Risk Assessment of an Electric Power System using Intelligent Power Routers

by

Carlos M. Torres Ortolaza

A thesis submitted in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE
in
ELECTRICAL ENGINEERING

UNIVERSITY OF PUERTO RICO
MAYAGÜEZ CAMPUS
2005

Approved by:

_____	_____
José R. Cedeño Maldonado, PhD Member, Graduate Committee	Date
_____	_____
Miguel Vélez Reyes, PhD Member, Graduate Committee	Date
_____	_____
Agustín A. Irizarry Rivera, PhD President, Graduate Committee	Date
_____	_____
Edgardo Lorenzo, PhD Representative of Graduate Studies	Date
_____	_____
Isidoro Couvertier, PhD Chairperson of the Department	Date

ABSTRACT

We seek to determine the reliability of Intelligent Power Routers (IPR) and the reliability change of an electric power system (PS) operated with and without IPR. The IPR is our module to provide scalable coordination in a distributed model for the next-generation PS. To calculate the change in PS' reliability operated with and without IPR, the IPR failure mechanisms and probabilities must be determined. Since there is no data on IPR reliability its failure mechanisms and probabilities will be estimated. We establish the failure modes for each IPR's element to estimate the IPR reliability, and simulate the behavior of a PS to measure its reliability change. The method used to capture this change, known as risk assessment, uses the probability of occurrence of an event and the impact that it produce. The procedure is discussed, and an example is presented using the 179-bus system for a given operating point.

RESUMEN

Buscamos determinar la confiabilidad de un Enrutador Inteligente de Potencia (IPR, por sus siglas en ingles) y el cambio en confiabilidad en un sistema de potencia eléctrica operado con y sin IPR. El IPR es nuestro módulo para proveer coordinación en un modelo distribuido para la próxima generación de la red de potencia. Para calcular el cambio en confiabilidad en un sistema de potencia operado con y sin IPR necesitamos determinar los mecanismos y probabilidades de falla del IPR. Debido a que no hay datos de la confiabilidad de un IPR sus mecanismos y probabilidades de falla serán estimados. Establecemos los modos de falla para cada componente del IPR para estimar la confiabilidad del IPR, y simular el comportamiento de un sistema de potencia para medir el cambio en su confiabilidad. El método usado para capturar ese cambio, conocido como evaluación de riesgo, usa la probabilidad de ocurrencia de un evento y el impacto q este produce. El procedimiento es discutido, y un ejemplo es presentado usando el sistema se 179 barras para cierto punto de operación.

To Lord,

to my family,

to life…

ACKNOWLEDGEMENTS

I would like to start expressing a sincere acknowledgement to my advisor, Dr. Agustín Irizarry. Thank you for your support, patience, and for each advice given to me during the last two years. I also want to thank Dr. José R. Cedeño and Dr. Miguel Vélez for serving as members of my graduate committee and for their support. Also, I want to thanks my partners of masters/research and "brothers-in-masters": Christian, Idalides, Janeth, Doeg, Noel, Emilio, Carlos, Camille, Jennifer, Linda, and specially Marianela for being my study partner and friend since early in the bachelor thru the masters.

At last, but the most important, I would like to thank my family, for their unconditional support, trust and love, and God for giving me the health, strength and motivation to finish this journey.

This work was supported in part by the National Science Foundation (NSF) thru award number 0224743 as well as by the University of Puerto Rico-Mayagüez.

TABLE OF CONTENTS

Page

TABLE LIST

Table **Page**

FIGURE LIST

Figure **Page**

1 INTRODUCTION

Almost all aspects of daily life in modern society depend on the use of electricity. The basic function of an electric power system is to satisfy the system load requirement as economically as possible and with a reasonable assurance of continuity and quality [1]. In many power systems the average duration of interruption that customers suffer is a total of two to three hours per year, but increasing load makes the power grid more stressed leading to blackouts more often [2]. Also, energy suppliers in a deregulated system must find ways to improve the productivity to be competitive, i.e. pushing the power system to its limits. Recent blackouts, like the blackout of August 14, 2003 in the Northeast United States and eastern Canada, were triggered by inadequate tree trimming plus computer and human failures [3]. These blackouts and the continuous increase of demand suggest that power utilities are more prone to outages and failures than ever before.

These reasons have forced the government and utility companies to evaluate ways of increasing system reliability and decreasing system downtimes. Addressing these concerns we are developing a model for the next generation power network using a distributed concept based on scalable coordination by an Intelligent Power Router (IPR). We want to show that by distributing network intelligence and control functions using the IPR, the system will have improved survivability, security, reliability, and re-configurability. Generally, security is defined as the ability of the power system to

withstand disturbances caused by faults and unscheduled removal of equipment without further loss of facilities or cascading [4].

