}^2 & \Phi_{21}^2 & \Phi_{22}^2 & \cdots & \Phi_{2n}^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \Phi_{n0}^2 & \Phi_{n1}^2 & \Phi_{n2}^2 & \cdots & \Phi_{nn}^2 \end{bmatrix} \tag{4}$$

$$\Phi^{(3)} = \begin{bmatrix} \Phi_{10}^3 & \Phi_{11}^3 & \Phi_{12}^3 & \cdots & \Phi_{1n}^3 \end{bmatrix} \tag{5}$$

Hidden layers H^1 and H^2 contain 10 nodes each, hidden layer nodes and their weight matrices are represented in (2)–(5). k denotes the number of hidden layers, $Z_0^{(k)}$ is the bias voltage for hidden layer, Φ^1 is the weight matrix between X_P and H^1, Φ^2 is the weight matrix between H^1 and H^2, Φ^3 is the weight matrix between H^2 and output Y_P. At each layer, the weighted sum of the previous layer inputs and their related weights are passed through the activation function to obtain the node's output. (6) and (7) represent the outputs of H^1 and H^2 respectively, and (8), (9) represent the output of the prediction layer.

$$\left.\begin{aligned} Z_0^1 &= g\left(\Phi_{10}^1 \cdot Z_b + \Phi_{11}^1 \cdot \Delta V_P + \Phi_{12}^1 \cdot V_{REF}\right) \\ h_1^1 &= g\left(\Phi_{20}^1 \cdot Z_b + \Phi_{21}^1 \cdot \Delta V_P + \Phi_{22}^1 \cdot V_{REF}\right) \\ &\vdots \\ h_n^1 &= g\left(\Phi_{n0}^1 \cdot Z_b + \Phi_{n1}^1 \cdot \Delta V_P + \Phi_{n2}^1 \cdot V_{REF}\right) \end{aligned}\right\} \tag{6}$$

$$\left.\begin{aligned} Z_0^2 &= g\left(\Phi_{10}^2 \cdot Z_0^1 + \Phi_{11}^2 \cdot h_1^1 + \cdots + \Phi_{1n}^2 \cdot h_n^1\right) \\ &\vdots \\ h_n^2 &= g\left(\Phi_{n0}^2 \cdot Z_0^1 + \Phi_{n1}^2 \cdot h_1^1 + \cdots + \Phi_{nn}^2 \cdot h_n^1\right) \end{aligned}\right\} \tag{7}$$

$$Y_P = g\left(\Phi_{10}^3 \cdot Z_b^2 + \Phi_{11}^3 \cdot h_1^2 + \Phi_{12}^3 \cdot h_2^2 + \cdots + \Phi_{1n}^3 \cdot h_n^2\right) \tag{8}$$

$$Y_P = f\left(V_{REF}, V_{dci}\right) \tag{9}$$

To design a methodology to mitigate the FDIA, an attack is initiated near the DC bus voltage sensor. The faulty sensor information is passed through the prediction layer, and the output obtained from the prediction layer is inaccurate, destabilizing the system. To make the system robust and reliable during cyber-attacks and disturbance conditions, the correction network is designed to give the correction term to the output of the prediction network. The effect caused by the FDIA is neutralized. The input layer of the correction network has two features ΔV_c and V_{REF} and bias Z_b initialized by the network, inputs for the correction network are shown in (10).

$$X_C = \begin{bmatrix} Z_b \\ \Delta V_C \\ V_{REF} \end{bmatrix} \tag{10}$$

ΔV_c is the difference between i^{th} bus DC voltage and i^{th} bus battery voltage, Z_b is the input layer bias. Similar steps are followed as (2)–(8) to obtain the output of the correction network Y_C as shown in (11).

$$Y_C = f\left(V_{dci}, V_{bi}, V_{REF}\right) \tag{11}$$

To determine the correct duty cycle Y_{final} for the switching of bi-directional converter, the outputs of prediction network and correction network are summed as shown in (12).

$$Y_{final} = Y_P + Y_C \tag{12}$$

In the DDNN training phase, the model is trained for numerous epochs to adapt to adverse scenarios such as FDIA, intermittent source and irregular loading conditions. Weight updation in each epoch is performed using the gradient descent optimization technique. The gradient descent technique uses the backpropagation method to update the weights. The detailed working of the backpropagation method for feedforward networks is shown in the algorithm-I.

