Real-Time AI-Based Anomaly Detection and Classification in Power Electronics Dominated Grids

Matthew Baker, *Student Member, IEEE*, Amin Y. Fard, *Student Member, IEEE*, Hassan Althuwaini, *Student Member, IEEE*, and Mohammad B. Shadmand, *Senior Member, IEEE*

***Abstract*—Real-time anomaly detection system (ADS) and anomaly classification system (ACS) techniques are becoming a crucial need for future power electronic dominated grid (PEDG). Artificial intelligence techniques such as recurrent neural networks, specifically long short-term memory (LSTM) provide a promising solution to detect anomalies in power grids. The main challenge is the implementation of these methods for real-time detection and classification for preventing catastrophic failure in PEDG. This article is addressing the challenge for detection and classification of anomalies in real-time in PEDG. The proposed approach is based on integration of model predictive control (MPC) and LSTM for realizing real-time ADS and ACS. The LSTM detection network can utilize the same time-series input data as the MPC, allowing for anomaly classification and correction. The proposed integrated LSTM-MPC approach has features of power electronics internal failure detection and corrective actions, which is an important aspect in future PEDG to differentiate inverters internal failures versus anomalies. Such internal failures include open circuit fault that needs to be detected and classified from a potential cyber-attack, allowing resilient operation of PEDG. The proposed integrated LSTM-MPC scheme for real-time ADS and ACS scheme is tested on a realistic 14-bus system dominated with inverters forming PEDG.**

***Index Terms*—Anomaly classification, anomaly detection, cyberattack, fault-tolerance, inverter fault detection.**

I. Introduction

THE power system is experiencing a massive change to be able to house ever-increasing distributed energy resources (DERs) across the grid, to decrease the dependency on nonrenewable-based sources, and shift it toward renewable resources, i.e., photovoltaics and wind. This new energy paradigm is called power electronics dominated grid (PEDG) [1]. With all the benefits the PEDG introduces, it brings up some challenges that need to be properly addressed prior to full implementation of such a complex system in the real world. These challenges include control, privacy, stability, planning, resilience, and cyber-physical security aspects [2].

The PEDG resilient operation is constrained with predefined boundaries for variables such as frequency, voltage, and power quality indices. Any anomaly could cause destructive consequences on the operation of the PEDG. These anomalies could have different characteristics such as component failure, faults, or malicious intrusive attacks. By considering the recent intrusive attempts on the power systems, cyber-physical security of the system gains extensive attention from governmental agencies and decision-making organizations, since it affects the national security. Thus, prevention, detection [4], mitigation [5], and, if needed, isolation of these cyber-physical intrusions are trending research topics for modern PEDG. High penetration of DERs in the grid requires various agents for proper functionality. These include smart meters, PMUs, observers, smart loads, and the hierarchical control architecture of the PEDG. Thus, it is necessary to incorporate multilayer anomaly detection and classification (MADC) systems performing in multiple timescales. This is inevitable to ensure the secure and seamless operation of the entire system.

One of the most common cyber-attacks on power systems is false data injection (FDI). FDIs target the data integrity of the system which would push the control system to adopt inadequate decisions [3], [4]. Attack consequences could vary, depending on the number of compromised assets, attacker's level of knowledge on the system, attack propagation, and its persistence [5], [6]. Even attacking one node of the system could impact the other nodes across the PEDG, since the compromised DER may impact the neighboring nodes' power quality and optimal operation of other DERs. The consequence of this attack is cascading failures across the grid. Thus, it is crucial for resilient operation of PEDG to isolate the anomalous nodes to avoid cascading failure across the PEDG that could results in catastrophic failure of the power grid.

The supervisory layer of the PEDG must be able to differentiate between these cyber intrusions and internal inverter failures to be able to make the most optimal decision for the PEDG. Without this knowledge, the supervisory layer will not be able to adopt the best decisions for a system with fleets of smart assets across it. In the literature, numerous inverter fault-tolerant control schemes are proposed [7], [8], [9], [10]. The existing solutions are mainly focusing on detection, location of the faulty switch, and updating the switching sequences accordingly. The missing piece of the puzzle in improving the

Manuscript received 27 June 2022; revised 21 September 2022 and 26 October 2022; accepted 17 November 2022. Date of publication 5 December 2022; date of current version 23 March 2023. This work was supported by the Qatar National Research Fund (QNRF is a member of Qatar Foundation) under Grant NPRP12S-0226-190158. This paper was presented in part at the IEEE International Conference on Smart Grid and Renewable Energy, Doha, Qatar, 2022. *(Corresponding author: Mohammad B. Shadmand.)*

The authors are with the Department of Electrical and Computer Engineering, University of Illinois Chicago, Chicago, IL 60607 USA (e-mail: mbaker36@uic.edu; ayouse9@uic.edu; halthu2@uic.edu; shadmand@uic.edu).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/JESTIE.2022.3227005.

Digital Object Identifier 10.1109/JESTIE.2022.3227005

resiliency of the PEDG is differentiating these internal faults from malicious intrusions. Differentiating between these allows for optimal corrective action. A critically important missing piece in exiting solutions is ensuring this process occurs in real-time. If the MADC cannot detect and classify the anomaly in a real-time-basis, the existing window for making proper decision might be missed.

The existing solutions for anomaly detection can be classified into two main categories, which are system model-based techniques [11], [12], and data-driven schemes [13], [14], [15], [16], [17]. Generally, in model-based approaches, a model of the system must be developed, and the system parameters must be estimated. Since there is not a training mechanism in model-based approaches, data mining is not needed. However, the main drawbacks of model-based techniques is scalability of the detection mechanism, meaning that if the system changes, a new model needs to be developed [18]. In model-based schemes, for detection purposes, usually an observer is designed to oversee the dynamic behavior of the system. The observers for these model-based techniques could use Kalman filter [19], principle component analysis [20], and weighted least-square [21]. These model-based techniques could be implemented in real-time applications. However, since they are highly dependent on the mathematical model of the system, they are prone to uncertainties, unforeseen disturbances, and computational burden as the system becomes more complex. Additionally, the model must be modified to account for any change in the PEDG. On the other hand, data-driven-based schemes can be used to perform effective detection and classification of wide range of anomalies such as FDIs in complex systems. As an example, artificial-neural-network-based approaches illustrated proper performance for nonlinear systems. These tools are an appealing candidate for anomaly detection system (ADS) and anomaly classification system (ACS) in PEDG. However, these schemes require huge datasets for training purposes in order to provide accurate performance. Other machine learning-based schemes such as *k*-nearest neighbor (*k*-NN), support vector machine (SVM) [22], [23], and deep learning [24] suffer from the same drawbacks and real-time implementation. As illustrated in [14] and [25], for power system applications, SVM illustrates better performance than *k*-NN, however, the performance of SVM highly depends on kernel type selection. In [26], a deep-learning-based method, which is modified version of WaveNet, was proposed and applied to IEEE 14-bus system while high penetration of renewable resources are considered. With all these methodologies, real-time implementation and scalability of the ADC and ACS are the remailing challenges.

Incorporating neural network (NN) based scheme, thus, has an opportunity to cooperate with control methods to ensure an impactful contribution. In this article, the inherent characteristics of model predictive control (MPC) is leveraged for effective real-time integration of NN-based network for realizing MADC in highly nonlinear PEDG. Conventional finite-set MPC determines optimal switching sequences based on the model and a cost function for optimization. The main focus of this article is to develop a framework for integration of MPC and NN for real-time MADC. The proposed work seeks to be a strong contender for scenarios in which the NN-based solutions do not significantly increase computational time compared to conventional MPC and where real-time detection of anomalies is of upmost importance. The work in [27] demonstrates an ability for MPC-based controllers to detect open circuit faults using the MPC cost function. This control scheme utilizes the main core of MPC to generate modified switching sequences constraint by the faulty switches without the need of major computation. The model used for generating the switching sequences is proven to be sufficient for open-circuit faults. However, for more comprehensive anomaly detection and classification, this article proposes an NN module integrated within the MPC framework. Therefore, a NN-based-detection scheme must provide additional utility which the conventional MPC itself cannot. The main technical challenge for NN integration with MPC for MADC is sufficient data collection for accurate classification in real-time.