Each IPR has embedded intelligence into them allowing the IPR to, for example; switch power lines, shed load and receive/broadcast local state variable information to and from other routers. The information exchange capability of the routers provides coordination among themselves to reconfigure the network, even when the designated principal control center of the system has collapsed due to a natural or man-made disaster [5]. However, when IPR is physically implemented in the power system, it will be another element on the grid, with a probability that it can fail. We have no doubt that if IPR works efficiently the reliability of the system will increase considerably, but if they fail the effect on the system may be harmful. We wish to study the reliability of a power system with IPR and without IPR. In order to perform this change in reliability assessment the IPR failure mechanisms and failure probabilities must be determined.

There are methods to study the reliability of power systems. Reliability indices such as Loss of Load Expectation (LOLE) and Loss of Load Probability (LOLP) have been used extensively in adequacy assessment as a measure of the system's failure probability [6]. Commonly, decisions in power systems are based in deterministic criteria [1]. The deterministic criteria typically adhere to the following steps [7]:

1. Study Parameters: Identify one or more study parameters for which a limit is desired.

2. Base Case Model: Develop a base case model of the planned operating system for the period under consideration.
3. Credible Contingency List: Develop a credible contingency list for each study parameter identified in Step 1.
4. Most Limiting Contingency: Identify the most limiting contingency, or contingencies, for each study parameter.
5. Critical Parameter Set: For each most limiting contingency, identify the critical parameters.
6. Boundary Determination: Identify the boundary for each critical parameter as the level where system performance following the most limiting contingency first violates minimum operating reliability criteria.

The criterion for judging operating point acceptability is then based on the identified limit. An operating point beyond this limit is unacceptable. Therefore, in theory, the deterministic approach tolerates no risk. In practice, operating engineers sometimes decide to violate the limits, particularly if there is strong economic incentive to do so [7].

Another drawback of this technique is that it does not reflect the probabilistic behavior of power systems. The well-being indices address this problem because it involves a combination of deterministic and probabilistic concepts created through the definition of system states [1], [6], [8] - [12]. The system states are defined as Healthy (H), Marginally Healthy (M), or at Risk (R). Basically, this method is only useful for an adequacy assessment. Adequacy is generally defines as the capability of the system to meet the system demand within major component ratings, including scheduled and

unscheduled outages of generation, transmission and distribution facilities [4]. A more elaborate assessment method is required to assess power system security because of power system dynamics. The currently available is risk assessment framework [13] - [24], where the expectation of the impact, or consequence, of events is calculated using the probability of occurrence and economic impact of such event. It could be used to determine the change in risk from a security point of view for a given operating point and disturbance when the system is operated with and without IPR.

The Risk Assessment framework was developed in the early 1990's by Dr J. McCalley of Iowa State University. Generally, risk is defined as the product of the probability of event occurs with the consequence (impact) of the event, i.e., [17]

$$Risk = P \times I \tag{1.1}$$

The main difference between deterministic and risk approaches resides not in the methods used to obtain the results. Instead, the main difference in the two approaches resides in the criterion used to judge operating point acceptability. Whereas one uses a deterministic criterion (stable or unstable for most severe contingency under worst-case disturbance scenario), the other uses a criterion based on probability and consequence (composite risk level from all contingencies). Therefore, the risk-based approach extends the deterministic approach. One of the appeals of this approach is ease of transition for system operators; the change is transparent to the operators except for new graphs and tables [18].

1.1 Objectives

IPR concept pretends to improve survivability, security, reliability and re-configurability of a power system, but there is a real risk that IPRs will fail due to the failure of one or more of its components. To predict or estimate the reliability of a system with IPR is necessary to:

- Establish the components of an IPR.
- Establish the failure modes and failure rate of each component of an IPR.
- Identify various configurations of the internal components of an IPR to study redundancy. An economic analysis of this redundancy is recommended to justify its investment.
- Establish the locations for IPR with a power system to avoid or mitigate specific problems.
- Determine the reliability increase in the power system operating with IPR.

1.2 Outline of the Thesis

This document consists of six chapters. Chapter 2 presents a literature review of special protection systems, power system assessment methods, probability and reliability theory. Chapter 3 describes the Intelligent Power Routers' functions, objectives and reliability. Chapter 4 describes the procedure to perform risk assessment for a system with and without IPR. Chapter 5 presents a discussion of the results of the assessment described in Chapter 4. Finally, the conclusions of the study and some recommendations for future work are presented in Chapter 6.

