Journal of Theoretical and Applied Information Technology
30th September 2011. Vol. 31 No.2

ISSN: **1992-8645** www.jatit.org E-ISSN: **1817-3195**

STATIC POWER SYSTEM SECURITY ASSESSMENT VIA ARTIFICIAL NEURAL NETWORK

[1]J.JASNI, [2]M.Z.A AB KADIR

[1]Senior Lecturer, Department of Electrical and Electronics Engineering, Faculty of Engineering, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia

[2]Assoc. Prof., Department of Electrical and Electronics Engineering, Faculty of Engineering, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia

E-mail: jas@eng.upm.edu.my, mzainal@eng.upm.edu.my

ABSTRACT

Maintaining system security is an important factor in the operation of a power system. The aim of this study is to evaluate the reliability using artificial neural network (ANN) in static security assessment to determine the security status of a power system. Feed Forward Back Propagation Neural Network is implemented to classify the security condition of IEEE 9 bus system. The input data of ANN are derived from offline Newton Raphson load flow analysis. The result obtained from the ANN method is compared with the Newton Raphson load flow analysis in terms of accuracy to predict the security level of IEEE 9 bus system and the computational time required by each method. The average time required by Newton-Raphson load flow analysis to evaluate security level of IEEE 9 bus system is 0.0481 seconds while the average time required by neural network is 0.0119 seconds. The accuracy of 13 hidden neurons feed forward back propagation neural network to predict the security level of IEEE 9 ***bus system is 98.57%. In conclusion, ANN is found to be reliable to evaluate the security level of IEEE 9 bus system.***

Keywords: *Newton-Raphson Load Flow, Contingency Analysis, Security Assessment, Feed Forward Back Propagation Neural Network***.**

1. INTRODUCTION

Power system security assessment is very crucial to determine whether a power system is reasonably safe from serious interference on its operation or in the emergency (insecure) state [1]. The power system security assessment can be divided into three major functions which are system monitoring, contingency analysis and security control. System monitoring provides up-to-date information such as voltages, currents, power flows and the status of circuit breaker through the telemetry system. From this system monitoring, operators can easily identify the system in the normal state or in abnormal condition. On the other hand, contingency analysis is carried out to evaluate the outage events in power system and it is a critical part in security assessment. During the insecure condition, security control will take the preventive actions to ensure the system is back to secure condition.

In static security assessment, load flow equations are required to identify the power flows and voltage levels throughout the transmission system [2]. Repeated power flow studies are run for each outage and then the operational limits are checked in order to evaluate the security status of the power system.

Load flow analysis (also known as power flow analysis) can be solved by three methods which are the Newton-Raphson method, Fast-Decoupled method and Gauss-Seidel method. The most common power flow method is the Newton-Raphson due to the fact that it can converge very quickly as the iteration begins near the desired root.

In static security analysis, contingency analysis is used to predict the possible systems outage and their effect [3]. Referring to [4], a power system is vulnerable to different types of contingencies. These contingencies analysis can be divided into three which are single element outage (N-1), multiple-element outage (N-2 or N-X) and sequential outage. When carrying out the contingency analysis, power flow analysis is required to find the new changes in power flow and bus voltage for each contingency.

In modern power system, fast security assessment is an importance task. This is due to the fast security assessment that enables the operators to identify the overload lines very quickly and can take the corrective action. Therefore, end users will have reliable and secure electricity. Artificial intelligence (AI) methods can be used to reduce the computation time of security assessment. The accuracy of AI method is in the acceptable range so the application of AI based approaches in the operation and control of power system become a trend in nowadays [5-6]. Artificial neural network (ANN) is one of AI method which has been emerged in recent years in power system especially in the power system security assessment.

ANN is modeled to reflect the configuration of the biological neuron. The X_1 and X_2 in Figure 1 provide the data used by the neuron in order to generate an output. W1 and W2 are the weights which are multiplied with the input signal. The weight increase or decrease of the input signal allows the neuron and the network as whole to be more accurately trained because the weight can be adjusted in order to generate the correct result. ‘B’ is bias value which is similar to the weights. It is used to adjust the total input value. This value is also changed during training so that the output is more accurate. The summation function allows the neuron to evaluate the total input. Therefore, it can generate the correct output signals required by the ANN. The active function generates the outputs required for the network so that a correct decision can be made.

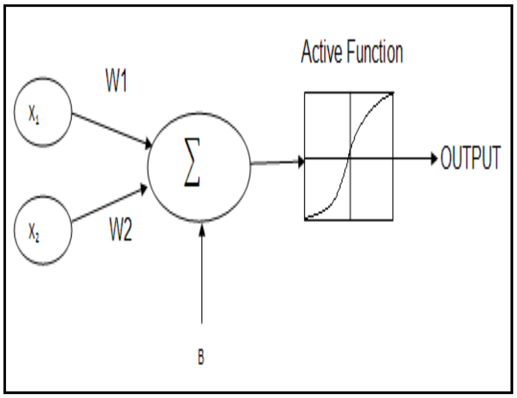

Figure 1: Components of ANN

ANN is more commonly used to perform static security assessment for power systems. The reason is because the ANN has potential in terms of speed and accuracy. Besides that, ANN had been successfully applied in the large power system compared to other methods like AC load flow and DC load flow.