Existing solutions mostly focus on detecting FDI attacks and they neglect the internal failure of the DERs [2]. Also, the existing literature, mostly focuses on detection only and they are not proposing any solutions after the detection is executed in real-time [2]. Additional utility is presented in classifying FDI attacks and circuit faults with a single NN. The main contribution of this article is the realization of a framework, which is able to detect and classify the anomalies across the PEDG in real-time. The proposed control scheme could be used at the primary layer of the control hierarchy of the PEDG to ensure detection and classification of anomalies of any nature, i.e., inverter internal failure or cyber-attack, in a real-time manner. Thus, integration of the proposed MADC in the primary control level at microseconds time scale results in smart self-learning inverters operating at the grid-edge toward resilient and secure PEDG. The considered attack model includes noise injection over the voltage and current measurements. The noise-based attacks are among the difficult-to-detect malicious activities, and their destructive impacts are considerable, varying from service interruptions to cascading failures across the grid. Specifically, the proposed control framework employs recurrent neutral networks (RNN). RNNs are utilized as feedforward NN techniques classification proved unable to determine fault classification [28]. Thus, for anomaly classification a deep NN topology is preferred. This category of neural networks are among the top candidates to perform classifications on time-dependent variables while taking into the account the previous inputs of the system [29]. Among different variants of RNNs, the long short-term memory (LSTM) employs an internal memory to create the predictions for next steps of the system [29], a perfect match to be integrated with MPC with long-time horizon prediction and optimization for the application in hand and real-time implementation. This internal memory with better predictive capabilities makes the LSTM the best option for fault classification within a system as complex as the PEDG. The initial part of the proposed framework employs LSTM in conjunction with MPC to perform anomaly detection and classification for inverters at the primary layer controller. The considered inverter topology in this article is cascaded multilevel inverted (CMI) due to its fault-tolerant capability [27], [30]. It is worth mentioning that the same approach could

be employed for any other inverter architecture to reach to a similar performance. After detection and classification, the proposed LSTM-MPC framework adopts corrective actions to performs self-healing model predictive control to ensure fault-ride through capability in the case of internal failure of the inverter. The integrated LSTM-based MADC with self-healing MPC enhances the resiliency and cybersecurity of the PEDG in the case of inverter internal failure and noise-injection-based cyber intrusions. Thus, to put it in a nutshell, the major contributions of the article are as follows.

1) An integrated MPC-LSTM technique for detecting and classifying anomalies in real-time followed by a self-healing solution and/or isolating the intruded DER in the network to ensure the resilient operation of the system by preventing cascading failure scenarios.
2) Comprehensive approach for data collection and training of LSTM for anomaly classification and effective mitigation in real-time, which is crucial for the application in hand.
3) Analysis and case studies to demonstrate the scalability of proposed LSTM-MPC.
4) Discussion on the hyperparameter selection process as a guideline for design of LSTM.

The rest of this article is organized as follows. Section II is a description of the PEDG system, LSTM, and MPC used. Section III details the collection of training data and the operation of the proposed LSTM-MPC. Section IV demonstrates the case studies. Finally, Section V concludes this article.

II. System Description

The proposed LSTM-MPC detects anomalies and, with the guidance of the supervisory controller, determines whether the anomaly would allow for continued operation of the affected DER. If the anomaly presents a larger threat, it may ultimately lead to isolation from rest of the grid to ensure harmonious operation of other DERs and nearby nodes. While the proposed LSTM-MPC can be applied to any power system, the proposed scheme is tested primarily using a 14-Bus system with high penetration of DERs as the PEDG, and a seven-level cascaded multilevel inverter as power electronic interface of each DER. To detect an anomaly, the NN system receives input data at each sampling instance T_s. This data is fed into the LSTM system, which is detecting for one of two potential anomalies considered in this article. Fig. 1 illustrate the schematic of the 14-Bus system with proposed LSTM-MPC.

Two classifications of anomaly are presented. The first detects whether a physical converter failure has occurred. In this article, it is an open circuit switch failure, a leading cause of semiconductor failure in power electronic systems [31]. This type of anomaly, once detected, allowing for continued operation. Thus, the supervisory controller can provide a corrective action to the MPC and continue operation. The second type of anomaly represents an FDI. This represents a potential cyber-attack on the current measurement sensors. When such a detection occurs, a DER can no longer be treated as a trusted source to the supervisory layer and, thus, must be isolated from the PEDG to prevent impact on nearby nodes and other healthy DERs. Therefore, corrective action is taken to prevent further attacks on the grid and ensure resilient operation.

TABLE I
CMI Operational Parameters

Parameter	Value
V_{dc}	100 V
Grid Voltage	220 V
Grid frequency	60 Hz
Filter resistance	10 mΩ
Filter inductance	25 mH
Sampling Time	10 μs
P_{ref}	5 kW:50 kW

The utility of the presented NN scheme is twofold. First, the NN scheme can detect potential anomalies in real-time. The goal of the NN detection scheme is to, in less than one line cycle, determine whether anomalous behavior exists and classify it as either a fault or cyber-attack; the unique contribution of this article. This quick detection allows for the supervisory layer to address anomalies before the impact is visible on the entire PEDG. The second feature of the NN approach is efficient use of computational resources. When the NNs are trained to reduce the computational burden, such as by having a single NN system detect numerous anomalies with the same input data, the local LSTM-MPC is operating efficiently. It also allows for further anomaly detection in future works where the single network approach can be used to classify more anomalies without extreme increase in the number of neurons. Thus, this two-level approach both on the local and supervisory level allows for discrete implementation. The proposed LSTM-MPC MADC framework is implemented on each phase of a CMI with the properties shown in Table I. A complete overview of the system implemented is seen in Fig. 1.

A. Communication Infrastructure of PEDG

The proposed control framework consists of MPC and NN parts working collaboratively to ensure short-term and long-term voltage and frequency stabilities of the PEDG. The MPC-based controller is utilized in the local controller. The local controller has the responsibility to receive the power set-points from the upper control layers, convert them to switching signals, and turn power electronic switches ON and OFF in the power stage accordingly. The reasons for opting MPC for the local controller include: easy to leverage into constrained multiobjective control problems, eliminating the hurdle of PID controller tuning for different operating points, better power quality, and proper for inner control loop with high compatibility with outer control loops. Considering these features, MPC is the best candidate for the local layer of the proposed controller. However, the local controller does not have proper knowledge of the entire PEDG, thus, the communication layer is required between the local layer of the controller and the supervisory layer.

The supervisory layer is responsible for overseeing the entire grid including generations, consumptions, reserved power, and power loss. Using all the gathered information, this layer assigned the power set-points for each individual inverter.

