Online Static Security Assessment Module Using Artificial Neural Networks

Sunitha R, *Member, IEEE*, R. Sreerama Kumar, *Senior Member, IEEE*, and Abraham T. Mathew, *Senior Member, IEEE*

***Abstract*—Fast and accurate contingency selection and ranking method has become a key issue to ensure the secure operation of power systems. In this paper multi-layer feed forward artificial neural network (MLFFN) and radial basis function network (RBFN) are proposed to implement the online module for power system static security assessment. The security classification, contingency selection and ranking are done based on the composite security index which is capable of accurately differentiating the secure and non-secure cases. For each contingency case as well as for base case condition, the composite security index is computed using the full Newton Raphson load flow analysis. The proposed artificial neural network (ANN) models take loading condition and the probable contingencies as the input and assess the system security by screening the credible contingencies and ranking them in the order of severity based on composite security index. The numerical results of applying the proposed approach to IEEE 118-bus test system demonstrate its effectiveness for online power system static security assessment. The comparison of the ANN models with the model based on Newton Raphson load flow analysis in terms of accuracy and computational speed indicate that the proposed model is effective and reliable in the fast evaluation of the security level of power systems. The proposed online static security assessment (OSSA) module realized using the ANN models are found to be suited for online application.**

***Index Terms*—Composite security index, contingency screening and ranking, multi-layer feed forward neural network, online static security assessment, radial basis function network.**

I. Introduction

MAINTAINING system security is an important requirement in the operation of a power system. Power system security assessment is the analysis performed to determine whether, and to what extent, a power system is reasonably safe from serious interference to its operation [1]. Three major functions involved in power system security assessment are system monitoring, contingency analysis and security control. System monitoring provides up-to-date information of bus voltages, currents, power flows and the status of circuit breaker through the telemetry system so that operators can easily identify the system in the normal state or in abnormal condition.

Manuscript received November 11, 2012; revised February 13, 2013 and April 25, 2013; accepted May 28, 2013. Date of publication June 26, 2013; date of current version October 17, 2013. Paper no. TPWRS-01264-2012.

S. R and A. T. Mathew are with the Department of Electrical Engineering, National Institute of Technology Calicut, Kerala 673601, India (e-mail: rsunitha@nitc.ac.in; atm@nitc.ac.in).

R. S. Kumar is with King Abulaziz University Jeddah, Jeddah 21589, Saudi Arabia (e-mail: sreeram@nitc.ac.in).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TPWRS.2013.2267557

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 and involves critical contingency screening and ranking [2]. If the system is found to be in *insecure*, security control will take the preventive or corrective control actions to ensure the system back to *secure* condition.

Static security assessment checks the degree of satisfaction for all relevant static constraints of post contingency steady states and is needed to solve a large set of nonlinear algebraic equations [3] for N and N-1 system conditions. The security analysis becomes more complex and difficult, as these studies need to be performed online for it to be more effective. Conventionally these analysis are performed offline, since the simulation take significant computation time. The large computational burden has been the main impediment in preventing the security assessment from online use [4]. On the other hand there is a pressing need for more accurate and powerful tool for security assessment [5]. The work presented in this paper was motivated by the attempt to significantly reduce the computation time required for security assessment so that the analysis can be converted from offline to online use, in order to assist the grid operators in their real time controller analysis. The trend towards deregulation has forced the modern utilities to operate their systems closer to security boundaries. This has fueled the need for faster and more accurate methods of security assessment [6].

The overall computational speed and accuracy of an online security assessment depends on the effectiveness of contingency screening and ranking method, the objective of which is to identify the critical contingencies among a list of possible contingencies. The contingency selection and ranking is conventionally performed by various schemes by computing a scalar performance index (PI) derived from DC or fast decoupled load flow solution for each contingency [7]. These methods generally employ a quadratic function as the performance index. This makes the contingency ranking prone to masking problems, where a contingency with many small limit violations is ranked equally with the one in which there are only a few large limit violations. Also, the selection of weighting factors in the performance index is found to be a difficult task, as it should be chosen based on both the relative importance of buses and branches and the power system operating practice [8], [9]. In addition, majority of the performance indices do not provide an exact differentiation between the *secure* and *non-secure* states. The performance indices were traditionally calculated separately for line flows and bus voltages, as the overall performance index defined as the sum or weighted-sum of the scalar performance indices for bus voltages and the line flows could not provide accurate results [10].

In [10], authors have proposed a single composite security index to indicate bus voltage and line flow limit violations which is calculated using Newton Raphson load flow technique. The index is defined in such a way that it completely eliminates the masking problem, and provides a better definition of security in which the *secure state* is indicated by an index value "0", while a value greater than "1" indicates *insecure state*. Index values lying between "0" and "1" indicate the *alarm limit*. It also avoids the difficult task of selecting the weights. This index works a projection of the multiple factors in to a hyperboloid region as a scalar value, considering both power flow and bus voltage violations, making it more robust. An overview is given in the following section.

While the newly introduced index ensures proper classification of security levels, the attempt could be to expedite the computations. In this direction, over the past few years, several approaches using artificial neural networks (ANN) have been proposed as alternative methods for static security assessment using both supervised and unsupervised architectures [11]–[14]. Since the ANNs reduce the online computational requirements and are quick in response time, these has the potential for online applications and can easily be adapted. The real time computational speed and strong generalization capability makes the ANN an ideal candidate for next generation security monitoring of power systems [15]. Fischi *et al.* [16] has applied ANN for online contingency screening and ranking and found that ANN has good potential in terms of speed and accuracy. Lu [17] has applied feed forward, error back propagation ANNs in protecting the generator transformer units of power system. One of the most important aspects of achieving good ANN performance has proven to be the proper selection of training features to represent all possible states of the system and presents an enormous computational exercise for large scale power systems [18].

