CHAPTER 1

INTRODUCTION

1.1 POWER SYSTEM OPERATION

Present day expansion of national power grids has been hampered by social, environmental and economic constraints. At the same time, power demand has dramatically increased. This combination of increased demand and limited physical expansion, which is expected to continue for the foreseeable future, forces many components of the grid to operate at or near their secure operating limits. Due to the economic reasons and uncertainties in the forecast of loads, the power supply reliability level does not attain 100 percent. The building of new EHV tie lines has resulted in further propagation of the effect of disturbances. The growth of interconnected systems also demands a high degree of security for normal operation. Consequently, the burden of the system operators has increased tremendously in their effort to ensure that all the customers must be satisfied with good quality of electric power supply at all the time. Therefore, it becomes a necessity to develop methods for effective control and operation of power system.

1.2 POWER SYSTEM SECURITY

The security of a power system is measured by the ability of the system to withstand contingency cases without violating normal operating conditions. The reliable way of testing the contingency case on a power system is to simulate the situation by a power flow solution. The power flow
in a network is strictly governed by the power balance equations. The power flow pattern depends mainly on the load, generation distributions and the network configuration. The amount of power generated by each unit is constrained by its capacity, the thermal rating of each line, its power flow limit, power handled by each transformer and voltage levels. In order to achieve the system security, all the above conditions may be expressed in the form of a set of equality and inequality constraints.

When all the equality and inequality constraints are satisfied, the system is said to be in the normal operating state. Under such conditions all the power system components work securely within boundary limits. But in practice, it is not sufficient just to maintain a power system in normal operating state. Disturbances such as outages of any equipment in the system or sudden increase / decrease of the load may cause the system to go to an undesirable emergency. Therefore, there is a pressing need for power system security. A set of probable disturbances (contingencies) is first specified. Supposing that a power system in the normal operating state is subjected to a set of disturbances, one at a time for every single disturbance, the system remains in the normal operating state, then the system is said to be secure otherwise it is insecure.

It is apparent that the larger the set of disturbances, more stringent is the security standard. The members of the set of disturbances will depend on the system considered and the standard of the security required. It is said that the secure normal operating state as a preferred state and the insecure normal operating state as an alert state. A power system should be maintained at the preferred state as long as possible. When the system goes into an alert state, control action should be taken to bring it to the preferred state. Such controls constitute the security controls.
The traditional regulated and monopoly structure of power industry throughout the world is eroding into an open-access and competitive environment. Due to less regulation in power flow pattern and more intensive use of available transmission facilities, power systems tend to operate closer to security boundaries. This is an increasing concern about security / stability problems in power system planning and operation.

In practice, designing the system to meet this criterion is somewhat conservative and costly. As the system becomes deregulated, power companies become more and more cost conscious. They are also driven to solutions where the Flexible AC Transmission Systems (FACTS) devices such as Static Var Compensator (SVC), Thyristor Controlled Series Compensators (TCSC) and Unified Power Flow Controller (UPFC) offer an alternative means to mitigate the overloads and enhance the system security.

Hence, the security assessment must be made periodically to maintain the reliability of a power system. The real time numerical data are to be effectively handled in the algorithms in order to get instantaneous results for maintaining good degree of reliability. The result provided by the algorithms must be crisp and not voluminous to the system operators for implementation. Further, the result should give appropriate guidance to the operator to take corrective or preventive action.

1.3 COMPUTATIONAL INTELLIGENT METHODS

In this thesis, Neural Network, Wavelet Transform Based Neural Network (WTNN), Wavelet Transform Based Particle Swarm Optimization Neural Network (WTPSONN) and Adaptive Neuro Fuzzy Inference System (ANFIS) techniques are used for solving power system security assessment problems. The Neural Network and the ANFIS represent broad classes of
“Machine-intelligent” Adaptive systems. The Neural Network and the ANFIS estimate input-output functions. Both are trainable dynamical systems and hence most suitable for on-line power system security assessment. They are model-free estimators and they learn from experience with numerical data. The Neural Network and the ANFIS encode the sampled information in a parallel distributed framework. Both frameworks are numerical. Neural Network and ANFIS are used to store, recognize and associatively retrieve patterns or database entries.

The Neural Network has the property of recognition without definition. Recognition without definition characterizes much intelligent behavior. It enables the system to generalize. In this work, Wavelet Transform is used for preprocessing the inputs and Particle Swarm Optimization (PSO) algorithm is used to get the optimized weights during training of Neural Network.

1.4 EVOLUTIONARY COMPUTATIONAL METHODS

In this work, Evolutionary Algorithms (EAs) such as Genetic Algorithm (GA), Differential Evolution (DE) and Particle Swarm Optimization (PSO) techniques are used for solving power system security enhancement problems by making use of one of the most promising applications of the family of power electronics devices called Flexible AC Transmission System devices (FACTS). The selection of suitable location of FACTS devices under normal and network contingencies is determined based on the degree of severity of the contingencies. The optimizations are performed on three parameters namely, the location of the device, settings and severity of overloading by considering TCSC device using Evolutionary Algorithms. The optimization performed on four parameters namely, the location of the devices, their types, their settings and cost of installation by
considering multi type FACTS Devices using Particle Swarm Optimization technique.

1.5 CONCLUSION

Thus, it is the time to use intelligent and evolutionary computational methods for solving power system security assessment/enhancement problems. The pattern of vector representing the power system variables related to the security are ranked according to the severity index by using Neural Network and ANFIS. The contingency ranking is made based on the performance indices namely, real power margin index, line overload index and voltage stability index using Neural Network, Wavelet Transform Based Neural Network, Wavelet Transform Based Particle Swarm Optimization Neural Network and Adaptive Neuro Fuzzy Inference System. The results of the systems considered are presented for various load conditions and transmission line outages. Real coded Genetic Algorithm, Differential Evolution and Particle Swarm Optimization techniques are also proposed in this work for solving security enhancement problems based on network contingencies.

The results show that the proposed methods are the good candidates and substitutes for the conventional methods in solving security assessment / enhancement problems.

This thesis has 8 chapters including introduction and conclusion. The detailed literature survey made in the area of power system security assessment / enhancement is presented in chapter 2. The recent techniques, Neural Networks, Adaptive Neuro Fuzzy Inference System, Wavelet Transform, Genetic Algorithm, Differential Evolution and Particle Swarm
Optimization used in this work for solving security assessment / enhancement problems are discussed in chapter 3.

Chapter 4 describes the formulation of contingency screening and ranking problem, implementation of the proposed algorithm using Wavelet Transform Based Neural Network and Wavelet Transform Based Particle Swarm Optimization Neural Network. Chapter 5 depicts performance indices for power system security assessment problem using Artificial Neural Network and Adaptive Neuro Fuzzy Inference System. The power system security enhancement problem solved by using Real Coded Genetic Algorithm, Differential Evolution and Particle Swarm Optimization based on the concept of (N-1) contingencies is covered in chapter 6. Chapter 7 deals the power system security enhancement problem solved by using Particle Swarm Optimization based on the concept of (N-1) and (N-2) contingencies. Chapter 8 is concluded by verifying the results obtained by the proposed approaches. The methods experimented in this work are quit suitable for solving power system security assessment / enhancement problems. They also eliminate the rigorous modeling and analysis as required in conventional approach. Appendices are intended to represent the data of the test systems used in this work.