Here, S_n is the linear sum of product of all the previous layer node outputs and their corresponding weights, where $n = 1, 2, 3$. $\hat{O}_i$ is predicted output of the network and O_i is the actual output of the network. E is the cost function, Z is the bias value.

Algorithm 1: Backpropagation algorithm for feedforward networks

Data: a set of training examples P, learning rate α
Result: optimize weights and bias units
Initialize weights randomly;
Creating a feedforward network with n_o input nodes, $n_1 = n_2 = n$ hidden layer nodes and n_3 output nodes;
while repeat till convergence **do**
  while performing feed forward neural network **do**
    $S_1 = \Phi^1 * X + Z_b$;
    $H^1 = f(S_1)$;
    $S_2 = \Phi^2 * H^1 + Z_0^{(1)}$;
    $H^2 = f(S_2)$;
    $S_3 = \Phi^3 * H^1 + Z_0^{(2)}$;
    $Y = f(S_3) = \hat{O}_i$;
  end
  while Compute cost function by mean squared error **do**
    $\text{cost}(E) = \frac{1}{2P}\sum_{i=1}^{P}\left|\hat{O}_i - O_i\right|^2$
  end
  while update weights using gradient descent in generalised manner **do**
    $\Phi^3 = \Phi^3 - \alpha * \left(\frac{\partial Y}{\partial \Phi^3} * \frac{\partial E}{\partial Y}\right)$;
    $\Phi^2 = \Phi^2 - \alpha * \left(\frac{\partial H^2}{\partial \Phi^2} * \frac{\partial Y}{\partial H^2} * \frac{\partial E}{\partial Y}\right)$;
    $\Phi^1 = \Phi^1 - \alpha * \left(\frac{\partial H^1}{\partial \Phi^1} * \frac{\partial H^2}{\partial H^1} * \frac{\partial Y}{\partial H^2} * \frac{\partial E}{\partial Y}\right)$;
  end
  while updating bias using gradient descent in generalised form **do**
    $Z \leftarrow Z - \alpha \sum_{i \in \beta}\left(\Phi^T H^{(k)} + Z - O_{(i)}\right)$;
  end
end

III. Results

A. Simulation

The design of primary control and secondary control of DCMG is performed under supervisory control mechanism with ring topology. The reference bus voltage is maintained at 48 V. The two primary objectives of the DCMG are to maintain the DC bus voltage regulation, i.e., at 48 V and to maintain the proportional load sharing. Supervised control DCMG is simulated in MATLAB 2022a platform. Fig. 4(a) shows the amount of power generated by the SPV sources at DCbus1, DCbus3 and Fig. 4(b) shows the total load demand. It can be observed from Fig. 4 that from 1 s to 2.5 s power demanded by the load is greater than the power generated from the SPV sources. At this instant, the BESS and HESS will contribute to meet the load demand.

1) DC bus voltage regulation: Fig. 5(a), (b), (c) shows the voltages of DCbus1, DCbus2, and DCbus3 respectively, which are maintained at a constant reference voltage around 48 V. For the time period between 1 s to 2.5 s there is decrease in power generated which is below the load demand and between 3 s to 4 s there is sudden increase in the load demand, in either of the cases the DC bus voltages are in the range of 47 V to 48 V, the variation is around 2%. According to IEEE standards the acceptable range of DC bus voltage regulation is ±5%.

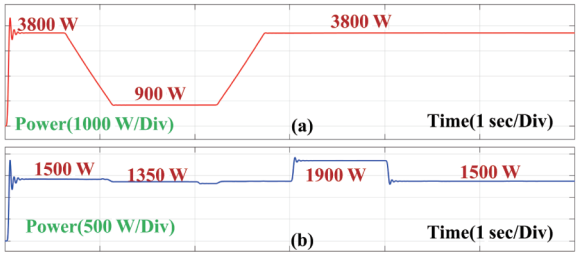

Fig. 4. (a) Power generated from PV sources (b) Load power demanded.