The main contribution of this paper consists of developing an online static security assessment (OSSA) module in order to overcome the large computational overhead of real time static security assessment procedure .The proposed module utilizes the composite security index (PI_c) for the fast and accurate static security evaluation. The proposed OSSA module is capable of doing three functions. 1) It computes the composite security index (PI_c) for the given operating condition and provides security status, 2) compute the composite security index for all the possible line outage conditions and identifies the critical contingencies having index values greater than "1" (contingency screening) and 3) the contingency ranking in the descending order of severity based on PI_c. The proposed OSSA module utilizes an ANN module that computes the composite security index for a particular loading and contingency condition. The training of the ANNs involves the development of composite security index for a wide range of loading conditions, for different contingencies. In this work a multi-layer feed forward network (MLFFN) and radial basis function network (RBFN) based OSSA modules are developed for IEEE 118-bus test system.

The remaining part of this paper is organized as follows: A brief description of the composite security index (PI_c) utilized in this paper for security assessment and critical contingency ranking [10] is given in the following section. It is followed by the proposed ANN models for online static security assessment. The test systems and the simulation results to demonstrate the effectiveness of the proposed ANN models for security assessment is presented in Section IV. Section V gives the concluding remarks.

II. Composite Security Index—An Overview

In this paper the composite security index defined in terms of both line flow and bus voltage limit violations is used for security state classification, online critical contingency screening and ranking. Two types of limits are defined for bus voltages and line loadings, namely the *security limit* and the *alarm limit*. The *security limit* is the maximum limit specified for the bus voltages and line flows. The *alarm limit* provides an alarm zone adjacent to the *security limit*, which gives an indication of closeness to limit violations. The alarm zone also provides a flexible means of specifying the cut-off point for contingency selection based upon numerically ranked security index [10]. It is also possible to treat the constraints on the bus voltage and the line flows as soft constraints, thereby the violation of these constraints, if not excessive, may be tolerated for short periods of time.

The system is considered *insecure* if one or more bus voltages or line flows exceed their *security limit*. If one or more bus voltages or line flows exceed their *alarm limit* without exceeding their *security limit*, the system is considered to be in the *alarm state*. If none of the voltages or line flows violates an *alarm limit*, the system is considered *secure*. This is indicated by an index value of "0".

It is assumed that the desirable voltage at each bus is known and is represented as V_i^d. The upper and lower *alarm limits* and *security limits* of bus voltages are represented as F_i^u, F_i^l, V_i^u and V_i^l, respectively. The normalized upper and lower voltage limit violations beyond the *alarm limits* are defined as in (1):

$$\begin{aligned} d_{v,i}^u &= \frac{[V_i - F_i^u]}{V_i^d} \; ; \; if \quad V_i > F_i^u \\ d_{v,i}^u &= 0 \qquad\quad ; if \quad V_i \le F_i^u \\ d_{v,i}^l &= \frac{[F_i^l - V_i]}{V_i^d} \; ; \; if \quad V_i < F_i^l \\ d_{v,i}^l &= 0 \qquad\quad ; \; if \quad V_i \ge F_i^l \end{aligned} \tag{1}$$

where V_i is the voltage magnitude at bus i. For each upper and lower limit of bus voltages, the normalization factor $g_{v,i}$ is defined in (2):

$$\begin{aligned} g_{v,i}^u &= \frac{[V_i^u - F_i^u]}{V_i^d} \\ g_{v,i}^l &= \frac{[F_i^l - V_i^l]}{V_i^d}. \end{aligned} \tag{2}$$

According to (1) and (2), it can be observed that the ratio (d/g) will give a value of "0" if the value of the bus voltage is in between the upper and lower alarm limit. Hence it is classified as *secure*. If the value of the bus voltage vector is above the upper alarm limit or below the lower alarm limit, it gives a value greater than "0". Moreover, if the value of the bus voltage is above the upper security limit or below the lower security limit,

the value of (d/g) vector will be greater than "1" and is in *insecure* condition. If the value of (d/g) vector is in between "0" and "1", it is said to be in the alarm limit. Similar explanations holds good for power flows as well.

For line flows, the limit violation vectors d_p and the normalization factor g_p are defined in the similar manner. Since only the maximum limits are required to be specified for the power flow through each line, two types of upper limits are specified for each line: the *alarm limit* P_F and the *security limit* P_P. The *security limit* is the specified maximum limit of the power flow through the line. The normalized power flow limit violation vectors for each line j can be defined as in (3):

$$\begin{aligned} d_{p,j} &= \frac{[|P_j| - P_{F,j}]}{Base\ MVA} \quad ; if \quad |P_j| > P_{F,j} \\ d_{p,j} &= 0 \quad ; if \quad |P_j| \le P_{F,j} \end{aligned} \tag{3}$$

where $|P_j|$ is the absolute value of the power flow through the line j. The normalization factor for each line j is defined in (4):

$$g_{p,j} = \frac{[P_{P,j} - P_{F,j}]}{Base\ MVA}. \tag{4}$$

In this case also, the system can be classified with respect to the power flow through the line, into secure, alarm or insecure, based on the value of (d/g) vector.