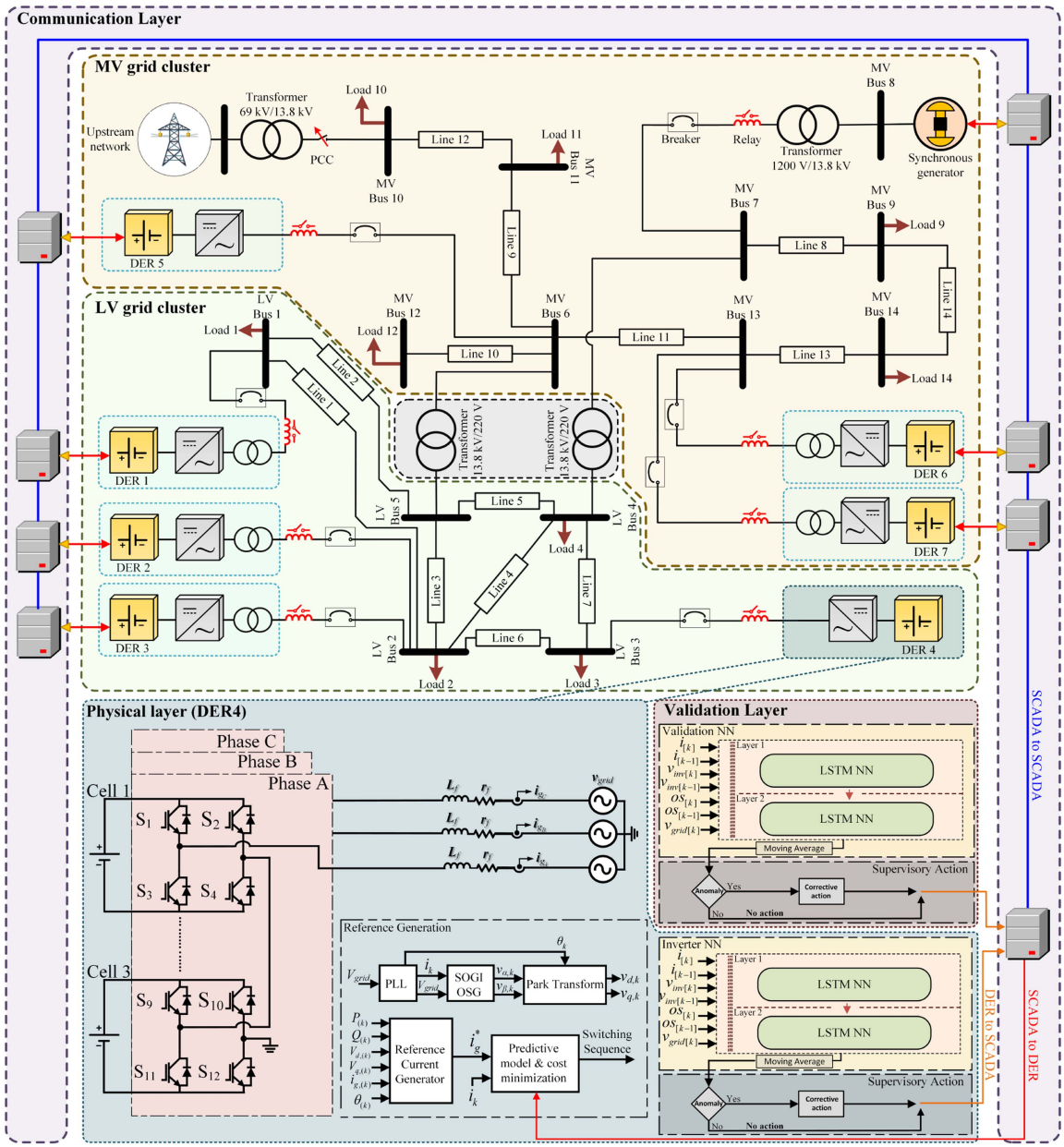

Fig. 1. Complete system under study for this work. The proposed neural network scheme exists as a per phase detection of the cascaded multilevel inverter at DER 4. This anomaly detection network is connected to the higher level 14-bus system at Bus 3. Anomalies are detected initially at the local controller, then verified at the supervisory level before corrective action is taken.

Various communication protocols are developed for smart grid applications for secure communications with minimal latency [32], [33], [34]. These protocols include, IEEE 802.15.4 (ZigBee), IEEE 802.11 (Wireless LAN (WLAN) or Wi-Fi), IEEE-802.16 (WiMAX), GSM and GPRS, and DASH7. But even with these improvements in communication protocols, the communication layer is the most vulnerable layer of the PEDG.

FDI attacks are possible attacks on the communication layer. In this article, the attacks considered are noise-based FDI attacks on the sensors measuring the current injected by the DERs. When there is communication between a supervisory controller and local controller, an attacker's plan can be to interfere with the communication layer and inject noise into the feedback loop or communication link of each individual inverter. In that case, although the supervisory layer has assigned specific set points to the MPC-based layer of the framework, the noise-based FDI attack prevents proper power injection when the measured current is incorrect. This means the balance between generation and consumption will deteriorate, and voltage or frequency stabilities of the system will be endangered. On the other hand, the supervisory layer of the PEDG needs an accurate model of the entire system to perform a load flow analysis to determine the voltage of each node and consequently determine the power set-points for each individual inverter. Within the concept of PEDG, where the distributed resources and consumers are changing dynamically according to the time of the day and season, having

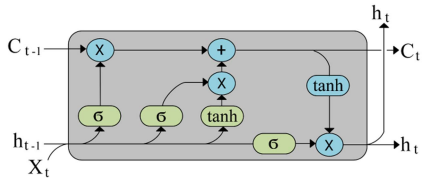

Fig. 2. Fundamental LSTM Cell.

a precise model of the system is almost impossible. This will paralyze the supervisory layer of the PEDG in the case of FDI attacks. For this reason, in the proposed control framework the supervisory layer of the controller is equipped with an NN-based algorithm. It performs the responsibilities of the supervisory layer without an accurate model of the entire integrated system. The proposed NN-based supervisory layer not only assigns the set points for each individual inverter, but also detects noise-based cyber intrusion. The proposed LSTM-MPC-based control framework enables the PEDG to differentiate between inverter internal failures and FDI attacks. This will enable the supervisory layer to take corrective actions using an MPC-based controller in the case of power stage failure of the inverter, or label the inverter as compromised in the case of FDI detection.

B. LSTM Description and Formulation

RNNs are a category of NNs, which analyze sequential data. Whereas more traditional methods, such as the feed forward neural network, produce outputs solely based on the current inputs to the NN. RNNs are trained to also incorporate past states of the network. These networks are strong contenders for anomaly classification, as instantaneous data may or may not be anomalous depending on where it occurs in a sequence. In this article, the LSTM RNN topology is used to enable the implementation of the LSTM cell, as shown in Fig. 2. The two activation functions used in each LSTM cell are the sigmoid and hyperbolic tangent functions, represented in

$$\sigma(x) = \frac{1}{1+e^{-x}} \tag{1}$$

$$\tanh(x) = \frac{e^{x}-e^{-x}}{e^{x}+e^{-x}} \tag{2}$$

Fig. 2 demonstrates each LSTM cell has 12 parameters determined through the training process. In this article, the structure of the LSTM network is constant; there is no variance in the number of features, LSTM layers, dropout rate, or classification layer. The major investigation for the training process is the number of hidden units in each LSTM layer. The training process accounting for changes in hidden states is detailed in Section III.

C. Model Predictive Control Formulation

The MPC applied for the CMI is shown in Fig. 1. This system is an adaptation of the finite-set MPC, which can eliminate switching sequences made impossible by an open circuit fault. This MPC scheme, as summarized in this section, is similar to the state-of-the-art approaches, with wide range of benefits for grid-tied inverter applications as highlighted in [35] and [36]. The proposed LSTM-MPC is focused on leveraging the inherent characteristics of state-of-the-art MPC with additional features. The MPC operates with a second order generalized integrator phase lock loop, which generates the grid angle needed for utilizing active and reactive power references, which are synchronized with the grid. The reference current i_k^* in (3) is determined from the active and reactive power references, and predicted current i_{k+1} in (4) is determined from using the forward Euler method

$$i_k^* = i_{d,k}^* \sin(\theta_k) + i_{q,k}^* \cos(\theta_k) \tag{3}$$

$$i_{k+1}[s] = \left[1 - \frac{R}{L}T_s\right] i_k + \frac{T_S}{L}[v_{inv,k+1}[s] - v_k]. \tag{4}$$

The cost function (5) is determined using i_k^* and i_{k+1}

$$J[s] = |i_k^* - i_{k+1}[s]| \, \forall s \in \mathbb{N} \leq 64 \text{ s.t. state } \mathrm{s}_{1x64}[s] = 0$$

$$s_{k+1} = \arg \text{ minimize}(J[s]) \tag{5}$$

where *s* is a specific switching state, and the array *states* lists, which of the switching sequences are permissible. Under normal operating conditions, *states* is a 1×64 array representing all valid switching states for a seven-level CMI. Whichever switching state minimizes the cost of (5) is applied to the inverter.