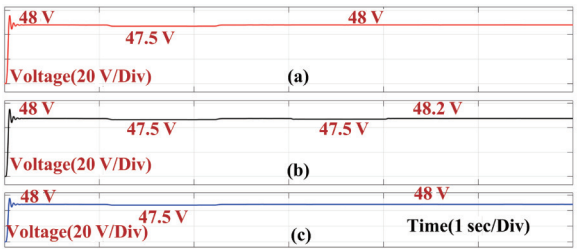

Fig. 5. (a) DCbus1 voltage (b) DCbus2 voltage (c) DCbus3 voltage.

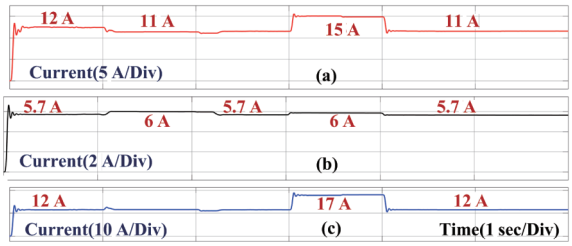

Fig. 6. (a) DCbus1 current (b) DCbus2 current (c) DCbus3 current.

2) Proportional load sharing: Fig. 6(a), (b), (c) shows the load sharing of DCbus1, DCbus2, and DCbus3 respectively. From Fig. 4 it can be observed that during the time period 3 s to 4 s the sudden increase in load demand is shared proportionally between DCbus1 and DCbus3 which are the generating sources. DCbus1 current is increased from 11 A to 15 A and DCbus3 voltage is increased from 12 A to 17 A. DCbus2 HESS is contributing a constant load of around 6 A.

3) FDI attack on DCbus1 voltage sensor: To analyse the performance of the proposed methodology under FDIA conditions, faulty data is injected near the DCbus1 voltage sensor. The input values received by the bidirectional converter are faulty values and consequently it effects the switching of the bidirectional converter.

Fig. 7 shows the voltage regulation of DCbus1 during the FDIA. From Fig. 7(a) it can be observed that the attack is launched on the sensor between 3 s to 5 s by injecting a faulty

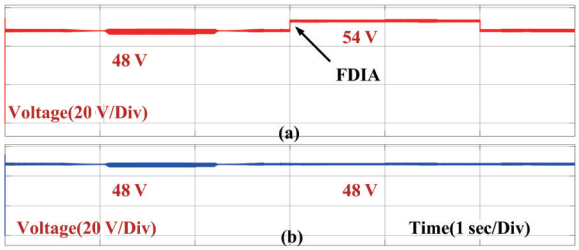

Fig. 7. (a) DCbus1 voltage sensor during FDIA (b) DCbus1 voltage.

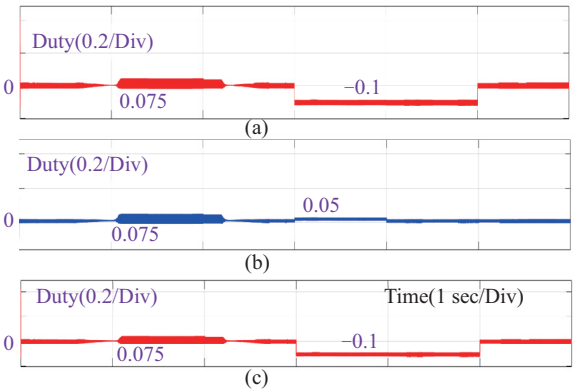

Fig. 8. (a) converter 1 correction network output (b) converter 2 correction network output (c) converter 3 correction network output.

data of 6 V. During this attack period, the DCbus1 voltage remained constant around 48 V as shown in Fig. 7(b).

4) Detection of FDI attack on DC bus voltage sensors: Role of correction network in the proposed methodology is to generate the correction factor to compensate error produced by the system dynamics or by FDI attaks. Detection of the FDI attacks on the bus voltage sensors can be achieved by monitoring the output of the correction network. Output of the correction network of converter 1, converter 2 and converter 3 are shown in Fig. 8(a), (b) and (c). FDI attack is launched on the DC bus voltage sensor 1 and DC bus voltage sensor 3 from 3 s to 5 s. Grid disturbances are observed between 1 s to 2.5 s, during grid disturbance, the output of the correction network is observed to be around 0.075 as shown in Fig. 8(a), (b) and (c). When an FDIA is launched on the DCbus1 and DCbus3 voltage sensors, the drastic change in the output of the correction network is observed as −0.1 which is shown in Fig. 8(a) and (c), whereas output of correction network of DCbus2 voltage remains positive around 0.05 as the sensor is attack free. Therefore, by monitoring the level and behaviour of the correction network output, FDI attacks can be detected and differentiated from system disturbances.