For an N-bus, M line system, there are $(\mathrm{N} + \mathrm{M})$ dimensional normalized limit violation vectors of both bus voltages and line flows. The concept of hyper-ellipse inscribed within the hyper-box is used for constructing the scalar valued composite security index PI_c from the vector valued limit violation vectors [10] and it is defined in (5) as

$$PI_c = \left[\sum_i \left(\frac{d^u_{v,i}}{g^u_{v,i}} \right)^{2n} + \sum_i \left(\frac{d^l_{v,i}}{g^l_{v,i}} \right)^{2n} + \sum_j \left(\frac{d_{p,j}}{g_{p,j}} \right)^{2n} \right]^{\frac{1}{2n}} \tag{5}$$

where "n" is the exponent used in the hyper ellipse equation. The value of "n" is chosen as "2", because the approximation of hyper-box to the hyper-ellipse has not improved beyond "n"$= 2$ [10].

From the definition of composite security index, the system is said to be in one of the three states as follows.

1) *Secure state* if $PI_c = 0$
2) *Alarm state* if $0 < PI_c \le 1$
3) *Insecure state* if $PI_c > 1$

The contingencies can be ranked in the descending order of severity based on PI_c.

III. Online Static Security Assessment Module Using ANN

In the proposed approach, power system security assessment against unplanned line outages are done by utilizing the high adaptation capability of ANNs, as these are better suited to deal with nonlinear problems. Fig. 1 shows the structure of the proposed OSSA module. The real and reactive power generation at the generator buses (P_G, Q_G), real and reactive power loads at all load buses (P_D, Q_D), the voltage magnitudes $(|V|)$ and phase angle δ for all buses are used for describing the system operating point and are chosen as the input for the security assessment module. This module is capable of providing the security status as well as the critical contingency screening and ranking in terms of composite security index for the given operating condition.

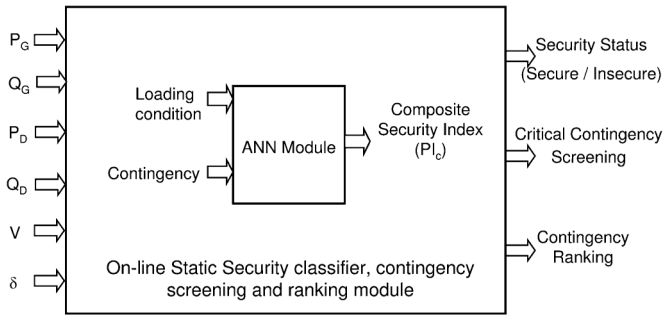

Fig. 1. Structure of online static security assessment (OSSA) module.

The proposed OSSA module utilizes an ANN module for which the loading condition and contingency are the inputs and composite security index as the output. The contingencies are represented as a binary number in which "0" represents no outage condition and "1" represents the outage of the corresponding line. Two types of ANNs viz. MLFFN and RBFN are used to implement the proposed OSSA module, details of which are given in the following subsections.

A. Multi-Layer Feed Forward Network (MLFFN)

In this paper, MLFFN consisting of two hidden layers having nodes with nonlinear activation functions is proposed for power system security assessment. Each node in one layer connects with a certain weight to every other node in the following layer. Real and reactive power demand at various load buses and binary numbers representing contingency are taken as the inputs to the MLFFN. The number of inputs mainly depends upon the topology of the system under consideration. The activation function used in the hidden layers is the "hyperbolic tangent" and at the output layer, the linear function is used. The network is trained with "Levenberg-Marquardt" back propagation algorithm [13] due to its good convergence properties. In order to obtain the optimum number of neurons in the hidden layer, the number of neurons in the first hidden layer is varied from 10 to 60 and the second hidden layer from 3 to 10. For each change, in the number of hidden units, the ANN was trained and the mean square errors are compared. The number of neurons with minimum mean square error is selected for the final structure of MLFFN.

B. Radial Basis Function Network (RBFN)

RBFN is a special class of feed forward neural network and consists of an input layer, a hidden layer and an output layer. The network is capable of performing nonlinear mapping of the input features into the output. The hidden layer consists of neurons with Gaussian activation functions, while the output layer neurons are with linear activation function. During training, all the input variables are fed to the neurons in the hidden layer directly through interconnections with unity weights and only

the weights between hidden and output layers are to be trained. Thus, RBFN gives faster convergence than the conventional MLFFN.

C. Data Generation, Training, and Testing

For the system under consideration, initially the probable contingencies are listed out. In this work only the line outages are considered. The training data are generated by varying the loads randomly between 50 and 150 percentage of their base case values. For each loading condition the pre and post-outage bus voltages and line flows are calculated with full iterations of Newton Raphson (NR) load flow analysis. For each case, the composite security index is calculated using (5) by taking the value of "n" as "2" [10]. Nearly 5000 training sets are generated for the test system under consideration.

Once the ANNs are trained, the trained module is tested for various random loading conditions, within the expected range of load variations. The trained ANN module can be used for online static security assessment module which takes a particular operating condition in terms of P_G, Q_G, P_D, Q_D, $|V|$, and δ as the input and provides the security status of the system for the given operating condition. It can also provide the composite security index value for all contingencies considered and the critical contingencies identified as those with index value greater than one. The contingencies can also be ranked in the order of severity based on the composite security index PI_c.

