Scientific Journal of Impact Factor(SJIF): 3.134
e-ISSN(O): 2348-4470
p-ISSN(P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 2,Issue 4, April -2015

POWER SYSTEM SECURITY ASSESSMENT AND CONTINGENCY ANALYSIS USING SUPERVISED LEARNING APPROACH

SreedeviSreekumaran[1], Lekshmi Nair[2], H.nagesh[3]
Department of electrical engineering, Acharya Institute of Science and Technology
Department of electrical engineering, Acharya Institute of Science and Technology
Department of electrical engineering, Acharya Institute of Science and Technolog

Abstract- *The most important requirement and need for proper operation of power system is maintenance of the system security. The security assessment analysis is done to determine until what period the power system remains in the safe operable mode. Contingency screening is done to identify critical contingencies in order to take preventive actions at the right time. The severity of a contingency is determined by two scalar performance indices: Voltage-reactive power performance index(PIvq) and line MVA performance index(PImva). Performance indices are calculated based on the conventional method known as Newton Raphson load flow program. Contingency ranking is done based on the severity of the contingencies. In this proposed work, contingency analysis is done with IEEE 14 bus. Since the system parameters are dynamic in nature and keeps on changing, there is need of soft computing technologies. Supervised learning approach that uses Feed-Forward Artificial Neural Network(FFNN) is employed using pattern recognition methodology for security assessment and contingency analysis. A feature selection technique based on the correlation coefficient has been employed to identify the inputs for thee FFNN. With these soft computing techniques, greater accuracy is achieved.*

Keywords-*Contingency analysis, Static security assessment, Neural network, Feature selection, Performance indices, Pattern recognition*

I. INTRODUCTION

Power system is a complex network comprising of generators, transmission lines, transformers, circuit breakers etc. Failure of any of these elements leads to contingencies. Power systems are operated in a way that overloads do not occur either in real time or under any contingency. This is often called maintaining system security. The study of contingency analysis is an important aspect of power system security. Power system planning faces enormous challenges and problems such as future load growth, type and availability of fuel for the generating units. Power system security is the ability of the electric systems to withstand sudden disturbances and continue to operate without interruption of supply to consumers. The main goal in security analysis is to increase the power system's ability to operate safely and within the operational constraints. Security analysis is broadly classified into static security assessment and transient security assessment. Static security assessment evaluates the post contingency steady state condition of the system neglecting the transient behavior and other time dependent variations. Transient security assessment evaluates the performance of the system after a disturbance. Security assessment provides information to operators about the operating states of a power system in the event of a contingency and hence proper measures can be taken within the safe time limit. Contingency analysis comprises a set of contingencies in which system behavior is observed. Each post-contingent scenario is evaluated in order to detect operational problems and the severity of violations.

Worst contingency cases are selected using ranking methods or screening methods. Contingency set comprises of various probable outages such as transmission line overloads or bus limit violations during power system operation. Such contingencies should be quickly identified and corrective measures should be taken. The process of identifying such contingencies is known as contingency selection. Contingency selection identifies critical contingencies and ranks them in order of their severity. Two commonly used methods are screening methods and ranking methods. Screening methods identifies cases causing limit violations. Ranking methods rank the contingencies in order of their severity. The majority of the methods are based on the evaluation by means of some performance index(PI). The conventional methods used are AC load flow and mathematical calculations. These methods are unsuitable for online applications because of high computational time requirement. Hence, it is necessary to develop fast, reliable and accurate on-line security assessment tools to ensure safe operation of the power system.