Sean and Khairuddin [7] had stated that ANN method is more accurate and much better in terms of computational time taken compared to decision tree and adaptive network based fuzzy interference system. Some different methods were proposed to determine the security states of a power system but error classification and computational time issues were not considered in these methods [8-11].

Many research proved the feed forward back propagation neural network suitable for application in power system security assessment. Fischer [12] showed how a number of back propagation neural networks which used the partial least-squares model can be trained to predict power system security after a contingency. This method is applied to the 10-machine New England Power System Model. Lu [13] had applied feed forward back propagation neural network in predicting power system bus voltage and generator transformer units. Sidhu and Lan [14] stated a good calculation accuracy, high contingency capturing rate and faster analysis can obtained by using back propagation feed forward neural network.

The feed forward back propagation neural network has high accuracy after training because the error between the actual and expected results is calculated so that the error in the output will be minimal. Another advantage of feed forward back propagation neural network is feed forward back propagation neural network algorithm is not as complicated and it can be improved by the partial least square technique to reduce high dimensional. Besides that, feed forward back propagation neural network is most popular choice for further study in dynamic behavior for security assessment [15-17].

2. METHODOLOGY

1. *Newton-Raphson Load Flow Analysis*

Newton-Raphson load flow analysis is performed to evaluate the security status of IEEE 9 bus system. The structure of IEEE 9 bus system is shown in Figure 2. Referring to Figure 2, IEEE 9-bus system consists of three buses with generators which are bus 1, bus 2 and bus 3, and three buses with load which are bus 5, bus 7 and bus 9. This 9 bus system also consists of 6 transmission lines which are line 8-7, line 7-6, line 8-9, line 6-5, line 9-4 and line 5-4.

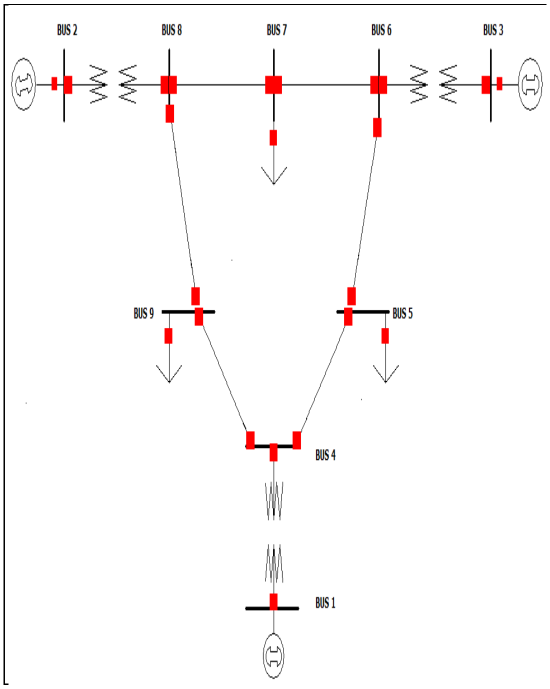

Figure 2: IEEE 9 bus system [18]

The Newton-Raphson load flow is implemented to calculate the new voltage at each bus and power flows in each line for every contingency cases. In this paper, N-1 contingency analysis is performed because this project only considers single line outage. The bus voltage limits and thermal line limit are the parameters to evaluate the security status of IEEE 9-bus test system.

The general form for the security status of IEEE 9 bus system is determined by the equation (1):

$$Z^L \geq Z(u, C_1) \geq Z^U \quad (1)$$

The superscripts L and U in equation (1) represent the lower and upper limits of $Z(u, C_1)$ respectively. $Z(u, C_1)$ is used to represents the line flows and bus voltages. During secure condition, equation (1) must satisfy the thermal line limit and bus voltage limit. When $Z(u, C_1)$ is used to represents the line flows and bus voltages, the equation (1) will become as equation (2) and (3) respectively.

$$V_{Min} < V_i < V_{Max} \qquad i = 1, \dots, n \quad (2)$$

$$S_i < S_{Max} \qquad i = 1, \dots, n \quad (3)$$

If the power system exceeds either the voltage limit or thermal line limit in equations (2) and (3) respectively, the power system is considered as insecure condition for that contingency case. If the power system inside the voltage limit and thermal line limit in equations (2) and (3) respectively, then the power system is considered as secure condition. Referring to [2], the minimum and maximum bus voltage value is 0.9 per unit and 1.1 per unit respectively. According to [19], the thermal line limit is 80%. This is due to the fact that when the thermal line reaches 80%, the operator still has time to take an action to bring the system back to secure condition. If thermal line limit is set as 100%, there is nothing can be done since the system already in insecure condition.