2 LITERATURE REVIEW

An IPR will improve system survivability, security, reliability, and re-configurability [5]. An IPR can be treated as a Special Protection System (SPS) because is generally accepted that a SPS has the following characteristics [25]:

- SPS can be armed or disarmed depending on the system conditions.
- SPS are "normally dormant" systems; initiating events usually occur less than once a year.
- SPS usually employ discrete, feed-forward control laws.
- The control action taken is predetermined in most cases.
- Typically, some form of communication is involved in the control action.

2.1 Special Protection Systems

Usually, a SPS is defined as a protection scheme that is designed to detect a particular system condition that is known to cause unusual stress to the power system, and to take some type of predetermined action to counteract the observed condition in a controlled manner [26]. Also, a SPS can be designed to detect a system condition that is known to cause instability, overload, or voltage collapse. To minimize the impact of a contingency is possible the opening of one or more lines, tripping of generators, intentional shedding of load, or other measures capable of handle the concerning problem.

In 1992 CIGRE and IEEE realized a survey to determine the experiences of SPS in power industries. Forty nine (49) utilities in seventeen (17) countries responded, and reported a total of 111 schemes [26]. A breakdown of the reported schemes revealed that Generation Rejection Schemes (GRS) are the most common scheme with a 21.6 % of the total responses. Next in frequency of use are Load Rejection (L/R) schemes and conventional Under-frequency Load Shedding (ULS) schemes, with 10.8% and 8.2% of the total responses, respectively [26].

TABLE 2.1 - Percentage of Most Common SPS Types [26]

Type of SPS	**Percentage**
Generator Rejection	21.6
Load Rejection	10.8
Under-frequency Load Shedding	8.2
System Separation	6.3
Turbine Valve Control	6.3
Load & Generator Rejection	4.5
Stabilizers	4.5
HVDC Controls	3.6
Out-of-Step Relaying	2.7
Discrete Excitation Control	1.8
Dynamic Braking	1.8
Generator Runback	1.8
VAR Compensation	1.8
Combination of Schemes	11.7
Others	12.6

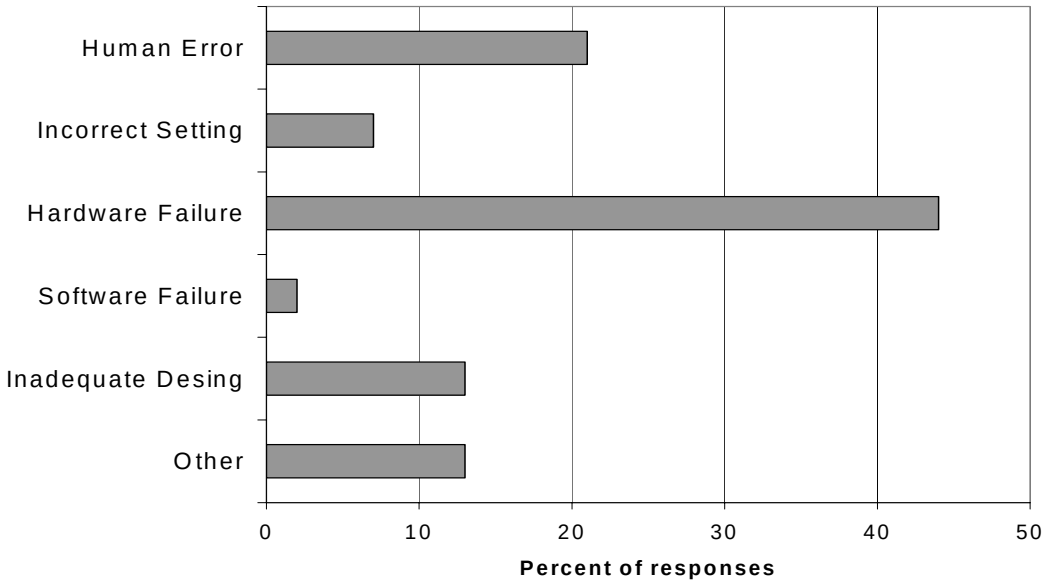

FIGURE 2.1 - Dominant Causes of SPS Failure [26]

One question in the questionnaire asked for the dominant cause of failure or problems with the SPS. Forty three (43) percent of the utilities agreed that the main problem with SPS is due with hardware failures. The complete response to this question is summarized in Figure 2.1