Various applications of Artificial Intelligence(AI) in security assessment and contingency analysis prove that this is a very promising research field. The speed of contingency screening has also increased due to the recent developments in Artificial Neural Networks. The ANN based methods can learn off-line from training data and is used for on-line classification of new data. This method is much faster than solving the model analytically. The choice of the number of hidden layers and hidden neurons are important in deciding the accuracy of the neural networks. In[1] an enhanced radial basis function neural network (RBFNN) approach is used for on-line ranking of the contingencies expected to cause steady state bus voltage and power flow violations. The advantage of this method is the simplicity in algorithm and

accuracy in classification. In[2] several indices are proposed for contingency screening in online DSA.Fast contingency screening is expected to be an integral part of any practical online dynamic security
analysis (DSA). Ranking of contingencies requires the use of severity indices. The application of multi-layer perceptron neural network to dynamic security contingency screening and ranking has been explored in [3-6].The information on the prevailing operating condition was used to provide contingency screening and ranking from a trained neural network. A back propagation trained multi-perceptron for power system contingency screening and static-security assessment has been used in [7-11].

Power system is said to be in secure condition if system's operating point remains in the acceptable ranges, even during disturbances in the power system. The need for power system security assessment is to have a power system which is reliable, safe, secure and continuous even during credible contingencies. It is the important task of operators to predict such contingencies and to initiate preventive control action as economic as possible so that system integrity and continuity of supply is maintained.

The power system contingencies are selected by calculating the performance indices using Newton Raphson load flow analysis and Artificial neural network. Once the contingencies are selected, ranking is done based on the performance indices calculated. Because of the dynamic nature of power system, ranking for both PI's is obtained separately to understand the effect of each for a particular contingent case. The contingency analysis by the conventional method using Newton Raphson method is time consuming as it gives the solution by considering one line outage at a time. This method will not be practical in real time as the power system consists a large number of contingencies. Therefore, there is a need to develop fast, accurate and flexible method. Artificial Neural Networks(ANN) has found great applications in the field of power system security assessment and contingency analysis because of its ability of synthesizing complex mappings quickly and accurately. The ANN based methods can learn off-line from training data and is used for on-line classification of new data. In this work, the model is based on supervised learning approach. The method calculates the appropriate PI's to identify the system limit violation. Ranking for both PI's is obtained separately to identify the effect of each for a particular contingent case.

The ANN model selected for on-line security evaluation is a four-layer feed forward multi-layer perception network trained with Resilient back propagation algorithm. The performance of any neural network mainly depends on the selection of the input features for training. It is essential to reduce the number of inputs and to select only the optimum number of inputs for input-output mapping. For large scale power systems, number of inputs may be large and hence, training process may be infeasible. It is therefore essential to eliminate the irrelevant variables for higher performance with less computational effort. The input features are selected using the feature selection method. The selected input is normalized. The input features selected are normalized values of pre-contingent real and reactive power output of generators and real and reactive demand at all the load buses of the system. The performance indices PIvq and PImva are taken as output features.

II. CONTINGENCY ANALYSIS

Power system consists of numerous electrical equipments and failure of any of these leads to power failure and affects the system parameters. It may obstruct the secure operations and reliability of the power systems. Power systems need to be operationally secure.

The unpredictable events in a power system that lead to failure of equipments is termed as "contingency". Contingency may be outage of a generator, transmission line or transformer. Hence, contingency analysis is performed to assess the effect of contingencies and to alert the system operators about the critical contingencies that violate the operating limits. The most common limit violations include transmission line and/or transformer thermal overloads and inadequate voltage levels at system buses. Contingency analysis consists of three basic steps:

- Contingency definition: It consists of all possible contingencies that may occur in a power system.
- Contingency selection: Critical contingencies are selected and ranked in order of their severity. Two methods used for this purpose are screening and ranking methods. Severity of the contingencies are done based on the performance indices.
- Contingency evaluation: Necessary control actions and security actions are taken to eliminate the effects of the contingencies in a power system.

Performance index(PI) method is used for identifying the severity of contingencies and ranking them in order of their severity. The severity of the contingencies are based on two scalar performance indices: Voltage-reactive performance index(PI_{VQ}) and line MVA performance index(PI_{MVA}).