IV. Test Systems and Simulation Results

The proposed work aims to develop an online static security assessment module using the MLFFN and RBFN network architectures, which can predict the security state of the system for a particular operating condition as well as critical contingency screening and ranking based on the composite security index. In order to investigate the effectiveness of the proposed method investigations are carried out on different standard test systems. The simulations results of IEEE 118-bus test system is discussed in the following subsection.

A. IEEE 118-Bus Test System

The OSSA using MLFFN and RBFN are developed for IEEE 118-bus test system. The system consists of 54 generators and 177 transmission lines and 9 transformers [19]. The single line diagram of the system is shown in Fig. 2.

All line outages, except the lines which are the only line connected to a generator bus, are considered and simulated for system security evaluation. To calculate the composite security index, both *alarm* and *security limits* are to be chosen for each bus voltages and line flows. $\pm 5\%$ and $\pm 7\%$ of the desired value are taken as the *alarm limit* and *security limit* respectively for the bus voltages. For PV buses the specified bus voltage is taken as the desired bus voltage and for PQ buses it is assumed to be "1 p.u". For line flows, 80% of the specified thermal limit is chosen as the *alarm limit*.

To develop the proposed OSSA module for IEEE 118-bus system, the training sets are generated for the proposed ANN architectures by computing the composite security index for different contingencies considering random loading conditions within the stipulated load ranges. The training parameters used for both MLFFN and RBFN architectures, to get the best convergence characteristics, are given in Table I. The performances of the trained MLFFN, RBFN and the performance of the proposed OSSA module are presented in the following subsections.

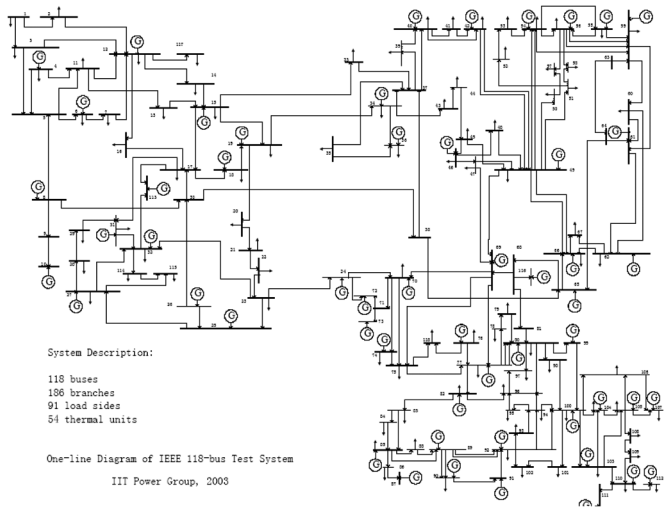

Fig. 2. Single line diagram of IEEE 118-bus test system (source: IIT Power Group, 2003).

TABLE I
Training Parameters

Parameter	MLFFN	RBFN
(1)	(2)	(3)
Maximum epochs	100	–
Performance goal	0	–
Minimum gradient	$1\text{x}10^{-10}$	–
Learning rate	0.01	–
Momentum coefficient	0.9	–
Gaussian function spread	–	90

1) MLFFN Based OSSA: The structure of MLFFN developed for the proposed OSSA consists of the real and reactive power loads and the binary number which represents the contingency as the inputs and the corresponding composite security index as the output. The number of neurons in the hidden layers, chosen with minimum mean square error is 30 and 10, respectively, for the respective hidden layers. The time required to train the MLFFN network is found to be 12 507.8 s. In order to get the best convergence characteristics, a series of computer simulations are done and chosen the acceptable one through inspection. Fig. 3 shows the variation of mean square error (MSE) with reference to the number of epochs obtained for training the MLFFN network. It is shown that the MSE obtained for IEEE 118-bus test system is 3.579×10^{-6}.

Once the ANNs are trained, the composite security index values for different loading conditions with different contingencies obtained with the proposed MLFFN architecture are compared with that obtained using (5) which is based on Newton Raphson load flow (NRLF) analysis. For a light load condition of 80% of the base load and a heavy load condition of 110% of the base load, 20 contingencies are selected randomly and numbered as shown in column 1 of Table II. The corresponding contingencies are given in columns 2 and 3, respectively. For

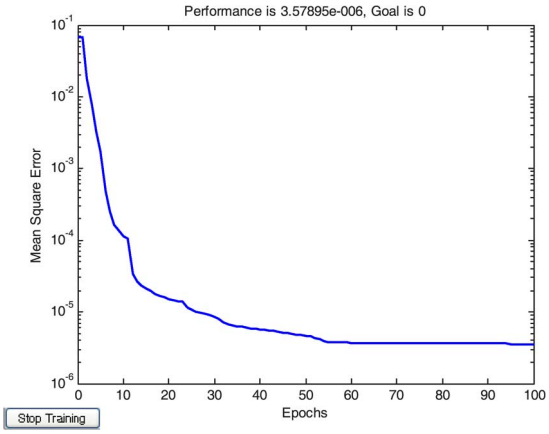

Fig. 3. Training of MLFFN for IEEE 118-bus test system.