Hardware failure occurs when some physical stress exceeds the capability of one or more installed components. Faulty design logic may occur as a result of inappropriate or incomplete study procedure during the design. Software failure results from errors in vendor written and user written embedded, application, and utility software. Human errors can be classified according to whether they are associated with construction, operating, or maintenance [14]. The CIGRE/IEEE join also defined four modes that an SPS may have, three of them indicating a failure:

- *Successful Operation*: A scheme operation that achieves the performance objective of the power system.
- *Failure*: A scheme operation that (i) fails to prevent or minimize the effect of power system disturbance in the event of a contingency of severity equal to, or less than, that specified or (ii) a scheme operation that should not have occurred and that results in a BES disturbance.
- *Unsuccessful Operation*: A scheme operation that fails to prevent or minimize the effect of a power system disturbance in the event of a contingency of severity greater than that specified in the design of the scheme.
- *Unnecessary Operation*: A scheme operation that should not have occurred and that does not result in, or contribute to disturbance.

SPS can provide rapid corrective actions and are often used to increase the transfer capability of the network [25]. These systems can be placed in service relatively quickly and inexpensively, so there are appealing alternatives to new transmission facilities, or to be more competitive in a deregulated market. When correctly operating, SPS significantly improve system response following a contingency. However, the failure of SPS to accurately detect the defined conditions, or the failure to carry out the required preplanned remedial action, can lead to serious and costly consequences [16], [14].

The survey by IEEE-CIGRE confirmed the belief of SPS failure costs are one of the highest that utilities can incur. Because SPS failure consequence is typically very high, the risk of SPS failure can be substantial even if probability is low [25].

2.2 Power System Assessment Methods

In the assessment of a power system, decision makers have to choose between two categories: probabilistic or deterministic methodology. Probability methods are widely used in generating evaluation. However, transmission system evaluation is mostly based on deterministic criteria and the main principle is based on maintaining adequate service under most likely outages, but to accept some degradation of performance such as lines overloads and station low voltages.

The essential weakness of deterministic criteria and techniques is that these do not and cannot account for the probabilistic and stochastic nature of system behavior and are not responsive to many of the parameters such as load and risk nature, which actually influence system reliability. The dilemma between the probabilistic and deterministic approaches can be alleviated by embedding deterministic considerations into probabilistic indices using a well-being model [6]-[12], which bridges the gap between these two approaches. In this approach, the composite generation and transmission system is classified into three system well-being state, namely, healthy, marginal and at risk, which are closely associated with the system operating states.

In the healthy state (normal state), the system has enough capacity reserve of generating units and branches to meet a deterministic criterion such as the loss of the largest generating unit while all the equipment and the operating constrains are within limits. The system operates in the marginal state (alert state) when it has no difficulty but

does not have sufficient margin to meet the specified deterministic criterion, that is, withstand the loss of any single generating unit or branch. If the individual load is either equal to (emergency) or greater that (extreme emergency) the available capacity of any component, the system will enter the state of risk. A bulk power system can enter the "at risk" state or marginal state from the healthy state due to the loss of certain operating capacity or due to a sizeable increase in the system load. With this approach, the system performance is evaluated using deterministic considerations and quantified by probabilistic indices.

2.3 Risk Assessment

Other approach to measure system reliability is with risk assessment/framework [13]-[24]. In measuring risk, it is essential that we distinguish between an outcome and a decision. One important distinction is that an outcome is an unavoidable result of a decision. Based on this distinction, we categorize transmission reinforcement, unit commitment, economic dispatch, and load interruption as decisions. In the context of overload assessment, the outcome of these decisions is the effects on the circuits. These effects, which include equipment damage and equipment unavailability, are random because they are heavily dependent on weather and on loadings, the randomness of the latter caused mainly by uncertainties in demand and equipment outages. Deterministic approaches do not provide answers to:

- Risk Quantification: How safe or how risky are the current system's operating conditions?

- Trend: How does the risk change as the operating conditions are relieved or stressed?
- Security-Economy Tradeoff How is increased risk associated with heavier use of facilities offset by the corresponding increase in benefit?

Generally, risk is defined as the product of the probability of event occurs with the consequence (impact) of the event, i.e., [17]

$$Risk = P \times I \tag{2.1}$$

Calculation of the risk index has the distinct advantage of providing a uniform basis of comparing various decisions. Risk depends on many factors such as the lead time, the amount of installed generating capacity, the size of the various generating units, the reliability parameters of all the components considered, the system load, the generating unit outputs in terms of active power and voltage and the system topology, etc.

