IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 9, Issue 7, July 2021

DOI 10.17148/IJIREEICE.2021.9725

STATIC SECURITY ASSESSMENT OF POWER SYSTEM

Prof. Vishal V. Mehtre[1], Mr. Sidhant Kumar [2], Mr. Nikhil Kr Singh[3]

Assistant Professor, Department of Electrical Engineering, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune, Maharashtra, India[1]

Student, Department of Electrical Engineering, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune, Maharashtra, India[2-3]

Abstract: The security assessment, based on which determinant decisions should be made for power system design, control and operation, is a challenging issue for utility engineers and network designers, especially in large-scale power systems. Numerous methods have been proposed and implemented for this purpose, and a variety of indices have been suggested to address the static security condition of power networks. Large-scale datasets of measurements in continually expanding power systems necessitate advanced knowledge in big data analytics. In this review paper, numerical techniques and machine learning-based methods are reviewed as two main categories for static security assessment in power systems based on principal features of static security status classification such as type of classifier, the static security index, and feature selection and extraction methods. This paper can be used as a useful reference for static security assessment of power systems.

Keywords: static security assessment, normal state, alert state , emergency state , artificial neutral network

I. INTRODUCTION

Power system security can be defined to remain secure without serious consequences to any one of a pre- selected list of credible disturbances or contingencies. Security Assessment (SA) is the analysis performed to determine whether, and to what extent, a power system is reasonably safe from serious interference to its operation. In other words power system security assessment is the process of determining if the power system is in a secure or alert (insecure) state, the secure state implies the load is satisfied and no limit violation will occur under present operating conditions and in the presence of unforeseen contingencies (i.e., outages of one or several lines, transformers or generators) .

The alert (or emergency) state implies that some limits are violated and / or the load demand cannot be met and corrective actions must be taken in order to bring the power system back to the secure state. Figure 1 shows the different operating states of the power system, which are classified as secure and insecure.

Security assessment of power systems can be divided into deterministic and probabilistic categories. While the former studies deterministic security criteria, for example, operational limitations of buses, lines, and transformers after an equipment outage such as a line, a generating unit or a transformer, the probabilistic security assessment considers the probability of occurring each contingency and analyses the power system security with a preset level of confidence.

II. STATIC SECURITY ASSESMENT

One of the main aspects of power system security is static security. Static security is defined as the ability of the system to reach a state within the specified secure region following a contingency. The standard approach to the security assessment problem is to perform the static security analysisfollowed by dynamic security analysis. The static security analysis evaluates the post contingent steady state of the system neglecting the transient behaviour and any other time dependent variations due to the changes in load generation conditions. On the other the dynamic security analysis evaluates the time dependent transition from the pre- contingent to the post contingent state. Most of the Energy Management Systems perform only the static security analysis and hence focus of this paper is on static security assessment.

DOI 10.17148/IJIREEICE.2021.9725

III. POWER SYSTEM OPERATING STATES

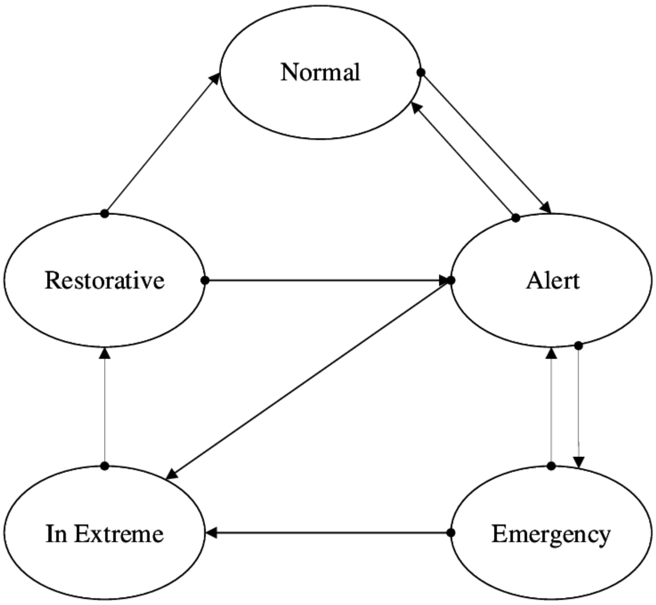

Figure 1 Operating states of power system

1. **Normal state:** In this state, all the system variables are within the normal range with no equipment being overloaded. The system is in a secure state with both ‘equality’ (total system 7 generation eqauls total system load) and ‘inequality’(bus voltages and equipment currents within the limits) constraints being satisfied. In this state, a single contingency cannot disrupt the system security and cannot cause any variable to violate the limit. The system has adequate spinning reserve.