Binary number is used to represent the security condition of a power system. Binary numbers 1 and 0 stand for the secure and insecure conditions, respectively.

2. *ANN Implementation*

ANN implementation is used to design the best ANN configuration. Later, the best configuration of ANN is used to predict the security status of IEEE 9 bus system. Figure 3 shows the sequence of the ANN implementation.

The process of ANN implementation starts from data collection and ends with the comparison accuracy for each hidden neuron. Percentages of classification accuracy and mean square error are used to represent the performance of ANN in terms of accuracy to predict the security level of IEEE 9 bus system.

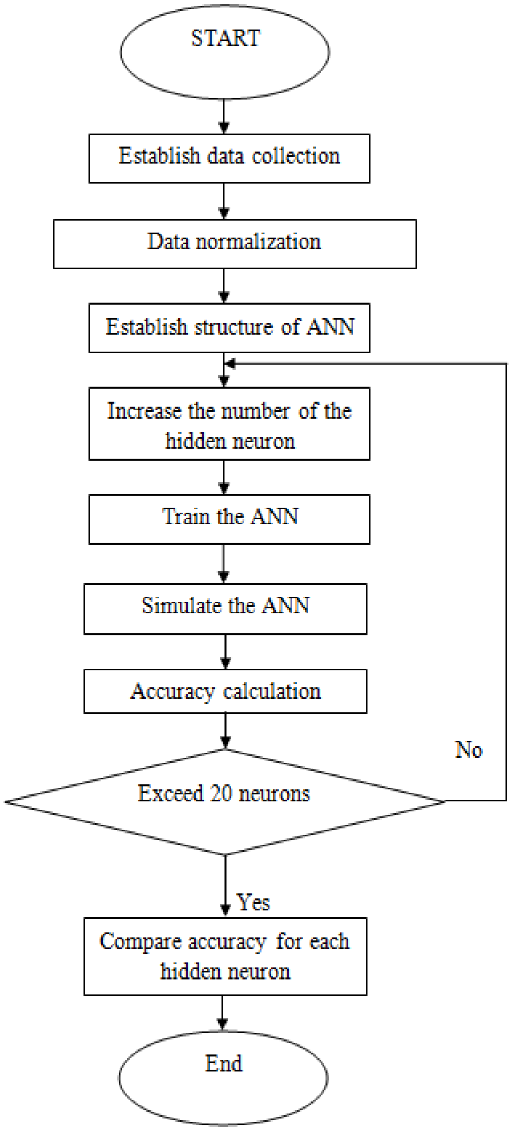
START
Establish data collection
Data normalization
Establish structure of ANN
Increase the number of the hidden neuron
Train the ANN
Simulate the ANN
Accuracy calculation
No
Exceed 20 neurons
Yes
Compare accuracy for each hidden neuron
End

Figure 3: ANN implementation flow chart

2.1 Data Collection

Input data of ANN are derived from offline Newton-Raphson load flow analysis. The input data consists of bus voltage value and line thermal value for each contingency case. In data collection, the input data are divided into two groups which are train data and test data, respectively.

The train data consisting of bus data and line data that run on the nominal condition which is at load of 100%. Later, the load will increase 2% from this nominal condition for every bus load until it reaches 120%.

For testing data, the load start in 101% then the load is increased up to 120%. Each time the load will increase 2% from load variation at 101% level. The collected data will be stored as the input data for normalization.

2.2 Data Normalization

The results in data collection are generally on widely different scales thereby data normalization is applied. Priddy and Keller [20] had stated normalizing the input data for the data collection is important because normalization can minimize the bias within the neural network. Hence, an accurate forecast output results will be obtained. Data normalization can also speed up training time because the training process for each feature in same scale.

The train and test data are normalized by using min-max normalization because most features are rescaled to lie within a range of 0 to 1. The min-max normalization is accomplished by using linear interpolation equation which is shown in equation (4):

$$x_i' = \frac{x_i - Min_{value}}{Max_{value} - Min_{value}}\left(Max_{target} - Min\ _{target}\right) + Min_{target} \quad (4)$$

Where:

Max$_{value}$ is initial maximum value of x.

Min$_{value}$ is initial minimum value of x.

Max$_{taget}$ is maximum value for range of interval.

Min$_{target}$ is minimum value for range of interval.

2.3 ANN Structure

The feed forward back propagation neural network has three layers which are the input layer, hidden layer and target layer. The input layer has 12 neurons since the number of variables in the input neural network is 12.

The number of hidden neurons are varying from 2 to 20 in order to compare the performance of each hidden neurons. The neural network will be trained for each change in the number of hidden neurons.