A bridge can be done between power system security and economics by the index of risk. The concept risk provides an economic measurement of system security that is compatible with the economic results of marker-based electricity trading [17]. This is more appealing to power system operators because is easier to analyze than only looking a probabilistic index.

2.4 Vulnerability Assessment

Besides risk assessment, there is another method to measure the reliability of a system, known as Vulnerability Assessment. Vulnerability is defined as the susceptibility of being hurt by some means. A vulnerability assessment identifies the levels of operational capability that remain after an event (outage, nature, attack, injury, etc.) [27]. Like power system assessment, current structural design of U.S. Navy ships is based on deterministic analysis methodologies and design rules/requirements, which are highly correlated with test data and at-sea experience [27].

Naval ships must be survivable under a hostile environment and the ship survivability is determined by the mathematical complement of killability. The killability is defined as the product of the susceptibility and the vulnerability. Mathematically, the susceptibility is defined as the probability of being hit (P_H), while the vulnerability is given by the probability of being killed if hit ($P_{K|H}$) [27].

In addition, the present vulnerability assessment of surface ships is given in a deterministic manner where the requirements stated in absolute terms must be met to ensure ship survivability. Naval ships are subjected to uncertainty in sea environments, structural configuration, material properties, and environmental and operating conditions [27]. While probabilistic methods have been applied extensively to quantify uncertainty of sea environments and estimate reliability of naval vessels under normal seaway loads, their extension to surface ships subjected to extreme dynamic loads due to collision,

grounding, and weapon effects has not been well explored. Therefore, it is imperative to develop a generalized simulation based probabilistic analysis tool, like a vulnerability assessment, such that no limitation is placed on the nature of input random processes.

2.5 Probability Theory

To have a better understanding of Risk Assessment method is necessary to take a look on probability basics. Ross [28], Papoulis [29] and Bertsekas [30] discuss the basics of probability, starting with defining a *set*. A set is a collection of objects, which are the elements of the set. If S is a set and x is an element of S, we write $x \in S$. If x is not an element of S, we write $x \notin S$. For example, the set of possible outcomes of a die roll is $\{1, 2, 3, 4, 5, 6\}$, or if there is a finite number of elements then $S = \{x_1, x_2, \ldots, x_n\}$. A set with no elements, called the empty set, is denoted by Ø.

The complement of a set S is the set of all elements of Ω (universal set of all possible elements) that do not belong to S, and is denoted by S^c. Note that $\Omega^c = \emptyset$. The union of two sets S and T is the set of all elements that belong to S or T (or both), and is denoted by $S \cup T$. The intersection of two sets S and T is the set of all elements that belong to both S and T, and is denoted by $S \cap T$.

Every probabilistic model involves a process (called the experiment) that will produce exactly one out of several possible outcomes. The set of all possible outcomes is

called the sample space of the experiment, and is also denoted by Ω. A subset of the sample space, that is, a collection of possible outcomes, is called an event.

The "likelihood" of any outcome, or of any set of possible outcomes (an event) is called the probability of A, satisfying the following axioms.

2.5.1 Probability Axioms

- (Nonnegativity) $P(A) \geq 0$, for every event A.
- (Additivity) If A and B are two disjoint events, then the probability of their union satisfies $P(A \cup B) = P(A) + P(B)$. Furthermore, if the sample space has an infinite number of elements and $A_1, A_2, \ldots$ is a sequence of pair wise disjoint events in Ω. Then, the probability of their union satisfies $P\left(\bigcup_{i=1}^{\infty} A_i\right) = \sum_{i=1}^{\infty} P(A_i)$ (Countable Additivity).
- (Normalization) The probability of the entire sample space Ω is equal to 1, that is, $P(\Omega) = 1$.

2.5.2 Conditional Probability

Conditional probability provides a way to reason about the outcome of an experiment, based on partial information. For example: In an experiment involving two successive rolls of a die, you are told that the sum of the two rolls is 7. How likely is it that the first roll was a 4?

The conditional probability of an event A, given an event B with $P(B) > 0$, is defined by

$$P(A \mid B) = \frac{P(A \cap B)}{P(B)} \tag{2.2}$$

and specifies a new (conditional) probability law on the same sample space Ω. In particular, all known properties of probability laws remain valid for conditional probability laws.

