Decision Tree Approach to Dynamic Security Assessment

A Project Report

Submitted by

V.V.Nikhil (EE09B091)

in partial fulfillment of the requirements

for the award of the degree of

BACHELOR OF TECHNOLOGY

AND

MASTER OF TECHNOLOGY

DEPARTMENT OF ELECTRICAL ENGINEERING

INDIAN INSTITUTE OF TECHNOLOGY MADRAS

MAY 2014

CERTIFICATE

This is to certify that the project entitled "**Decision Tree Approach to Dynamic Security Assessment**" submitted by **Mr. V.V.Nikhil (EE09B091)** is a bonafide record of work carried out by him in partial fulfillment for the award of dual degree of **Bachelor of Technology** in **Electrical Engineering** and **Master of Technology** in **Power Systems and Power Electronics**. The contents of this report, in full or in parts, have not been submitted and will not be submitted to any other Institute or University for the award of any degree or diploma.

Dr. K. SHANTI SWARUP

Professor

Department of Electrical Engineering

Indian Institute of Technology Madras

Chennai – 600036

Date:

ACKNOWLEDGEMENT

I wish to express my deep sense of gratitude and indebtedness to my project guide, Dr. K. S. Swarup, Professor in Department of Electrical Engineering, for his most valuable guidance, discussions, suggestions and encouragement, from the conception to the completion of this project. His moral support, unreserved co-operation and generosity, which enabled me to complete the work successfully, will be everlasting in my memory.

I would also like to thank the maker of the open source softwares MATPOWER, MATDYN and WEKA which helped me perform various tasks during the course of my project.

I would also like to thank my professors and friends from my undergraduate studies while at Indian Institute of Technology, Madras. The preparation and experience I gained were invaluable.

ABSTRACT

Electric power is becoming one of the most important resources in the modern world. Since most of this electric power is supplied by the transmission and distribution system, nowadays more attention is paid on the security of the power system. All over the world, there are some trends to introduce the deregulated power system into the power system operation, and to increase the stability of electric power supply. As a result, making accurate predictions for the power system operating conditions is an important task for the current power system research. The research mainly interests in checking if the operating conditions are acceptable after contingencies.

Dynamic Security Assessment (DSA) is proposed and studied under such context. Historically, various numerical, methods have been adopted for carrying out DSA. These are time consuming and computationally intensive. So faster and easily computable methods for Security Assessment are the need of the hour. With the advances in technology, several new methods which are more effective than the earlier adopted methods have been developed. One of them is the use of Decision Trees (DTs) for Dynamic Security Assessment. The real time system data can be obtained which helps in identifying current system operating condition and hence used it in predicting whether the system is dynamically secure or not.

Key words: power system security, dynamic security assessment, decision tree

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

CA	Classification Accuracy
DAE	Differential Algebraic Equations
DSA	Dynamic Security Assessment
DSD	Dynamic Security Database
DT	Decision Tree
IS	Intelligent System
LS	Learning Set
MC	Misclassification of Class
MVA	Mega Volt Ampere
MW	Mega Watt
OC	Operating Condition
OP	Operating Point
PMU	Phasor Measurement Unit
SCADA	Supervisory Control And Data Acquisition
SSA	Static Security Assessment
TDS	Time Domain Simulation

TEF	Transient Energy Function
TS	Testing Set
TSA	Transient Security Assessment

1 INTRODUCTION

1.1 Project Motivation

The 2012 blackouts which affected 22 Indian states has indicated that the operation and control of the power system needs to be improved. Even though the operators have access to a huge amount of data, they were not able to take the proper actions in time to prevent the blackouts. Motivated by this harsh reality, this thesis is focused on empowering the operators by helping them take decisions easily by predicting the security of the power system. Instead of using a model of the power system to estimate the state, measured variables are used as input data to the algorithm. The algorithm classifies secure from insecure states of the power system using the measured variables directly. The algorithm is trained beforehand with data from a model of the power system.

This thesis uses Decision Trees to determine to classify the whether the power system can withstand the (n-1) contingencies during variety of operation conditions. The decision tree once generated can be deployed online and used to predict when the system is going into an insecure state, thus helping the operators at any early stage and enable them to take proper evasive actions.

1.2 Objective and Scope of Project

The objective of the project is to develop an efficient method to perform DSA. In this project, the (n-1) contingencies of a variety of operating conditions are simulated and using the status of the system during these contingencies and operating conditions, a decision tree is built. This is used to classify the given system. I have tested the method developed on the WSCC 9 bus system. The scope of the present work is limited to dynamic security assessment and classification. The list of credible contingencies used for the simulation study in the present work includes only the increase in load demand and single line outages.

1.3 Thesis Structure

Chapter 2 introduces the aspect of power system security. It will help to answer questions like what is power system security, how it is different from stability.

Chapter 3 discusses about the different types of security and how to differentiate between them. It will also introduce the historical methods used to perform dynamic security assessment.

Chapter 4 gives an introduction to Decision Trees. In this chapter, decision trees as predictive tool will be discussed and illustrated with a generic example.

Chapter 5 discusses about the proposed scheme where decision trees are used as classifiers for dynamic security assessment.

Chapter 6 will explain the case study solved using the proposed scheme and present the results obtained from the simulations performed.

2 POWER SYSTEM SECURITY

Power system is one of the most complex artificial systems in the world. Its responsibility is to maintain a secure and economical process of electricity generation, transmission, and distribution. This chapter introduces the basic concepts of power system security.

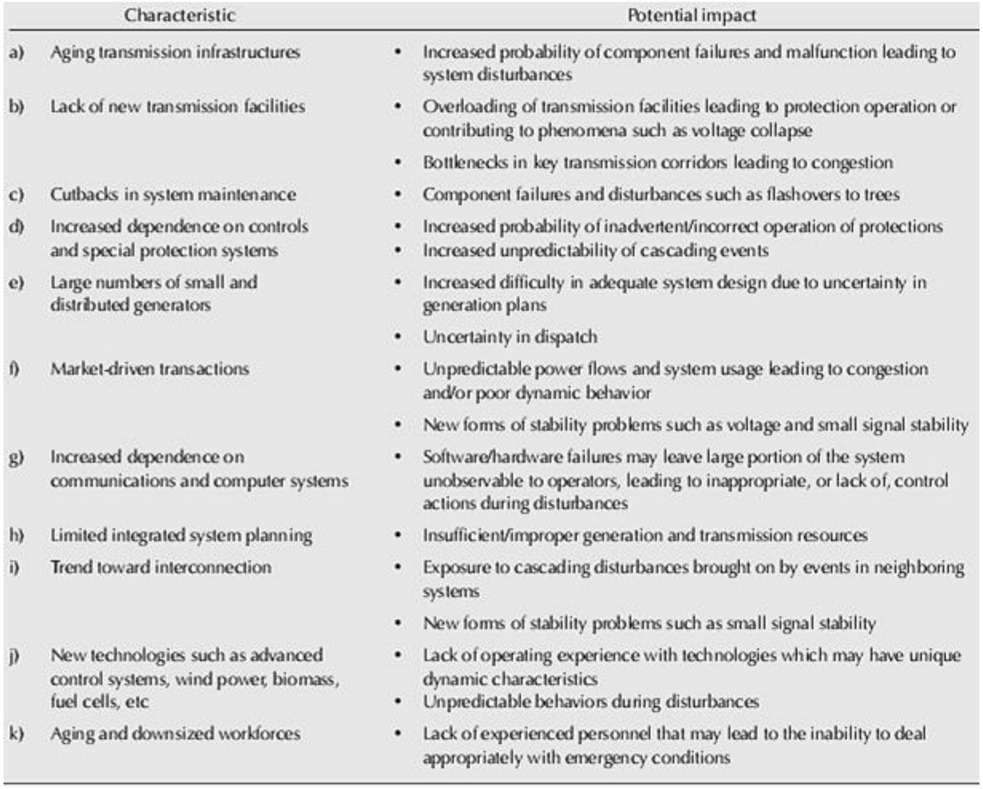
2.1 Power System Security

According to the IEEE, Power System Security is defined as the degree of risk in its ability to survive imminent disturbances (contingencies) without interruption of customer service. It relates to robustness of the system to imminent disturbances and, hence, depends on the system operating condition as well as the contingent probability of disturbances [1]. Power system security is usually assessed on the basis of security standards, i.e., the relationship between outages of generation and transmission plant and the level of any acceptable loss of demand. An ‘N-1’ security standard requires the system to work satisfactorily following loss of any one of its N elements.

During the times of regulated and vertically integrated power systems, systems tended to be more secure for a number of reasons. First, as the grids were designed, built, and operated by the government, integrated planning ensured that generation and transmission facilities kept pace with the load growth, thereby limiting overloading and equipment failures that could lead to system disturbances. Maintenance programs were also, in general, rigorous. From an operations perspective, forecasting system conditions was simpler because there were fewer generation and transmission owners and they were operating in a carefully planned and cooperative manner. As a result, systems were exposed to fewer potential disturbances, were more robust in their responses to disturbances that did occur, and were more predictable in their patterns of operation.

However, the evolution of the electric power industry toward open markets over the last decade has introduced a number of factors that have increased the possible sources for system disturbances, reduced the robust-ness of systems, and reduced the predictability of operation. Some of these factors are described in Table 1.1.

