IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 5, 2019, accepted November 20, 2019, date of publication December 5, 2019,
date of current version December 23, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2957884

Development of Adaptive Artificial Neural Network Security Assessment Schema for Malaysian Power Grids

AHMED N. AL-MASRI[1], (Member, IEEE), MOHD ZAINAL ABIDIN AB KADIR[2,3], (Senior Member, IEEE), ALI SAADON AL-OGAILI[2], AND YAP HOON[4]

[1]College of Computer and Information Technology, American University in the Emirates, Dubai 503000, UAE
[2]Institute of Power Engineering, University Tenaga Nasional, Kajang 43000, Malaysia
[3]Center for Electromagnetic and Lightning Protection Research, Advanced Lightning, Power, and Energy Research, Faculty of Engineering, Universiti Putra Malaysia, Seri Kembangan 3400, Malaysia
[4]School of Engineering, Faculty of Innovation and Technology, Taylor's University, Subang Jaya 47500, Malaysia

Corresponding author: Ahmed N. Al-Masri (ahmedalmasri@ieee.org)

ABSTRACT The mission of the power system operator has become more complicated than before due to increasing load demand, which causes power systems to operate near their security limits. The deregulation of electricity markets, which requires independent system operation driven by economic considerations, is still an essential requirement of modern power systems. This study presents an enhanced model of developed adaptive artificial neural network (AANN) technique for security enhancement of Malaysian power grids, inclusive of a remedial action (generation redispatch/load shedding) at any scale of system operation. Automatic data knowledge generation systems for AANN inputs and data selection and extraction methods are developed. Results show that the proposed AANN can provide the required amount of generation redispatch and load shedding accurately and promptly for computing large sample data.

INDEX TERMS Security assessment, artificial neural network (ANN), backpropagation, remedial action, contingency analysis.

I. INTRODUCTION

The security of power system operations remains an essential issue in many countries. Normal operations are imperative to ensue in any post-contingency situation. Checking the security of power systems requires tools that quantify power system safety concerns arising from operational interferences. Power system security assessment encompasses static security assessment (SSA) and dynamic security assessment (DSA). An SSA involves security situation factors, such as overload and overvoltage. During the post-contingency conditions via the load flow calculation of the power system. Conversely, DSA analyses the post-fault transient stability of the power system in real time [1]–[3].

Recent noteworthy occurrences of blackout incidents are a disturbance in Western Europe in September 2003 [4], a power shutdown in northern India in July 2012 [5], a power cut in Pakistan in January 2015 [6]–[8], and a widespread power blackout in March 2015 in Turkey [9]. Malaysia faced a similar incident when a blackout affected the entire Peninsular Malaysian power grid in August 1996 [10]. Such blackouts can cripple the economy by disrupting all types of commerce and cause public safety problems. Immediate restoration of power is the primary concern during power outages, but it requires careful planning in the execution of the restoration. The reenergizing of power system modules must happen in the correct sequence; errors can destroy individual components, such as generator units, transmission lines, and substation buses [11].

After a grid disturbance, the SSA of the power system ensues to determine whether the steady-state operating condition infringes the system's operational constraints. The power network must maintain equilibrium, and energy distribution must remain within acceptable limits. Overload conditions often arise due to the disconnection of sections of the power grid. These electrical power overload conditions cause

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

additional thermal load and risk burning out components. Recent studies have considered security monitoring solutions using static power system approaches to prevent line outages. These studies have focused on two types of solutions, namely, conventional methods and (2) artificial intelligence (AI) algorithms. Both solutions provide tools that assist policymakers and grid operators to plan a reliable power network [12]–[14]. The conventional method utilizes a scalar performance index (PI) that forms the basis for judging the static security performance of the power system. For example, the authors in [15] proposed a method for calculating voltage PI using Newton–Raphson load flow. Testing the PI requires classifying the voltage security level by performing (N−1) contingency on an IEEE 39-bus test system. The authors in [3] used an algorithm named least absolute shrinkage and selection operator (LASSO). LASSO applies to an online SSA (OSSA) and bases itself on an applied security index, which selects and screens contingencies. However, many of these studies have ignored the regulation capability of the power system by using adjustable devices, such as the transformers and reactive power compensation devices in the power system.

Other suggested power system security technologies for evaluation, which incorporate statistical learning theory, include backpropagation artificial neural networks (BPANNs) [16], self-organizing-map (SOM) neural networks [17], adaptive neuro-fuzzy inference system (ANFIS) [18], support vector machines (SVM) [19], and artificial neural networks (ANNs) [20]. Most studies have discussed the applications of feedforward backpropagation (FFBP) ANN, which can resolve many problems, and its extensive use has suggested reliability [21], [22]. However, backpropagation (BP) learning algorithms contain numerous parameters that need random tuning; as an over gradient method, it has overfitting problems, and it might slowly converge to reach the local minima.

The authors in [23] applied a SOM method to a data set consisting of tested online data from an actual power system. They classified the load profile from a Greek power system to obtain the security criterion by regression to reliably estimate the post-disturbance variables. They used a hybrid method of learning based on input–output or peer-to-peer mapping called ANFIS. The ANFIS model forms ''if–then'' decision pairs, and it has remarkable appeal because it uses nonlinear modeling to extract rules in time series and forecasting [24]. The authors in [25] applied support vector regression with ANFIS models to obtain four security statuses, namely, standard, alert, emergency_1, and emergency_2. They used these statuses to classify the security of the system. ANNs should be adept at solving nonlinear functions, sorting data, recognizing patterns, optimizing processes, predicting or forecasting outcomes, identifying system processes, and simulating and managing system functions [26]. The authors in [27] applied an ANN algorithm to enhance the security of power systems. In [28], the static security index was predicted by adopting the ANN algorithm for contingency screening and ranking. In [13], the ANN algorithm was applied to enhance the security of power systems. In [14], an ANN module was used for SSA by considering the voltage and load flow in the power system

A team of scientists led by Rumelhart and McClelland in 1986 first proposed BPANN, a multilayered feedforward network that trains using an error BP algorithm. BPANN has become the most commonly used neural network model [29]. In [30], an integrated radial basis neural network with particle swarm optimization was used to reduce the training time and improve the intelligent agent performance for SSA with a single contingency. However, the authors considered the security index as part of the security assessment, which could be considered state of the art, and developed further to include the remedial actions. In [28] and [31], multilayer feedforward artificial neural network was applied for security classification and contingency selection and ranking and then compared it with radial basis function network implementation. Both techniques showed the competence of accurately assessing the security of the power system against single-line outage and significantly faster than other conventional methods. These techniques demonstrated the online implementation for SSA and monitoring. The adaptive artificial neural network (AANN) takes this further by including the remedial action with the security assessment to act rationally with the system conditions.

The offline training speed for the AI system presents a challenging issue in the static risk assessment calculation [32]. A statistical analysis of wind farm historical data was used to train a chain model and SVM. However, the system could not adapt a new case after training. The adaption issue increases system performance, especially in large power system applications.

Meng-yu and Hsiao-dong [33] tested the accuracy of power flow and quasi-static state under different load conditions. The numerical evaluation showed some misclassifications of some security cases with heavy loading conditions. However, the load variations and generation redispatch patterns were considered during the increases in loading conditions. The authors suggested developing a full power flow model by including reactive power/voltage control aspects, which has been considered in the AANN algorithm.

This study aims to develop an AANN application module based on the ANN algorithm. To this end, the methodology is enhanced to screen contingencies and develop a security assessment ranking that subsequently reduced the computation scale of a real-time SSA. This developed application comprises the following procedural elements. (1) Automatic SSA data generation is developed. It evaluates the security of the power system's operating status and distinguishes them as secure, alarmed, and insecure states. (2) Variables, such as the status of the lines and the corresponding security to the developed AANN module, are adapted in the power system. (3) Prediction is performed on the basis of the power system variables under operating state from the test after adapting the new data to the training sets.

The main contributions of this study are as follows.