Let $A_1, \ldots, A_n$ be disjoint events that form a partition of the sample space (each possible outcome is included in one and only one of the events $A_1, \ldots, A_n$ and $\bigcup_{i=1}^{n} A_i = \Omega$) and assume that $P(A_i) > 0$, for all $i = 1, \ldots, n$. Then, for any event B,

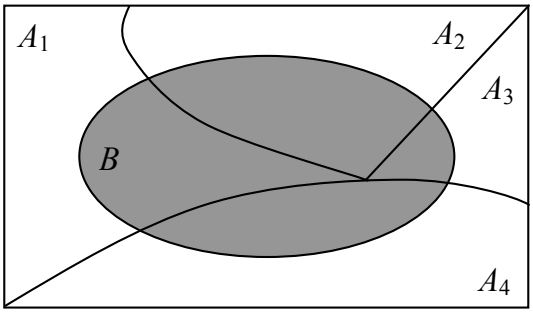

FIGURE 2.2 - A disjoint events

$$P(B) = P(A_1 \cap B) + \cdots + P(A_n \cap B) = P(A_1)P(B \mid A_1) + \cdots + P(A_n)P(B \mid A_n) \tag{2.3}$$

Equation 2.3 is known as Total Probability Theorem. The total probability theorem is often used in conjunction with the following theorem, Bayes' Rule, which relates

conditional probabilities of the form $P(A \mid B)$ with conditional probabilities of the form $P(B \mid A)$, in which the order of the conditioning is reversed.

Let $A_1, A_2, \ldots, A_n$ be disjoint events that form a partition of the sample space, and assume that $P(A_i) > 0$, for all i. Then, for any event B such that $P(B) > 0$,

$$P(A_i \mid B) = \frac{P(A_i)P(B \mid A_i)}{P(B)} = \frac{P(A_i)P(B \mid A_i)}{P(A_1)P(B \mid A_1) + \cdots + P(A_n)P(B \mid A_n)} \tag{2.4}$$

Bayes' rule (or Bayesian probability) is a formalism that allows us to reason about beliefs under conditions of uncertainty. Some number of "causes" may result in a certain "effect." If we observe the effect, we want to infer the cause. The events $A_1, \ldots, A_n$ are associated with the causes and the event B represents the effect [30].

2.5.3 Independence

Two events A and B are said to independent if $P(A \cap B) = P(A)P(B)$. If in addition, $P(B) > 0$, independence is equivalent to the condition $P(A \mid B) = P(A)$.

- If A and B are independent, so are A and B^c, A^c and B, and A^c and B^c.
- Two events A and B are said to be conditionally independent, given another event C with $P(C) > 0$, if $P(A \cap B \mid C) = P(A \mid C)\, P(B \mid C)$.
- Independence does not imply conditional independence, and vice versa.

2.5.4 Discrete Random Variables

A random variable X is a real-valued function of the experimental outcome $\left(X:\Omega\to\Re\right)$. That is, a rule of correspondence that assigns it a numeric value to each result in Ω. R_x denotes the value range of X. If R_x is a countable set, then X is said to be discrete. For a discrete random variable X, we define the probability mass function $p(a)$ of X by

$$p(a) = P\{X = a\} \tag{2.5}$$

The probability mass function $p(a)$ is positive for at most a countable number of values of a. That is, if X must assume one of the values $x_1, x_2, \ldots$, then

$$p(x_i) > 0, \qquad i = 1,2, \ldots$$

$$p(x) = 0, \qquad \text{all other values of } x$$

Since $P(\Omega) = 1$, and $X[(\Omega)] = R_x$ (X must take on one of the values x_i), we have

$$\sum_{x\in R_x} p\left(x_i\right) = 1 \tag{2.6}$$

The cumulative distribution function F can be expressed in terms of $p(a)$ by

$$F(a) = \sum_{all\, x_i \le a} p\left(x_i\right) \tag{2.7}$$

Bernoulli, Binomial, Geometric, and Poisson are the most common discrete random variables.

2.5.5 Continuous Random Variables

A random variable X is called continuous if its probability law can be described in terms of a nonnegative function f_x, called the probability density function (PDF) of X, which satisfies

$$P(X \in A) = \int_B f_x(x)\,dx \tag{2.8}$$

for every subset A of the real line. Note that to qualify as a PDF, a function f_x must be nonnegative, i.e., $f_x(x) \geq 0$ for every x, and must also satisfy the normalization equation

$$\int_{-\infty}^{\infty} f_x(x)\,dx = P(-\infty < X < \infty) = 1 \tag{2.9}$$

In particular, the probability that the value of X falls within an interval is

$$P(a \leq X \leq b) = \int_a^b f_x(x)\,dx \tag{2.10}$$

and can be interpreted as the area under the graph of the PDF. For any single value a, we have

$$P(X = a) = \int_a^a f_x(x)\,dx = 0 \tag{2.11}$$

Uniform, Exponential, Gamma, Normal are the most common continuous random variables.