Table 1.1 Factors affecting Power System Security



	Characteristic	Potential impact
a)	Aging transmission infrastructures	• Increased probability of component failures and malfunction leading to system disturbances
b)	Lack of new transmission facilities	• Overloading of transmission facilities leading to protection operation or contributing to phenomena such as voltage collapse • Bottlenecks in key transmission corridors leading to congestion
c)	Cutbacks in system maintenance	• Component failures and disturbances such as flashovers to trees
d)	Increased dependence on controls and special protection systems	• Increased probability of inadvertent/incorrect operation of protections • Increased unpredictability of cascading events
e)	Large numbers of small and distributed generators	• Increased difficulty in adequate system design due to uncertainty in generation plans • Uncertainty in dispatch
f)	Market-driven transactions	• Unpredictable power flows and system usage leading to congestion and/or poor dynamic behavior • New forms of stability problems such as voltage and small signal stability
g)	Increased dependence on communications and computer systems	• Software/hardware failures may leave large portion of the system unobservable to operators, leading to inappropriate, or lack of, control actions during disturbances
h)	Limited integrated system planning	• Insufficient/improper generation and transmission resources
i)	Trend toward interconnection	• Exposure to cascading disturbances brought on by events in neighboring systems • New forms of stability problems such as small signal stability
j)	New technologies such as advanced control systems, wind power, biomass, fuel cells, etc	• Lack of operating experience with technologies which may have unique dynamic characteristics • Unpredictable behaviors during disturbances
k)	Aging and downsized workforces	• Lack of experienced personnel that may lead to the inability to deal appropriately with emergency conditions

Contingencies may be external or internal events (for instance, faults subsequent to lightning versus operator-initiated switching sequences) and may consist of small/slow or large/fast disturbances (for example, random behaviour of the demand pattern versus generator or line tripping). Usually, numerical simulation of the contingency scenario is used to assess the effect of a contingency on a power system in a given state. However, the non-linear nature of the physical phenomena and the growing complexity of real-life power systems make security assessment difficult. For example, monitoring a power system every day calls for fast sensitivity analysis to identify the salient parameters driving the phenomena, and suggestions on how to act on the system so as to increase its level of security.

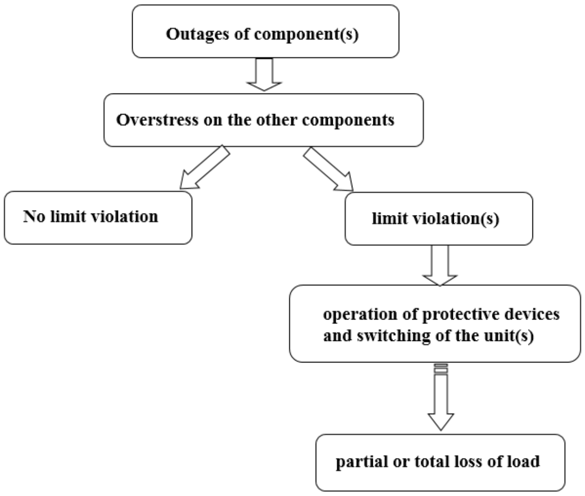

Outages of component(s)
Overstress on the other components
No limit violation
limit violation(s)
operation of protective devices and switching of the unit(s)
partial or total loss of load

Figure 2.1 Power System Security

Reliability of a power system refers to the probability of its satisfactory operation over the long run. It denotes the ability to supply adequate electric service on a nearly continuous basis, with few interruptions over an extended time period [1]. Power system stability is the ability of an electric power system, for a given initial operating condition, to regain a state of operating equilibrium after being subjected to a physical disturbance, with most system variables bounded so that practically the entire system remains intact.

Reliability is the overall objective in power system design and operation. To be reliable, the power system must be secure most of the time. To be secure, the system must be stable but must also be secure against other contingencies that would not be classified as stability problems e.g., damage to equipment such as an explosive failure of a cable, fall of transmission towers due to ice loading or sabotage. As well, a system may be stable following a contingency, yet insecure due to post-fault system conditions resulting in equipment overloads or voltage violations.

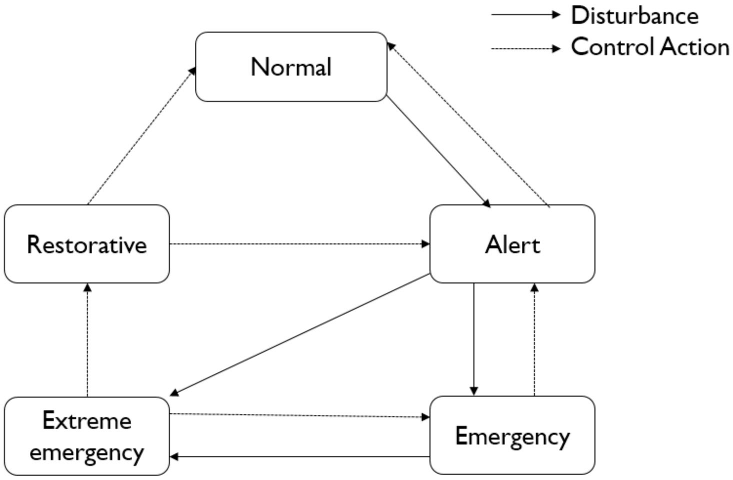


Figure 2.2 Power System Operational States

Figure 2.2 depicts the operational states of a power system and the ways in which transition can occur from one state to another. The operation of a power system is usually in a normal state. Voltages and the frequency of the system are within the normal range and no equipment is overloaded in this state. The system can also maintain stability during disturbances considered in the power system planning. The security of the power system is described by Thermal, voltage and stability limits. The system can also withstand any single contingency without violating any of the limits. The system transits into the emergency state if a disturbance occurs when the system is in the alert state. Many system variables are out of normal range or equipment loading exceeds short-term ratings in this state. The system is still complete. Emergency control actions, more powerful than the control actions related to alert state, can restore the system to alert state. The emergency control actions include fault clearing, excitation control, fast valving, generation tripping, generation run back-up, HVDC modulation, load curtailment, blocking of on-load tap changer of distribution system transformers and rescheduling of line flows at critical lines. The extreme emergency state is a result of the occurrence of an extreme disturbance or action of incorrect of ineffective emergency control actions. The power system is in a state where cascading outages and shutdown of a major part of power system might happen. The system is in unstable state. The control actions needed in this state must be really powerful. Usually load shedding of the most unimportant loads and separation of the system into small independent parts are required.

Every small change in load is a disturbance that causes a change in system conditions. However, system security is assessed for larger changes that cause major changes in system conditions. These changes are mainly caused by contingencies. Most commonly contingencies result in relay operations that are designed to protect the system from faults or abnormal conditions. Typical relay operations result in the loss of a line, transformer, generator, or major load.

Various components in a power system respond to changes that occur and may reach an equilibrium condition that is acceptable according to some criteria. Mathematical analysis of these responses and the new equilibrium condition is called security analysis.

The decision drivers of security can be classified and the corresponding time frames for making security related decision are given in Table 1.2.

Table 1.2 Security Related Decisions

Time Frame	**Decision Maker**	**Decision**	**Basis for Decision**
On-line Assessment (Minutes to hours)	Operator	How to constrain the economic operation to maintain the normal state?	Operating rules, online assessment, and cost
Operational Planning (Hours to months)	Analyst	What should be the operating rules?	Minimum operating criteria, reliability and cost
Planning (Months to years)	Analyst	How to reinforce/maintain the transmission system?	Reliability criteria for system design and cost.

2.2 On-Line Security Analysis

There are three basic elements of on-line security analysis and control, namely, monitoring, assessment and control. They are tied together in the following framework:

Step 1: *Security Monitoring:* Using real-time system measurements, identify whether the system is in the normal state or not. If the system is in an emergency state, go to step 4. If load has been lost, go to step 5.

Step 2: *Security Assessment:* If the system is in the normal state, determine whether the system is secure or insecure with respect to a set of next contingencies.

Step 3: *Security Enhancement:* If insecure, i.e., there is at least one contingency which can cause an emergency, determine what action should be taken to make the system secure through preventive actions.

Step 4: *Emergency Control:* Execute proper corrective action to bring the system back to the normal state following a contingency which causes the system to enter an emergency state. This is sometimes called remedial action.

Step 5: *Restorative Control:* Restore service to system loads.

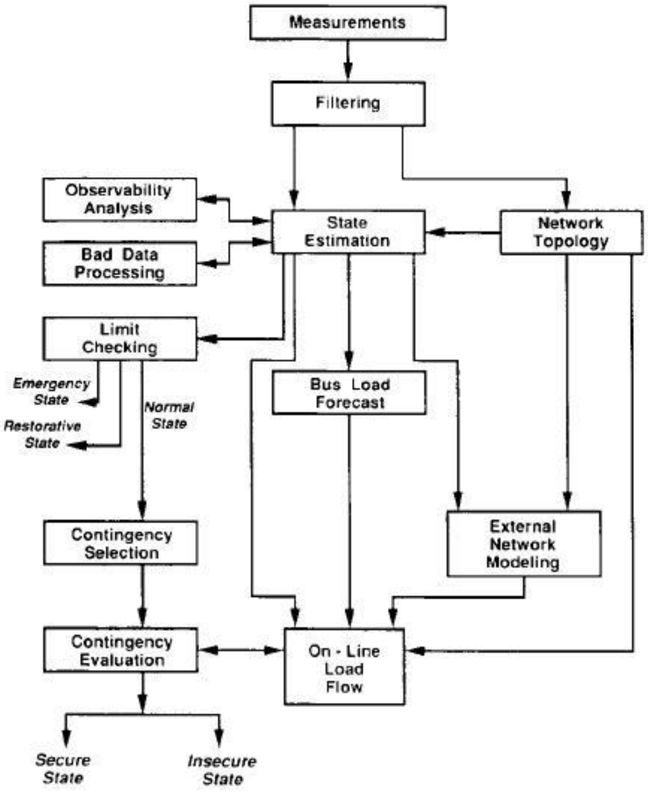


Figure 2.3 Major components of on-line security analysis [2]

The major components of On-Line Security Analysis are shown in Figure 2.3. The monitoring component starts with the real-time measurements of physical quantities such as line power flows, line current flows, power injections, and bus voltage magnitudes. The measurement data are transferred from various locations to the control center. The data received is then filtered through a simple check of reasonability and consistency. The remaining data are first systematically processed to determine the network topology. Then the available data are further processed to obtain an estimate of the system state variables (bus voltage magnitudes and phase angles for normal steady-state). State estimation is a mathematical procedure for computing the “best” estimate of the state variables of the power system based on the available data, which are in general corrupted with errors.