2.1. Voltage-reactive performance index(PI_{VQ})

Voltage-reactive power performance index evaluates the severity of the contingency derived from the voltage limit violation of a bus or a node and the reactive power generation limit violation of a generator at a node. PI_{vq} corresponding to each load pattern and each single line outage consists of two terms, defined by

$$PI_{VQ} = \sum_{i=1}^{N_B} \left(\frac{W_{Vi}}{M}\right) \left[\frac{|V_i - V_i^{Sp}|}{\Delta V_i^{Lim}}\right]^M + \sum_{i=1}^{N_G} \left(\frac{W_{Gi}}{M}\right) \left[\frac{Q_i}{Q_i^{max}}\right]^M \quad (1)$$

Where $\Delta V_i^{lim} = V_i - V_i^{max}$ for $V_i > V_i^{max}$ and $V_i^{min} - V_i$ for $V_i < V_i^{min}$

V_i is the post-contingent voltage at the i^{th} bus, V_i^{Sp} is the specified voltage magnitude at bus i, V_i^{max} is the maximum limit of voltage at bus i, V_i^{min} is the minimum limit of voltage at bus i, N_B is the number of buses in the system, W_{Vi} is the real non-negative weighting factor, M(=2n) is the order of the exponent for penalty function, Q_i is the reactive power produced at bus i, Q_i^{max} is the maximum limit for reactive power production of a generating unit, N_G is the number of generating units, W_{Gi} is the real non-negative weighting factor.

2.2. Line MVA performance index(PI_{MVA})

Scalar performance indices measure system stress in terms of load bus voltage violations or transmission line overloads. Contingencies depend upon the loads at different buses i.e. a critical contingency may be a non-critical one at some other loading condition. Hence, the ranking of different contingencies may also differ at different loading conditions. The system loading conditions greatly influence the performance of the system.

$$PI_{MVA} = \sum_{i=1}^{N_L} \left(\frac{W_{Li}}{M}\right) \left[\frac{S_i^{post}}{S_i^{max}}\right]^M \quad (2)$$

Where S_i^{post} is the post-contingent MVA flow of line, S_i^{max} is the MVA rating of line i, N_L is the number of lines in the system, W_{Li} is the real non-negative weighting factor, M is the order of the exponent for penalty function.

III. STATIC SECURITY ASSESSMENT

Static security assessment addresses, whether after a disturbance, power system reaches steady state operating condition without violating any of the constraints. Power system static security status is classified into three different security levels in terms of PI's, namely, Class I (Mostcritical contingencies), Class II (Critical contingencies) and Class III (Noncritical contingencies). Based on the security status, severity of contingencies is identified and ranking is done. Class I indicate that they are never safe under any operating condition and requires immediate attention. Class II indicate that they are not safe under any operating condition since there is violation of some or all operating constraints and these contingencies require proper preventive control actions. Class III indicate that they are always safe/secure for any operating condition. During normal operation of power system, the following constraints should be satisfied:

$$\sum_i P_{Gi} = P_D + P_L \quad (3)$$

$$\sum_i Q_{Gi} = Q_D + Q_L \quad (3)$$

Where P_{Gi} and Q_{Gi} are the real and reactive powers of generator at bus i, P_D and Q_D are the total real and reactive load demands, P_L and Q_L are the real and reactive losses in the transmission network. Inequality constraints must always be imposed on the system to ensure secure operation. These constraints are:

$V_{min} < V_j < V_{max}$ for j=1 to N_B (4)
$S_l < S_{lmax}$ for l=1 to N_L (4)
$P_{Gi,min} < P_{Gi} < P_{Gi,max}$ for i=1 to N_G (4)
$Q_{Gi,min} < Q_{Gi} < Q_{Gi,max}$ for i=1 to N_G (4)

Where V_j is the voltage at bus j, S_l is the apparent power of line l, N_B, N_L *and* N_G are the number of buses, lines and generators respectively.

The general optimal power flow can be stated as, minimizing the objective function,

$$\sum_i F_i\,(P_{Gi}) \qquad (5)$$

where F_i is the cost of the i^{th} generating unit.