The more hidden neurons are used to train the neural network, the more computational time will be consumed due to the fact that the neural network requires longer time for solving more complicated problems [21].

In the target layer, the neural network has two output vector which is either 0 for insecure or 1 for secure but naturally, neural network output is a closer analogue value in a range [0, 1]. Therefore, the output of neural network more than or equal 0.9 will be considered as secure condition while output of neural network less than or equal 0.1 will be considered as insecure condition.

2.4 *Training ANN*

Training process of neural network is to identify the topology of neural network and its interconnect weights. Training process is important since it will ensure the neural network reacts with the fastest speed and without losing any important data. The training speed depends on the speed factor such as the learning rule, the transfer function of neurons or initialization of the network [22]. During the training, neural network needs enough knowledge information in order to simulate a good prediction of power system security.

In the training process of the neural network, a set of network inputs and target outputs are required. During training, the weights and biases of the network are iteratively adjusted to minimize the network performance function.

The feed forward back propagation neural network can be trained with different training algorithms. These algorithms use the gradient of the performance function to adjust the weights. Therefore, the network error will be minimized and obtain a better performance. The gradient is determined using a technique called back propagation, which involves performing computations backward through the network.

The basic back propagation training algorithm is it updates the network weights in negative gradient direction. There are two different methods to apply gradient descent algorithm which are incremental mode and batch mode. For incremental mode, after all input is called to the neural network, the gradient of the network weights is computed and the weights are updated. For batch mode, each input is called to the neural network before the weights are updated.

Batch gradient descent and batch gradient descent with momentum are often too slow for practical problems. The faster algorithms of training are the variable learning rate back propagation (VLRBP), resilient back propagation (RBP), conjugate gradient (CG), Quasi-Newton (QN) and Levenberg-Marquardt (LM). The VLRBP and RBP are the heuristic techniques which are the same techniques with the batch gradient descent and batch gradient descent with momentum. Whilst the CG, QN and LM use the standard numerical optimization techniques.

In this work, LM training technique is used due to its faster training and good convergence [23]. Besides that, LM algorithm is suitable for medium-size neural network and its algorithm was designed to approach second-order training speed without having to compute the Hessian matrix. For example, when mem_reduc is set to 2, then only half of the Jacobian is computed at one time. This saves half the memory used by the calculation of the full Jacobian. The parameter mem_reduc determines how many rows of the Jacobian are to be computed in each submatrix.

2.5 *Performance Neural Network*

The performance of the feed forward back propagation neural network is evaluated by the percentages of classification accuracy (CA) and mean squared error (MSE) [24]. The percentages of CA for the neural network are calculated by using equation (5).

$$\mathrm{CA}\ (\%) = \frac{\text{number of sample classified correctly}}{\text{total number of cases}} \mathrm{X}100 \qquad (5)$$

The MSE is calculated by using equation (6). MSE is average squared error between the network outputs and the target outputs. In a best configuration neural network, the mean square error in the network is very small. The neural network use least MSE algorithm to adjust the weights and biases of the neural network in order to minimize the MSE.

$$\mathrm{MSE} = \frac{1}{n}\sum_{k=1}^{n}(\,\mathrm{E_k})^2$$
$$= \frac{1}{n}\sum_{k=1}^{n}(\,|\mathrm{DO_k} - \mathrm{AO_k}|)^2| \qquad (6)$$

Where:

n is number of sample in the data set.
DO_k is desired output obtained from off-line simulation.
AOk is actual output obtained from neural network trained classifier.

The neural network configuration which has the highest accuracy of prediction and lowest value of mean square error will be considered as best performance of neural network configuration.

3. RESULTS AND ANALYSIS

1. Newton-Raphson Load Flow Analysis

The system is considered as secure condition when the power system fulfils the two conditions. The first condition is the bus voltage level in the system is in the limit $0.9< V_i <1.1$ per unit. The second one is the thermal line flow in the system shall not exceed 80%. In contrast, the system is considered as insecure condition when either the bus voltage level exceed the limit $0.9< V_i <1.1$ per unit or the thermal line flows exceed the limit 80%.
Referring to Figure 4, the system is in insecure condition during line outages of 8-9 and 9-4. This is due to the bus 9 voltage level is below the 0.9 per unit, which is the acceptable minimum voltage level. Therefore, the bus 9 voltage level is unacceptable. While line outages happen in line 7-8, 6-7, 9-4 and 4-5, the system is in secure condition since the bus voltages are within the maximum and minimum voltage criteria level.