1. An OSSA module that screens and ranks the severity of contingencies automatically is developed in this study. This module considers the effects of adjustable devices and identifies the operating status using current operating point variables (its computational time challenge that has been solved by using the AANN).
2. A novel method is developed based on AANN algorithm. The method predicts the security status and evaluates the operating status from any cascading case by suggesting the estimated generator redispatch and/or load shedding.
3. The system considers the varying base load conditions and generation aspects to estimate the remedial control action in a short computational time.

The rest of this paper is organized as follows. Section 2presents the implementation of the proposed AANN method in security assessment. Section 3 describes the tests and the findings. The final section concludes and highlights the important contributions of this work.

II. AANN IMPLEMENTATION IN SECURITY ASSESSMENT

An AANN is applied to predict the optimum amount of generation redispatch and load shedding in megawatts. The definition of an AANN emphasizes its use in conjunction with an automatic data generation method. However, the additional adjective, that is, adaptive, refers to the enhancement of the ANN to be adaptive with the power system changing, not just within the neural network. Another aspect is to improve the learning for the BP algorithm by using the root mean square error (RMSE) for the error concentration [27].

The AANN is developed to be included as a steady-state security assessment tool for supplying a possible control action to mitigate an insecure situation when a credible contingency occurs. It is based on function approximation, which is centered on the mapping between a pre-disturbance operation point and the security margin, including the control action of the contingencies. The AANN is developed by object-oriented programming using Python 2.7, which allows parallel processing for multiple neural networks. The implementation of the AANN for the Malaysian power grid security assessment shown in Fig. 1, which requires four neural networks running in parallel. Two stopping criteria factors are considered for the AANN training schema. The first factor is when the RMSE reaches a performance goal value. The second factor is when the training reaches a certain number of iterations, and the network cannot reach the threshold error value. The limitation of the neural network is that the time taken for the training depends on the stopping criteria. For the first training, the neural network takes a long time when the RMSE is selected with a small value. Thus, numerous iterations should be assumed to stop the process. The AANN testing error increases with the RMSE. Therefore, a change in the number of hidden nodes should be applied. For this study, the selection of 4.0E+4 epochs shows good promise for the Malaysian power system.

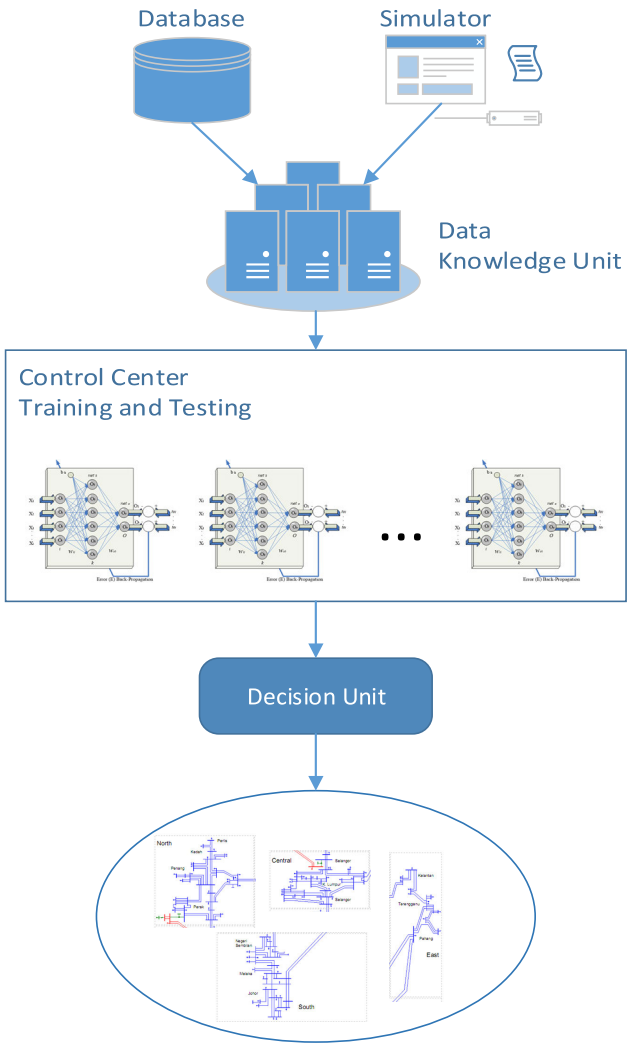

FIGURE 1. AANN implementation for power system security assessment.

Practically, in a large system, a clustering method is used on the basis of system islands or areas [34]. The system is divided into many areas on the basis of the number of buses, generators, and loads. Furthermore, several networks are used to handle a large system, where each area uses different neural network architectures at the control central unit. Parallel computing can be implemented for the proposed control method because it has been previously used for the voltage and line flow security assessment [35] to speed up the training time of the neural network. At the final stage, the predicted action with optimal amount is finalized at the decision unit before final implementation.

A. AUTOMATIC DATA KNOWLEDGE GENERATION

The superior quality of data is essential for the neural network approach. Therefore, training data should be correctly generated, and the neural network should have good generalization capability. Therefore, the power system simulator will ensure all generated cases at different load levels are included in

the training data knowledge. The following several points are considered for the developed AANN:

1. The automatic procedure at the data knowledge unit guarantees good data quality because various system operating points and contingencies are demonstrated for each load level by the simulator.
2. The accuracy and applicability of the proposed approach are based on the use of feature selection and extraction methods in data generation. Parameters from the contingency analysis are extracted as statistical features and used as an input feature for the classification problem. The simulation model is developed using PSSe software engine to build the training knowledge data for the neural network. However, the AANN adapts any new simulated case, making the neural network extendable.
3. The training data are generated from the minimum load up to maximum load level by constant increments. In this manner the capability of the robust AANN in detecting a situation and recommending an appropriate action can be verified.
4. Optimization methods are used for the parameter estimation of the AANN. The RMSE equation improves the neural network sensitivity when the error reaches its minimum with a reduced number of iterations. Three optimization methods are used for the parameter estimation of the AANN.
    a) The number of hidden neurons is optimized for the best AANN performance.
    b) The optimization includes the selection of control actions to eliminate the voltage violations and line overloads.
    c) AANN is used to predict the optimum amount of generation redispatch and load shedding in megawatts after a contingency occurs to enhance system security

    These factors enhance the performance of the neural network application in predicting the desirable output accurately. The automatic data knowledge generation is based on the variation of operating points, which, in turn, is based on the load profile, production, contingency, and operational practices. Most contingency effects can be reduced by applying preventive/corrective control action. Conversely, the output or target data (amount of generation redispatch and load shedding) are automatically generated for each contingency to be included with a sample of the neural network. Generation rescheduling and load shedding are considered as a solution for increasing system reliability and security.

Each load level or operating point is analyzed by power flow computation. All contingencies are considered without any ranking process to allow the AANN to solve the control issue. However, the training might be slow but not the testing, and not all contingencies require control action. The security

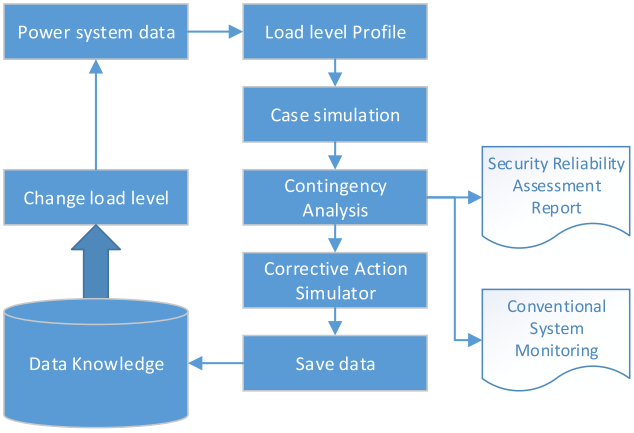

FIGURE 2. Schema of automatic data generation system.

margins are determined using the load flow by a simple computation method.

The load level profile is selected using the system load profile, as shown in Fig. 2 (usually it functions from a minimum operating point of 60% up to the maximum operating point of 100% using a specific increment of load scale distributed over all loads). The data are divided into different schemas, where the data has to be saved before the training. These schemas are divided as follows:

- Contingency analysis data: contain bus voltage, terminal line flow, and generation/ load amounts for each area and subarea;
- Corrective action data: contain the amount of generation redispatch and load shedding.