2.5.6 Markov Chains

Markov chains are stochastic process in which the state changes at certain discrete time instants, indexed by an integer variable n. At each time step n, the Markov chain has a state, denoted by X_n, which belongs to a finite set S of possible states, called the state space. We will assume that $S = \{1, \ldots, m\}$, for some positive integer m. The Markov chain is described in terms of its transition probabilities P_{ij}: whenever the state happens to be i, there is probability P_{ij} that the next state is equal to j. Mathematically,

$$P_{ij} = P(X_{n+1} = j \mid X_n = i), \quad i, j \in S \tag{2.12}$$

The main assumption in doing Markov processes is that the transition probabilities P_{ij} apply whenever state i is visited, no matter what happened in the past, and no matter how state i was reached. The transition probabilities P_{ij} must be of course nonnegative, and sum to one:

$$\sum_{j=1}^{m} p_{ij} = 1, \quad \text{for all } i. \tag{2.13}$$

All of the elements of a Markov chain model can be put in a transition probability matrix, which is simply a two-dimensional array whose element at the i^{th} row and j^{th} column is P_{ij}:

$$\begin{bmatrix} P_{11} & P_{12} & \cdots & P_{1m} \\ P_{21} & P_{22} & \cdots & P_{2m} \\ \vdots & \vdots & \vdots & \vdots \\ P_{m1} & P_{m2} & \cdots & P_{mm} \end{bmatrix} \tag{2.14}$$

It is also helpful to lay out graphically the model, whose nodes are the states and whose arcs are the possible transitions. By writing the numerical values of P_{ij} near the corresponding arcs, one can visualize the entire model in a way that can make some of its major properties readily apparent.

Now let us define the *n*-step transition probabilities P_{ij}^{n} to be the probability that a process in state *i* will be in state *j* after *n* additional transitions. That is,

$$P_{ij}^{n} = P(X_{n+m} = j \mid X_m = i), \qquad n \geq 0,\ i, j \geq 0 \tag{2.15}$$

Of course $P_{ij}^{n} = P_{ij}$. The Chapman-Kolmogorov equations provide a method for computing these *n*-step transition probabilities. These equations are

$$P_{ij}^{n+m} = \sum_{k=0}^{\infty} P_{ik}^{n} P_{kj}^{m} \qquad \text{for all } n, m \geq 0, \text{ all } i, j \tag{2.16}$$

and are understood by noting that $P_{ik}^{n} P_{kj}^{m}$ represents the probability that starting in *i* the process will go to state *j* in $n + m$ transitions through a path which takes it into state *k* at the n^{th} transition. Hence, summing over all intermediate states *k* yields the probability that the process will be in state *j* after $n + m$ transitions. Formally,

$$P_{ij}^{n+m} = \sum_{k=0}^{\infty} P_{kj}^{m} P_{ik}^{n} \tag{2.17}$$

If we let $P^{(n)}$ denote the matrix of n-step transition probabilities P_{ij}^{n}, then Equation 2.16 asserts that

$$P^{(n+m)} = P^{(n)} \cdot P^{(m)} \tag{2.18}$$

where the dot represents matrix multiplication. Hence, in particular,

$$P^{(2)} = P^{(1+1)} = P \cdot P = P^2 \tag{2.19}$$

and by induction

$$P^{(n)} = P^{(n-1+1)} = P^{n-1} \cdot P = P^n \tag{2.20}$$

That is, the n-step transition matrix may be obtained by multiplying the matrix P by itself n times.

2.6 Reliability Theory

Reliability is defined as the probability that a system (component) will function over some time period t [31]. Reliability should not be confused with availability or dependability. Availability is a measure of the degree to which an item is in an operable and committable state at the start of the period or interval [32]. Meanwhile, dependability is a measure of the degree to which an item is operable and capable of performing its required function or functions at any (random) time during a specified time period [32], given item availability at the start of the period.