5) FDI attack on DCbus1 and DCbus3 voltage sensors: To test the robustness of the proposed methodology, FDI attack is performed on the multiple voltage sensors at same instant. In this test case, FDI attack is launched on the DCbus1 voltage sensor and DCbus3 voltage sensor as shown in Fig. 9(a) and (c) respectively by injecting false data of 6 V at same time period, i.e., from 3 s to 5 s. During this faulty period, the DC bus voltages of bus1 and bus3 are maintained constant at 48 V as shown in Fig. 9(b) and (d). This concludes that the proposed methodology for FDI attack mitigation is efficient during the attack scenarios, for individual sensor attack and multiple sensor attacks. Also, the designed system is tested under the intermittent source generations and dynamic load variations.

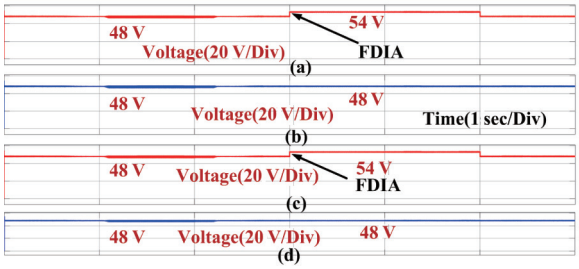

Fig. 9. (a) DCbus1 voltage sensor during FDIA (b) DCbus1 voltage (c) DCbus3 voltage sensor during FDIA (d) DCbus3 voltage.

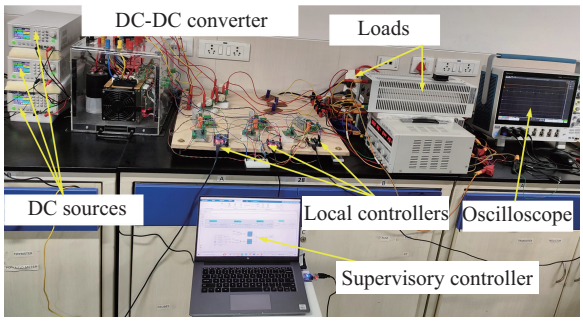

Fig. 10. Real time hardware setup of 3 Bus DC Microgrid.

TABLE I
DESIGN SPECIFICATIONS OF 3 BUS DC MICROGRID

Parameters	Value	Quantity
Input voltage (V_b)	50−62 V	3
Output voltage (V_o)	36−48 V	3
Output current (I_o)	0−15 A	3
Inductor (L_b)	720 μH	3
Capacitor (C_b)	470 μF	3
Load (R)	50 Ω, 5 A	3

B. Hardware Implementation

Real time implementation of DC microgrid is performed, 3 bus DCMG is setup in ring main topology. As shown in Fig. 10 three micro-controllers are used as the local controllers for each converter and designed DDNN algorithm is implemented in PC which acts as the supervisory controller, the measured values from the sensors will be collected into supervisory control algorithm and the pulses generated from the algorithm is given to the local controllers of each converter. The specifiations of DC microgrid converters are shown in Table I.

1) DC bus voltage regulation: For the input of 60 V as each

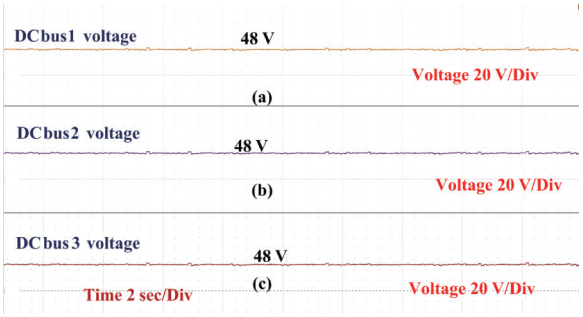

Fig. 11. (a) DCbus1 voltage (b) DCbus2 voltage (c) DCbus3 voltage.