IV. DATA GENERATION FOR SECURITY ASSESSMENT AND CONTINGENCY ANALYSIS

The flowchart for the proposed method is shown in figure 1. The steps to be followed for data generation of security assessment and contingency analysis are:

1. A large number of load patterns have been generated by randomly changing the real and reactive loads at all the buses and real and reactive power generation at the generator buses.
2. During simulation, the system load has been changed from 1.0(base case) per unit to 1.6 per unit of base case in steps of 0.025. Optimal power flow for each load case is solved. Here, m is taken as 1.6.
3. All credible contingencies are considered. For each operating condition, a contingency is simulated. N-1 contingency is the most common event in power systems and therefore, only single line outages are considered. Here, n= 20
4. Single line outages corresponding to each load pattern are simulated by Newton Raphson method and the violations of the limits are checked. Keep the load level constant and simulate each contingency several times to obtain a wide range of patterns, Here, z= 10.
5. The performance indices, PI_{VQ} *and* PI_{MVA}, are calculated by the post-contingent state of the system. The obtained values are normalized between 0.1 and 0.9 for each contingent case.
6. The system state, contingency type and the corresponding security are noted for every operating point and for all the contingencies.
7. The whole data is divided into training set and testing set for performance evaluation.

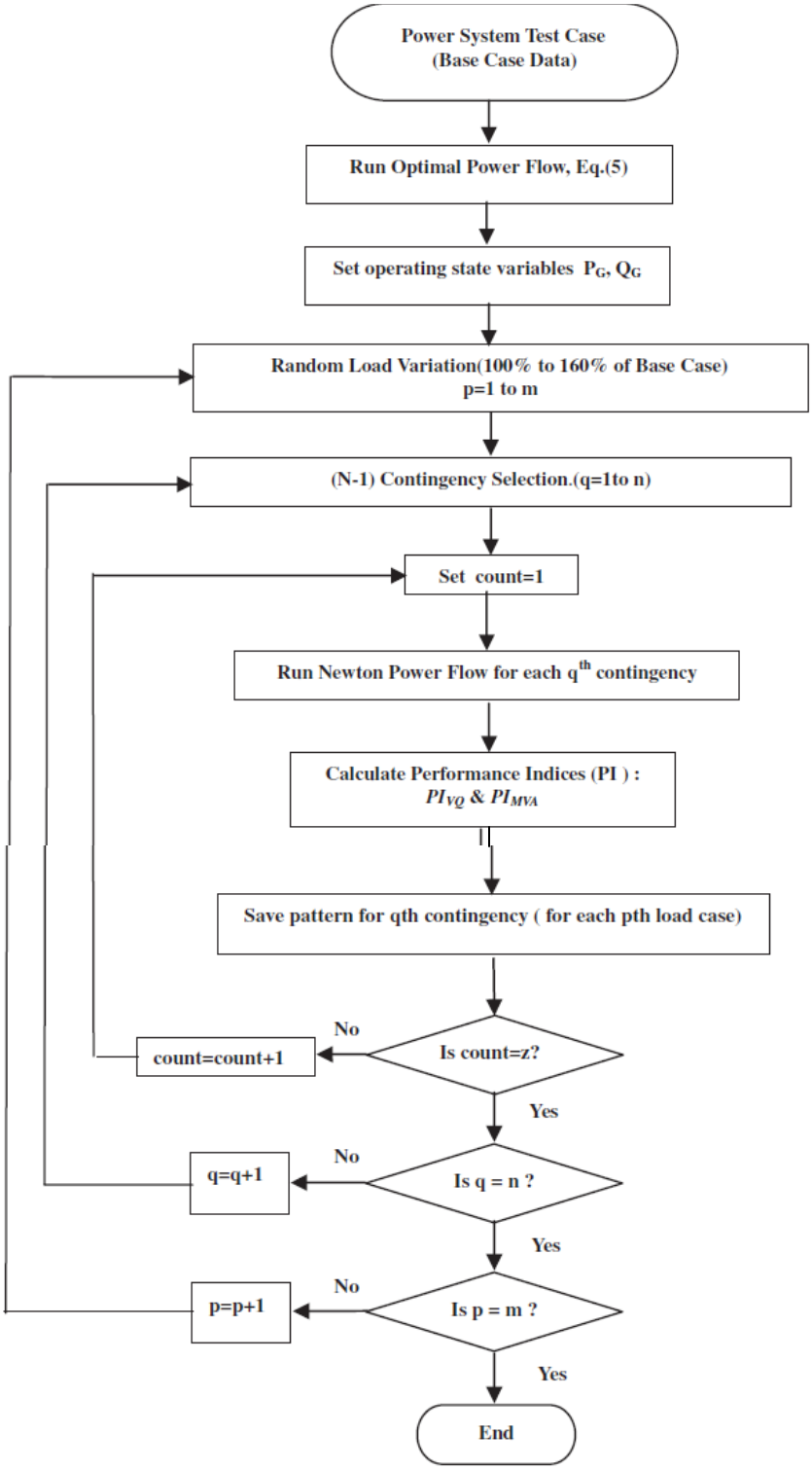

Figure 1. Data generation for security assessment and contingency analysis

V. PROPOSED METHODOLOGY

5.1. Feature selection

The performance of any neural network mainly depends on the selection of the input features. It is essential to reduce the number of inputs and select only the optimum number of inputs. For large scale power systems, the number of input variables may be extremely large making the training process infeasible. Hence, only the relevant features should be selected for higher performance. ANN's are trained for these selected