A set of contingencies is needed to assess whether a normal operating state is secure or not. A set of important and plausible disturbances is created. Security assessment currently involves primarily steady-state load flow analysis. Stability constraints are expressed in terms of the limits on line flows and bus voltages. Therefore, to assess the system response to contingencies, a contingency evaluation is carried out using the on-line load flows. The on-line load flow uses the actual load flow model from the state estimation solution together with a system representation of the unmonitored network and neighboring systems, i.e., an external network model. Because the contingencies are future events, a bus load forecast is needed. Certain implementations of the state estimator render the external model observable by strategic placement of pseudo-measurements. Then the state estimate is performed on the entire model in one step.

3 DYNAMIC SECURITY ASSESSMENT

3.1 Types of Security Assessment

If the analysis evaluates only the expected post disturbance equilibrium condition (steady-state operating point), then it is called Static Security Assessment (SSA). Static or steady state security is the ability of the system to supply load without violating operating conditions following a contingency. Conventionally, SSA is performed by analytically modeling the network and solving the algebraic load flow equations repeatedly for all prescribed outages, one at a time.

If the analysis is used for determining whether the system oscillations, following a fault, result in loss of synchronization among the system generators, then it is called Transient Security Assessment (TSA). It pertains to the rotor angle stability of the system. Transient energy is the excess energy possessed by the system at the instant of fault clearing that must be absorbed by the network for stability to be maintained. Critical energy indicates the maximum capacity of system to absorb the accumulated energy during disturbance. The Transient Energy Function (TEF) based method is adopted to determine the transient security level of a power system.

Dynamic Security Assessment (DSA) has been formally defined by the IEEE, Power Engineering Society (PES) working group on DSA as an evaluation of the ability of a certain power system to withstand a defined set of contingencies and to survive the transition to an acceptable steady state condition. In other words, it is the ability of the system to withstand all the contingencies, maintaining synchronism for a long duration after the system is found to be transiently secure.

SSA can be used quickly to determine if a system is insecure by simply looking at the static outcome of each contingency. However, to know whether the system is fully secured, DSA must be performed. It determines if the associated dynamics of each contingency are acceptable.

Security Assessment approaches can be classified either as deterministic or probabilistic. Deterministic methods provide very simple rules to make decisions. These methods, however are expensive and hence researchers are looking at techniques which indicate whether the system is secure which are also economically viable.

3.2 Conventional Methods for Dynamic Security Assessment

Mathematically, a dynamic security problem can be expressed as a large set of Differential Algebraic Equations (DAEs), which are difficult to be solved analytically. Conventional methods for DSA are mainly based on Time Domain Simulation (TDS) techniques. In TDS techniques, the system dynamic trajectories are simulated by solving the DAEs using step-by-step integrations. The major advantages of TDS include [3]:

- Provide essential information about relevant parameters of system dynamic evolution with time
- Consider any power system modeling and stability scenario

- Reach the required accuracy, provided that the modeling of a power system is correctly designed and its parameters accurately known.

However there are also a couple of shortcomings of adopting this method:

- This is a computation intensive method as it may require to solve several thousands of differential and algebraic equations for a simulation time of 10-20 seconds while deployed in a power station. Besides the number of contingencies to be considered will also be huge.
- The TDS can only provide the system dynamic trajectories and offer very limited information about system security characteristics. Hence, for dynamic security assessment (DSA) aspect, it can only give a binary answer about secure or insecure; for dynamic security control (DSC) aspect, the computation process is usually not transparent and interpretable.

This method, being very time consuming, is generally used only in off-line applications. The process consists of conducting TDS on forecasted operating conditions and disturbances and heuristically finding a secure operating condition in a trial-and-error way. In on-line operating phase, the analysis results are used by operators in a look-up pattern.

3.3 Advances in Dynamic Security Assessment

The direct methods for DSA were quite sufficient in a period when the power system was simpler. Since the 1900s, the power system undergone some drastic changes like increased integration of renewable energy and more recently, the evolving smart grids. These changes have improved the efficiency of the system, both economically and environmentally, but at the same time complicated the system operating conditions, making the conventional off-line approaches become inadequate and non-economical.

With increased renewable energy (especially wind and solar) connection, the system becomes further more unpredictable due to the inherent uncertainties of these energies. Off-line methods thereby become inapplicable to capture realistic operating conditions in the highly uncertain environment. As a consequence, there is an unprecedented need for real-time dynamic security analysis tools, which are able to monitor and evaluate the dynamic security conditions of the power system in a continuous and on-line real-time environment, and provide timely and economical security control solutions whenever necessary.

As modern power system is increasingly large, resulting into a growing larger database, there is a pressing demand for more computationally efficient and high-accuracy DSA models that can allow more effective real-time implementation and on-line updating. The advent of Intelligent System (IS) technologies provides an alternative and promising methodology for much faster and information-rich dynamic security analysis. The Intelligent System is built beforehand off-line and when applied on-line, the computation time for obtaining the system stability information is dramatically reduced by eliminating the needs for calculating the DAEs.

Unlike analytical methods, which are based on solving the DAEs, an Intelligent System can capture the relationship between power system operating states and the dynamic security status, by generating a pattern from the dynamic security database (DSD). Once identified, the System requires only the inputs to determine the corresponding dynamic security conditions. As soon as the input is fed, the DSA results can be given within very short delays, and the results can be utilized in real-time, combined with other extracted knowledge to decision support.

Typical Structure of the Intelligent System will be as shown in Figure 3.1

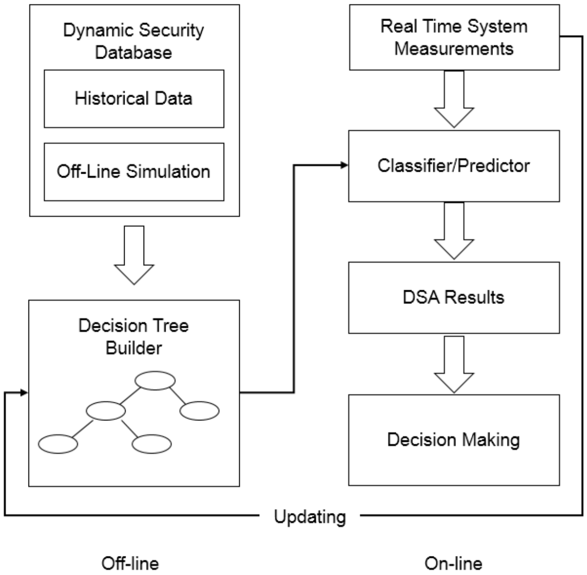


Figure 3.1 Structure of an Intelligent System

Compared with other methods, the Intelligent System is advantageous in the following aspects.

- Real-time security status should be evaluated for the system at the given instant or for some time in the immediate future. The Intelligent System requires only a split second to decide the status of the system and hence would give the operators much more response time to take necessary remedial actions.

- Intelligent System is constructed by learning from a database. It can discover and extract useful information on the system's dynamic security characteristics, which aids in better understanding of the power system and developing Dynamic Security Control strategies.
- Analytical methods strictly need accurate and full descriptions of power system, including power flow and system model parameters. However, this information can be faulty or even unavailable in real-time environment. In contrast, the Intelligent System requires only significant and/or available input parameters to perform DSA.
- Rather than exhaustively performing TDS on each pre-assumed scenario, the IS can, at the same time, handle a wide range of DSA cases, previously seen and unseen.

4 DECISION TREES

Decision tree is one of the inductive learning algorithms that generate a classification tree to classify the data. It is based on the "divide and conquer" strategy. The classification tree is made by recursive partitioning of the feature space, based on a training set. At each branching, a specific decision rule is implemented, which may involve one or more combinations of the attribute inputs or features [7].