III. Neural Network Detection Scheme: LSTM-MPC

A. Data Collection

The LSTM-MPC is created by training data collected from the MPC system described in Section II-B. The diagram of the LSTM-MPC operational principle is shown in Fig. 3. The aim in data collection for this system is to ensure real-time detection is possible, and no additional measurements or sensors are necessary beyond those needed by conventional MPC. Additionally, proper simulation of the grid voltage during the collection of training data will allow for scalability of the LSTM-MPC into a wider range of power system topologies. If the system needs to be retrained for changing system properties such as the number of switches, power level, and voltage level the same process as described here can still be utilized. This eases the requirements for data collection and allows for more general usage of this system and training process. With this design principle in mind for collecting data, the data considered as input to the NN are 1×7 array *INP* given by

$$INP = \begin{bmatrix} i_{[k]}, i_{[k-1]}, V_{inv[k]}, V_{inv[k-1]} \\ OS_{[k]}, OS_{[k-1]}, V_{grid[k]} \end{bmatrix} \tag{6}$$

where at sampling instant *k*, $i_{[k]}$ and $i_{[k\text{-}1]}$ are the inductor currents, $V_{inv[k]}$ and $V_{inv[k\text{-}1]}$ are the inverter voltages, $OS_{[k]}$ and $OS_{[k\text{-}1]}$ are the optimal switching states applied by the MPC, and $V_{grid[k]}$ is the grid voltage at the point of common coupling. The voltage and current measurements are the same as the measurements used in the MPC cost function formulation. The optimal states are the output of the MPC formulation and, thus, the switching states applied. Therefore, the variables chosen are impactful to detecting anomalies involving FDI and fault failures as it will impact the data of *INP* adversely and noticeably.

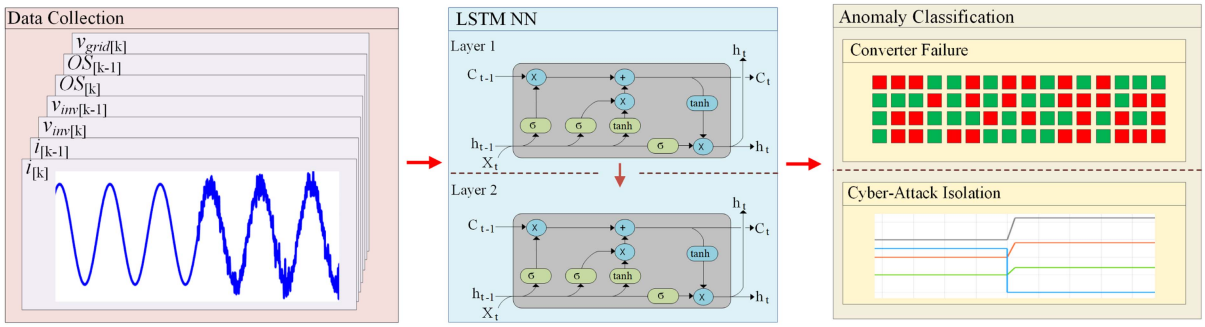

Fig. 3. Operational diagram of the LSTM-MPC. The input data of INP is collected in step one. Then, is given to the 2-layer LSTM-MPC to create a probability of anomaly in step two. The number of hidden units in each layer of step two is variable and based on the results of Table II. The final step triggers corrective action when the probability passes the trigger threshold, as explained in Section III.

The aim of the NN training process is to ensure proper network structure and training procedure, which can detect these anomalies in real-time and accurately.

The DER as described in Section II and Table I is created in MATLAB/Simulink version 2021b to collect training data. The Simscape Specialized Power systems toolbox is utilized for solving power flow equations at each discrete step instance. The data creation is executed in this environment as it would also be used to verify the network operation in the case studies section. Thus, a comprehensive dataset is collected from a realistic PEDG bus as a true replica of DER in real world. In fact, this model can be considered as the digital twin of an actual physical system for collecting comprehensive data set for training purpose of NN network. Matching the training data accumulation to the method in which the system is tested and operated eliminates additional noise or unrealistic data, which might potentially skew the training process.

1) Open Circuit Fault Data: To collect data for an internal fault anomaly, the DER operates as a three-phase system with a seven-level CMI. An open circuit fault is simulated through the opening of a breaker in series with the faulted switch. Thus, for open circuit faults, the potential number of faulty switches in each inverter is 36. To ensure sufficient training data is collected, the simulation is run 36 times with a different switch causing an open circuit fault in each instance. For the data collection scheme, the simulation in each iteration is run for 1 s of simulation time where the open circuit fault occurs at 0.5 s. As the system operates with a line frequency of 60 Hz, 30 complete line cycles occur for each open circuit fault. This amount of data is sufficient for NN training and not so large as to unnecessarily increase training time. The seven inputs of *INP* are collected at a sampling rate of 100 kHz, as well as the 1×36 array denoting the status of each fault. Should a controller need the NN to operate at a slower frequency, the entire dataset can be under sampled to the required frequency. Combining the sample rate simulation time and number of iterations along with the input and class data for the network, a total of 25 200 000 data points from this collection process are used for training the fault anomaly detection NN scheme. These data are grouped into blocks 50 sample long to minimize the sample size needed for classification, leading to improved response time. Finally, data are randomly split into training, validation, and testing subsets, which are divided as 70%, 15%, and 15% of the total data acquired, respectively.

2) False Data Injection Data: Data collection for the FDI attack follows a similar setup as the open circuit fault data. To model an FDI attack, white noise is injected into the current sensor, which outputs normally distributed random noise. The noise has a power of 0.1. The attack occurs at 0.5 s, halfway through the data collection time of 1 s. To accumulate data for a wide range of situations, the amplitude of the noise and the power reference are varied. The output of the noise generator is multiplied by a constant N_{FDI}, which varies from 0 to 2 in increments of 0.05. A total of 32 200 000 data points from this collection process are used for the FDI anomaly detection NN scheme. The data are grouped into blocks the same as the fault data.

B. Training

1) Neural Network Topology: With the training data collected, the next step is to describe the operation LSTM system. The fully trained MADC is able to determine when an anomaly is probable, which of the two classes the anomaly is in, and signals to the supervisory controller that corrective action is needed. The LSTM-MPC has three classes to represent the training data, "normal," "fault," and "cyberattack." Should different data be collected to train another LSTM-MPC, the number of classes will change to match the additional data and classifications. To create more balanced training data, half of the "normal" class of data from each data collection process is excluded from the training data set. The final data set classes are approximately 29.2% "fault," 37.4% "cyberattack," and 33.3% "normal." The goal of the LSTM-MPC is to have an accuracy above 90%. This data is sufficiently balanced to meet this goal since 90% accuracy requires high accuracy of each class and no individual class can dominate training. After detection, the supervisory controller can confirm the anomaly with a mirrored NN, should extra validation be required. Finally, corrective action is implemented.