With these schemas, the neural network can determine its output over various levels of system operating points. However, a small increment of load level results in generating additional cases or patterns and vice versa. The scaling of a nonslack generator is required before running the load flow solution to ensure no mismatch tolerance in the system, which is used to check for the largest initial active or reactive power mismatch. In other words, no additional generation occurs when the load is increased or decreased. The maximum and minimum machine active power output, namely, PMAX and PMIN, are entered in megawatts and set as power limits contained in the working case.

Contingency analysis is used for security assessment. Thus, a report can be presented at this stage for the bus voltage or line overloading violation, as shown in Fig. 3, where i is the bus number, and three security classifications exist, namely, alert, emergency, and extreme emergency. These classifications are estimated using conventional methods for testing and verification purposes (Appendixes A.1–A.4).

The aforementioned reports help in enhancing the system design by diagnosing the weak parts of the system. However, the contingency analysis depends on the model of the power system, which is used to study the outage effects and alert the operator of any overload or voltage violation.

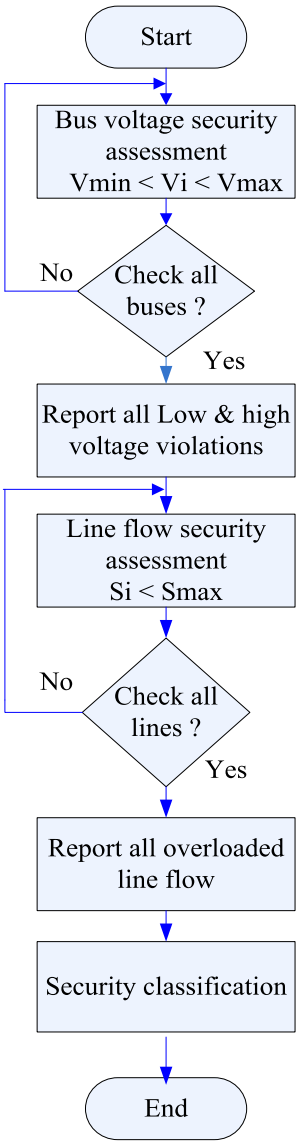

FIGURE 3. Schema of security assessment.

After corrective action is taken and stored in the data knowledge, the running case is saved for the record. Continually, this procedure is repeated until the maximum load level at which the system can operate without suffering any blackout case is reached.

B. DATA NORMALIZATION

Normalization is conducted at the beginning of the AANN to convert the data into a form that the neural function can handle [27]. Negative values are presented for generator rescheduling. Hence, normalizing the vector data for the inputs and targets are required to position all the data in the range between -1 and 1 to prevent any volatility in the network weights. For the same reason, the selection of the activation function for the hidden and output nodes is based on the input and output data range [36]. The number of neurons in the hidden layer is not specified. Therefore, an optimization method is developed to handle this matter [37]. The two other factors that can affect the ANN output are the learning rate coefficient, which changes the size of the weight adjustments, and the momentum term, which can improve the convergence rate when added to a grand expression. An effective selection method for the learning and momentum rates, which was reported in [38], is considered in the current study.

C. TRAINING PROCESS

The BP algorithm is similar to the perceptron network algorithm with more than one layer, as shown in Fig. 4. It contains three layers. The first one is connected to the inputs. The second layer contains the activation function. The third layer is the output of the network. The FFBP algorithm is the most commonly used method for training multilayer feedforward networks [39]. This technique was popularized by Rumelhart et al. [40], and it is similar to the perceptron network algorithm with more than one layer (Fig. 4). In the current work, FFBP is developed as a training algorithm for the AANN. The proposed network architecture consists of three layers that satisfy the performance requirements.

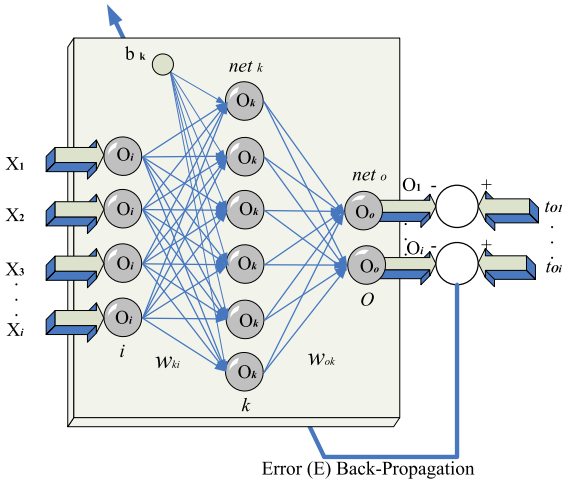

FIGURE 4. BP model architecture.

The weights are initialized with random values. The error is calculated at every single iteration, and the learning procedure is repeated for all patterns ($p = 1, 2, \ldots, N$) or epochs ([Input, Output]) to correct the initial value for all the weights. The BP algorithm has a high mathematical foundation. With smooth training, it can provide accurate testing results.

The AANN is applied to enhance system security by controlling the generator supplies and loads. In other words, the AANN is used to predict the optimum amount of generation redispatch and load shedding in megawatts after a contingency occurs to enhance the system security.

During training, the inputs are applied against their output targets and propagated through the network layers to calculate the sum of the errors. An enhancement is determined by using the sum of theRMSE, as shown in Equation (1). The RMSE

```
Initiate random seed Matrix for all weights first_run
Initiate tanh(-0.1*x) function for all nodes (neurons)
Read the inputs and outputs
Initiate the number of hidden layer neurons
Create the activation functions for all nodes
Create the required weights
Backpropagate with optimal learning rate and momentum factor
For every output node:
    calculate the error function for the output nodes
For every hidden node:
    Initiate the error value
    For every output node:
        Calculate the error function for the hidden nodes
Update the weights in hidden and output layers
Initiate the RMSE
For every node in output layer:
    Evaluate the RMSE based on selected target
    Return RMSE
```

FIGURE 5. Training for the first time running "Training_new".

```
Read the latest used weight for the same number neurons
Update the activation functions for all nodes(neurons)
Backpropagate with optimal learning rate and momentum factor
For every output node:
    calculate the error function for the output nodes
For every hidden node:
    Initiate the error value
    For every output node:
        Calculate the error function for the hidden nodes
Update the weights in hidden and output layers
Initiate the RMSE
For every node in output layer:
    Evaluate the RMSE based on selected target
    Return RMSE
```

FIGURE 6. Training for new data adaption "Training_adapt".

shows a better performance than the mean square error in terms of sensitivity and accuracy.

$$RMSE = E_{sum} = \sqrt{\frac{1}{N}\sum_{p=1}^{N}(t_o^p - O_o^p)^2}, \quad (1)$$

where N is the total number of patterns.

The activation function of the hidden and output neurons is a hyperbolic tangent function (the advantage of using a function is to be symmetrical with respect to the origin [40]). The threshold error (RMSE) is calculated for finding the training error. Fig. 5 presents the pseudocode of the training process at the first stage. The AANN is plugged into the system where the training is performed to adapt any new data (not included in the first training data set) for the same power system area or cluster, as shown in Fig. 6. The AANN training class for each power system area or cluster is shown in Fig. 7.

D. TESTING PROCESS

Testing is the last step of the implementation approach to verify the model performance. Once the networks finish the training process and reach one of the two stopping criteria, network testing is required to verify the AANN and check if it is working remarkably under the required conditions. To this end, another input data set called testing data, which is not included in the training, is generated. In other words, the same system model with different load scales to those used in the training is selected. In this manner, a data set with the same

```
Data Normalization
Training (patterns, number of maximum iterations, performance
         threshold, learning rate and momentum factor)

For i in range of maximum number of iterations:
    Initiate total error function (TEF)
    For every pattern:
        Read input and output data
        Update the activation functions
        Update the weights in hidden and output layers
        TEF = TEF + Backpropagate error
        Print RMSE
        If TEF < performance threshold:
              Break
              print Performance level reached in i iterations
        Else:
              Break
              Print AANN could not reach the required performance in
              i iterations
```

FIGURE 7. Training for AANN algorithm "Training".

number of inputs but under different operating conditions is generated.