4.1 Decision Tree Structure

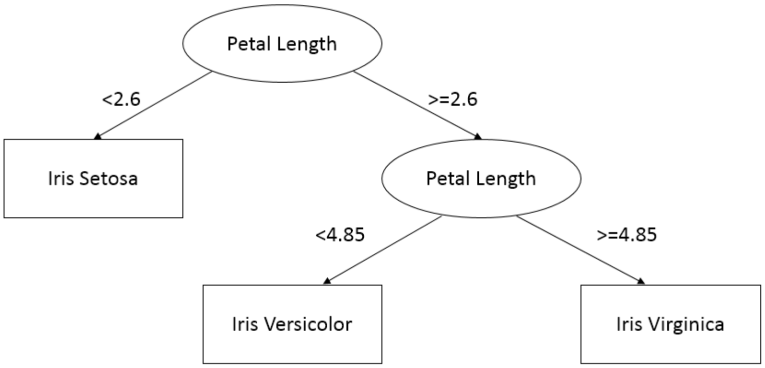


Figure 4.1 A sample Decision Tree

Figure 4.1 illustrates a simple decision tree using petal length as the input. A decision tree is composed of a root node, a set of interior nodes, and terminal nodes, called "leaves". The root node and interior nodes, referred to collectively as non-terminal nodes, are linked into decision stages. The terminal nodes represent final classification. The classification process i s implemented by a set of rules that determine the path to be followed, starting from the root node and ending at one terminal node, which represents the label for the object being classified. At each non-terminal node, a decision has to be taken about the path to the next node.

4.2 Working of a Decision Tree

A decision tree classifier is a hierarchical structure where at each level a test is applied to one or more attribute values that may have one of two outcomes. The outcome may be a leaf, which allocates a class, or a decision node, which specifies a further test on the attribute values and forms a branch or sub-tree of the tree. Classification is performed by moving down the tree until a leaf is reached. The method for constructing a decision tree as summarized by Quinlan [7] is as follows:

Step 1: Let T be the set of training instances.

Step 2: Choose an attribute that best differentiates the instances in T.

Step 3: Create a tree node whose value is the chosen attribute.

- Create child links from this node where each link represents a unique value for the chosen attribute.
- Use the child link values to further subdivide the instances into subclasses.

Step 4: For each subclass created in step 3:

- If the instances in the subclass satisfy predefined criteria or if the set of remaining attribute choices for this path is null, specify the classification for new instances following this decision path.
- If the subclass does not satisfy the criteria and there is at least one attribute to further subdivide the path of the tree, let T be the current set of subclass instances and return to step 2.

4.3 Types of Decision Tree Algorithms

There are many decision tree algorithms of which the notable ones are:

- ID3 (Iterative Dichotomiser 3)
- C4.5 (successor of ID3)
- CART (Classification And Regression Tree)
- CHAID (CHi-squared Automatic Interaction Detector)
- MARS (Multivariate Adaptive Regression Splines)

Most decision tree algorithms have the same basic structure: take the data, find a split based on an attribute that maximizes some purity measure, take the two halves of the data created by the split, and recurse until some stopping criteria is reached. Then prune back to reduce over-fitting. Decision tree classifiers differ in the ways they partition the training sample into subsets and thus form sub-trees. C4.5 induction algorithm uses information theory [8] to evaluate splits. CART uses Gini Index to split the training samples [9] and some methods use Chi -Square measure. Many studies have been done comparing C4.5 decision tree algorithm with other classifiers and found that C4.5 based on the Information theory is more accurate and gives reliable results [10] [11]. The other advantage of C4.5 algorithm is that it can convert decision tree into corresponding classification rules. Rules are more comprehensive, easy to understand and easy to implement. Hence, the C4.5 algorithm is used to develop the decision tree in this thesis.

4.3 Advantages of using Decision Trees

Amongst the other Intelligent System approaches, Decision Trees have advantages:

- **Simple to understand and interpret.** People are able to understand decision tree models after a brief explanation.
- **Requires little data preparation.** Other techniques often require data normalization, dummy variables need to be created and blank values to be removed.
- **Able to handle both numerical and categorical data.** Other techniques are usually specialized in analyzing datasets that have only one type of variable. (For example, relation rules can be used only with nominal variables while neural networks can be used only with numerical variables.)
- **Uses a white box model.** If a given situation is observable in a model the explanation for the condition is easily explained by boolean logic. (An example of a black box model is an artificial neural network since the explanation for the results is difficult to understand.

- **Possible to validate a model using statistical tests.** That makes it possible to account for the reliability of the model.
- **Robust.** Performs well even if its assumptions are somewhat violated by the true model from which the data were generated.
- **Performs well with large datasets.** Large amounts of data can be analysed using standard computing resources in reasonable time.

The attractive advantage of DT over other Intelligent System approaches is the ability to provide explicit classification rules, i.e. nodes and their thresholds and associated paths. With these rules, the stability assessment can be transparent and interpretable. Furthermore, the rules provide insight into critical system operating variables relating to stability, i.e. the variables shown at tree nodes. This is the primary reason for using Decision Trees ahead of the other techniques available to perform the predictive analytics.

5 DECISION TREE APPROACH TO DYNAMIC SECURITY ASSESSMENT

This thesis proposes an approach to online Dynamic Security Assessment Decision Trees. This scheme will enable the operator to get knowledge of the security level of the system as quickly as possible and in an efficient manner.

5.1 Proposed Scheme

The algorithm for the proposed scheme is shown in Figure 5.1. The proposed scheme is developed in three stages:

1. Firstly, operating conditions for the next 24 hours is forecasted. All the single line to ground faults are simulated at those operating conditions and stored in a database. This is called the Dynamic Security Database.
2. Using this database as the learning and the testing set, we build a Decision Tree. The Decision tree is used to identify the Critical Attributes (CAs) from the system parameters that characterize the system dynamic performance and evaluate the thresholds that result in insecurity. These CAs are the measurements which need to be made using the PMU or SCADA.
3. Around an hour before the online deployment, the Decision Tree is updated with the projected operating conditions, available after performing short term load forecasting and running the TDS on these new OCs. The real-time measurements available through the

Phasor Measurement Units (PMUs) or Supervisory Control and Data Acquisition (SCADA) units are then fed to the DT and the security level is found out.

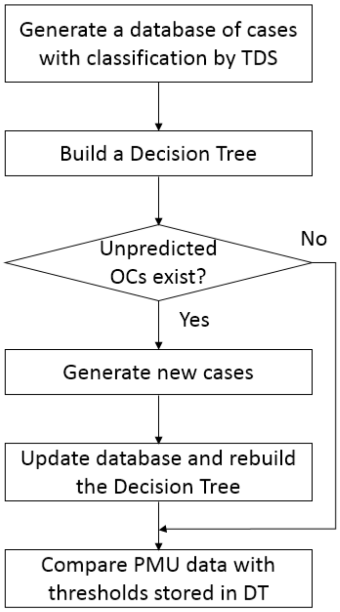

Generate a database of cases with classification by TDS
Build a Decision Tree
Unpredicted OCs exist?
No
Yes
Generate new cases
Update database and rebuild the Decision Tree
Compare PMU data with thresholds stored in DT

Figure 5.1 Proposed scheme involving Decision Trees for DSA

In previous attempts, potential insecurity was identified by simply observing these CAs using traditional SCADA-based data which is not synchronized across the system. The application of wide-area-based PMU measurements allows the synchronized monitoring of the CAs and their variation with changing system conditions. Most previous efforts make security predictions based on the security classes assigned to the terminal nodes. This is based on the assumption that the attributes and their thresholds decided by training data are always valid and accurate. However, if some unpredictable system conditions occur, the training data, and the CAs or thresholds may lack validity. As a result, the terminal nodes, which are sensitive to CAs and their thresholds, will also be unreliable.

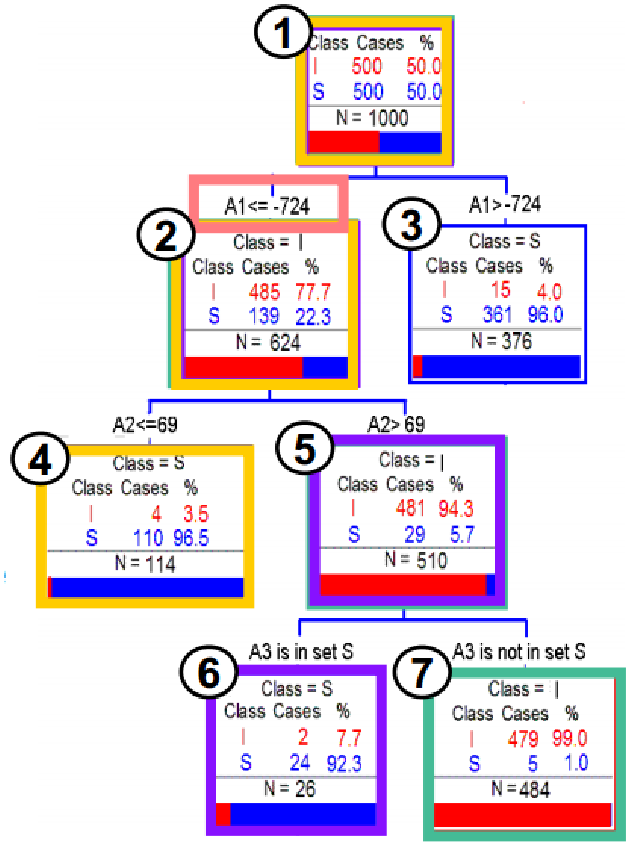


Figure 5.2 Sample Decision Tree for Dynamic Security Assessment

A sample decision tree is shown in Figure 5.2. The tree is trained by a DSD, which consists of 1000 instances each corresponds to an OP (defined by power system operational features) and the security labels subject to a contingency (denoted by “S” class for secure or “I” class for insecure). It shows the various decisions that are to be taken by the DT. At the first node, it checks whether A1 is greater than -724 or not. Based on the answer, it takes the branch to node 2 or node 3. If A1 is greater than -724, then the system is secure. Otherwise, a check if A2 is greater than 69 is made.