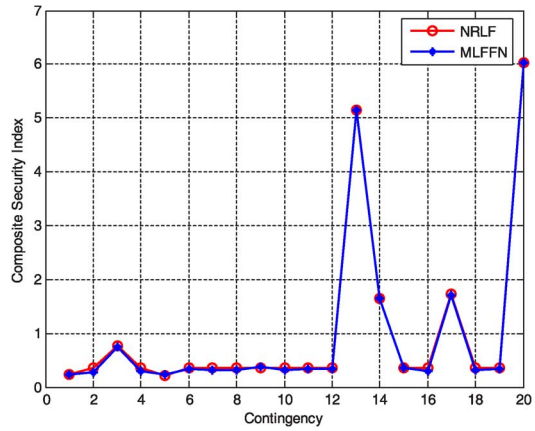

Fig. 4. Composite security indices for light load condition (80% of base load).

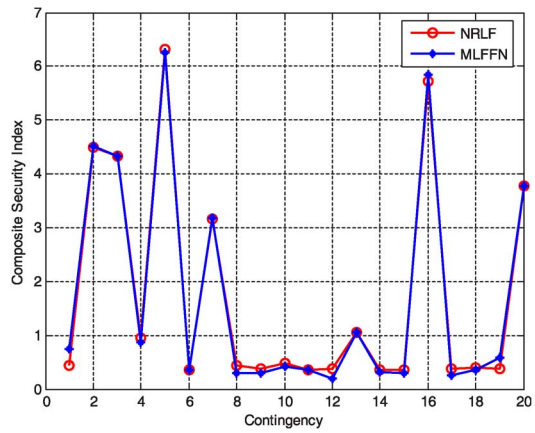

Fig. 5. Composite security indices for heavy load condition (110% of baseload).

TABLE II
RANDOMLY SELECTED CONTINGENCIES FOR TESTING THE MLFFN AND RBFN FOR DIFFERENT LOADING CONDITIONS

Contingency Number	Contingencies considered for MLFFN		Contingencies considered for RBFN	
	80% of base load	110% of base load	90% of base load	base load
(1)	(2)	(3)	(4)	(5)
1	L 89-92	L 49-66	L 77-80	L 54-55
2	L 49-66	L 100-104	L 101-102	L 104-105
3	L 75-77	L 25-27	L 1-3	L 69-3
4	L 17-31	L 68-116	L 15-19	L 40-41
5	L 49-51	L 38- 37	L 80-99	L 4-11
6	L 93-94	L 35- 37	L 50-57	L 82-83
7	L 81-80	L 100-103	L 103-105	L 77-78
8	L 56-59	L 89- 90	L 88-89	L 68-116
9	L 49-69	L 15-19	L 77-82	L 66-67
10	L 80-96	L 4- 5	L 47-49	L 49-54
11	L 11-12	L 100-106	L 23-25	L 8-30
12	L 71-73	L 26- 30	L 22-23	L 74-75
13	L 4-11	L 40-41	L 30-17	L 88-89
14	L 54-56	L 77-80	L 55-56	L 49-50
15	L 40-42	L 37- 40	L 100-101	L 48-49
16	L 100-103	L 59-60	L 61-62	L 55-56
17	L 4-5	L 2-12	L 80-98	L 89-92
18	L 91-92	L 12-117	L 56-59	L 80-96
19	L 27-115	L 24-70	L 48-49	L 106-107
20	L 75-118	L 55-56	L 54-59	L 98-100

example, at 80% loading condition, contingency number 3 represents the line outage L 75–77, which is the outage of line connected between buses 75 and 77. All the line outages given in various Tables can be identified in the same manner.

For each case, the composite security indices obtained with trained MLFFN network and that calculated using (5), are plotted against the contingency number as shown in Figs. 4 and 5, respectively. It can be observed from the figures that the trained MLFFN network performed well and are accurate in predicting the composite security index, for all contingencies.

2) RBFN Based OSSA: The RBFN is also trained using the same training set that is developed for MLFFN. In this case, the number of neurons in the hidden layer is equal to the number of training sets. The RBFN is trained to an accuracy of 11.252×10^{-11}. The time required for training the RBFN was only 294.44 s, which is very less compared to that required for training the MLFFN. For evaluating the performance, the composite security indices obtained with trained RBFN are compared with those computed using (5) based on NRLF analysis.

In this case also two loading condition are considered, the base load condition and the light load condition of 90% of the base load. 20 contingencies are randomly selected for each loading condition as shown in columns 4 and 5 of Table II. Figs. 6 and 7 compare the composite security indices obtained with RBFN with those obtained using (5) for the various contingency cases. It is observed that the trained RBFN is capable of computing the index values as accurate as that by NRLF analysis.

3) Online Static Security Assessment Module: In the previous subsections it is observed that both MLFFN and RBFN are capable of accurately predicting security status of the power system for a particular contingency by computing the composite security index. The trained ANNs can now be used for implementing the proposed OSSA module.

The OSSA module performs the complete security assessment for the given operating condition by predicting the security state, screening the most credible contingencies and ranking them in the order of severity based on composite security index.

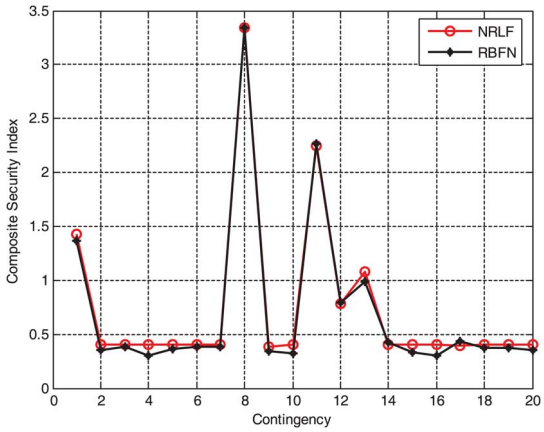

Fig. 6. Composite security indices for light load condition (90% of baseload).