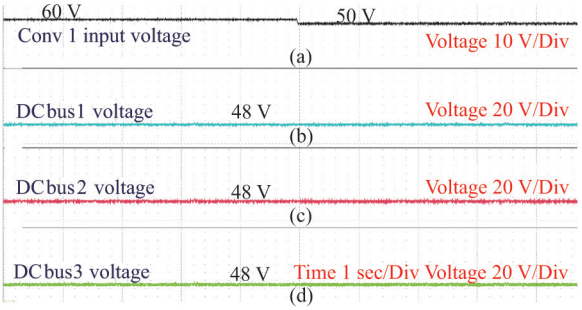

Fig. 12. (a) converter 1 input voltage (b) DCbus1 voltage (c) DCbus2 voltage (d) DCbus3 voltage.

converter input, the DDNN algorithm is implemented to control the switches of the converter and obtain the reference bus voltage of 48 V. Fig. 11(a)–(c) indicates the DC bus voltages of bus1, bus2 and bus3 respectively which are same as the reference voltage value. This shows that the algorithm is working effectively for DC voltage regulation.

2) Source voltage change at bus1: Considering the possibility of intermittency in renewable sources, the proposed technique is validated for source changes. Initially the input voltage of the converters is maintained at 60 V later source value is changed for 50 V at 5 s as shown in Fig. 12(a). It is observed from Fig. 12(b)–(d) that the bus voltages of each bus remained constant at 48 V.
3) Load changes at DCbus1: To examine the working of the proposed algorithm for dynamic loading conditions, load-1 connected to DCbus1 is changed from 2 A to 1.5 A at 4.5 s, and then increased to 2.2 A and further to 2.7 A at 7.5 s and 13.5 s respectively as shown in Fig. 13(a). In all these load changing conditions the bus1 voltage is remained constant at reference value. This shows that the system designed is resilient towards load changes.
4) FDI attack at bus2 voltage sensor: A cyber-attack scenario is considered in evaluation of the algorithm by implementing FDI attack on bus1 voltage sensor and bus2 voltage sensor individually, a fault data in addition to the sensor data is given to the controller, sensor data falsification is performed before giving to the controller. Fig. 14(a) shows the sensor voltage in which a falsified data of 7 V is injected at DCbus2 voltage sensor. Even though a FDI attack is performed near bus2 the DCbus2 voltage remains constant

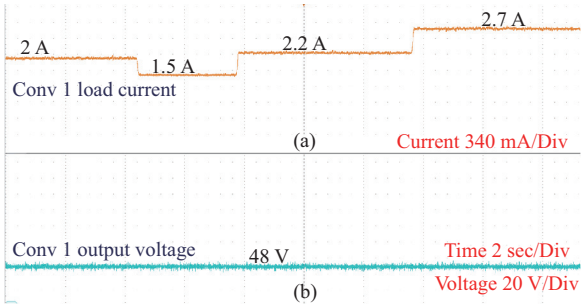

Fig. 13. (a) DCbus1 load current (b) DCbus1 voltage.

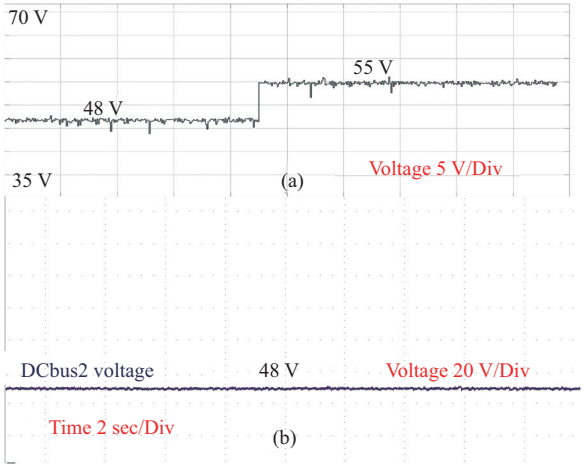

Fig. 14. (a) DCbus1 voltage sensor waveform (b) DCbus1 voltage.