2. **Alert state:** If the security level of the system falls below some specified threshold, the system then enters the alert state and is termed as ‘insecure’. The system variables are still within limits. This state may be brought about by a single contingency, large increase in system load or adverse weather conditions. Preventive control steps taken to restore generation or to eliminate disturbance can help in restoring the system to the normal state. If these restorative steps do not succeed, the system remains in the alert state. Occurrence of a contingency with the system already in alert state, may cause overloading of equipments and the system may enter emergency state. If the disturbance is very severe, the system may enter into extremis state directly from alert state.

3. **Emergency state:** If the preventive controls fail or if a severe disturbance occurs, the system enters emergency state. The transition to this state can occur either from normal state or alert state. In this state the balance between generation and load is still maintained (equality constraints still satisfied) and the system remains in synchronism. Failure of these components results in system disintegration. Emergency control actions like disconnection of faulted section, re-routing of power excitation control, fast valuing, and load curtailment have to be taken. It is most urgent that the system be restored to normal or alert state by means of these actions.

4. **In-extremis state:** If the emergency control actions fail when the system is in emergency state, then the system enters into in-extremis state. The system starts to disintegrate into sections or islands. Overloaded generators start tripping leading to cascade outages and possible ‘blackout’. Control actions, such as load shedding and controlled system operation are taken to save as much of the system as possible from a widespread blackout.

5. **Restorative state:** The restorative state represents a condition in which control action is being taken to restart the tripped generators and restore the interconnections. The system transition can be either to normal or alert state depending on system conditions. The sequence of events that result in system transition from normal to in-extremis state may take from few seconds to several minutes. The control actions may be initiated from the central energy control centre either through operators or automatically.

IV. STATIC SECURITY ASSESSMENT TECHNIQUE

The power system security assessment methods can be categorized from the viewpoint of classifiers, feature selection and extraction techniques which are used to assess the security status of the power system. These features can speed up or speed down the security assessment and can improve or weaken the accuracy. The references in the SSA area can

DOI 10.17148/IJIREEICE.2021.9725

also be categorized from power system implementation perspective, in which the contingency, correlation between the random data generation, type of input data, and the way of their measurement and different security indices are considered. These aspects affect the comprehensiveness of the proposed methods. The mentioned categorization is shown in Figure 2

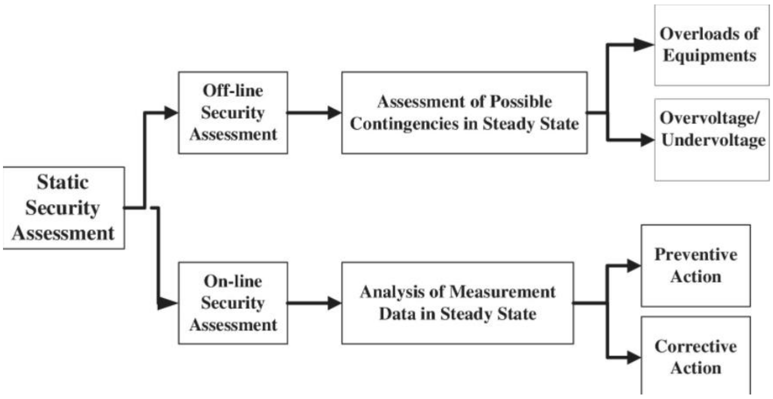
Static Security Assessment
Off-line Security Assessment
Assessment of Possible Contingencies in Steady State
Overloads of Equipments
Overvoltage/ Undervoltage
On-line Security Assessment
Analysis of Measurement Data in Steady State
Preventive Action
Corrective Action

Figure 2 Categorization of security assessment problems

In conventional practice security assessment is obtained by analytically modeling the network and solving load flow equation repeatedly for all the prescribed out ages, one contingency at a time. These analytical techniques are usually time consuming and therefore not always suitable for real time applications. Also these methods suffer from the problem of misclassification or / and false alarm. Misclassification arises when an active contingency is classified as critical. With recent advancements in information processing and learning techniques, ANN based methods for security assessment is a viable alternative.