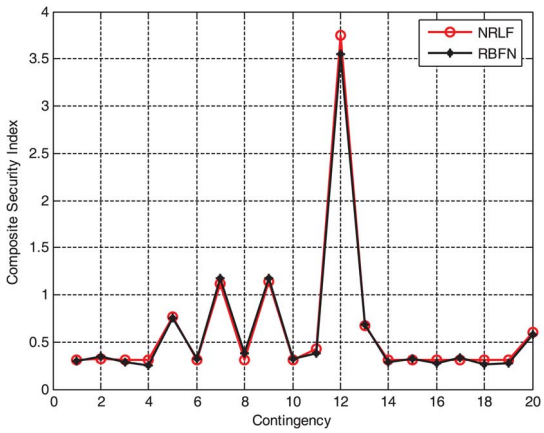

Fig. 7. Composite security indices for base load condition.

According to this index the *secure states* are represented by an index value of "0" and the *insecure states* by "1". If the index value is in between "0" and "1" the system is said to be in the *alarm state*.

Three sets of operating conditions, normal load, light load and heavy load, are considered for evaluating the performance of proposed OSSA. 75% and 120% of the base load has been taken as the light load and heavy load conditions respectively. For each loading conditions static security assessment has been carried out using the proposed OSSA module and conventional NRLF method using (5). Some 30 contingencies are selected and ranked in the order of severity based on the composite security index computed using (5) and are shown in Tables III–V for different loading conditions.

Table III shows the contingency rank list under light load condition. In this table, column 1 represents the different line outages considered under this operating condition and these contingencies are ranked according to severity using the index value computed using (5) as given in column 2. The corresponding index values obtained using the proposed OSSA module that utilizes the previously trained MLFFN and RBFN are shown in columns 3 and 4, respectively. For light load conditions it can be observed that for all the critical contingencies with index value greater than "1", the proposed OSSA module based on both network architectures, could also rank them exactly as in that of column 2.

TABLE III
CONTINGENCY RANK LIST UNDER LIGHT LOAD CONDITION FOR IEEE 118-BUS TEST SYSTEM

Contingency (Line outage)	Composite Security index using Eqn.(5)	Composite Security index using MLFFN	Composite Security index using RBFN
(1)	(2)	(3)	(4)
L 89- 90	30.77467	30.79216	30.76343
L 89-92	22.6849	22.59828	22.58463
L 49-66	12.50035	12.49966	12.50787
L 26-30	11.10473	11.08885	11.0977
L 42-49	8.855254	8.868847	8.832592
L 8-5	7.673895	7.665424	7.603819
L 63-59	6.030314	6.03175	6.019245
L 100-103	5.146244	5.146525	5.154932
L 88-89	3.274825	3.295642	3.284094
L 38-37	2.971544	2.979996	2.996509
L 25-27	2.788457	2.787199	2.768381
L 23-25	2.23811	2.22856	2.249759
L 77-80	1.751164	1.744447	1.7382
L 75-118	1.730267	1.712572	1.716365
L 17-18	1.690907	1.63594	1.546399
L 34-37	1.674199	1.673635	1.70351
L 4-5	1.652656	1.657158	1.668521
L 38-65	1.54419	1.438483	1.450369
L 30-17	1.087362	1.065643	1.047073
L 85-88	0.86094	0.874068	0.93098
L 49-51	0.759738	0.753391	0.763203
L 51-52	0.735913	0.735972	0.788052
L 23-32	0.714508	0.685859	0.699994
L 22-23	0.710073	0.702922	0.731382
L 2-12	0.634583	0.630272	0.654894
L 49-54	0.501442	0.497536	0.506015
L 62-67	0.358969	0.296216	0.348179
L 105-106	0.358886	0.289864	0.307813
L 77-82	0.349044	0.347004	0.393697
L 76-118	0.193888	0.192249	0.307049

The contingency rank list under normal load condition is shown in Table IV. The columns of the table are also ordered similar to that of Table III. Under Normal load condition also it can be seen that all contingencies except the last 2, are exactly ranked as that of column 2.

The rank list under heavy load condition given in Table V can also be explained in the same manner. In this case it can be observed that all critical contingencies with indices greater than "1" are ranked very well as that of column 2 for heavy load condition. It can be observed from the tables that the proposed OSSA module designed for a particular system can accurately perform the static security assessment for all loading conditions.

The effectiveness of the proposed OSSA is also investigated by evaluating the computation time required for online static security assessment. In Table VI, the overall computation time required for conducting static security assessment using conventional NRLF method and the proposed OSSA module are shown. Column 1 gives the computation time required, if full iterations of NRLF is used for the security assessment. Traditionally, for online applications only 1 to 3 iterations are used