Many contingencies can be tested under various load levels. Thus, the verification method compares the AANN output with the original output, as calculated by using the PSSTME simulator [41]. The result is displayed and saved after destabilization, which is conducted to return to the original values of the generator redispatch/load shedding in megawatts. Once the network completes training and passes the testing step, it is ready to be connected to the power system for predicting the optimum amount of generation redispatch and load shedding under steady-state analysis or real-time operation. The implemented testing is presented in Fig. 8.

```
Data normalization
Nodes activation
Read the last saved weights for the same used number of neurons
For every output pattern:
    Update the activation nodes for inputs, hidden and output layers
    Print the output result
Print timing process
Destabilize the generator re-dispatch and load shedding output
Compare the result with original simulated output
Print final error in MW for every output
Solve power flow security assessment
Save (bus voltage, line flow) after control action
Generate security assessment report
```

FIGURE 8. Testing for AANN algorithm "Testing".

III. RESULTS AND DISCUSSION

The novelty of this work is avoiding the retraining for new loading scenarios. Therefore, a long training is required to reach the expected results, and it is required for one time once the AANN is installed into the system. The new loading scenarios do not take a long time (depending on the number of cases that need to be adapted) because it is a discrete training process. Thus, the neural network starts from the last point (In the condition that it is the same system). The only case that requires to start the training again is when new transmission lines exist, the network structure is changed, or new generators are installed.

Regarding testing, error decreases up to some epochs and then increases. The final optimal results are achieved after a long optimization process and stability check. Stability check is performed by monitoring errors and ensuring that the error values are not frequently increased over the training and testingprocesses. The optimal network is used over different load level scenarios to check the validity of the developed AANN.

The proposed method is tested on a practical 87-bus system after an initial training of approximately 3 h. Nevertheless, the time during the adaption process is only a few moments. A long time is required for training a large-scale power system comprising several thousand buses. In this regard, the proposed method is addressed to reduce the computational time during the ANN training when the system configuration is changed slightly. The new cases are generated by the automatic data generation model and adapted to the AANN data knowledge. The weights between the neural network layers are changed and saved for the next adaption. The AANN output (amount of generation redispatch and load shedding) is compared with the actual data from the conventional steady-state security assessment and control to evaluate the performance of the suggested AANN.

The Peninsular Malaysian grid is divided into four areas, namely, north, east, central, and south (Fig. 9). The northern area is divided into four zones representing the states of Perlis, Kedah, Pulau Pinang, and Perak. The eastern area includes the zones of Kelantan, Terengganu, and Pahang. The central area consists of Selangor and Wilayah Persekutuan. The southern area comprises the states of Negeri Sembilan, Melaka, and Johor. The total of the system production and system load is 10652.4 and 10456.5 MW, respectively (the year is 2007). The percentage of system losses is 1.84% over the total generation. The subsystems interchange the power between each other to satisfy system security. A strategy of using a different neural network for controlling each area is applied. In this case, four neural networks are used to provide the optimal amount of generation redispatch and load shedding.

The new algorithm is demonstrated on the Malaysian power grid by using the developed AANN tool written in Python 2.7, which is tested on Windows 7 with Intel Core i7 processor and 4 GB RAM. The neural network is tested on three load levels (i.e., light load, medium load, and heavily congested) to check the capability of using an adaptive neural network application tool for security assessment.

The (N−1) contingency analysis is conducted on the system for the automatic data knowledge generation. Then, it is used to estimate the control action with different loading margins for any line outage. The data knowledge has four data sets representing the four areas in the system. Therefore, different AANN architectures are designed to provide an optimal value of the preventive/corrective action when the system is under a contingency and control action is required. The number of hidden neurons is adjusted on the basis of the network inputs and outputs in each area. The AANN

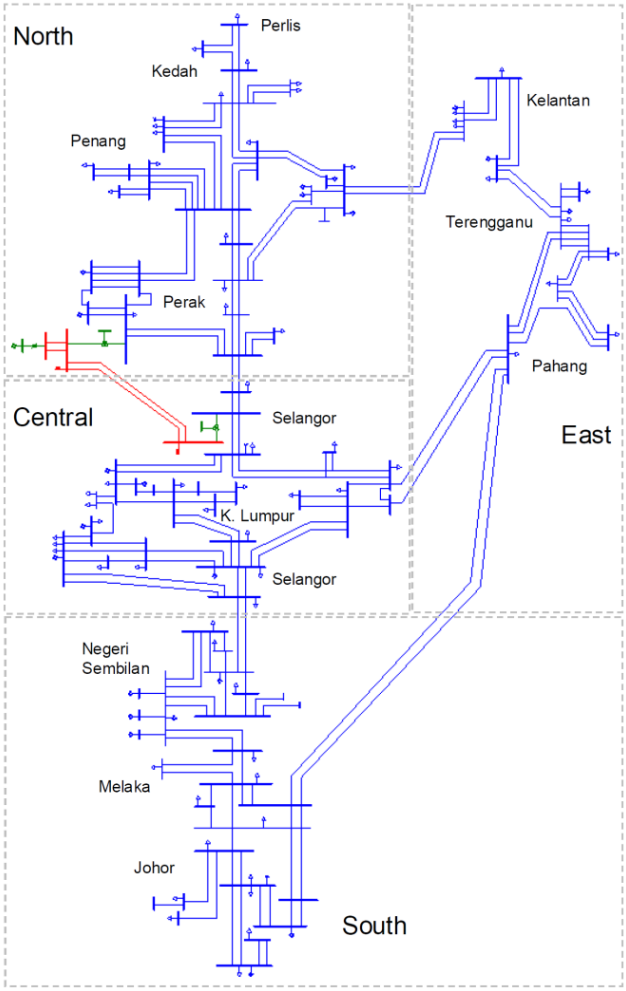

FIGURE 9. Single-line diagram of the Malaysian power grid.

TABLE 1. Adaptive neural network architecture for each area.

Area	North	East	Central	South
Number of neurons in the input layer	81	33	65	62
Number of neurons in the output layer	23	12	23	21
Number of neurons in the hidden layer	38	38	38	36

configuration, including its input, hidden, and output layers for each area, is presented in Table 1. The number of neurons in the input layer is fixed by the number of selected buses and lines. The number of neurons in the output layer is fixed by the number of selected generators and loads. The number of neurons in the hidden layer is based on optimization method, which depends on system training and testing errors.

The number of neurons in the input layer depends on the number of buses and lines in a particular area. Likewise, the number of neurons in the output layer depends on the number of generators and loads in the selected area. This

method has been applied in many studies, such as in [42]. Four clustered AANNs are used in parallel for the Peninsular Malaysian grid (central, east, north, and south). The number of neurons in the output layer depends on the number of generators and loads in each selected area for generation redispatch and load shedding. Therefore, the total number of outputs are 79 (23+12+23+21) with 79 remedial actions when it is required.

The inputs are bus voltages and thermal flow percentages exclusive of transformers and generator buses. For all the cases conducted, the weights and thresholds are initialized with random values between −0.5 and +0.5. In addition, the number of hidden neurons is optimized for best AANN performance. The momentum factor is dynamically changed in the range of 0.1–0.04 on the basis of the redundancy of the RMSE in the BP algorithm to provide a smooth training error curve. The change results in a remarkable performance. The learning rate is set as constant at 0.01 for best accuracy.