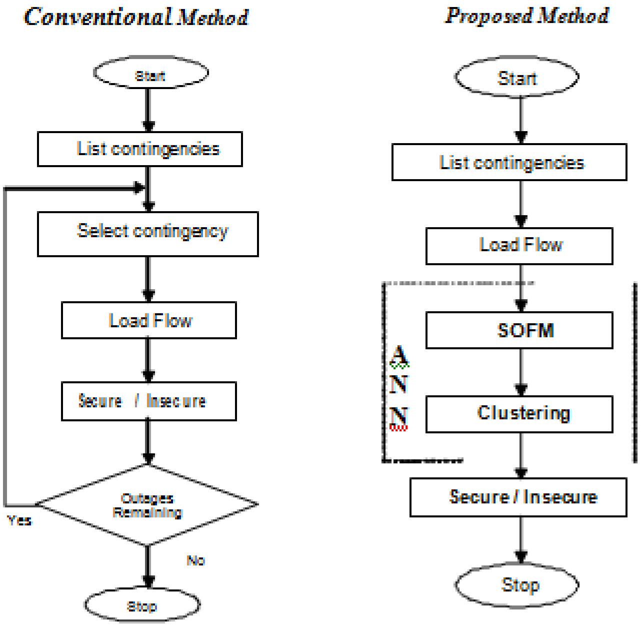

Figure 3 Comparison between Conventional and Proposed method

ARTIFICIAL NEURAL NETWORK: The artificial neural network (ANN) is employed to assess the SSS of the power system. An ANN is based on a collection of connected units or nodes called artificial neurons, which loosely model the neurons in a biological brain. Each connection, like the synapses in a biological brain, can transmit a signal to other neurons. An artificial neuron that receives a signal then processes it and can signal neurons connected to it. The "signal" at a connection is a real number, and the output of each neuron is computed by some non-linear function of the sum of its inputs. The connections are called edges. Neurons and edges typically have a weight that adjusts as learning proceeds. The weight increases or decreases the strength of the signal at a connection. Neurons may have a threshold

DOI 10.17148/IJIREEICE.2021.9725

such that a signal is sent only if the aggregate signal crosses that threshold. Typically, neurons are aggregated into layers. Different layers may perform different transformations on their inputs. Signals travel from the first layer (the input layer), to the last layer (the output layer), possibly after traversing the layers multiple times.

V. CONCLUSION

Power system security can be defined to remain secure without serious consequences to any one of a pre- selected list of credible disturbances or contingencies. Security Assessment (SA) is the analysis performed to determine whether, and to what extent, a power system is reasonably safe from serious interference to its operation. One of the main aspects of power system security is static security. Static security is defined as the ability of the system to reach a state within the specified secure region following a contingency. The standard approach to the security assessment problem is to perform the static security analysis followed by dynamic security analysis. The static security analysis evaluates the post contingent steady state of the system neglecting the transient behaviour and any other time dependent variations due to the changes in load generation conditions. The power system security assessment methods can be categorized from the viewpoint of classifiers, feature selection and extraction techniques which are used to assess the security status of the power system. These features can speed up or speed down the security assessment and can improve or weaken the accuracy.

VI. REFRENCES

[1]. Ejebe G.C and Wollenberg B.F., 'Automatic Contingency Selection', IEEE Transactions on Power Apparatus and Systems, Vol. PAS-98, No.1 Jan/Feb 1979.

[2]. Weerasooriya, S., El-Sharkawi, M W., Damborg, M., Marks II, R J., 'Towards the Static Security Assessment of a large scale Power System using Neural Networks', IEEE Proceeding-C, vol.139, No.1, Jan 1992, pp 64-70

[3]. Teuvo Kohonen, '‘The Self-Organizing Map’, Proceeding of IEEE, Vol.78, Sep 1990, PP 1464-1476.

[4]. Dagmar Niebur and Alain J. Germond, ‘Unsupervised neural net classification of power system static security states', Electrical Power and Energy Systems, Vol.14, No2/3 April/June 1992, PP 233 – 242.

[5]. K Shanti Swarup and P. Britto Corthis, “ANN Aproach Assesses System Security”, IEEE Computer Applications in Power, Vol.15, July 2002,PP.32-38.