TABLE IV
CONTINGENCY RANK LIST UNDER NORMAL LOAD CONDITION FOR IEEE 118-BUS TEST SYSTEM

Contingency (Line outage)	Composite Security index using Eqn.(5)	Composite Security index using MLFFN	Composite Security index using RBFN
(1)	(2)	(3)	(4)
L 89-90	30.72274	30.70915	30.76397
L 89-92	22.13343	22.17843	22.2346
L 49-66	13.95447	13.97213	13.96378
L 26-30	11.11361	11.16046	11.15891
L 42-49	10.8184	10.83116	10.82033
L 8-5	9.877564	9.879072	9.922228
L 63-59	8.336436	8.324746	8.33207
L 100-103	5.919138	5.929475	5.926148
L 38-65	4.254504	4.305763	4.328086
L 25-27	3.92187	3.915343	4.008146
L 38-37	3.805559	3.804339	3.806466
L 88-89	3.751192	3.541358	3.553415
L 34-37	2.664418	2.677165	2.687728
L 4-5	2.659783	2.663542	2.679747
L 75-118	2.314439	2.345193	2.380645
L 23-25	2.25746	2.243015	2.274598
L 17-18	2.006658	2.020747	1.841953
L 23-32	1.334433	1.367712	1.402003
L 30-17	1.161755	1.204462	1.214158
L 49-54	1.137538	1.045284	1.172911
L 22-23	0.972325	0.973497	0.987615
L 49-51	0.967663	0.950367	0.959115
L 51-52	0.951275	0.948278	0.954239
L 2-12	0.845761	0.855156	0.855043
L 85-88	0.526807	0.514764	0.487236
L 77-80	0.468261	0.613312	0.566954
L 105-106	0.325068	0.245833	0.30732
L 62-67	0.314383	0.29805	0.295486
L 77-82	0.313163	0.083887	0.137254
L 76-118	0.291389	0.269893	0.29375

TABLE V
CONTINGENCY RANK LIST UNDER HEAVY LOAD CONDITION FOR IEEE 118-BUS TEST SYSTEM

Contingency (Line outage)	Composite Security index using Eqn.(5)	Composite Security index using MLFFN	Composite Security index using RBFN
(1)	(2)	(3)	(4)
L 89-90	30.68431	30.69064	30.57721
L 89-92	21.60709	21.59364	21.56884
L 49-66	15.43777	15.42804	15.41776
L 42-49	12.65241	12.64625	12.59951
L 8-5	12.57885	12.62605	12.72366
L 26-30	11.13607	11.1058	11.08838
L 63-59	10.7251	10.73833	10.71523
L 38-65	7.523053	7.531563	7.500998
L 100-103	6.718624	6.648888	6.506102
L 25-27	5.077763	5.072529	4.993065
L 38-37	4.937004	4.904507	4.779564
L 88-89	4.02071	3.846698	3.723943
L 4-5	3.67819	3.667859	3.60367
L 34-37	3.670279	3.654841	3.621906
L 75-118	3.097383	3.088766	3.001241
L 17-18	2.373354	2.36972	2.382122
L 23-25	2.293345	2.286124	2.112377
L 30-17	2.25353	2.24058	2.219249
L 23-32	1.981868	1.939126	1.855336
L 49-54	1.803599	1.974055	1.678708
L 22-23	1.444453	1.454043	1.429162
L 2-12	1.424524	1.495353	1.413967
L 49-51	1.201993	1.249842	1.24838
L 51-52	1.192547	1.200815	1.153724
L 77-82	0.98983	1.021061	1.106625
L 77-80	0.842121	0.885914	0.81308
L 105-106	0.531447	0.604768	0.715869
L 85-88	0.516371	0.563205	0.62986
L 62-67	0.50676	0.686934	0.671646
L 76-118	0.471519	0.519065	0.524092

in order to reduce the computation time [9]. It is observed from [10] that the composite security index computed with 3 iterations of NRLF gives the same result as that with full iteration and the computation time taken is given in column 2 of Table VI.

In columns 3 and 4 of Table VI, the computation time required for static security assessment using the proposed OSSA module utilizing MLFFN and RBFN architectures, respectively, are given. It can be observed that the proposed OSSA module is well suited for online applications.

TABLE VI
COMPUTATION TIME REQUIRED FOR ONLINE STATIC SECURITY ASSESSMENT FOR IEEE 118-BUS SYSTEM

NRLF		**Proposed OSSA module**	
(Full iteration)	**(3 iterations)**	**MLFFN**	**RBFN**
(1)	(2)	(3)	(4)
799.891 s	301.65 s	1.438 s	1.172 s

V. CONCLUSION

This paper has proposed a computationally efficient artificial neural network technique for assessing the security of the power system against line outages. MLFFN and RBFN have been used for realizing the online static security assessment module which can identify the security status, screen the critical contingencies and rank them in the decreasing order of severity for any operating condition. To accurately identify the security status of the system the composite security index, which is a function of both power flow and bus voltage limit violations, developed by the authors have been used. The training set for ANN adequately represents the entire range of power system operating states and is defined in terms of loading condition as well as contingencies. The effectiveness of the proposed OSSA module is demonstrated on IEEE 118-bus test system in terms of accuracy of computation and reduction in computation time required for static security assessment. Proposed OSSA based on both MLFFN and RBFN architectures are capable of accurately assessing the security of the system against outages significantly faster than the conventional techniques.

REFERENCES

[1] K. Morison, L. Wang, and P. Kundur, "Power system security assessment," *IEEE Power and Energy Mag.*, vol. 2, no. 5, pp. 30–39, Sep./Oct. 2004.