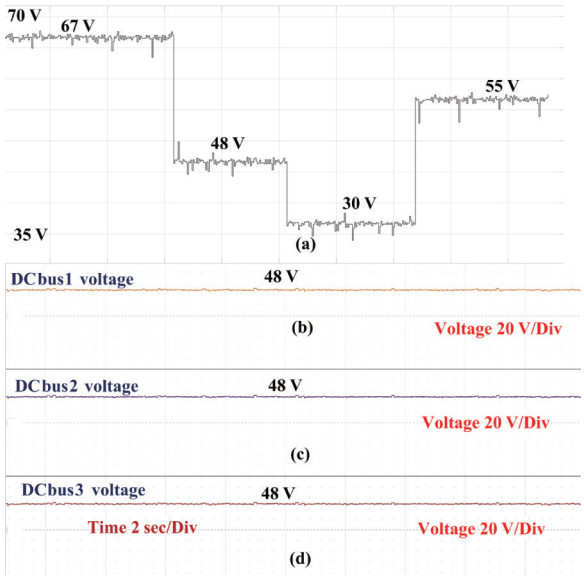

Fig. 15. (a) DCbus1 voltage sensor waveform (b) DCbus1 voltage (c) DCbus2 voltage (d) DCbus3 voltage.

without any deviations as shown in Fig. 14(b).

5) Multiple FDI attacks at bus1 voltage sensor: Time varying FDI attack is performed on DCbus1 voltage sensor, where the data with both positive and negative amplitude is injected as shown in Fig. 15(a). Even though there are

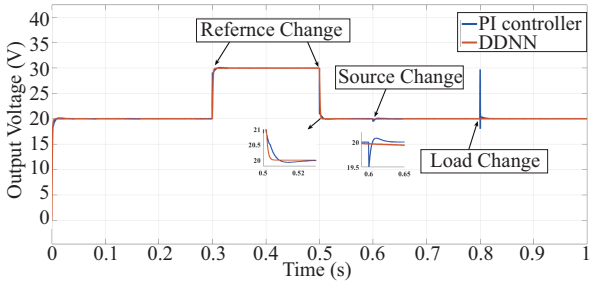

Fig. 16. DDNN controller vs. PI controller during reference change, source change and load change.

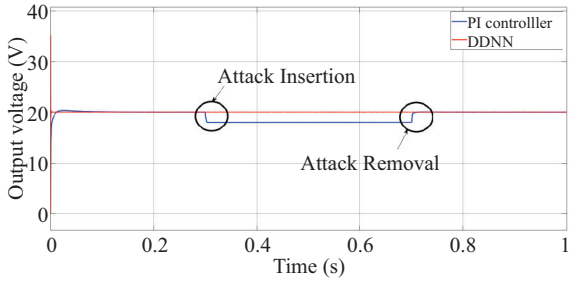

Fig. 17. DDNN controller vs. PI controller during reference change, source change and load change.

multiple FDI attacks with large amplitudes, a constant dc bus voltages are observed from Fig. 15(b)–(d).

C. Comparative Study

To analyze the effectiveness of the proposed scheme, AI based DDNN controller is compared with the traditional Proportional-Integral (PI) controller. PI controller is widely used in the industry because of its simplicity and effective performance, but PI controller tuning mechanism is very difficult task especially when the system needs to give better performance in both steady state and transient state. PI controller is also very sensitive towards the parametric changes in the circuit which makes the controller dependent on the circuit parameters. Use of PI controller limits the operation to a specific range of values and fixed ratings, small variations in the component ratings like inductor and capacitor due to ageing effect or environmental changes will effect the performance of the controller. To overcome the limitations of the PI controller, AI based controller is designed.

To analyze the transient performance of the designed DDNN controller and PI controller, source change, load change and reference changes are considered. From Fig.16 it can be observed that at 3 s reference value is changed from 20 V to 30 V and again changed to 20 V at 5 s, source change is performed at 6 s and load change at 8 s. During this system changes, the performance of PI controller and DDNN controller are analyzed. It is observed that the DDNN controller gives best results compared to PI controller during all system changes. The comparison between PI and DDNN is performed during FDIA scenario, information from the output voltage sensor is attacked and falsified before reaching the controller. The falsified information is fed to the controller and output voltage is observed. From Fig. 17 it can be seen that false data is injected at 0.3 s and false data removal at 0.7 s during this attack scenarios PI controller is unable to maintain the output voltage as reference voltage whereas no deviation from the reference voltage is found for DDNN controller. From this comparative studies it can be concluded that DDNN controller performs better than PI controller during system changes and able to detect and mitigate FDI attack.