2) Hyperparameters Selection: The LSTM network is trained in MATLAB 2021b. Determining the exact hyperparameters of the system, specifically the number of LSTM units in each of the two layers, is cause for further investigation to the specific control system. In this article, various hyperparameters are tested and examined to pick the most proper NN system for anomaly detection. Top priorities of operation in the 14-bus system are accuracy, detection speed, computational effort, and scalability. Accuracy is crucial for resilient operation of PEDG,

TABLE II
LSTM HYPERPARAMETERS

LSTM units	Anomaly Detection Accuracy	Computational Burden
1×1	89.69%	59.74%
2×1	83.32%	62.70%
2×2	83.32%	59.49%
3×1	89.95%	59.69%
3×3	92.30%	59.40%
5×3	90.11%	59.99%
5×5	93.02%	59.57%
10×5	95.47%	59.54%
10×10	96.66%	59.39%
20×10	97.80%	59.65%
20×20	97.87%	59.68%
25×13	97.71%	59.71%
25×25	98.12%	59.61%
50×25	98.79%	61.29%
50×50	98.64%	60.16%
100×50	98.80%	65.81%
100×100	98.71%	67.75%

fast detection speeds allow the MADC to take corrective action fast enough to prevent a violation of grid standards, low computational effort enables the anomaly detection network to run in parallel with the MPC, and scalability allows for deployment even in changing grid topology, perhaps due to more DERs coming online. Finally, a scalable system Therefore, the operation of the MPC will be used as a benchmark for the NN operation. The lower the execution rate, the better the NN system. While other hyperparameters such as batch size, learning rate, and activation function, may be considered necessary for other applications, the concerns of this article are primarily on execution rate of the scheme once the NN has been developed. Therefore, the hyperparameters adjusted are the number of neurons in each of the two layers of the LSTM.

Hyperparameter tuning is performed by adjusting the number of LSTM units in each layer. It is determined two layers are sufficient to correctly identify faults. In this article, the number of units will vary from 1 through 100 for the first layer, and the second layer will consist of either an equal number of units, or half (rounding up) the units of the first layer. The results of the hyperparameter tuning are seen in Table II. This table provides the hyperparameters of various LSTM networks along with the accuracy and computational effort required to execute each NN. Both the number of neurons and number of layers are seen in the leftmost column. For example, "10 × 5" denotes a two-layer network of 10 and 5 neurons, respectfully. The "anomaly detection accuracy" is the accuracy of the network using the testing data after five epochs of training. All other hyperparameters of the system remain constant, as described in Table III.

The computational rate is determined using the Performance Advisor Simulink Profiler in MATLAB/ Simulink. To account for variances in computational time due to hardware variance on the testing computers, the NN processing time is shown as a percentage of the processing time to enact the computations necessary for the MPC. For example, if the MPC required 100 s of total execution time in the profiler, and the NN system needed 75 s, the computational burden is considered 75%. This generalization allows for consistent data comparisons across machines of differing computational speeds.

TABLE III
LSTM TRAINING PARAMETERS

Parameter	Value
Maximum Epochs	5
Mini Batch size	256
Validation Frequency	300
Gradient Threshold	1
Optimizer	Adam
Data sample length	50
Dropout Rate	0.2

From the results generated in Table II, an optimal LSTM network is selected for implementation into the final system. The network selected is the least computationally expensive network with an accuracy of at least 90%. Thus, the 10 × 10 network is used; its accuracy is 96.66% with a computational burden of only 59.39%.

C. Corrective Action

After the LSTM-MPC has been trained, it is incorporated into the system as the "inverter neural network" shown in Fig. 1. During operation, the inputs to the LSTM-MPC are the data of *INP* at each sampling instance. The trained 10 × 10 LSTM-MPC produces a probability an anomaly has occurred. The three trained classification for the network are "normal," "fault," or "cyberattack." The LSTM-MPC produces a number from 0-1 for each class, where the higher the number is, the higher the probability the data is of the specified class. To prevent false positives from affecting an operational DER, the outputs of the fault detection network are fed into a moving average filter to filter out potential false positives and ensure a fault is only triggered when enough successive terms indicate high probability of a fault. Then, if the moving average filter exceeds a threshold V_t, the anomaly fault flag is tripped, and the supervisory controller is notified. Before V_t is exceeded for either "fault" or "cyberattack," the system is assumed to be "normal". For this article, $V_t = 0.16$ for the fault detection and $V_t = 0.45$ for the cyberattack detection. This threshold is manually set low enough to ensure fast response time, but high enough to prevent false positives. The threshold can be adjusted depending on the accuracy of the NN, as well as the desired response time of the system operator. After V_t is exceeded, the supervisory controller confirms the anomaly and takes corrective action. Two corrective actions are implemented here: when an internal fault occurs, the corrective action detailed in [27] is executed, where *states* is updated to remove faulty switching states. If an FDI attack is determined, the bus is isolated and power references are adjusted, as explained in Section IV and (7).

IV. DISCUSSION AND VALIDATION

To verify the effectiveness of the proposed LSTM-MPC as an effective MADC, anomalies are intentionally created in Phase A of DER 4 of the 14-bus system. These can be either open circuit faults, or FDI attacks.

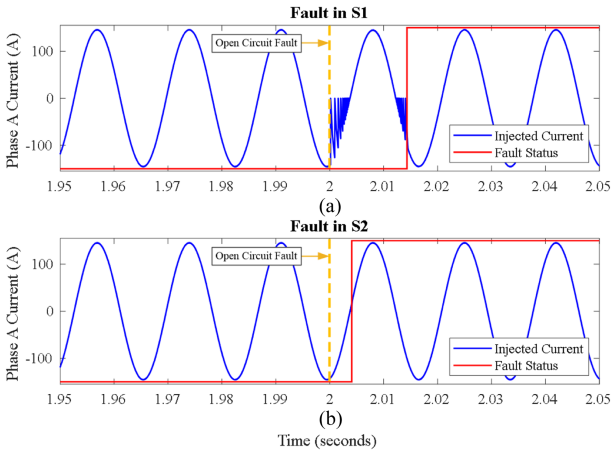

Fig. 4. Results of the first case study, verifying the neural network's ability to detect and correct an open circuit fault in Phase A of DER 4 of the 14-bus system. In both simulations, an open circuit fault occurs at t = 2 s. When the fault detection network has high enough confidence to determine a fault, the Fault Status flag goes HIGH and the states array is updated to exclude *switching* states requiring the faulty switch to be closed. (a) Fault occurs in S1. (b) Fault occurs in S2.

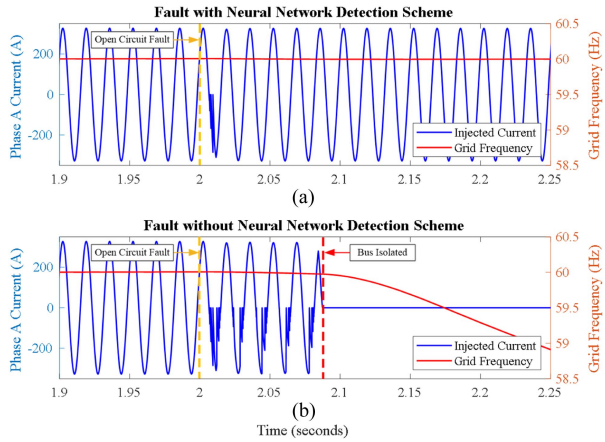

Fig. 5. Results of the second case study, which examines the impact of the fault correction network across a 14-bus system. In both simulations, an open circuit fault occurs in S1 at t = 2 s. (a) Detection network is present. It detects and applies corrective action to mitigate the fault in under one line cycle, allowing for continued operation. (b) No mitigation technique is present. The low power quality after the fault forces DER 4 to isolate from the 14-bus after five line cycles. Since the synchronous generator is unable to compensate, the system frequency collapses.