If A2 is lesser than or equal to 69, then the system is secure. If this condition isn't met, then a last check to see if A3 is present in set S or not is performed. If A3 is present in the set S, then the system is secure and insecure otherwise. The security assessment of an unknown OP consists of dropping its features (F1 and F2) down the tree from the root node, i.e. Node 1 at the topmost of the tree, until a terminal node is reached along a path. Such a classification procedure can be done very quickly, and thus it can be applied in on-line environment to enable earlier detection of the risk of insecurity.

6 CASE STUDY AND IMPLEMENTATION

The proposed method of decision tree approach to dynamic security assessment has been developed on the WSCC 9 bus system, under increased loading conditions in order to exhibit instances of instability caused by faults. The one-line diagram of the WSCC 9 bus system is shown in Figure 6.1.

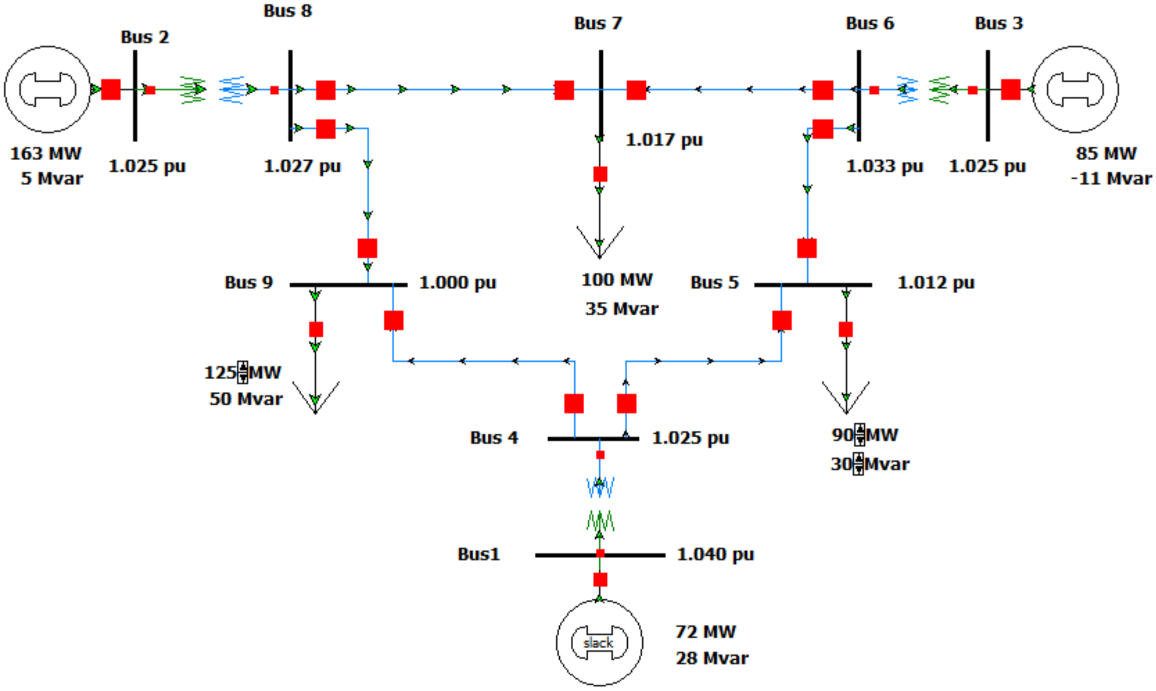


Figure 6.1 Simulation of the WSCC 9 bus system

The trees are constructed using a test set of 30 operating points obtained by varying the system's active load and generation from 50% to 200%, in steps of 5%, of base case and distributing among all buses in proportion to their respective base value. For each operating condition, the performance of the system during the (N-1) line to ground faults is evaluated. With the data generated, the Dynamic Security Database is built. The database is used for the decision tree building and verification and then deployed on on-line where we get real-time system information from the Measurement Units (either the PMU or SCADA) and using these measurements, classify the current operating state as secure or insecure using the Decision Tree.

Sample plots of the Time Domain Simulations are shown in Figures 6.2 to 6.6. The simulations are made for the case when the line between buses 5 and 6 suffers a balanced 3 phase fault at t=0.2s and the fault is removed at t=0.4s. Based on the TDS studies the security of the system is determined.

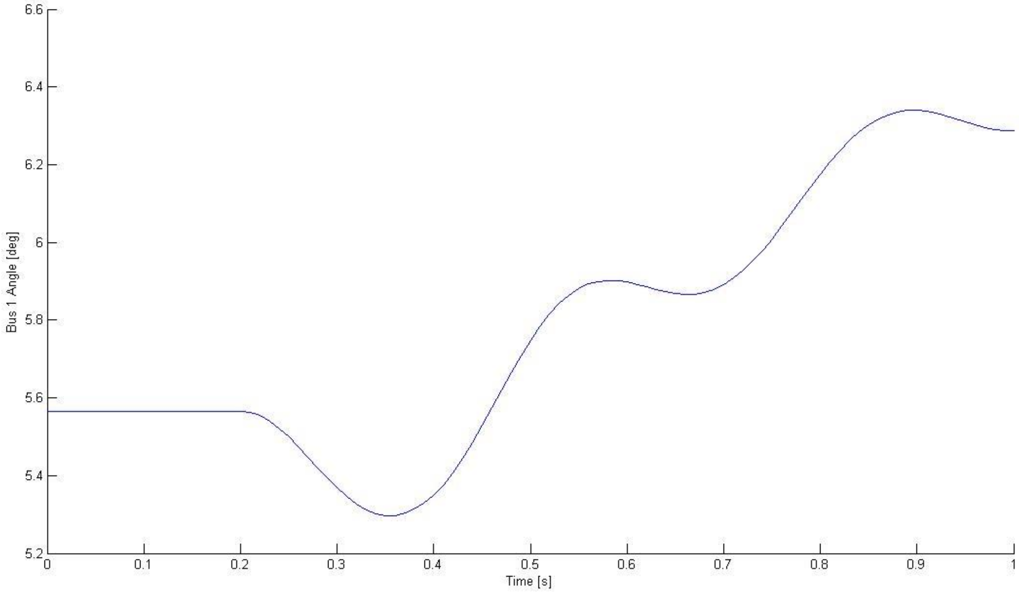


Figure 6.2 Plot of the phase angle of Bus 1 when a line fault occurs at t= 0.2s and is removed at t= 0.4s

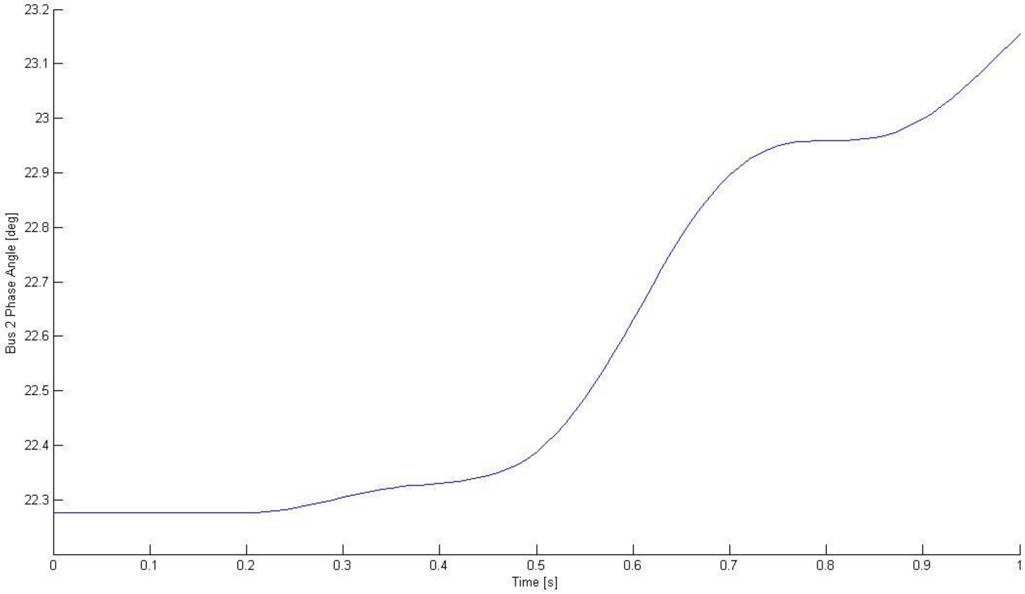


Figure 6.3 Plot of the phase angle of Bus 2 when a line fault occurs at t= 0.2s and is removed at t= 0.4s