IV. Conclusion

A dual deep neural network methodology is proposed to control the operation of DCMG and mitigate the FDI attacks. It is observed that the proposed methodology achieves voltage regulation and proportional load sharing during normal operating conditions. Also, the working of the proposed scheme under the FDI attacks is demonstrated. The methodology is tested for FDI attacks on one sensor individually and multiple sensors simultaneously. It can be proclaimed that the proposed methodology is resilient toward FDI attacks, and works efficiently during fault conditions. The amount of deviation observed during all the disturbance conditions is around ±2%. It can be concluded that the proposed methodology is effective in DCMG control and fault resilience. Implementing deep learning in DCMG control and cyber-attack mitigation can be further applied to distributed control. Advanced AI techniques like reinforcement learning can be implemented further to make our system more reliable and intelligent.

References

[1] A. Mittal, A. Rajput, K. Johar, and R. Kandari. Microgrids, their types, and applications. in *Microgrids*. [Online]. 2022, pp. 3–40. Available: https://www.sciencedirect.com/science/article/pii/B9780323854634000083#!

[2] Y. Shen, M. Fei, and D. Du, "Cyber security study for power systems under denial of service attacks," in *Transactions of the Institute of Measurement and Control*, vol. 41, no. 6, pp. 1600–1614, Apr. 2019.

[3] Q. Wang, W. Tai, Y. Tang, and M. Ni, "A review of the false data injection attack against the cyber physical power system," in *IET Cyber-Physical Systems: Theory & Applications*, vol. 4, no. 2, pp. 101–107, Jun. 2019.

[4] P. Wlazlo, A. Sahu, Z. Mao, H. Huang, A. Goulart, K. Davis, and S. Zonouz, "Man-in-the-middle attacks and defense in a power system cyber-physical testbed," in *IET Cyber-Physical Systems: Theory & Applications*, vol. 6, no. 3, pp. 164–177, Feb. 2021.

[5] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," in *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp.1630–1638, Jul. 2017.

[6] F. C. Schweppe and J. Wildes, "Power system static-state estimation, part I: exact model," in *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-89, no. 1, pp. 120–125, Jan. 1970.

[7] D. Della Giustina, M. Pau, P. A. Pegoraro, F. Ponci, and S. Sulis, "Electrical distribution system state estimation: measurement issues and challenges," in *IEEE Instrumentation & Measurement Magazine*, vol. 17, no. 6, pp. 36–42, Dec. 2014.

[8] O. A. Beg, L. V. Nguyen, T. T. Johnson, and A. Davoudi, "Signal temporal logic-based attack detection in DC microgrids," in *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 3585–3595, Jul. 2019.

[9] D. Jin, Z. Li, C. Hannon, C. Chen, J. Wang, M. Shahidehpour, and C. W. Lee, "Toward a cyber resilient and secure microgrid using software-defined networking," in *IEEE Transactions on Smart Grid*, vol. 8, no. 5,