A. *Fault Detection Verification*

The first case study is to verify the LSTM-MPC can correctly identify a fault in both the positive and negative voltage levels of Phase A. In this article, P_{ref} is 16 kW and Q_{ref} is 0 kW. A fault occurs at $t = 2$ s for each test. In test one, the fault occurs in switch S_1 and in the second test the fault occurs in switch S_2. When the output of the moving average filter exceeds V_t the updated *states* matrix is applied preventing any faulty switch from being utilized in the "closed" state. The results of each test are seen in Fig. 4. When S_1 fails, the fault is detected and corrected in 14.32 ms; when S_2 fails, the fault is detected and corrected in 4.08 ms. As seen in each example, the proposed LSTM-MPC scheme can quickly identify faults in less than one line cycle. This allows quick identification for each fault and prevents the need to isolate the faulty DER due to inferior current quality for grid standards, thus providing real-time solution at the grid-edge.

B. *Impact of Compromised DER Isolation*

To demonstrate the added benefit of the open circuit fault detection network, the second case study compares the proposed network to a system without any fault detection. In this case study, DER 4 is considered a major contributor to power generation in the 14-bus system. The P_{ref} is increased to 20 kW, the 14-bus system is operated during low loading conditions, and the synchronous generator has a maximum capacity of 100 kW. For simplicity, all other DER generators remain constant. Therefore, failure of DER 4 will lead to an inability to supply power across the system as the synchronous generator is unable to provide the needed power and frequency support. In this case study the open circuit fault occurs in switch S_1 at 2 s. Fig. 5(a) shows the LSTM-MPC system operating to take corrective action to ensure proper operation despite the fault. Fig. 5(b) shows the alternative, where the open circuit fault occurs at 2 s. After five-line cycles, DER 4 must isolate from the 14-bus network due to unacceptable power quality. Thus, the power injected by the DER becomes zero. With the synchronous generator unable to provide the necessary power to regulate frequency, it rapidly denigrates and the frequency of the entire system collapses. Therefore, the LSTM-MPC scheme ensures the DER does not cause system collapse even when an open circuit fault occurs in a critical DER.

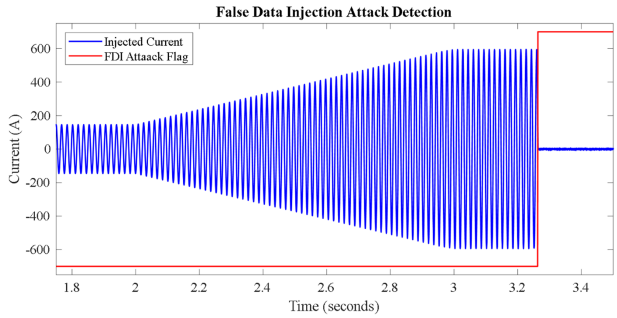

Fig. 6. Results of the third case study. Here, the robustness of the NN during FDI is shown, as changes in the power reference do not cause. When FDI does occur, the system responds promptly by alerting the supervisory controller, which is then able to isolate the attacked DER from the system to minimize the effects on the rest of the system.

C. *Changing Power Reference in Response to Anomalies*

The case study here demonstrates the LSTM-MPC scheme's ability to detect an FDI attack, as well as the system robustness to changing P_{ref} values. A change in P_{ref} can represent an anticipated load increase, change in solar irradiance if the DER is a PV system, or any other ramp increase in power generation. In this article, the system operates under the same initial conditions presented in Section VI-B. At $t = 2$ s, the P_{ref} for DER 4 ramps up at a rate of 5000 kW/s. At $t = 3$ s, P_{ref} ceases to increase. Once this state is reached, an FDI attack occurs on the current sensor when t = 3.25 s. The results of this case study are shown in Fig. 6. As depicted, the proposed LSTM-MPC scheme operates

TABLE IV
BUS VOLTAGES DURING FDI ATTACK

Bus	Per-Unit Voltage Before FDI	Per-Unit Voltage After FDI (without NN)	Per-Unit Voltage After FDI (with NN)
1	0.913	0.892	0.907
2	0.913	0.887	0.903
3	0.991	0.919	0.934
4	0.958	0.940	0.954
5	0.930	0.915	0.930
6	0.932	0.916	0.931
7	0.953	0.936	0.951
8	0.967	0.951	0.966
9	0.947	0.931	0.945
10	0.923	0.907	0.922
11	0.927	0.911	0.925
12	0.928	0.912	0.927
13	0.937	0.921	0.936
14	0.942	0.925	0.940

as designed. No false positive occurs during the change in P_{ref}, and the proposed scheme determines a FDI in 13.4 ms after it occurs, which is less than one line cycle.

D. Impact of the LSTM-MPC on the System Resiliency

The fourth case study investigates the effect of isolating a DER under attack. In this scenario, a FDI attack occurs at DER 4 at $t = 4.5$ s, injecting noise into the current sensor. The increased harmonics caused by the noise injection and the reduced power quality of the DER causes breakers to trip, isolating the DER from the grid. The scenario is tested under two conditions, with and without the LSTM-MPC scheme. Without the LSTM-MPC, the supervisory layer is not alerted to the anomaly and mismatch occurs between the power generation and demand. With the proposed LSTM-MPC, the anomaly is properly identified and verified by the supervisory controller 12.0 ms after the attack. The corrective action in this scenario accounts for the removal of DER 4 and its power contributions are evenly divided amongst the remaining DERs using

$$P_{ref,n} = P^{*}_{ref,n} + P_{ref,4}\frac{P^{*}_{ref,n}}{P_{\text{avalible}}} \tag{7}$$

where $P_{ref,n}$ is the power reference for DER n, $P^{*}_{ref,n}$ is the power reference of DER n before the attack, and P_{avalible} is the power generated by the safe DERs before the attack. Another approach can replace (7) should it be desired by the supervisory controller. The results of the system under both scenarios are recorded in Table IV and Fig. 7. Table IV displays the voltage at each bus before the attack, as well at the voltage at 5 s. With the LSTM-MPC and corrective action taken, the average voltage deviation is 0.7% the p.u. voltage before the fault, compared to an average deviation of 2.2% without the corrective action. Additionally, with the corrective action, all buses are >0.9 V p.u., whereas buses 1 and 2 do not meet this criterion without the LSTM-MPC network.

E. Scalability Analysis

The previous case studies incorporate the LSTM-MPC to a DER connected to an IEEE 14-bus system. The DER is rated for a grid voltage of 220 V and 60 Hz, as per the parameters in

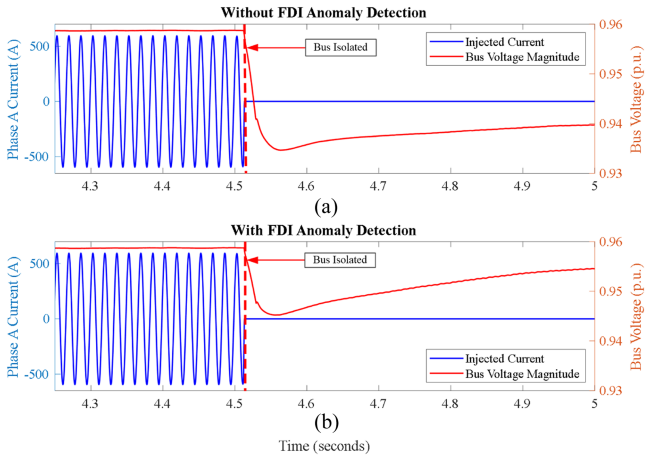

Fig. 7. Fourth case study demonstrates the impact of corrective action after an FDI attack is determined. The bus voltage and current injected by Phase A are shown at the bus with the FDI. (a) Without the anomaly corrective action. (b) With anomaly detection and corrective action. After isolation from the system, the system with the NN scheme has a smaller impact on the bus voltage due to the corrective action taken by the supervisory controller after the fault.