The data knowledge of the training data containing (N−1) contingencies starts from the minimum load level (60% of the total system load) up to the maximum load with a 5% increment. The training patterns are generated by increasing the total load by 5%, assuming the increases are distributed equally. However, this practice is applied in the simulation stage in the industry, and the same practice by the Advance Power Solution Company is followed. This company provides consultation, simulation, and testing to verify the system configuration in the Peninsular Malaysian grid and prove the AANN performance and robustness to be applied for the power system SSA, which can supply the neural network with historical data in any further research. The main contribution of this study is the generation redispatch and load shedding in each zone. The distribution system simulation provides the load changing in each load. Therefore, the 5% increase, starting from the minimal load operating at 60%, can be covered. During testing, a different point is assigned to obtain new data within the range of 5%. The data can also be generated randomly. However, this possibility can be considered in another study where the AANN can be tested. The total number of contingencies used in the training data is shown in Table 2.

TABLE 2. Training data knowledge for the Peninsular Malaysian grid.

	North	East	Central	South
Number of contingencies + Base case	72	32	60	53
Number of patterns	648	288	540	477

Meanwhile, the testing data sets are generated at different load levels (Table 3). Each area is tested using three load level scenarios to check the AANN accuracy at different operating points. Three testing load scenarios for each area are demonstrated to verify the AANN performance corresponding to a various level of security. The number of generators, loads, buses, branches, and switched shunts are listed in Table 4.

TABLE 3. Testing load scenarios in the Peninsular Malaysian grid.

North		
Load scenario	Total generation (MW)	Total load (MW)
Light load	2340.379	1129.521
Medium load	2672.511	1462.822
Heavily congested	3045.975	1833.156
East		
Load scenario	Total generation (MW)	Total load (MW)
Light load	1362.191	540.0613
Medium load	1764.149	699.4237
Heavily congested	2210.769	876.493
Central		
Load scenario	Total generation (MW)	Total load (MW)
Light load	2231.441	3204.767
Medium load	2889.899	4150.437
Heavily congested	3621.519	5201.18
South		
Load scenario	Total generation (MW)	Total load (MW)
Light load	1018.334	1483.886
Medium load	1318.826	1921.754
Heavily congested	1652.706	2408.274

TABLE 4. Number of generators, loads, buses, branches, and switched shunts.

Area	Generators	Loads	Buses	Branches	Switched Shunts
North	7	18	30	61	6
East	4	10	10	21	3
Central	5	22	27	54	4
South	7	15	26	45	1
Total	23	65	93	172	14

Generally, a contingency in one area can affect the security in another area due to the power interchange among these areas. However, further development is required to eliminate these problems. In this case study, an individual area controller is considered a solution for the power system security assessment.

Fig. 10 shows the testing results obtained from the AANN for the northern area of the system. The percentage RMSE of the training is 2.1524% using 4.0E+4 epochs. The difference between the maximum error and baseload (1129.521 MW) is in the neighborhood of 50 MW, thereby indicating an accuracy of more than 95.57% in the AANN test results.

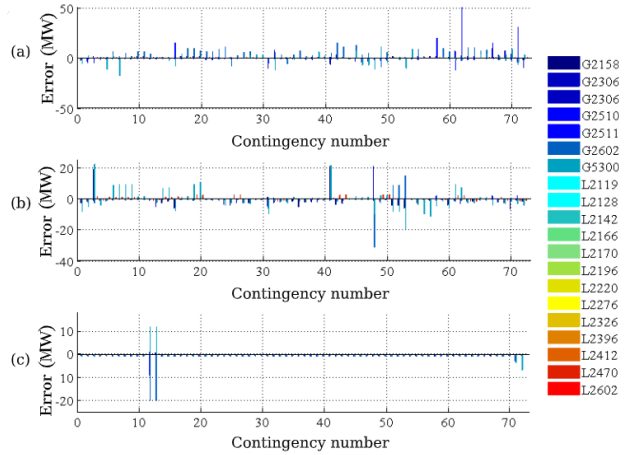

FIGURE 10. Sample of AANN testing result for the northern area: (a) light load, (b) medium load, and (c) heavy load.

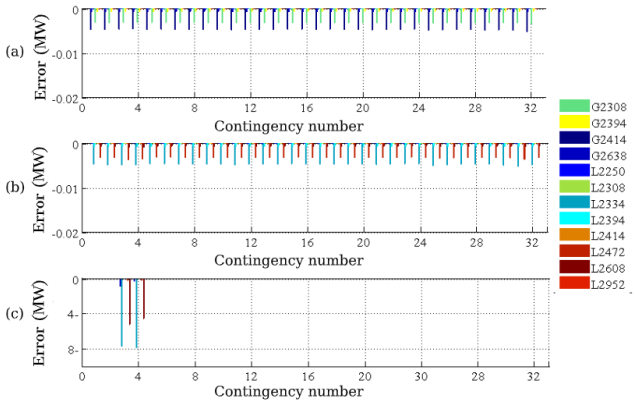

FIGURE 11. Sample of AANN testing result for the east area: (a) light load, (b) medium load, and (c) heavy load.

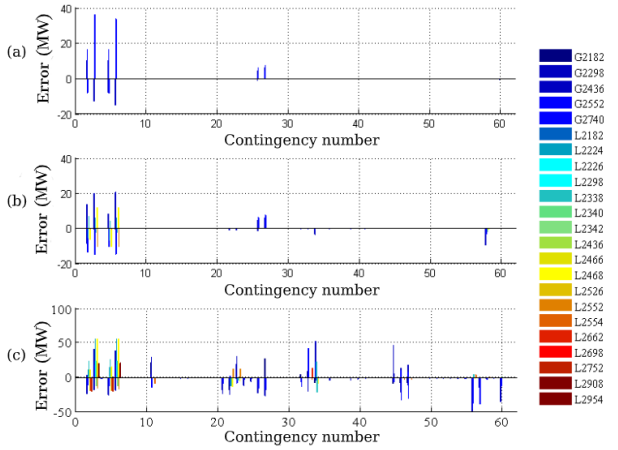

FIGURE 12. Sample of AANN testing result for the central area: (a) light load, (b) medium load, and (c) heavy load.

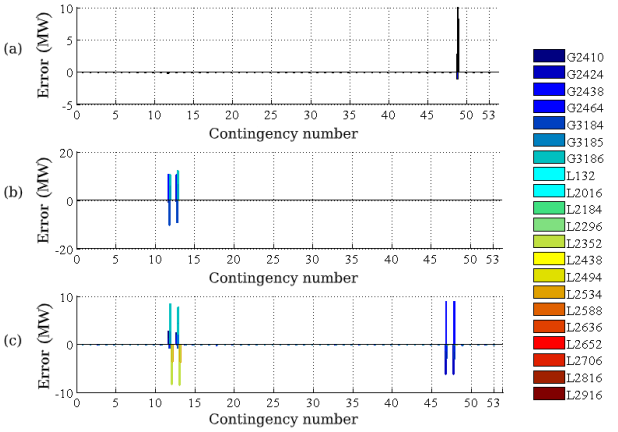

FIGURE 13. Sample of AANN testing result for the southern area: (a) light load, (b) medium load, and (c) heavy load.

The AANN specifies the range of operation and the control actions allowed for different equipment and automatic controls. The most severe contingency depends on the location and the type of stability phenomenon considered. The influences of equipment outage or automatic controls are different, and they are specified for each security issue.

The east area of the system has a reduced number of contingencies. Hence, it has a better AANN performance, with an RMSE of 0.2111%, during training compared with other areas. Fig. 11 shows the AANN testing error in MW for each unit. The maximum difference between the actual and AANN outputs is less than 8 MW (Case (c) in Fig. 11). On this basis, the accuracy is approximately 99.99%.

For the central area, the AANN training RMSE is 1.71% using 4.0E+4 epochs. Fig. 12 shows a clear trend of an increase in the AANN testing error for some units. This increase is caused by the security criteria arising inside an area when the load is more than the generation. However, comparing the maximum testing error shows a significant accuracy of less than 52 MW with respect to the total load of 5201.18 MW when the system is highly loaded. The AANN performance in this area is approximately 99.99%.

As shown in Fig. 13, the AANN controller performs well in the southern area of the system. The training RMSE is 2.35% using 4.0E+4 epochs. Therefore, the AANN tool can provide the optimal amount of generation redispatch and load shedding in megawatts. The AANN performance is approximately 99.99%.

Modern energy management systems frequently perform a steady-state security assessment and control to provide the power system the capability to withstand numerous credible contingencies.