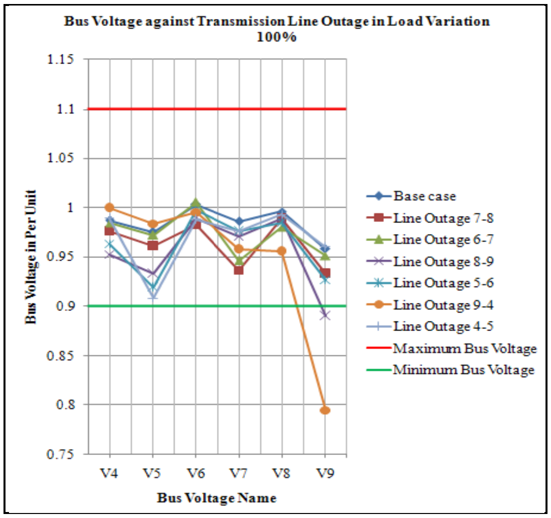

Figure 4: Bus voltage against transmission line outage in load variation 100%

Referring to Figure 5, the system is in insecure condition during line outage 8-9 due to the thermal flow in transmission line 5-6 exceeded the 80% thermal line limit. Therefore, the thermal flow in line 5-6 is unacceptable.

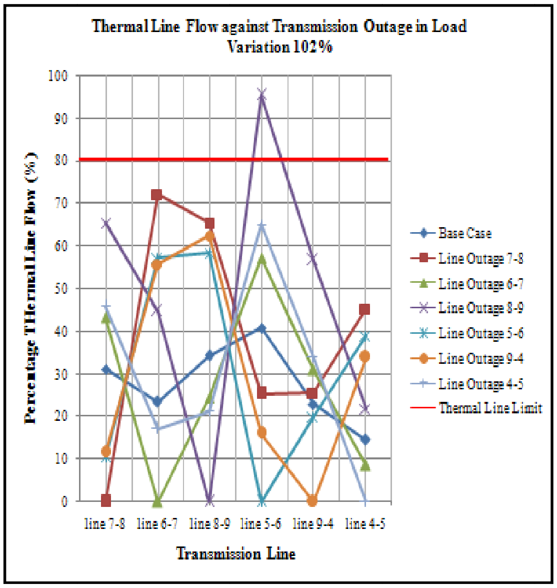

Figure 5: Bus voltage against transmission line outage in load variation 104%

Figure 6 shows the security status for IEEE 9 bus system at load variation of 100% and 120%. For the load variation of 100%, line outage 8-9 and 9-4 cause the system in insecure condition. Whilst for the load variation of 120%, the system is in insecure condition for the line outages of 7-8, 8-9, 5-6, 9-4 and 4-5, respectively.

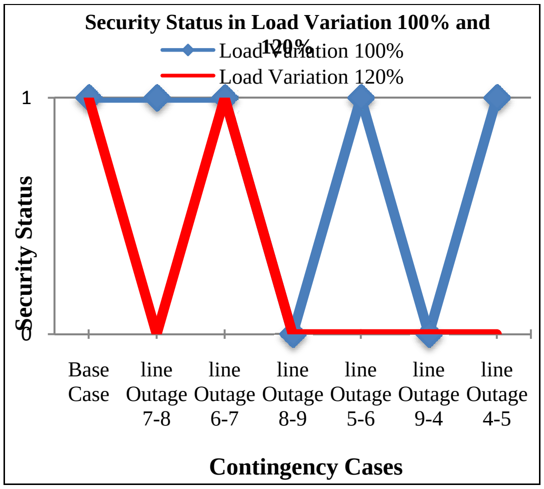

Figure 6: Security status in load variation 100% and 120%

When there is an increase in load variation in the power system, the impedance in the power system will increase. Therefore, there is progressive fall of voltage occurs in buses. The progressive fall of voltage happens because some of the voltages drop in the impedance of power system. Besides that, power which sent to the load is also increased when the load is increased. As a result, the number of buses exceed bus voltage limit and the number of transmission lines exceed the thermal line limit are increased. Hence, insecure cases are increased in the system when the load is increased.

2. *Data Collection*

The The data obtained in offline Newton-Raphson load flow by using the MATLAB software are used as input data for data collection. The data derived from offline Newton-Raphson load flow have matrix size [12X147]. In data collection, these input data are divided into two groups which are train data and test data. The matrix size of train data is [12X77] while the matrix size of test data is [12X70].

Table 1 shows the train data at load variation of 104%. Referring to the table, the number of variables in the train data are 12 which consist of 6 buses voltage and 6 thermal lines. The 6 buses voltages are V_4, V_5, V_6, V_7, V_8 and V_9. The 6 thermal lines are line 7-8, line 6-7, line 8-9, line 5-6, line 9-4, and line 4-5.

The bus voltages V_1, V_2 and V_3 are not included in the train data and test data because they are generator buses. They will be controlled by the (automatic voltage regulator) AVR system. The advantage of the AVR system is power source is not affected by sudden loads change. The AVR system will maintain the output voltage within the specified limits.

In train data, there are 40 train data in secure condition while 37 train data in insecure condition. For test data, there are 37 test data which are secure status while 33 test data are insecure status.