features. So, pre-contingentreal and reactive power output of generators and real andreactive demand at all the load buses of the system are considered as input features. The performance indices of the system, PI_{VQ} *and* PI_{MVA} are taken as output features. An approach based on correlation coefficient is used to select features for the FFNN. The correlation coefficient can be obtained from:

$$C_{ij} = \frac{E\{x_i x_j\} - E\{x_i\}E\{x_j\}}{\sigma_i \sigma_j} \qquad i, j=1,2,\ldots\ldots n$$

All the low ranked features, having C_{ij} greater than 0.95 are discarded.

5.2.Data normalization

The input/output training and testing data are scaled in the range of 0.1 to 0.9 for each load pattern. For some line outages, load flow solution fail to converge at some point. Such contingencies are placed on the top of the list, i.e. most critical contingencies. Here, each input or output parameter x is normalized as x_n before being applied to neural network according to:

$$x_n = \frac{0.8 \times (x - x_{min})}{x_{max} - x_{min}} + 0.1$$

5.3.Proposed FFNN model for calculating performance indices

The ANN model selected for on-line security evaluation is afour-layer feed forward multi-layer perception network trainedwith Resilient back propagation algorithm as shown in Fig.2. Multi-layer perceptron networks using back-propagation algorithm are the standard algorithm for any supervised learning approach. The number of inputs is the number of selected features. The normalized values of real and reactive power output and real and reactive demand at all the load buses are taken as input features. The outputs are PI_{VQ} *and* PI_{MVA} which classify the contingency as secure or insecure. The multi-layered perceptron network operates in two modes: training and testing. In the training mode, a set oftraining data is used to adjust the weights of the network interconnectionsso that the network responds in a specified manner. In thetesting mode, the trained network is evaluated by the test data.Ranking is obtained for both the performance indices separately employing two FFNN's as shown in the figure.