The assessment of these contingencies involves the selection of credible contingencies and then the estimation of the system response to each particular contingency. Therefore, a remedial action and optimization process should be concerned with the selection of control actions to eliminate the voltage violations and line overloads. In this system, the AANN shows good promise in

A.1 Security assessment report for the northern area.

Light load

Flow violations > 80% of rating A

From bus	To bus	Bus (kV)	Rating	AMP flow	Flow (%)	Contingency no.	Security classification
62	2602	275	487	450.1	92.4	SINGLE 47	Emergency
2130	2698	275	683	683.7	100.1	SINGLE 61	Extreme emergency
2130	2698	275	683	683.7	100.1	SINGLE 60	Extreme emergency
2276	2306	275	487	487.5	100.1	SINGLE 31	Extreme emergency
2306	2602	275	487	454.9	93.4	SINGLE 2	Emergency

Low-voltage range violations

None

High-voltage range violations

Bus no.	Voltage level (kV)	Bus voltage (p.u.)	Contingency no.	Security classification
2128	275	1.05848	UNIT 71	Insecure
2142	275	1.0533	UNIT 71	Insecure
2166	275	1.05473	UNIT 71	Insecure
2170	275	1.0525	UNIT 71	Insecure
2196	275	1.05331	UNIT 71	Insecure
2220	275	1.06063	UNIT 71	Insecure
2248	275	1.05592	UNIT 71	Insecure
2326	275	1.05593	UNIT 71	Insecure
2412	275	1.05388	UNIT 71	Insecure
2470	275	1.05923	UNIT 71	Insecure
2722	275	1.05437	UNIT 71	Insecure
2814	275	1.05332	UNIT 71	Insecure
5500	500	1.05114	SINGLE 15	Insecure
5510	500	1.05121	SINGLE 15	Insecure

Medium load

Flow violations > 80% of rating A

From bus	To bus	Bus (kV)	Rating	AMP flow	Flow (%)	Contingency no.	Security classification
62	2602	275	487	392.3	80.6	SINGLE 47	Alert
2119	2130	275	683	658.3	96.4	SINGLE 12	Emergency
2119	2130	275	683	658.3	96.4	SINGLE 11	Emergency
2130	2698	275	683	653	95.6	SINGLE 61	Emergency
2130	2698	275	683	653	95.6	SINGLE 60	Emergency
2276	2306	275	487	487.5	100.1	SINGLE 2	Extreme emergency

Low-voltage range violations

None

High-voltage range violations

Bus no.	Voltage level (kV)	Bus voltage (p.u.)	Contingency no.	Security classification
2128	275	1.05424	UNIT 71	Insecure
2166	275	1.05137	SINGLE 50	Insecure
2220	275	1.05651	UNIT 71	Insecure
2248	275	1.05248	SINGLE 50	Insecure
2326	275	1.05071	UNIT 71	Insecure
2470	275	1.05529	UNIT 71	Insecure
2722	275	1.05115	SINGLE 50	Insecure

A.1 *(Continued.)* Security assessment report for the northern area.

Heavily congested

Flow violations > 80% of rating A

From bus	To bus	Bus (kV)	Rating	AMP flow	Flow (%)	Contingency no.	Security classification
2119	2130	275	683	674.3	98.7	SINGLE 12	Emergency
2119	2130	275	683	674.3	98.7	SINGLE 11	Emergency
2130	2698	275	683	624.2	91.4	SINGLE 61	Emergency
2130	2698	275	683	624.2	91.4	SINGLE 60	Emergency
2276	2306	275	487	420.2	86.3	SINGLE 11	Alert

Low-voltage range violations

None

High-voltage range violations

Bus no.	Voltage level (kV)	Bus voltage (p.u.)	Contingency no.	Security classification
2220	275	1.05115	SINGLE 50	Insecure

A.2 Security assessment report for the east area.

Light load

Flow violations > 80% of rating A

None

Low-voltage range violations

None

High-voltage range violations

None

Medium load

Flow violations > 80% of rating A

None

Low-voltage range violations

None

High-voltage range violations

None

Heavily congested

Flow violations > 80% of rating A

From bus	To bus	Bus (kV)	Rating	AMP flow	Flow (%)	Contingency no.	Security classification
2250	2334	275	587	587.2	100	SINGLE 2	Extreme emergency

Low-voltage range violations

None

High-voltage range violations

None

handling single contingencies at different load levels with high-speed response time (less than one millisecond per contingency).

A.3 Security assessment report for the central area.

Light load

Flow violations > 80% of rating A

From bus	To bus	Bus (kV)	Rating	AMP flow	Flow (%)	Contingency no.	Security classification
72	2338	275	587	587.6	100.1	SINGLE 4	Extreme emergency
72	2340	275	587	587.6	100.1	SINGLE 5	Extreme emergency
73	2338	275	587	587.6	100.1	SINGLE 1	Extreme emergency
73	2340	275	587	587.6	100.1	SINGLE 2	Extreme emergency
2340	2684	275	683	752.4	110.2	SINGLE 26	Extreme emergency
2340	2684	275	683	752.4	110.2	SINGLE 25	Extreme emergency

Low-voltage range violations

None

High-voltage range violations

Bus no.	Voltage level (kV)	Bus voltage (p.u.)	Contingency no.	Security classification
2908	275	1.05599	SINGLE 16	Insecure
5520	500	1.05641	SINGLE 44	Insecure

Medium load

Flow violations > 80% of rating A

From bus	To bus	Bus (kV)	Rating	AMP flow	Flow (%)	Contingency no.	Security classification
72	2338	275	587	554.4	94.4	SINGLE 4	Emergency
72	2340	275	587	554.2	94.4	SINGLE 5	Emergency
73	2338	275	587	554.4	94.4	SINGLE 1	Emergency
73	2340	275	587	554.2	94.4	SINGLE 2	Emergency
2340	2684	275	683	912.7	133.6	SINGLE 26	Extreme emergency
2340	2684	275	683	912.7	133.6	SINGLE 25	Extreme emergency
2698	2130	275	683	567.7	83.1	SINGLE 44	Alert
2698	2130	275	683	567.7	83.1	SINGLE 44	Alert

Low-voltage range violations

None

High-voltage range violations

Bus no.	Voltage level (kV)	Bus voltage (p.u.)	Contingency no.	Security classification
2908	275	1.05559	SINGLE 16	Insecure
5520	500	1.05601	SINGLE 44	Insecure

Heavily congested

Flow violations > 80% of rating A

From bus	To bus	Bus (kV)	Rating	AMP flow	Flow (%)	Contingency no.	Security classification
72	2338	275	587	677.6	115.4	SINGLE 4	Extreme emergency
72	2340	275	587	743.1	126.6	SINGLE 5	Extreme emergency
73	2338	275	587	677.6	115.4	SINGLE 1	Extreme emergency
73	2340	275	587	743.1	126.6	SINGLE 2	Extreme emergency
2182	2226	275	587	487	83	SINGLE 32	Alert
2338	2468	275	683	683.7	100.1	SINGLE 20	Extreme emergency
2339	2468	275	683	656.1	96.1	SINGLE 21	Emergency
2340	2684	275	683	1093.3	160.1	SINGLE 26	Extreme emergency
2340	2684	275	683	1093.3	160.1	SINGLE 25	Extreme emergency
2436	2752	275	683	721.3	105.6	SINGLE 46	Extreme emergency
2436	2954	275	1000	871.9	87.2	UNIT 55	Alert
2684	3WN DTR	WN D 2	1000	908	90.8	UNIT 57	Emergency
2698	2130	275	683	694.9	101.7	SINGLE 44	Extreme emergency
2698	2130	275	683	694.9	101.7	SINGLE 44	Extreme emergency
2752	2956	275	683	683.7	100.1	SINGLE 31	Extreme emergency
5520	3WN DTR	WN D 1	1000	920.9	92.1	UNIT 57	Emergency

Low-voltage range violations

None

High-voltage range violations

Bus no.	Voltage level (kV)	Bus voltage (p.u.)	Contingency no.	Security classification
2908	275	1.05514	SINGLE 16	Insecure
5520	500	1.05553	SINGLE 44	Insecure

IV. CONCLUSION

This study presents an enhanced algorithm for the schema of Malaysian power system security assessment inclusive of remedial actions using developed AANN application. The AANN presented was designed to determine the effects of different disturbances and estimate the optimal amount of generation redispatch and load shedding in megawatts. Feature selection and data extraction methods, as well as power system clustering, were used to reduce the number of inputs and enhance the model generalization capability. The RMSE equation also brought advantages in terms of improving neural network sensitivity. This improvement was confirmed by the results obtained from testing. The proposed algorithm showed good promise to provide an appropriate solution for secure operation. The advantages of the presented approach are as follows.