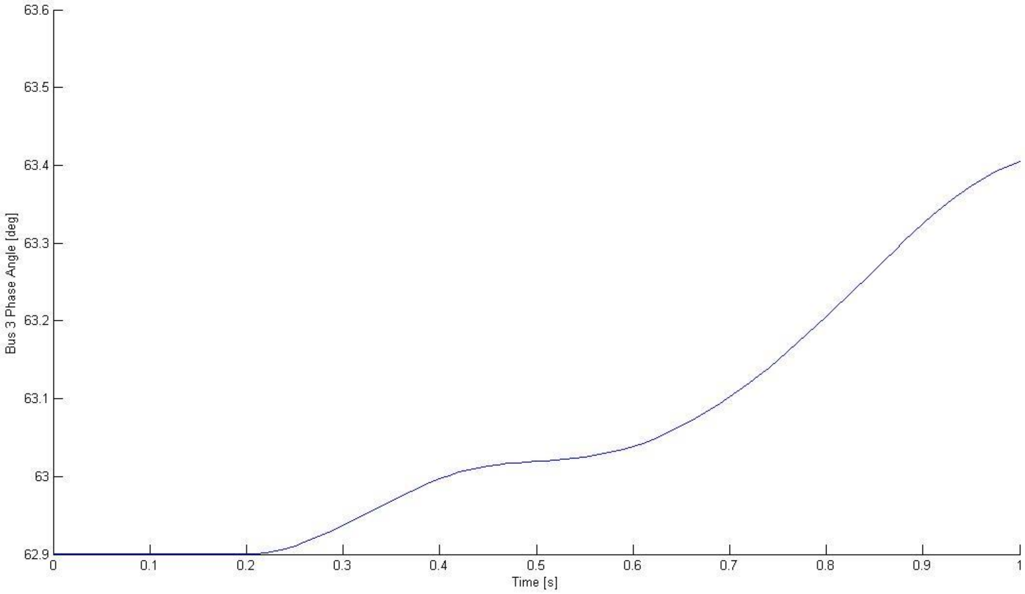


Figure 6.4 Plot of the phase angle of Bus 3 when a line fault occurs at t= 0.2s and is removed at t= 0.4s

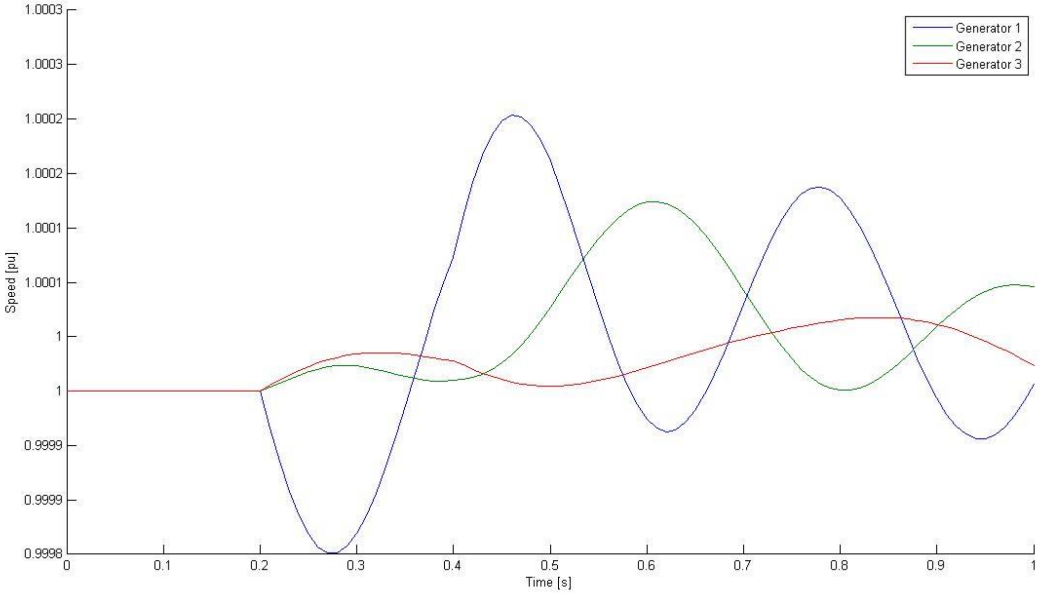


Figure 6.5 Plot of the generator speeds when a line fault occurs at t=0.2s and is removed at t=0.4s

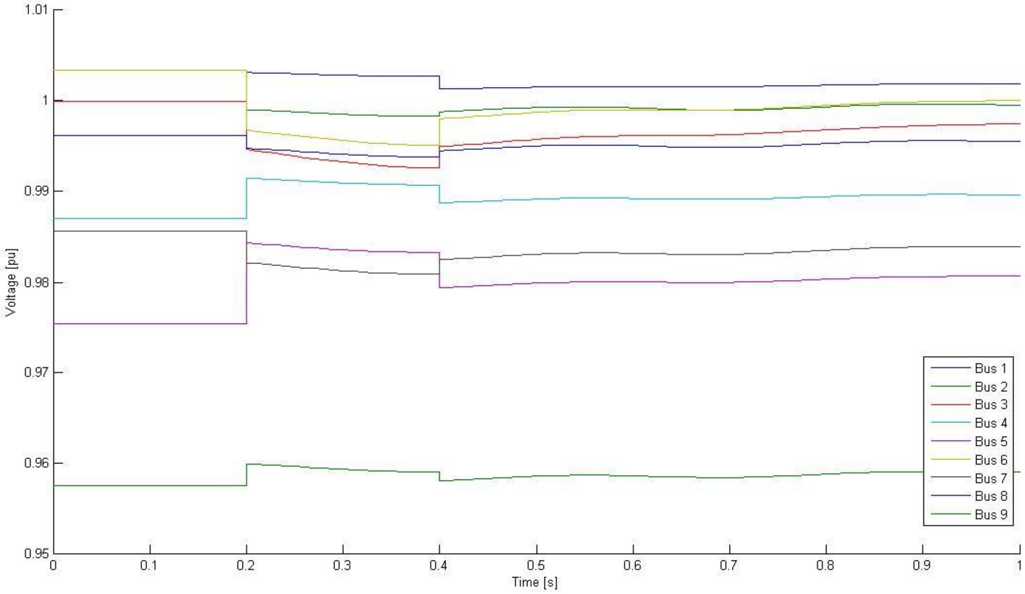


Figure 6.6 Plot of the bus voltages when a line fault occurs at t=0.2s and is removed at t=0.4s

The Classification Accuracy (CA) and the misclassification of a class (MC) are used as the performance measures for the decision tree.

$$CA\ (\%) = \frac{No.of\ samples\ classified\ correctly}{Total\ number\ of\ samples\ in\ data\ set} \times 100$$

$$MC_S\ (\%) = \frac{No.of\ misclassification\ in\ class\ "secure"}{Total\ number\ of\ samples\ belonging\ to\ class\ "secure"}$$

$$MC_I\ (\%) = \frac{No.of\ misclassification\ in\ class\ "insecure"}{Total\ number\ of\ samples\ belonging\ to\ class\ "insecure"}$$

The details about the cases considered and the splitting of the cases into Learning Set and the Testing set is shown in Table 6.1. We split the total of cases into a Learning Set, to be used for the creation of the DT and a Testing Set, to test the performance of the DT generated. We split the total set in the ratio 3:1, i.e 75% of the total cases are taken as Learning Set and the 25% of the cases are taken as the Testing Set.

Table 6.1 Data for building the DT for DSA

	Learning Set	Testing Set	Total
Cases belonging to class “secure”	91	31	122
Cases belonging to class “insecure”	227	75	302
Total Operating Cases	318	106	424

The resulting Decision Tree is shown in Figure 6.7. The Decision uses the Phase Angles and the voltages of each bus as well as the real and reactive power flows in each of the transmission lines as the attributes for the decision tree.

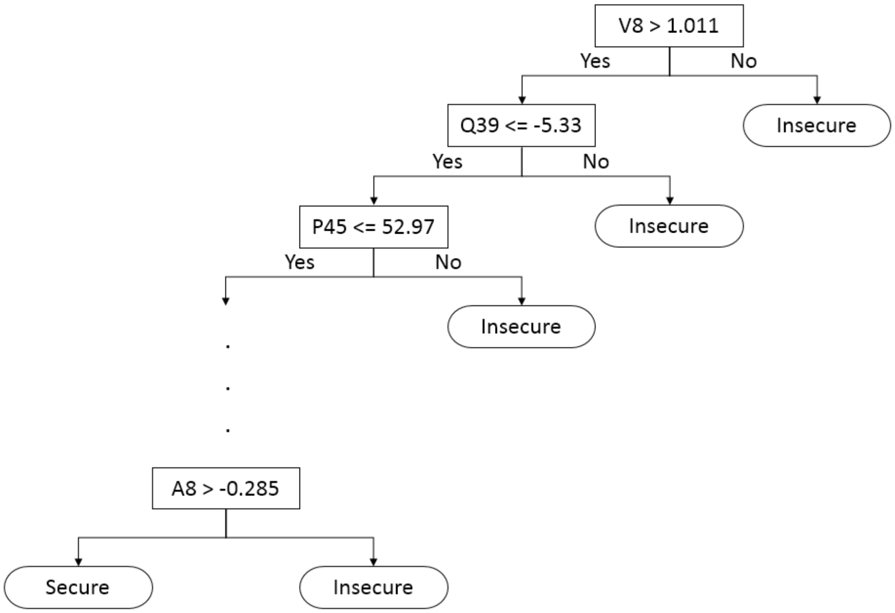


Figure 6.7 Decision Tree for Dynamic Security Assessment

Table 6.2 Performance of the DT

	Occurrences	Number of cases to be classified	Percentage
Classification Accuracy	82	106	77.36
Misclassification in class “secure”	11	31	35.38
Misclassification in class “insecure”	13	75	17.33

The classification results obtained are shown in Table 6.2. It can be observed from these results that the usage of Decision Tree to determine the security status of the system is fairly accurate. The security classification problem aims to minimize the misclassification in class “insecure”, as they indicate the wrong classification of insecure states, leading to a severe blackout. Thus the Decision tree model capable of predicting the security status of the system accurately and quickly is found suitable for on-line implementation. The real-time measurement of only selected features are used for the classification. Such an application will allow the operator to monitor the status of the system security from time to time, and take appropriate control actions, whenever needed.