Table 1: Train data in load variation 104%

Load Variation	**104%**						
Case	Base Case	C1	C2	C3	C4	C5	C6
V4 (p.u.)	0.986	0.974	0.982	0.951	0.961	0.999	0.988
V5 (p.u.)	0.973	0.956	0.969	0.931	0.915	0.979	0.898
V6 (p.u.)	1.002	0.979	1.005	0.988	0.996	0.992	0.985
V7 (p.u.)	0.983	0.93	0.942	0.97	0.974	0.951	0.972
V8 (p.u.)	0.995	0.988	0.978	0.989	0.985	0.949	0.991
V9 (p.u.)	0.955	0.93	0.948	0.885	0.924	0.771	0.958
line 7-8 (%)	31.5	0	44.1	65.3	11	10.3	47.4
line 6-7 (%)	24.1	73.5	0	43.6	57.3	58.9	18.1
line 8-9 (%)	33.8	65.3	23.7	0	57.4	64.5	19.9
line 5-6 (%)	40.1	26.4	57.1	94.1	0	15.9	66.5
line 9-4 (%)	24	25.2	32.5	57.8	19.5	0	36.2
line 4-5 (%)	15.4	46.8	8.8	20.5	39.8	36.9	0

3. *Data Normalization*

The results in data collection are generally on widely different scales thereby the gap different between bus voltage and thermal lines are large. In order to solve the gap different between bus voltage and thermal line, data normalization is implemented. In this p\work, the max-min normalization is used to rescale the bus voltage and thermal line lie within a range of 0 to 1.

Table 2 shows the normalization data at load variation of 104%. All the bus voltage and thermal line value are located in the range of 0 to 1. By comparing data in Tables 1 and 2, the gap different between bus voltage value and thermal line value in Table 2 is smaller than Table 1. The smaller gap difference in the input data of neural network can speed up the training process. Besides that, the smaller gap difference in the input data also gives an accurate forecasts output results.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 2: Normalization data in load variation 104%

Load Variation	**104%**						
Case	Base Case	C1	C2	C3	C4	C5	C6
V4	0.7586	0.5517	0.6897	0.1552	0.3276	0.9828	0.7931
V5	0.9219	0.7891	0.8906	0.5938	0.4688	0.9688	0.3359
V6	0.9302	0.3953	1.0000	0.6047	0.7907	0.6977	0.5349
V7	0.9700	0.4400	0.5600	0.8400	0.8800	0.6500	0.8600
V8	0.9918	0.9344	0.8525	0.9426	0.9098	0.6148	0.9590
V9	0.9889	0.9332	0.9733	0.8330	0.9198	0.5791	0.9955
line 7-8	0.4817	0.0000	0.6743	0.9985	0.1682	0.1575	0.7248
line 6-7	0.2464	0.7515	0.0000	0.4458	0.5859	0.6022	0.1851
line 8-9	0.3350	0.6472	0.2349	0.0000	0.5689	0.6392	0.1972
line 5-6	0.4143	0.2727	0.5899	0.9721	0.0000	0.1643	0.6870
line 9-4	0.3514	0.3690	0.4758	0.8463	0.2855	0.0000	0.5300
line 4-5	0.2337	0.7102	0.1335	0.3111	0.6039	0.5599	0.0000

4. Neural Network Performance

The neuron in hidden layer is varied from 2 neurons to 20 neurons. The different number of neurons in hidden layers are used to determine the accuracy of prediction for the neural network. Figure 7 shows that 13 hidden neurons in hidden layer have the highest accuracy to predict the security status of the system. The accuracy of 13 hidden neurons is 98.5%. Therefore in this work, 13 hidden neurons are used to predict the security status of the system.

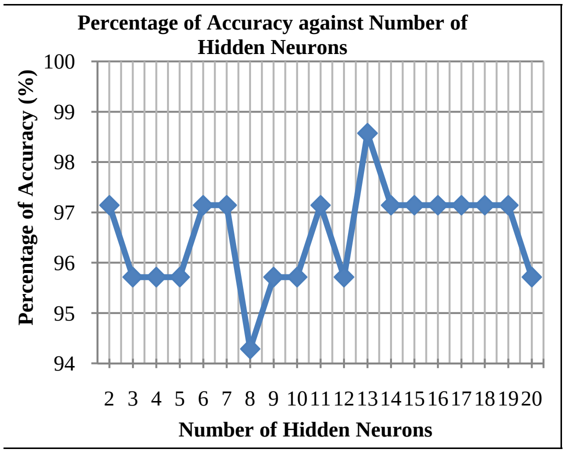

Figure 7: Percentage accuracy of neural network against number of hidden neuron

MSE performance index for the 13 hidden neurons for training is shown in Figure 8. The value of mean square error is 1.74171×10^{-12} which is very small. This reflects the right selection of 13 hidden neurons for providing the highest accuracy to predict the security level of the system.