pp. 2494–2504, Sept. 2017.
[10] T. R. B. Kushal, K. Lai, and M. S. Illindala, "Risk-based mitigation of load curtailment cyber attack using intelligent agents in a shipboard power system," in *IEEE Transactions on Smart Grid*, vol. 10, no. 5, pp. 4741–4750, Sept. 2019.
[11] N. Nikmehr and S. M. Moghadam, "Game-theoretic cybersecurity analysis for false data injection attack on networked microgrids," in *IET Cyper-Physical Systems: Theory & Applications*, vol. 4, no. 4, pp. 365–373, Dec. 2019.
[12] W. Cai, R. Shea, C. -Y. Huang, K. -T. Chen, J. Liu, V. C. Leung, and C. -H. Hsu, "A survey on cloud gaming: Future of computer games," in *IEEE Access*, vol. 4, pp. 7605–7620, Aug. 2016.
[13] M. Chlela, D. Mascarella, G. Joos, and M. Kassouf, "Fallback control for isochronous energy storage systems in autonomous microgrids under denial-of-service cyber-attacks," in *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4702–4711, Sept. 2018.
[14] S. Zhao, F. Blaabjerg, and H. Wang, "An overview of artificial intelligence applications for power electronics," in *IEEE Transactions on Power Electronics*, vol. 36, no. 4, pp. 4633–4658, Apr. 2021.
[15] D. Gerbec, S. Gasperic, I. Smon, and F. Gubina, "Allocation of the load profiles to consumers using probabilistic neural networks," in *IEEE Transactions on Power Systems*, vol. 20, no. 2, pp. 548–555, May 2005.
[16] A. A. Majd, H. Samet, and T. Ghanbari, "K-NN based fault detection and classification methods for power transmission systems," in *Protection and Control of Modern Power Systems*, vol. 2, no. 2, pp. 359–369, Dec. 2017.
[17] H. Wang, J. Ruan, G. Wang, B. Zhou, Y. Liu, X. Fu, and J. Peng, "Deep learning-based interval state estimation of AC smart grids against sparse cyber attacks," in *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4766–4778, Nov. 2018.
[18] H. S. Khan, I. S. Mohamed, K. Kauhaniemi, and L. Liu, "Artificial neural network-based voltage control of DC/DC converter for DC microgrid applications," in *2021 6th IEEE Workshop on the Electronic Grid (eGRID)*, New Orleans, LA, USA, 2021, pp. 1–6.
[19] M. R. Habibi, H. R. Baghaee, F. Blaabjerg, and T. Dragičević, "Secure control of DC microgrids for instant detection and mitigation of cyber-attacks based on artificial intelligence," in *IEEE Systems Journal*, vol. 16, no. 2, pp. 2580-2591, Jun. 2022.

Koduru Sriranga Suprabhath received the B.Tech. degree in Electrical and Electronics Engineering from the GITAM University, Hyderabad, India, in 2016. M.Tech. in power systems from Jawaharlal Nehru Technological University, Hyderabad, India, in 2019. He is currently working towards Ph.D. degree in the area of cyber physical systems and power electronics at department of Electrical and Computer Engineering, Mahindra University, Hyderabad, India. His current research interest include application of artificial intelligence in power electronics and power systems, modelling and secure control of microgrids, and cyber-physical systems.

Machina Venkata Siva Prasad received the B.Tech. degree in Electronics and Communication Engineering from the Anna University, Chennai, India, in 2016. M.Tech. in Digital Electronics and Communication Systems from Jawaharlal Nehru Technological University, Anantapur, Anantapuramu, India, in 2019. He is currently working towards Ph.D. degree in the area of cyber physical systems and power electronics at department of Electrical and Computer Engineering, Mahindra University, Hyderabad, India. His current research interest include application of artificial intelligence in power electronics and cyber-physical systems.

Sreedhar Madichetty received the B.Tech. degree from the Jawaharlal Nehru Technological University, Anantapur, Anantapuramu, India, in 2010, and the M.Tech. (Topper and Gold Medal) and the Ph.D. degrees from the KIIT University, Bhubaneswar, India, in 2012 and 2015, respectively. In 2014, he joined the Department of Electrical and Electronics Engineering, Birla Institute of Technology and Science, Pilani, India, as a Lecturer. In 2017, he joined as SERB sponsored NPDF at IIT Delhi and moved to Trinity College-Dublin, Ireland in 2019 as a senior research fellow. He is currently working as Associate Professor in Department of Electronics and Computer Engineering at Ecole Centrale School of Engineering, Mahindra University, Hyderabad, India. He has authored more than 50 research articles (including papers in international journals, conferences, and book chapters). His research interests include power electronics, cyber-physical systems and renewable energy systems. Dr. Madichetty is a senior member of IEEE.

Sukumar Mishra received the M.Tech. and Ph.D. degrees in electrical engineering from the National Institute of Technology, Rourkela, India, in 1992 and 2000, respectively. He is currently a Professor with the Indian Institute of Technology Delhi, New Delhi, India, and has been its part for the past 17 years. He is the founder of Silov Solutions Private Limited, a company that specifically deals in products related to renewable energy sources utilizable at household scale as well as at commercial setups. Since March 2020, he has been the Associate Dean Research and Development with IIT Delhi. He has been granted fellowships from academies like NASI (India), INAE (India), and professional societies like IET (U.K.), IETE (India), and IE (India). He has also been recognized as the INAE Industry Academic Distinguished Professor.