7 CONCLUSIONS AND FUTURE WORK

Power system dynamic security analysis is an essential task for protecting power system against credible contingencies. Conventional methods for dynamic security assessment are mainly based on time-domain simulation techniques, which usually suffer from excessively high computational burden and inability to provide useful information about system dynamic security characteristics and guideline for control.

Using the decision trees, this research developed a series of alternative and more efficient algorithms and tools for real-time and information-rich DSA. The proposed method is able to infer stability control rules (for either single- or multi-contingency) from a strategically trained DT. The rules can be readily incorporated into a standard OPF model for on-line preventive control.

The proposed methods for DSA can be applied to other general classification and regression problems in power engineering. In particular, the proposed ensemble learning and decision-making rules for multiple ELMs are able to identify potentially inaccurate ensemble output, hence can be extended to predict confidence interval, which can then be applied to wind power forecasting and electricity price forecasting problems.

REFERENCES

1. Kundur, P.; Paserba, J.; Ajjarapu, V.; Andersson, G.; Bose, A.; Canizares, C.; Hatziargyriou, N.; Hill, D.; Stankovic, A.; Taylor, C.; Van Cutsem, T.; Vittal, V., "Definition and classification of power system stability IEEE/CIGRE joint task force on stability terms and definitions," *Power Systems, IEEE Transactions on* , vol.19, no.3, pp.1387,1401, Aug. 2004
2. Balu, N.; Bertram, T.; Bose, A.; Brandwajn, V.; Cauley, G.; Curtice, David; Fouad, A.; Fink, L.; Lauby, M.G.; Wollenberg, B.F.; Wrubel, Joseph N., "On-line power system security analysis," *Proceedings of the IEEE* , vol.80, no.2, pp.262,282, Feb 1992
3. Pavella, Mania, Damien Ernst, and Daniel Ruiz-Vega. *Transient stability of power systems: a unified approach to assessment and control*. Vol. 581. Springer, 2000.
4. Kundur, Prabha. *Power system stability and control*. Eds. Neal J. Balu, and Mark G. Lauby. Vol. 7. New York: McGraw-hill, 1994.
5. K. Sun, S. Likhate, V. Vittal, V. Kolluri, and S. Mandal, “An online dynamic security assessment scheme using phasor measurements and decision trees,” *IEEE Trans. Power Syst*., vol.22, no.4, pp. 1935-1943, Nov. 2007.
6. Wu, Xindong, et al. "Top 10 algorithms in data mining." *Knowledge and Information Systems* 14.1 (2008): 1-37.
7. Quinlan, John Ross. *C4. 5: programs for machine learning*. Vol. 1. Morgan kaufmann, 1993.
8. Shannon, Claude Elwood. "A mathematical theory of communication." *ACM SIGMOBILE Mobile Computing and Communications Review* 5.1 (2001): 3-55.

9. Breiman, Leo, et al. *Classification and regression trees*. CRC press, 1984.

10. Blackmore, K., and T. R. J. Bossomaier. "Comparison of See5 and J48. PART algorithms for missing persons profiling." *First International Conference On Information Technology & Applications (ICITA 2002)*. 2002.

11. German, G. W. H., G. West, and M. Gahegan. "Statistical and AI techniques in GIS classification: a comparison." *Proceedings of SIRC99-The 11th Annual Colloquium of the Spatial Information Research Centre*. 1999.

12. L. Wehenkel, "Machine Learning Approaches to Power System Security Assessment," IEEE Intelligent Systems Magazine, vol. 12, 1997, pp. 60-72.

13. http://en.wikipedia.org/wiki/Decision_tree_learning

APPENDIX A: WSCC 9 BUS SYSTEM DATA

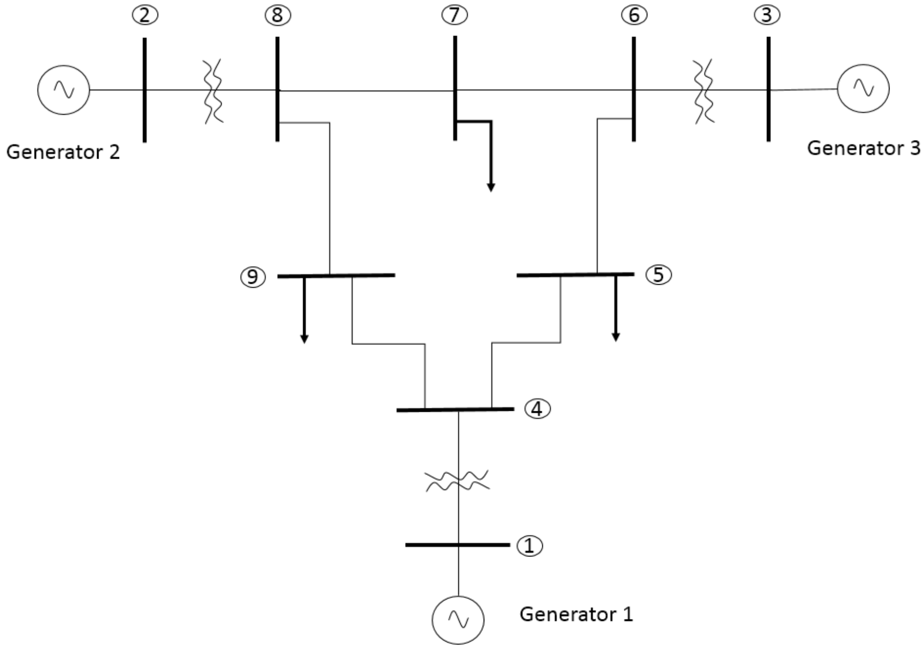


Figure A.1 WSCC 9 Bus System

A1 Bus Data

Table A.1 Bus Data for the WSCC 9 Bus System

Bus Number	**Bus Type**	**P_d**	**Q_d**	**G_s**	**B_s**	**V_m**	**V_a**	**Base KV**
1	Slack	0	0	0	0	1	0	345
2	PV	0	0	0	0	1	0	345
3	PV	0	0	0	0	1	0	345
4	PQ	0	0	0	0	1	0	345
5	PQ	90	30	0	0	1	0	345
6	PQ	0	0	0	0	1	0	345
7	PQ	100	35	0	0	1	0	345
8	PQ	0	0	0	0	1	0	345
9	PQ	125	50	0	0	1	0	345

A2 Generator Data

Table A.2 Generator Data for WSCC 9 Bus System

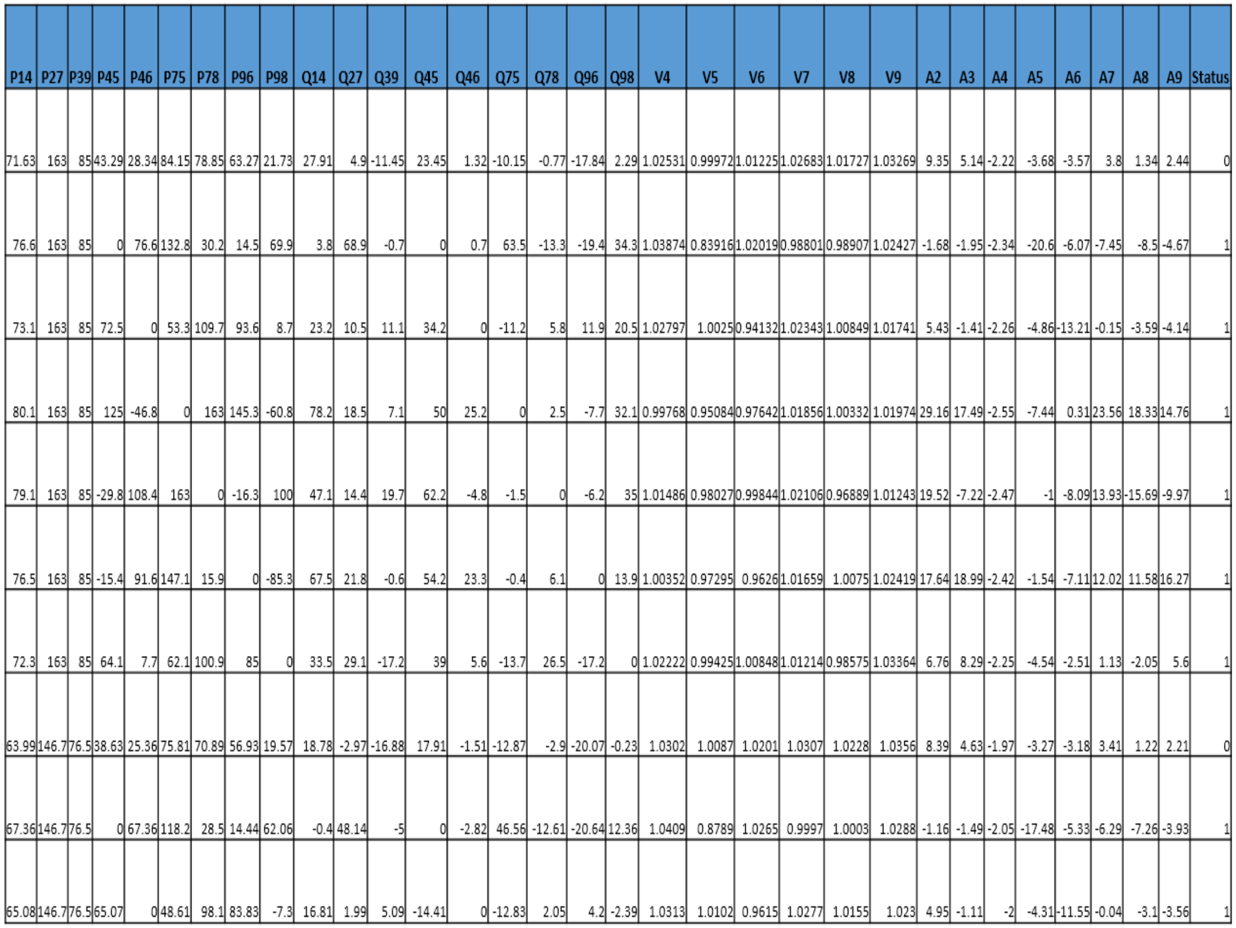
Bus Number	P_g	Q_g	P_{max}	P_{min}	Q_{max}	Q_{min}	V_g
1	0	0	250	10	300	-300	1
2	163	0	300	10	300	-300	1
3	85	0	270	10	300	-300	1