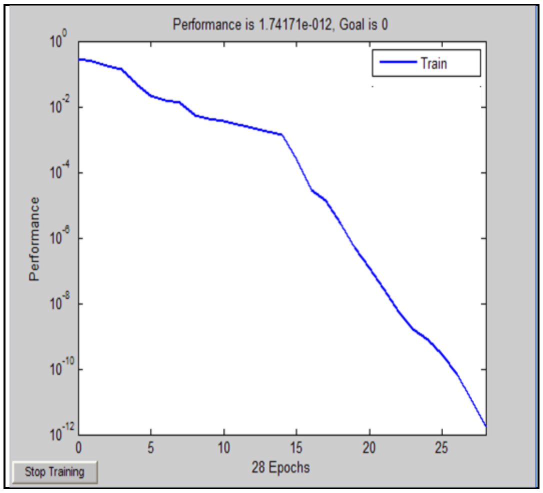

Figure 8: Mean square error against number of epochs

The function of linear regression analysis is to compare the actual output of neural network with the corresponding target output. The closer the R value to 1, the more accurate the prediction.

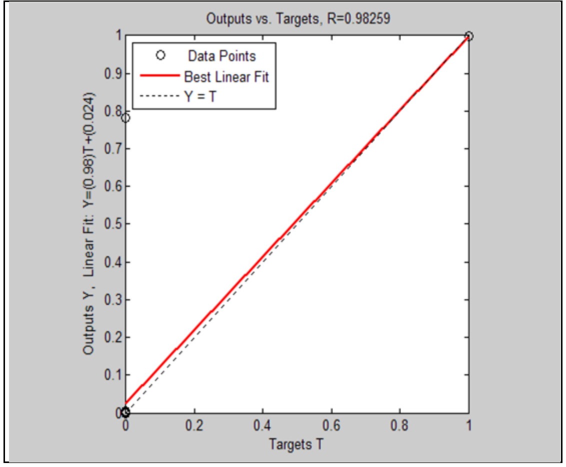

Figure 9: Linear regression of 13 hidden neurons trained neural network

Figure 9 shows the R value of linear regression of 13 hidden neurons is 0.98259 which is indeed very close to 1. Again, the good results obtained from MSE and linear regression analysis proved that the justification of the selection in providing the best performance of the neural network

4. CONCLUSIONS

This paper proves that static security assessment using the ANN method is reliability. The ANN method had been implemented in this project by using IEEE 9 bus system. The structure of feed forward back propagation neural network in this project had performed in well condition because it gave a high accuracy of prediction to the security level in the power system. The proper selection number of hidden neurons is required to ensure the high performance of a neural network. Besides that, data normalization is required to implement in all the input data of neural network in order to make sure the train data and test data in the same range. In a nutshell, ANN is reliability to apply in power system static security assessment.

REFERENCES

[1]. A. B. Alves and A. Monticelli, “Static security analysis using pipeline decomposition”, IEE Proceedings on Generation, Transmission and Distribution, Vol. 145, No. 2, 1998, Page(s) 105 - 110.

[2]. I. S. Saeh and A. Khairuddin, “Static security assessment using artificial neural network”, IEEE International Conference on Power and Energy, 2008, Page(s) 1172-1177.

[3]. A. Oonsivilai and K. A. Greyson, “Power System Contingency Analysis Using Multiagent Systems”, IEEE Transactions on Power Systems, Vol. 14, No. 3, 2009, Page(s) 355-360.Wood A.J. & Wollenberg B.F. 1996. *Power Generation, Operation and Control*, John Wiley & Sons.

[4]. A. J. Wood, and B. F. Wollenberg, “Power Generation, operation and control”, New York: John Wiley & Sons, 1996.

[5]. S. Sharma, L. Srivastava, M. Pandit, and S. N. Singh, “Identification and determination of line overloading using artificial neural network”, Proceedings of International Conference, PEITSICON-2005, Kolkata (India), 2005, Page(s) A13-A17.

[6]. V.S. Vankayala, and N.D. Rao, “Artificial neural network and their application to power system”, IEEE International Symposium on Circuits and Systems, Vol. 12, No. 2, 1993, Page(s): 67-69.

[7]. I. S. Sean and A. Khairuddin, “Implementation of Artificial Intelligence Techniques for Steady State Security Assessment in Pool Market”, International Journal of Computer Science and Security, Vol. 3, No. 1, 2009, Page(s) 1-9.

[8]. L. A. Wehenkel “Auxiliary Tools and Hybrid Techniques, Automatic Learning Techniques in Power Systems”, USA: Kluwer Academic Publishers, 1998.

[9]. M. El-Sharkawi and R. Atteri, “Static Security Assessment of Power System Using Kohonen Neural Network”, IEEE Proceedings of the Second International Forum on Applications of Neural Networks to Power Systems, Vol. 148, No 4, 1993, Page(s) 329-334.