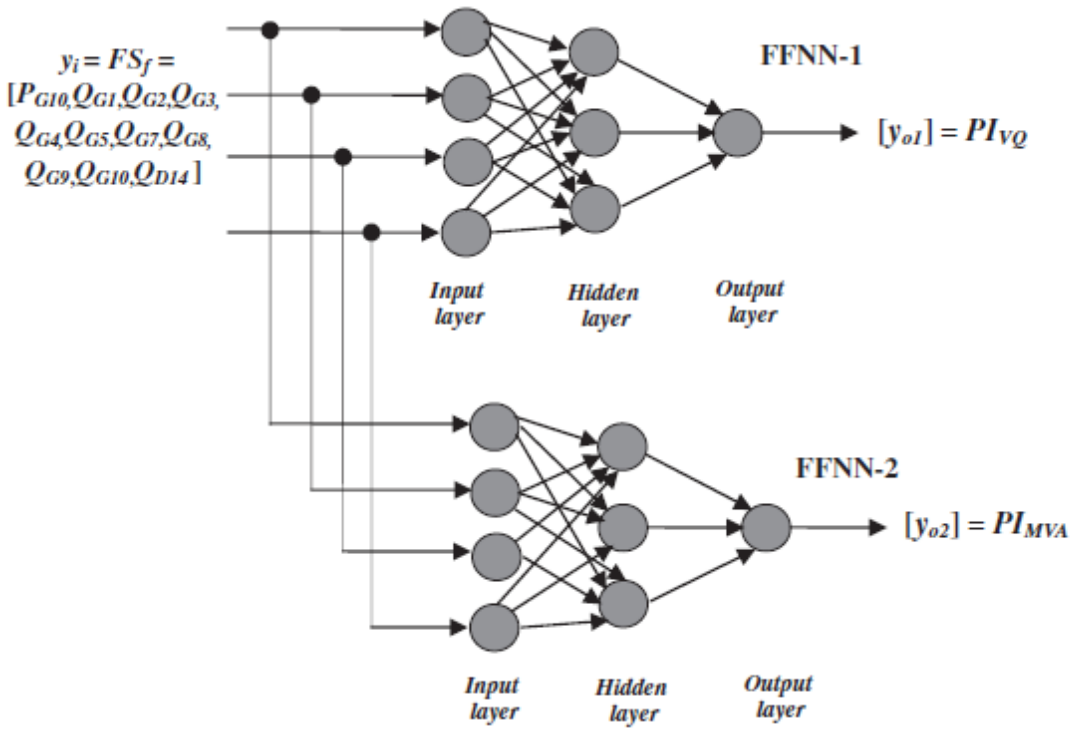

Figure 2. Proposed FFNN for contingency screening and ranking

Once the training of the neural network is successful, the estimation of PI's is instantaneous. Screening is done using pattern recognition and contingencies are classified accordingly. Ranking is also performed. The output determines whether a pattern belongs to a particular Class I,II or III. Thuscontingency screening and security assessment are performed at the same time.

5.4.Training and testing patterns

Theload patterns were generated by randomly changing the load ateach bus and generation at PV buses accordingly. Single line outagecontingencies are considered here for on-line ranking, as they are the most frequent in occurrence. The PI values will be usedas target values for FFNNs. A total of 11 input features (pre-contingent variables) are sufficient for contingency analysis. Data consists of 3264 patterns which is divided into two groups, one for training and the other for testing.

VI. SIMULATION RESULTS

The proposed work is tested on IEEE- 14 bus. The system has 20 transmission lines, 5 generators and 14 buses. From line contingency screening and ranking, 4000 patterns were generated by randomly varying the loads and generation from 100% to 160% of base case. For each system topology, corresponding to 20 single line outages are simulated 10 times, 200(20*10) to obtain different operating conditions resulting in total of 4000(200*20). Out of 4000 patterns, 736 patterns correspond to the case where Newton-Raphson fail to converge and hence, these cases have been excluded from the training data. A total of 3264 patterns have been taken to analyze the performance of the proposed model. All the simulations are carried out using MATLAB.The test results of the proposed FFNN network for contingency screening and ranking is shown in Table 1. It is observed that normalizedvalues of PI obtained by the proposed model are close todesired values of PI obtained from NR method. Ranking results of the proposed method and the NR method are the same.

Table 1. Sample results of PI calculations and contingency analysis

case	Out No	Line No	PIvq_NR NR	PImva NR	PIvq NN	PImva_NN NN
1	2800	8-9	0.2509	0.1430	0.2352	0.1413
2	2400	16-17	0.4696	0.1485	0.4707	0.1467
3	2600	12-13	0.2517	0.3412	0.2695	0.3194
4	118	4-5	0.1918	0.2054	0.1725	0.2129
5	3200	18-19	0.9000	0.1029	0.8996	0.1048
6	2100	11-12	0.2524	0.3402	0.2734	0.3007
7	1800	7-9	0.1411	0.2390	0.1524	0.2419
8	2156	4-3	0.1625	0.1624	0.1613	0.1621
9	2680	9-19	0.6836	0.3001	0.6412	0.2952