A3 Line Data

Table A.3 Line Data for WSCC 9 Bus System

From Bus	To Bus	Resistance (R)	Reactance (X)	Charging (B)
1	4	0	0.0576	0
4	5	0.017	0.092	0.158
5	6	0.039	0.17	0.358
3	6	0	0.0586	0
6	7	0.0119	0.1008	0.209
7	8	0.0085	0.072	0.149
8	2	0	0.0625	0
8	9	0.032	0.161	0.306
9	4	0.01	0.085	0.176

APPENDIX B: SAMPLE DATA FOR DYNAMIC SECURITY DATABASE



P14	P27	P39	P45	P46	P75	P78	P96	P98	Q14	Q27	Q39	Q45	Q46	Q75	Q78	Q96	Q98	V4	V5	V6	V7	V8	V9	A2	A3	A4	A5	A6	A7	A8	A9	Status
71.63	163	85	43.29	28.34	84.15	78.85	63.27	21.73	27.91	4.9	-11.45	23.45	1.32	-10.15	-0.77	-17.84	2.29	1.02531	0.99972	1.01225	1.02683	1.01727	1.03269	9.35	5.14	-2.22	-3.68	-3.57	3.8	1.34	2.44	0
76.6	163	85	0	76.6	132.8	30.2	14.5	69.9	3.8	68.9	-0.7	0	0.7	63.5	-13.3	-19.4	34.3	1.03874	0.83916	1.02019	0.98801	0.98907	1.02427	-1.68	-1.95	-2.34	-20.6	-6.07	-7.45	-8.5	-4.67	1
73.1	163	85	72.5	0	53.3	109.7	93.6	8.7	23.2	10.5	11.1	34.2	0	-11.2	5.8	11.9	20.5	1.02797	1.0025	0.94132	1.02343	1.00849	1.01741	5.43	-1.41	-2.26	-4.86	-13.21	-0.15	-3.59	-4.14	1
80.1	163	85	125	-46.8	0	163	145.3	-60.8	78.2	18.5	7.1	50	25.2	0	2.5	-7.7	32.1	0.99768	0.95084	0.97642	1.01856	1.00332	1.01974	29.16	17.49	-2.55	-7.44	0.31	23.56	18.33	14.76	1
79.1	163	85	-29.8	108.4	163	0	-16.3	100	47.1	14.4	19.7	62.2	-4.8	-1.5	0	-6.2	35	1.01486	0.98027	0.99844	1.02106	0.96889	1.01243	19.52	-7.22	-2.47	-1	-8.09	13.93	-15.69	-9.97	1
76.5	163	85	-15.4	91.6	147.1	15.9	0	-85.3	67.5	21.8	-0.6	54.2	23.3	-0.4	6.1	0	13.9	1.00352	0.97295	0.9626	1.01659	1.0075	1.02419	17.64	18.99	-2.42	-1.54	-7.11	12.02	11.58	16.27	1
72.3	163	85	64.1	7.7	62.1	100.9	85	0	33.5	29.1	-17.2	39	5.6	-13.7	26.5	-17.2	0	1.02222	0.99425	1.00848	1.01214	0.98575	1.03364	6.76	8.29	-2.25	-4.54	-2.51	1.13	-2.05	5.6	1
63.99	146.7	76.5	38.63	25.36	75.81	70.89	56.93	19.57	18.78	-2.97	-16.88	17.91	-1.51	-12.87	-2.9	-20.07	-0.23	1.0302	1.0087	1.0201	1.0307	1.0228	1.0356	8.39	4.63	-1.97	-3.27	-3.18	3.41	1.22	2.21	0
67.36	146.7	76.5	0	67.36	118.2	28.5	14.44	62.06	-0.4	48.14	-5	0	-2.82	46.56	-12.61	-20.64	12.36	1.0409	0.8789	1.0265	0.9997	1.0003	1.0288	-1.16	-1.49	-2.05	-17.48	-5.33	-6.29	-7.26	-3.93	1
65.08	146.7	76.5	65.07	0	48.61	98.1	83.83	-7.3	16.81	1.99	5.09	-14.41	0	-12.83	2.05	4.2	-2.39	1.0313	1.0102	0.9615	1.0277	1.0155	1.023	4.95	-1.11	-2	-4.31	-11.55	-0.04	-3.1	-3.56	1

Table B.1 Dynamic Security Database

70.77	146.7	76.5	114	-43.23	0	146.7	131.05	-54.55	61.69	10.74	1.89	38.07	18.92	0	-2.13	-13.2	11.82	1.0066	0.9662	0.9903	1.0224	1.0103	1.0249	26.04	15.61	-2.23	-6.53	0.32	21.02	16.36	13.16	1
69.86	146.7	76.5	-27.34	97.21	146.7	0	-14.56	91.06	34.08	5.23	13.32	38.54	-7.68	-7.58	0	-9.58	19.54	1.0219	0.933	1.009	1.0257	0.9815	1.0183	17.4	-6.28	-2.17	-0.85	-7.14	12.4	-13.81	-8.75	1
67.82	146.7	76.5	-14.41	82.23	132.5	14.21	0	76.49	52.88	11.5	-1.07	30.86	18.09	-5.85	4.48	0	-4.33	1.0114	0.9861	0.9763	1.0219	1.0138	1.0265	15.72	16.95	-2.13	-1.34	-6.26	10.7	10.3	14.51	1
64.56	146.7	76.5	57.91	6.66	55.96	90.74	76.5	0	24	18.74	-16.72	18.88	2.59	-15.75	21.47	-20.14	0	1.0273	1.0037	1.0165	1.0175	0.9946	1.0355	6.08	7.47	-1.99	-4.03	-2.23	1.03	-1.79	5.05	1
79.39	179.3	93.5	48.03	31.36	92.47	86.83	69.62	23.88	37.51	13.39	-5.66	29.17	4.22	-7.24	1.4	-15.46	4.9	1.0202	0.9903	1.0041	1.0227	1.0114	1.0296	10.32	5.66	-2.47	-4.11	-3.97	4.19	1.46	2.68	0
86.76	179.3	93.5	0	86.76	148.3	31.01	13.53	79.98	8.62	94.97	13.31	0	4.57	85.27	-14.8	-18.23	26.56	1.0363	0.7886	1.0133	0.9733	0.9753	1.0188	-2.43	-2.59	-2.66	-24.51	-6.9	-8.8	-9.9	-5.6	1
81.42	179.3	93.5	81.42	0	57.87	121.43	103.67	-10.17	29.85	19.77	26.51	25.85	0	-9.45	9.86	20.37	0.87	1.0245	0.9945	0.9194	1.0188	1.001	1.0113	5.88	-1.76	-2.52	-5.44	-15.02	-0.28	-4.13	-4.79	1
89.87	179.3	93.5	139.92	-50.06	0	179.3	159.53	-66.03	96.2	27.21	21.65	55.2	31.77	0	7.64	-1.39	17.91	0.988	0.9342	0.9613	1.0143	0.9957	1.014	32.37	19.44	-2.89	-8.41	0.3	26.18	20.39	16.42	1
88.64	179.3	93.5	-31.17	119.81	179.3	0	-18.18	111.67	61.38	24.91	35.61	56.78	-1.59	5.42	0	-2.64	32.67	1.0072	0.9663	0.9871	1.0157	0.9555	1.0061	21.71	-8.22	-2.79	-1.16	-9.1	15.53	-17.69	-11.27	1
85.42	179.3	93.5	-15.55	100.97	161.73	17.58	0	93.49	83.29	33.16	8.39	46.91	28.8	5.85	7.54	0	3.47	0.995	0.9587	0.9479	1.0107	1.0006	1.0216	19.62	21.1	-2.73	-1.76	-8	13.41	12.91	18.11	1
80.25	179.3	93.5	71.48	8.78	68.14	111.16	93.5	0	43.56	40.27	-9.17	30.41	8.71	-11.57	31.75	-14.1	0	1.0168	0.9844	1.0001	1.0064	0.9764	1.0316	7.46	9.12	-2.51	-5.06	-2.8	1.22	-2.32	6.15	1

Table B.2 Dynamic Security Database (contd.)