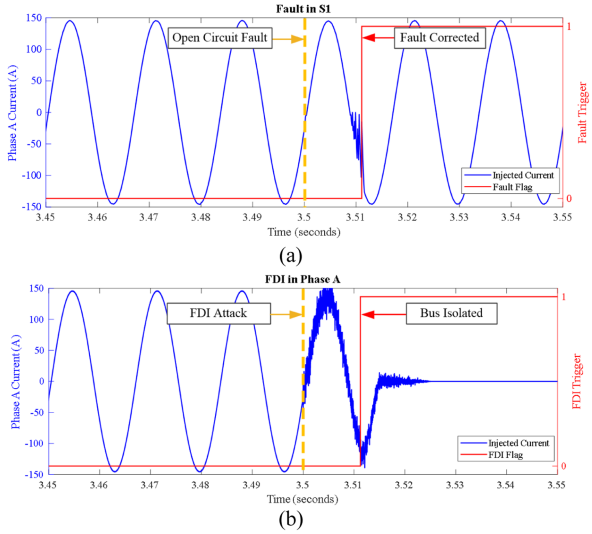

Fig. 8. Results of the fifth case study. The topology of the power system is expanded into a total of 18 buses by introducing additional loads and distribution lines. (a) Open circuit fault occurs at t = 3.5 s. (b) FDI attack occurs at t = 3.5 s. Despite the change in system architecture, the LSTM-MPC remains capable of detecting both anomalies and triggering corrective action.

Table I. These parameters accurately describe the low voltage operation of the 14-bus system. This match allows for easy implementation of the LSTM-MPC in DER 4 at Bus 3. This implies the LSTM-MPC is properly trained to operate in any power system topology; with the important assumption that the bus the LSTM-MPC is connected to is accurately reflected in the training data. Changing the topology of the system should not prevent the LSTM-MPC from operating properly.

To verify this assumption, the 14-bus system is expanded to 18 buses in this case study. The LSTM-MPC is tested in conditions where the DER matches Case Study 1. Two anomaly scenarios are tested. First, a switch failure in S_1 occurs at 3.5 s, and second, an FDI attack occurs in the current sensor of Phase A at 3.5 s. The results of these tests are seen in Fig. 8. Similar to the case

studies involving the original 14 bus system, the LSTM-MPC is capable of detecting both anomalies in less than one line cycle. The fault is mitigated after 11.10 ms and the FDI after 11.26 ms. These results support the premise that the topology of the power system is of little impact to the well trained LSTM-MPC. If the DER is connected to a bus where training data is collected with appropriately, the system can be scaled easily to detect these anomalies locally.

V. Conclusion

This article presents an anomaly detection and correction scheme for PEDG. The proposed MADC and corrective action is based on an integration of LSTM and MPC, which features real-time solutions for enhancing the resiliency of PEDG when anomalies occurs. In the proposed scheme, when an anomaly is detected, the supervisory layer controller can implement corrective action to ensure the power system continues proper operation. The data collection technique and training process of the long short-term memory network is described as well as the methodology of selecting proper hyperparameters. The training data is selected to increase scalability of the LSTM-MPC should the network topology expand as more DERs are integrated into the PEDG. An optimal LSTM network is used to test and validate the operation of the network. The case studies verify the system ability to allow robust deployment after anomalies occur, and the impact of the corrective actions by the supervisory controller is demonstrated.

Acknowledgment

The statements made herein are solely the responsibility of the authors.

References

[1] A. Khan, M. Hosseinzadehtaher, M. B. Shadmand, S. Bayhan, and H. Abu-Rub, "On the stability of the power electronics-dominated grid: A new energy paradigm," *IEEE Ind. Electron. Mag.*, vol. 14, no. 4, pp. 65–78, Dec. 2020.

[2] O. H. Abu-Rub, A. Y. Fard, M. F. Umar, M. Hosseinzadehtaher, and M. B. Shadmand, "Towards intelligent power electronics-dominated grid via machine learning techniques," *IEEE Power Electron. Mag.,* vol. 8, no. 1, pp. 28–38, Mar. 2021.

[3] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Trans. Smart Grid,* vol. 11, no. 3, pp. 2218–2234, May 2020.

[4] R. Das, G. Karmakar, J. Kamruzzaman, and A. Chowdhury, "Measuring trustworthiness of smart meters leveraging household energy consumption profile," *IEEE J. Emerg. Sel. Topics Ind. Electron.,* vol. 3, no. 2, pp. 289–297, Apr. 2022.

[5] A. Sargolzaei, A. Abbaspour, M. A. Al Faruque, A. Salah Eddin, and K. Yen, "Security challenges of networked control systems," in *Sustainable Interdependent Networks*. Berlin, Germany: Springer, 2018, pp. 77–95.

[6] K. Xiahou, Y. Liu, and Q. H. Wu, "Decentralized detection and mitigation of multiple false data injection attacks in multiarea power systems," *IEEE J. Emerg. Sel. Topics Ind. Electron.,* vol. 3, no. 1, pp. 101–112, Jan. 2022.

[7] B. Lu and S. K. Sharma, "A literature review of IGBT fault diagnostic and protection methods for power inverters," *IEEE Trans. Ind. Appl.,* vol. 45, no. 5, pp. 1770–1777, Sep./Oct. 2009.

[8] A. M. S. Mendes and A. J. Marques Cardoso, "Voltage source inverter fault diagnosis in variable speed AC drives, by the average current park's vector approach," in *Proc. IEEE Int. Electric Mach. Drives Conf.*, 1999, pp. 704–706.

[9] K. Rothenhagen and F. W. Fuchs, "Performance of diagnosis methods for IGBT open circuit faults in three phase voltage source inverters for AC variable speed drives," in *Proc. Eur. Conf. Power Electron. Appl.*, Sep. 2005, Paper 10.

[10] R. Peuget, S. Courtine, and J.-P. Rognon, "Fault detection and isolation on a PWM inverter by knowledge-based model," *IEEE Trans. Ind. Appl.,* vol. 34, no. 6, pp. 1318–1326, Nov./Dec. 1998.

[11] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using Kalman filter," *IEEE Trans. Control Netw. Syst.,* vol. 1, no. 4, pp. 370–379, Dec. 2014.

[12] W. Ao, Y. Song, and C. Wen, "Adaptive cyber-physical system attack detection and reconstruction with application to power systems," *IET Control Theory Appl.,* vol. 10, no. 12, pp. 1458–1468, 2016.

[13] A. Abdullah, "Ultrafast transmission line fault detection using a DWT-based ANN," *IEEE Trans. Ind. Appl.,* vol. 54, no. 2, pp. 1182–1193, Mar./Apr. 2018.

[14] M. Ozay, I. Esnaola, F. T. Yarman Vural, S. R. Kulkarni, and H. V. Poor, "Machine learning methods for attack detection in the smart grid," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 27, no. 8, pp. 1773–1786, Aug. 2016.

[15] J. Yan, H. He, X. Zhong, and Y. Tang, "Q-learning-based vulnerability analysis of smart grid against sequential topology attacks," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 1, pp. 200–210, Jan. 2017.

[16] S. A. Foroutan and F. R. Salmasi, "Detection of false data injection attacks against state estimation in smart grids based on a mixture Gaussian distribution learning method," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 2, no. 4, pp. 161–171, 2017.

[17] F. Li et al., "Detection and identification of cyber and physical attacks on distribution power grids with PVs: An online high-dimensional data-driven approach," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 10, no. 1, pp. 1282–1291, Feb. 2022.