Table 2. Results of PI classification obtained by proposed FFNN

```
""PIvq""
 --------------
 Class_1 = 1092
 --------------
 Class_2 =  390
 --------------
 Class_3 = 1782
 --------------
""PImva""
 --------------
 Class_1 =  115
 --------------
 Class_2 =  909
 --------------
 Class_3 = 2240
 --------------
```

Table 3 gives the performance evaluation of the proposed model. The results show that the ANN's presented excellent performance, with very few occurrences of false alarms and contingency misses. False alarms are defined as those cases in which a secure case has been classified as insecure and misses are those in which an insecure case is classified as secure.

Table 3. Performance evaluation of the proposed model

PIMVA	
(Training results)	
Total operating scenarios	3264
no. of training samples	2800
no. of features selected	11
training data)	0.99234
validation data)	0.99475
testing data)	0.99101
MSE (train)	2.176*10-3
Total time for training (s)	18.0193
Testing results	
No. of testing samples	464
Total time for testing (s)	0.4397
MSE (Test)	2.247*10-3
Number of misclassification	07/7830
Of false alarms	0.021 %
Of misses	0.542 %
Classification accuracy	99.87 %
PIVQ	
(Training results)	
Total operating scenarios	3264
no. of training samples	2800
no. of features selected	11
training data)	0.99546
validation data)	0.99565
testing data)	0.997518
MSE (train)	2.556*10-3
Total time for training (s)	9.0193
Testing results	
No. of testing samples	464
Total time for testing (s)	0.7426
MSE (Test)	2.985*10-3
Number of misclassification	24/7830
Of false alarms	0.314 %
Of misses	0.924 %
Classification accuracy	99.64 %

VII. CONCLUSIONS

A more faster and efficient learning algorithm has beenused to confirm the suitability of the proposed model for onlineapplications. The contingency analysis results indicates the ability of the methodology to screen all the contingencies and rank them in the order of their severity.

VIII. REFERENCES

[1] Jain T, Srivastava L, Singh SN. Fast voltage contingency screening using radialbasis function neural network. IEEE Trans Power Syst 2003;18(4):1359–66.
[2] Fu C, Bose A. Contingency ranking based on severity indices in dynamicsecurity analysis. IEEE Trans Power Syst 1999;14(3):980–5.

[3] Mansour Y, Vaahedi E, El-Sharkawi MA. Large scale dynamic security screeningand ranking using neural networks. IEEE Trans Power Syst 1997;12(2):954–60.
[4] Mansour Y, Vaahedi E, El-Sharkawi MA. Dynamic security contingencyscreening and ranking using neural networks. IEEE Trans Neural Networks1997;8(4):942–50.
[5] Chan KW, Edwards AR, Dunn RW, Daniels AR. On–line dynamic securitycontingency screening using artificial neural networks. IEE ProcGener, TransmDistrib 2000;147(6):367–72.
[6] Kamwa I, Grondin R, Loud L. Time-varying contingency screening for dynamic security assessment using intelligent-systems techniques. IEEE Trans PowerSyst 2001;16(3):526–36.
[7] Fischl R, Kam M, Chow JC, Ricciardi S. Screening power system contingencyusing a back propagation trained multiperceptron. In: IEEE proc of 1989 ISCAS,Portland, USA; 1989. p. 486–9.
[8] Thomas RJ, Sakk E, Hashemi K, Ku BY, Chiang HD. On-line security screeningusing an artificial neural network. In IEEE proc of 1990 ISCAS, New Orleans,USA; 1990. p. 2921–4.
[9] Weerasooriya S, El-Sharkawi MA, Damborg MJ, Marks II RJ. Towards staticsecurityassessment of a large-scale power system using neural networks. IEEProc-C 1992;139(1):64–70.
[10] Swarup KS. Artificial neural network using pattern recognition for securityassessment and analysis. Neurocomputing 2008;71:983–98.
[11] Souza J, Filho M, Schilling M. Fast contingency selection through a pattern analysis approach. Electr Power Syst Res 2002;62:13–9.