1. The weights can be updated when new cases need to be adapted.
2. The testing procedure of the AANN model is rapid.
3. A security indication is provided quickly with a control action to recover the system from any security interruption.
4. Power system network clustering is applied to reduce the number of inputs/outputs. As a result, it can control each area individually and consider different network topologies.
5. The training data provide the opportunity for the AANN model to control the system under a contingency for a wide range of load levels.
6. Economic operation is increased by achieving minimum power losses when the system is operating under a contingency.
7. The accuracy of the proposed approach is based on automatic data generation and the use of feature selection and extraction methods.

A.4 Security assessment report for the southern area.

Light load

Flow violations > 80% of rating A

None

Low-voltage range violations

None

High-voltage range violations

None

Medium load

Flow violations > 80% of rating A

From bus	To bus	Bus (kV)	Rating	AMP flow	Flow (%)	Contingency no.	Security classification
2352	2464	275	487	487.5	100.1	SINGLE 46	Extreme emergency
2352	2464	275	487	487.5	100.1	SINGLE 46	Extreme emergency

Low-voltage range violations

None

High-voltage range violations

None

Heavily congested

Flow violations > 80% of rating A

From bus	To bus	Bus (kV)	Rating	AMP flow	Flow (%)	Contingency no.	Security classification
2352	2464	275	487	487.5	100.1	SINGLE 46	Extreme emergency
2352	2464	275	487	487.5	100.1	SINGLE 46	Extreme emergency

Low-voltage range violations

None

High-voltage range violations

None

The proposed method showed better accuracy than the neuro-fuzzy logic controller method when it was applied to the Peninsular Malaysian grid for determining the amount of load shed, for which the neuro-fuzzy logic controller achieved accuracy was in the range of 93%–99%. By contrast, the proposed method achieved accuracy in the range of 95%–99.99%. However, the AANN implementation included preventive/corrective control action consisting of generation redispatch and load shedding, whereas methods in References [43], [44] considered only load shedding as a control action. The results proved the capability of the proposed algorithm for steady-state security assessment and control within one millisecond.

APPENDIX

See Tables A.1–A.4.

ACKNOWLEDGMENT

The authors would like to express their great appreciation to the Advanced Power Solutions Sdn. Bhd. for the facilities provided and data support during the planning and development of this research work.

REFERENCES

[1] S. Kamali and T. Amraee, "Blackout prediction in interconnected electric energy systems considering generation re-dispatch and energy curtailment," *Appl. Energy*, vol. 187, pp. 50–61, Feb. 2017.
[2] R. Zaman and T. Brudermanna, "Energy governance in the context of energy service security: A qualitative assessment of the electricity system in Bangladesh," *Appl. Energy*, vol. 223, pp. 443–456, Aug. 2018.
[3] Y. Li, Y. Li, and Y. Sun, "Online static security assessment of power systems based on lasso algorithm," *Appl. Sci.*, vol. 8, no. 9, p. 1442, Aug. 2018.
[4] G. Andersson, P. Donalek, R. Farmer, N. Hatziargyriou, I. Kamwa, P. Kundur, N. Martins, J. Paserba, P. Pourbeik, J. Sanchez-Gasca, R. Schulz, A. Stankovic, C. Taylor, and V. Vittal, "Causes of the 2003 major grid blackouts in North America and Europe, and recommended means to improve system dynamic performance," *IEEE Trans. Power Syst.*, vol. 20, no. 4, pp. 1922–1928, Nov. 2005.
[5] S. Mukherjee, "Northern India power grid failure due to extraterrestrial changes," *Earth Sci. Climate Change*, vol. 6, no. 2, pp. 1–3, Feb. 2015.
[6] I. Ahmad, F. Khan, S. Khan, A. Khan, A. W. Tareen, and M. Saeed, "Blackout avoidance through intelligent load shedding in modern electrical power utility network," *J. Appl. Emerg. Sci.*, vol. 8, no. 1, pp. 48–57, 2018.
[7] I. Marwat, F. Khan, and A. Rehman, "Avoidance of blackout using automatic node switching technique through ETAP," *Int. J. Sci. Eng. Res.*, vol. 8, no. 10, pp. 715–720, Oct. 2017.
[8] O. P. Veloza and F. Santamaria, "Analysis of major blackouts from 2003 to 2015: Classification of incidents and review of main causes," *Electr. J.*, vol. 29, no. 7, pp. 42–49, Sep. 2016.
[9] A. Ukil, *Intelligent Systems and Signal Processing in Power Engineering*. Berlin, Germany: Springer-Verlag, 2007.
[10] N. A. Ahmad and A. A. Abdul-Ghani, "Towards sustainable development in Malaysia: In the perspective of energy security for buildings," *Procedia Eng.*, vol. 20, pp. 222–229, Jul. 2011.
[11] D. N. A. Talib, H. Mokhlis, M. S. A. Talip, K. Naidu, and H. Suyono, "Power system restoration planning strategy based on optimal energizing time of sectionalizing islands," *Energies*, vol. 11, no. 5, pp. 1–17, May 2018.
[12] Q. Zhou, J. Davidson, and A. A. Fouad, "Application of artificial neural networks in power system security and vulnerability assessment," *IEEE Trans. Power Syst.*, vol. 9, no. 1, pp. 525–532, Feb. 1994.
[13] S. Varshney, L. Srivastava, and M. Pandit, "ANN based integrated security assessment of power system using parallel computing," *Int. J. Elect. Power Energy Syst.*, vol. 42, no. 1, pp. 49–59, Nov. 2012.
[14] H. Jmii, A. Meddeb, and A. Chebbi, "Voltage contingency ranking for IEEE 39-bus system using Newton–Raphson method," *WSEAS Trans. Power Syst.*, vol. 12, no. 29, pp. 248–253, 2017.
[15] Y. J. Lin, "Prevention of transient instability employing rules based on backpropagation based ANN for series compensation," *Int. J. Elect. Power Energy Syst.*, vol. 33, no. 10, pp. 1776–1783, Dec. 2011.
[16] K. S. Swarup and P. B. Corthis, "Power system static security assessment using self-organizing neural network," *J. Indian Inst. Sci.*, vol. 86, pp. 327–342, Jul./Aug. 2006.
[17] K. Pandiarajan and C. K. Babulal, "An ANFIS approach for overload alleviation in electric power system," *J. Elect. Syst.*, vol. 10, no. 2, pp. 179–193, Jun. 2014.
[18] S. Kalyani and K. Shanti Swarup, "Classification and assessment of power system security using multiclass SVM," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 41, no. 5, pp. 753–758, Sep. 2011.
[19] I. S. Saeh and M. W. Mustafa, "Artificial neural network for power system static security assessment: A survey," *J. Teknol.*, vol. 66, no. 1, pp. 753–758, Dec. 2010.
[20] A. K. Sharma, A. Saxena, B. P. Soni, and V. Gupta, "Voltage stability assessment using artificial neural network," in *Proc. IEEMA Eng. Infinite Conf. (eTechNxT)*, New Delhi, India, 2018, pp. 1–5.
[21] R. K. Misra and S. P. Singh, "Steady-state security analysis using artificial neural network," *Electr. Power Compon. Syst.*, vol. 32, no. 11, pp. 1063–1081, Jun. 2010.
[22] E. M. Voumvoulakis, A. E. Gavoyiannis, and N. D. Hatziargyriou, "Application of machine learning on power system dynamic security assessment," in *Proc. Int. Conf. Intell. Syst. Appl. Power Syst.* Niigata, Japan: Toki Messe, 2007, pp. 1–6.
[23] M. F. Z. Souza, Y. Reis, A. B. Almeida, I. Lima, and A. C. Z. de Souza, "A neuro-fuzzy method as tool for voltage security assessment of systems with distributed generation," in *Proc. 3rd Renew. Power Gener. Conf. (RPG)*, Naples, Italy, 2014, pp. 1–6.
[24] M. Amroune, I. Musirin, T. Bouktir, and M. M. Othman, "The amalgamation of SVR and ANFIS models with synchronized phasor measurements for on-line voltage stability assessment," *Energies*, vol. 10, no. 11, p. 1693, Oct. 2017.
[25] S. Saravanan, S. Kannan, and C. Thangaraj, "Forecasting India's electricity demand using artificial neural network," in *Proc. IEEE Int. Conf. Adv. Eng. Sci. And Manage. (ICAESM)*, Nagapattinam, India, Mar. 2012, pp. 79–83.