[18] O. Boyaci et al., "Graph neural networks based detection of stealth false data injection attacks in smart grids," *IEEE Syst. J.,* vol. 16, no. 2, pp. 2946–2957, Jun. 2022.

[19] H. M. Khalid and J. C.-H. Peng, "Immunity toward data-injection attacks using multisensor track fusion-based model prediction," *IEEE Trans. Smart Grid,* vol. 8, no. 2, pp. 697–707, Mar. 2017.

[20] Z.-H. Yu and W.-L. Chin, "Blind false data injection attack using PCA approximation method in smart grid," *IEEE Trans. Smart Grid,* vol. 6, no. 3, pp. 1219–1226, May 2015.

[21] R. Deng, G. Xiao, and R. Lu, "Defending against false data injection attacks on power system state estimation," *IEEE Trans. Ind. Inform.*, vol. 13, no. 1, pp. 198–207, Feb. 2017.

[22] S. Zhang, Y. Wang, M. Liu, and Z. Bao, "Data-based line trip fault prediction in power systems using LSTM networks and SVM," *IEEE Access,* vol. 6, pp. 7675–7686, 2018.

[23] H. Goyel and K. S. Swarup, "Data integrity attack detection using ensemble based learning for cyber physical power systems," *IEEE Trans. Smart Grid*, to be published, Aug. 2022.

[24] G. Abdelmoumin, D. B. Rawat, and A. Rahman, "On the performance of machine learning models for anomaly-based intelligent intrusion detection systems for the Internet of Things," *IEEE Internet Things J.,* vol. 9, no. 6, pp. 4280–4290, Mar. 2022.

[25] J. Yan, B. Tang, and H. He, "Detection of false data attacks in smart grid with supervised learning," in *Proc. Int. Joint Conf. Neural Netw.*, Jul. 2016, pp. 1395–1402.

[26] F. Almutairy, L. Scekic, R. Elmoudi, and S. Wshah, "Accurate detection of false data injection attacks in renewable power systems using deep learning," *IEEE Access*, vol. 9, pp. 135774–135789, 2021.

[27] M. Easley, M. Baker, A. Khan, M. B. Shadmand, and H. Abu-Rub, "Self-healing model predictive controlled cascaded multilevel inverter," in *Proc. IEEE Energy Convers. Congr. Expo.*, 2019, pp. 239–244.

[28] M. W. Baker, H. Althuwaini, and M. B. Shadmand, "Artificial intelligence based anomaly detection and classification for grid-interactive cascaded multilevel inverters," in *Proc. 3rd Int. Conf. Smart Grid Renewable Energy*, Mar. 2022, pp. 1–6.

[29] V. Sze, Y.-H. Chen, T.-J. Yang, and J. S. Emer, "Efficient processing of deep neural networks: A tutorial and survey," *Proc. IEEE,* vol. 105, no. 12, pp. 2295–2329, Dec. 2017.

[30] N. A. Rahim, M. F. M. Elias, and W. P. Hew, "Transistor-clamped H-bridge based cascaded multilevel inverter with new method of capacitor voltage balancing," *IEEE Trans. Ind. Electron.,* vol. 60, no. 8, pp. 2943–2956, Aug. 2013.

[31] S. Yang, D. Xiang, A. Bryant, P. Mawby, L. Ran, and P. Tavner, "Condition monitoring for device reliability in power electronic converters: A review," *IEEE Trans. Power Electron.,* vol. 25, no. 11, pp. 2734–2752, Nov. 2010.

[32] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on smart grid communication infrastructures: Motivations, requirements and challenges," *IEEE Commun. Surv. Tut.,* vol. 15, no. 1, pp. 5–20, First Quarter 2013.

[33] US Department of Energy, "Communications requirements of smart grid technology," 2010. [Online]. Available: https://www.energy.gov/sites/default/files/gcprod/documents/Smart_Grid_Communications_Requirements_Report_10-05-2010.pdf
[34] M. Ghorbanian, S. H. Dolatabadi, M. Masjedi, and P. Siano, "Communication in smart grids: A comprehensive review on the existing and future communication and information infrastructures," *IEEE Syst. J.,* vol. 13, no. 4, pp. 4001–4014, Dec. 2019.
[35] S. Vazquez et al., "Model predictive control: A review of its applications in power electronics," *IEEE Ind. Electron. Mag.*, vol. 8, no. 1, pp. 16–31, Mar. 2014.
[36] C. R. D. Osório et al., "Modulated model predictive control applied to LCL-filtered grid-tied inverters: A convex optimization approach," *IEEE Open J. Ind. Appl.*, vol. 2, pp. 366–377, 2021.

Matthew Baker (Student Member, IEEE) received the B.S. degree in electrical engineering from Rockhurst University, Kansas City, MO, USA, in 2018. Since 2020, he has been working toward the Ph.D. degree in power electronics and controls with the Department of Electrical and Computer Engineering, University of Illinois Chicago, Chicago, IL, USA.

From 2018 to 2020, he was a Ph.D. student with the Department of Electrical and Computer Engineering, Kansas State University, Manhattan, KS, USA. He has internship experiences at the Electric Power Research Institute in 2022, and Sandia National Laboratories in 2021 and 2022.

Amin Y. Fard (Student Member, IEEE) received the B.Sc. degree from Azarbaijan Shahid Madani University, Tabriz, Iran, in 2011, and the M.Sc. degree with "second rank honor" from the University of Tabriz, Tabriz, Iran, in 2014, both in electrical power engineering. Since 2020, he has been working toward the Ph.D. degree in power electronics and controls with the Department of Electrical and Computer Engineering, University of Illinois Chicago, Chicago, IL, USA.

From 2014 to 2018, he was with Roshdiyeh Higher Education Institute as a Lecturer, the supervisor with Electrical Machinery and High Voltage Laboratories, and the Educational Manager with the Engineering Faculty. He was a Ph.D. student with K-State University from 2018–2020. His research interests include renewable energy systems like photovoltaic systems and wind turbines, power electronics, distributed generation, and power quality.

Hassan Althuwaini (Student Member, IEEE) received the B.S. degree in electrical engineering from Kansas State University, Manhattan, KS, USA, in 2019.

He was a Research Assistant with JKLab.org from 2018 to 2019. He was with the Department of Electrical and Computer Engineering, The University of Illinois Chicago in Jan. 2021 to continue his M.S studies under the supervision of Prof. M. Shadmand. His research interests include smart microgrids, energy storage system, characterization of SiC, and GaN power devices.

Mohammad B. Shadmand (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from Texas A&M University, College Station, TX, USA, in 2015.

From 2015 to 2016, he was an Instructor with the Department of Electrical and Computer Engineering, Texas A&M University. From 2016 to 2017, he was a Research Engineer with the Renewable Energy and Advanced Power Electronics Research Laboratory, College Station, TX, USA. From 2017 to 2020, he was an Assistant Professor with the Department of Electrical and Computer Engineering, Kansas State University, Manhattan, KS, USA. Since 2020, he has been an Assistant Professor with the University of Illinois Chicago, Chicago, IL, USA. He has authored and coauthored more than 100 journal and conference papers. His current research interests include distributed self-learning control schemes, advanced model predictive control, grid-following and grid-forming inverters, and intrusion detection system for power electronics dominated grids.

Dr. Shadmand was the recipient of Michelle Munson Serban Simu Keystone Research Scholar, Kansas State University in 2017, the 2019 IEEE Myron Zucker Faculty-Student Research Grant, and has awarded multiple best paper awards at different IEEE conferences. He was a Technical Program Co-Chair of the 2019 and 2022 IEEE Smart Grid and Renewable Energy Conference. He was an Associate Editor for IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, IEEE TRANSACTIONS ON INDUSRTY APPLICATION, and *IET Renewable Power Generation*.