[10]. S. Weerasooriya and M. El-Sharkawi, “Use of karhunen-loe've expansion in training neural networks for static security assessment”, IEEE Proceedings of the First International Forum on Applications of Neural Networks to Power Systems, Vol. 2, 1991, Page(s) 608 - 612.

[11]. R. Fischl, “Application of neural networks to power system security: technology and trends”, IEEE World Congress on Computational Intelligence, Vol. 151, No.3, 2004, Page(s) 361-366.

[12]. D. Fischer et al., “Automatic contingency grouping using partial least squares and feed forward neural network technologies applied to the static security assessment problem”, IEEE Large Engineering Systems Conference on Power Engineering, 2003.

[13]. Y. P. Lu et al., “Neural network based generator-transformer protection”, Proceedings of Third International Conference on Machine Learning and Cybernetics, 2004.

[14]. T. S. Sidhu, and C. Lan, “Contingency screening for steady-state security analysis by using FFT and artificial neural networks”, IEEE Transactions on Power Systems, Vol. 15, 2000, Page(s) 421 – 426.

[15]. E. S. Karapidakis, and N. D. Hatziargyriou, “Application of artificial neural networks for security assessment of medium size power systems”, 10th Mediterranean Electrotechnical Conference, Vol. 3, 2002, Page(s) 1189 -1192.

[16]. Q. Zhou, J. Davidson, and A. A. Fouad, “Application of artificial neural networks in power system security and vulnerability assessment”, IEEE Transactions on Power Systems, Vol. 9, 1994, Page(s) 525 – 532.

[17]. C. A. Jensen et al., “Inversion of feed forward neural networks algorithms and applications”, Proceedings of the IEEE, Vol. 87, No. 9, 1999, Page(s) 1536-1549.

[18]. F. Milano, “Power System Analysis Toolbox”, 2005

[19]. R. K. Saket, R. C. Bansal and C. Gurmit Singh, “Reliability evaluation of power system

considering voltage stability and continuation power flow", Journal of Electrical System, Vol. 32, 2007, Page(s) 48-60.

[20]. K.L. Priddy and P.E. Keller, "Artificial neural network: an introduction", USA: SPIE, 2005

[21]. H. Demuth, M. Beale and M. Hagan, "Neural network toolbox 5 user's guide", USA: The Math Works, Inc, 2006.

[22]. R. Amerongen, A general-purpose version of the fast decoupled load flow, IEEE Transactions on Power Systems, vol. 4, no.4, 1990, pp. 760 - 770.

[23]. A. A. Suratgar, M. B. Tavakoli and A. Hoseinabadi,"Modified Levenberg-Marquardt Method for Neural Network Training", World Academy of Science, Engineering and Technology, Vol. 6, 2005, Page(s) 46-48.

[24]. S. Kalyani and K. Shanti Swarup, "Study of Neural Network Models for Security Assessment in Power System", International Journal of Research and Reviews in Applied Sciences, Vol. 1, 2009, Page(s) 104-117.

AUTHOR PROFILES:

Jasronita Jasni Jasronita Jasni graduated with a BEng degree in Electrical Engineering from Universiti Teknologi Malaysia, Malaysia in 1998 and received her Master Degree from the same University in 2001 in Electrical Engineering. She is been awarded PhD degree from University Putra Malaysia in May 2010. Currently she is a lecturer in the Department of Electrical and Electronic Engineering, Universiti Putra Malaysia, Malaysia. She is an IEEE member. Her research interests include power system analysis for static and dynamics, load flow analysis, embedded generation and renewable energy.

M. Z. A. Ab Kadir graduated with B.Eng degree in Electrical and Electronic from Universiti Putra Malaysia in 2000 and obtained his Ph.D from the University of Manchester, United Kingdom in 2006 in High Voltage Engineering. Currently, he is an Associate Professor in the Department of Electrical and Electronics Engineering, Faculty of Engineering, Universiti Putra Malaysia. To date he has authored and co-authored over 50 technical papers comprising of national and international conferences proceedings and citation indexed journals. His research interests include high voltage engineering, insulation coordination, lightning protection, lightning injury and power system transients. Dr. Ab Kadir actively involved in the professional activities and currently is an IEEE Member (PES, EMC, Insulation and Dielectric Societies), Member of Malaysia Energy Centre (PTM), Ex- Comm. IEEE Malaysia Section, Ex-Comm. IEEE PES Chapter, Working Group Member of IEEE PES Lightning Performance on Overhead Lines and also the Chairman/Director of Centre of Excellence on Lightning Protection (CELP), Universiti Putra Malaysia (UPM). He is also a member of the International Board of Advisors for National Lightning Safety Institute (NLSI), USA and Malaysian National Committee of CIGRE.