[2] K. Morison, "Power system security in the new market environment: Future directions," in *Proc. IEEE PES Winter Meeting*, 2000, pp. 78–83.
[3] A. B. Alves and A. Monticelli, "Static security analysis using pipeline decomposition," *Proc. Inst. Elect. Eng., Gen., Transm., Distrib.*, vol. 145, no. 2, pp. 105–110, Mar. 1998.
[4] R. Schainker, P. Miller, W. Dubbelday, P. Hirsch, and G. Zhang, "Real-time dynamic security assessment: Fast simulation and modeling applied to emergency outage security of electric grid," *IEEE Power and Energy Mag.*, vol. 4, no. 2, pp. 51–58, Mar./Apr. 2006.
[5] P. Zhang, F. Li, and N. Bhatt, "Next generation monitoring, analysis and control for the future smart control centre," *IEEE Trans. Smart Grid*, vol. 1, no. 2, pp. 186–192, Sep. 2010.
[6] C. A. Jensen, M. A. El-Sharkawi, and R. J. Marks, II, "Power system security assessment using neural networks: Feature selection using fisher discrimination," *IEEE Trans. Power Syst.*, vol. 16, no. 4, pp. 757–763, Nov. 2001.
[7] T. A. Mikolinnas and B. F. Wollenberg, "An advanced contingency selection algorithm," *IEEE Trans. Power App. Syst.*, vol. PAS-100, no. 2, pp. 608–617, Feb. 1981.
[8] H. Song and M. Kezunovic, "Static analysis of vulnerability and security margin of the power system," in *Proc. PES IEEE Transmission and Distribution Conf. Expo., T&D*, May 2006, pp. 147–152.
[9] T. F. Halpin, R. Fischl, and R. Fink, "Analysis of automatic contingency selection algorithms," *IEEE Trans. Power App. Syst.*, vol. PAS-103, no. 5, pp. 938–945, May. 1984.
[10] Sunitha R., R. Sreerama Kumar, and A. T. Mathew, "A composite security index for on-line static security evaluation," *Elect. Power Compon. Syst.*, vol. 39, no. 1, pp. 1–14, Jan. 2011.
[11] V. S. Vankayala and N. D. Rao, "Artificial neural network and their application to power system—A bibliographical survey," *Elect. Power Syst. Res.*, vol. 28, pp. 67–69, 1993.
[12] I. S. Saeh and A. Khairuddin, "Static security assessment using artificial neural network," in *Proc. IEEE Int. Conf. Power and Energy*, Dec. 2008, pp. 1172–1177.
[13] T. S. Sidhu and C. Lan, "Contingency screening for steady-state security analysis by using FFT and artificial neural networks," *IEEE Trans. Power Syst.*, vol. 15, no. 1, pp. 421–426, Feb. 2000.
[14] K. S. Swarup and P. B. Corthis, "ANN approach assesses system security," *IEEE Comput. Applicat. Power*, vol. 15, no. 3, pp. 32–38, Jul. 2002.
[15] Y. Xu, Z. Y. Dong, J. H. Zhao, P. Zhang, and K. P. Wang, "A reliable intelligent system for real time dynamic security assessment of power system," *IEEE Trans. Power Syst.*, vol. 27, no. 3, pp. 1253–1263, Aug. 2012.
[16] R. Fischl, "Application of neural networks to power system security: Technology and trends," in *Proc. IEEE World Congr. Computational Intelligence*, Jul. 1994, vol. 6, pp. 3719–3723.
[17] Y. P. Lu *et al.*, "Neural network based generator transformer protection," in *Proc. 3rd Int. Conf. Machine Learning and Cybernetics*, Shanghai, China, Aug. 2004, vol. 7, pp. 4295–4301.
[18] S. Weerasooriya, M. A. El-Sharkawi, M. Damborg, and R. J. Marks, II, "Towards static security assessment of a large scale power system using neural networks," *Proc. Inst. Elect. Eng., Gen., Transm., Distrib.*, vol. 139, no. 1, pp. 64–70, Jan. 1992.
[19] Power System Test Case Archive. [Online]. Available: http://www.ee.washington.edu/research/pstca/.

Sunitha R (M'08) received the B.Tech (electrical and electronics) and M.Tech (energetics) degrees from Regional Engineering College Calicut (presently National Institute of Technology Calicut), India, in 1996 and 1999, respectively.

She is presently working as an Assistant Professor in the Department of Electrical Engineering, National Institute of Technology, Calicut, Kerala, India. Her research interests include power system security, power system dynamics and stability, and FACTS controllers.

R. Sreerama Kumar (SM'03) received the B.Tech degree from NSS College of Engineering Palakkad, Kerala, India, the M.Tech degree from the Indian Institute of Technology Madras, and the Ph.D. degree from the Indian Institute of Science Bangalore, India.

He is working as a Professor (DSM and EE Chair) in King Abdulaziz University, Jeddah, Saudi Arabia. He has authored five books and has more than 80 technical publications in reputed journals and conferences. His current fields of interest include power system security, demand side management, and smart grid.

Dr. Sreerama Kumar is the recipient of the prestigious national award, constituted by the Indian Society for Technical Education, for Promising Engineering Teacher for the year 2003 for creative work done in technical education and the ISTE national award for the best engineering college Teacher of Kerala state in 2008. He is Fellow of the Institution of Engineers (India).

Abraham T. Mathew (SM'13) received the Ph.D. degree from the Indian Institute of Technology Delhi in 1996.

He is working as a Professor in the Department of Electrical Engineering, National Institute of Technology, Calicut, Kerala, India. He has authored and co-authored several papers and has been referee to several journals and conferences, and reviewed several books of leading publishers. His current area of interest includes multi-agent systems, 2-D signal processing, and the use of soft computing techniques in bio-signal processing.

Dr. Mathew is a Fellow of the Institution of Electronics and Telecommunication Engineers and an active member of several professional bodies.