[26] A. N. Al-Masri, M. Z. A. Ab Kadir, H. Hizam, and N. Mariun, "A novel implementation for generator rotor angle stability prediction using an adaptive artificial neural network application for dynamic security assessment," *IEEE Trans. Power Syst.*, vol. 28, no. 3, pp. 2516–2525, Aug. 2013.
[27] R. Sunitha, R. S. Kumar, and A. T. Mathew, "Online static security assessment module using artificial neural networks," *IEEE Trans. Power Syst.*, vol. 28, no. 4, pp. 4328–4335, Nov. 2013.
[28] W. Sun and Y. Xu, "Financial security evaluation of the electric power industry in China based on a backpropagation neural network optimized by genetic algorithm," *Energy*, vol. 101, pp. 366–379, Apr. 2016.
[29] M. Lekshmi and M. S. Nagaraj, "Online static security assessment module using radial basis neural network trained with particle swarm optimization," in *Intelligent and Efficient Electrical Systems* (Lecture Notes in Electrical Engineering), vol. 446, M. Bhuvaneswari and J. Saxena, Eds. Singapore: Springer, 2018.
[30] P. Sekhar and S. Mohanty, "An online power system static security assessment module using multi-layer perceptron and radial basis function network," *Int. J. Elect. Power Energy Syst.*, vol. 76, pp. 165–173, Mar. 2016.
[31] Z. Yun, Q. Zhou, Y. Feng, D. Sun, J. Sun, and D. Yang, "On-line static voltage security risk assessment based on Markov chain model and SVM for wind integrated power system," in *Proc. 13th Int. Conf. Natural Comput., Fuzzy Syst. Knowl. Discovery (ICNC-FSKD)*, Guilin, China, 2017, pp. 2469–2473.
[32] M.-Y. Ruan and H.-D. Chiang, "On the accuracy of the online static security assessment under different models: Assessment and basis," *IEEE Trans. Power Syst.*, vol. 34, no. 6, pp. 4352–4360, Nov. 2019.
[33] A. Maiorano and M. Trovato, "A neural network-based tool for preventive control of voltage stability in multi-area power systems," *Neurocomputing*, vol. 23, nos. 1–3, pp. 161–176, Dec. 1998.
[34] V. S. S. Vankayala and N. D. Rao, "Artificial neural networks and their applications to power systems–a bibliographical survey," *Elect. Power Syst. Res.*, vol. 28, no. 1, pp. 67–79, Oct. 1993.
[35] A. N. Al-Masri, M. Z. A. Ab Kadir, H. Hizam, N. Mariun, A. Khairuddin, and J. Jasni, "Enhancement in static security assessment for a power system using an optimal artificial neural network," *Int. Rev. Elect. Eng.*, vol. 5, no. 3, pp. 1095–1102, May 2010.
[36] S. Rajasekaran and G. A. V. Pai, *Neural Networks, Fuzzy Logic and Genetic Algorithms: Synthesis and Applications*. New Delhi, India: PHI Learning, 2011.
[37] K. J. Hunt, D. Sbarbaro, R. Zbikowski, and P. J. Gawthrop, "Neural networks for control systems—A survey," *Automatica*, vol. 28, no. 6, pp. 1083–1112, Nov. 1992.
[38] D. Rumelhart, G. Hinton, and R. Williams, "Learning internal representations by error propagation," *Nature*, vol. 323, pp. 533–536, Oct. 1986.
[39] *Program Application Guide for PSS E Version 32.0, Siemens Power Technologies International*, Siemens, Munich, Germany, 2009, vol. 2.
[40] D. E. Rumelhart, G. E. Hinton, and R. J. Williams, "Learning internal representations by error propagation," Inst. Cogn. Sci., Univ. California San Diego, San Diego, CA, USA, Tech. Rep. ICS-8506, 1985.
[41] A. M. A. Haidar, A. Mohamed, A. Hussain, and N. Jaalam, "Artificial Intelligence application to Malaysian electrical powersystem," *Expert Syst. Appl.*, vol. 37, no. 7, pp. 5023–5031, Jul. 2010.
[42] R. Hooshmand and M. Moazzami, "Optimal design of adaptive under frequency load shedding using artificial neural networks in isolated power system," *Int. J. Elect. Power Energy Syst.*, vol. 42, no. 1, pp. 220–228, Nov. 2012.

AHMED N. AL-MASRI received the Ph.D. degree from University Putra Malaysia. He is currently an Associate Professor with the College of Computer Information Technology, American University in the Emirates. He has over eight years of experience in teaching and research in the fields of electrical engineering and artificial intelligence. His current research interests include E-learning, the Internet of Things, data analytics, machine learning, and data mining. He is a regular Editor of various journals specializing in electrical power system and artificial intelligence.

MOHD ZAINAL ABIDIN AB KADIR received the B.Eng. degree in electrical and electronic engineering from Universiti Putra Malaysia (UPM), in 2000, and the Ph.D. degree in high-voltage engineering from The Universiti of Manchester, U.K., in 2006. He is currently a Professor with the Faculty of Engineering, UPM, after serving as the Head of Department and the Deputy Dean (Research and Innovation), from 2011 to 2014 and from 2014 to 2017, respectively. He is also currently being a seconded to Universiti Tenaga Nasional (UNITEN), as a Strategic Hire Professor, under BOLD 2025 Initiative. He is the Chair for the National Mirror Committee of TC 81 on Lightning Protection, the Past Chair of the IEEE PES Malaysia, a WG member of the IEEE PES Lightning Performance on Overhead Lines, a Research Advisor of the African Center for Lightning and Electromagnetic, and the Advisor of the Center for Electromagnetic and Lightning Protection Research, UPM. He is a local convener for CIGRE C4 on System Technical Performance, a working group member of SC C4.39 on Surge Arrester, and a board member of the National Lightning Safety Institute, USA. He is a Professional Engineer and a Chartered Engineer. He is also a Distinguished Lecturer of the IEEE PES.

ALI SAADON AL-OGAILI received the B.Sc. degree in electrical engineering from Baghdad University, Baghdad, Iraq, in 2005, and the M.Sc. and Ph.D. degrees in electrical power engineering from UPM, Serdang, Malaysia, in 2012 and 2018, respectively.

He is currently a Postdoctoral Researcher with the Institute of Power Engineering, Tenaga Nasional University. His research interests include power electronic circuit design and simulation, electric vehicles, and solar energy.

YAP HOON was born in Sitiawan, Perak, Malaysia, in 1990. He received the B.Eng. degree in electrical and electronic engineering and the Ph.D. degree in electrical power engineering from UPM, Serdang, Malaysia, in 2013 and 2017, respectively.

After completing his Ph.D., he served as a Postdoctoral Researcher at the Advanced Lightning, Power, and Energy Research Centre, UPM. He is currently a Lecturer with Taylor's University. His research and teaching interests include power electronics, power quality, artificial intelligence, and multilevel inverter.