If T (a continuous random variable) is allowed to be the time to failure of the system (component); $T > 0$, then reliability can be expressed as

$$R(t) = P\{T > t\} \tag{2.21}$$

where $R(t) \geq 0$, $R(0) = 1$, and $\lim_{t\to\infty} R(t) = 0$. For a given value of t, $R(t)$ is the probability that the time to failure is greater than or equal to t. If we define

$$F(t) = 1 - R(t) = P\{T \leq t\} \tag{2.22}$$

where $F(0) = 0$, and $\lim_{t\to\infty} F(t) = 1$. Therefore, $F(t)$ is the probability that a failure occurs before time t. We will refer to $R(t)$ as the reliability function and $F(t)$ as the *cumulative distribution function* (CDF) of the failure distribution. A third function, defined by

$$f(t) = \frac{dF(t)}{dt} = -\frac{dR(t)}{dt} \tag{2.23}$$

is called the *probability density function* (PDF). This function describes the shape of the failure distribution. The PDF, $f(t)$, has these two properties:

$$f(t) \geq 0 \qquad \text{and} \qquad \int_0^\infty f(t)\,dt = 1 \tag{2.24}$$

Given the PDF, $f(t)$, then

$$F(t) = \int_0^t f(t')\,dt' \tag{2.25}$$

$$R(t) = \int_{t}^{\infty} f(t')\,dt' \tag{2.26}$$

The function R(t) is normally used when reliabilities are being necessary, which function $F(t)$ is normally used for failure probabilities. Graphing the PDF, $f(t)$, provides a visual representation of the failure distribution. The probability of a failure occurring within some interval of time [a,b] may be found using any of the three probability functions, since

$$P\{a \le T \le b\} = F(b) - F(a) = R(a) - R(b) = \int_{a}^{b} f(t)\,dt \tag{2.27}$$

2.6.1 MTTF and MTBF

The mean time to failure (MTTF) is a basic measurement of reliability for non-repairable items [32]. It is defined by

$$\text{MTTF} = \int_{0}^{\infty} R(t)\,dt \tag{2.28}$$

Mean time to failure (MTBF) is another measure for reliability calculation. If the MTBF is large enough, usually is equivalent to MTTF. MTBF is related with reliability in the following way

$$R(t) = e^{-\frac{t}{\text{MTBF}}} \tag{2.29}$$

2.6.2 Hazard Rate Function

Another function, called the *failure rate* or *hazard rate function*, is often used in reliability. It provides an instantaneous (at time t) rate of failure. Set

$$\lambda(t) = \frac{f(t)}{R(t)} \tag{2.30}$$

Then $\lambda(t)$ is known as the instantaneous hazard rate or failure rate function. Failure rates in some cases may be characterized as increasing (IFR), decreasing (DFR), or constant (CFR) when $\lambda(t)$ is an increasing, decreasing, or constant function. A particular hazard rate function will uniquely determine a reliability function,

$$R(t) = \exp\left[-\int_0^t \lambda(t')\,dt'\right] \tag{2.31}$$

A failure distribution that has a constant failure rate is called an exponential probability distribution. It is one of the most common failure distributions in reliability engineering. Random failures will follow this distribution. It should dominate during the useful life of a system or component. It is also one of the easiest distributions to analyze statistically. A well-known characteristic of the CFR model, one not shared by other failure distributions, is its lack of memory. In other words, the time to failure of a component is not dependent on how long the component has been operating. The probability that the component will operate for the next 500 hr is the same regardless of whether the component is brand new, has been operating for several hundred hours, or

has been operating for several thousand hours. This property is consistent with the completely random and independent nature of the failure process.

To develop the CFR model let assume that $\lambda(t) = \lambda$, $t \geq 0$, $\lambda > 0$. Then from equation (2.31)

$$R(t) = \exp\left[-\int_0^t \lambda dt'\right] = e^{-\lambda t}, \quad t \geq 0 \tag{2.32}$$

and

$$F(t) = 1 - e^{-\lambda t} \tag{2.33}$$

To find the MTTF, we use equation (2.28):

$$\text{MTTF} = \int_0^\infty e^{-\lambda t} dt = \frac{e^{-\lambda t}}{-\lambda}\Bigg|_0^\infty = \frac{1}{\lambda} \tag{2.34}$$

It is necessary to point out that $\text{MTTF} = \int_0^\infty R(t)\,dt \equiv E(x)$, since $x \geq 0$ and $E(x) = \frac{1}{\lambda}$ if $x \sim \text{Exp}(\lambda)$.

2.6.3 Failure Modes

Complex systems fail by some reasons resulting from different physical phenomena or different failure characteristics of individual components. A useful analysis approach in reliability engineering is to classify these failures according to the mechanisms or components causing the failures. These categories of failures are then

referred to as failure modes. If $R_i(t)$ is the reliability function for the i^{th} failure mode, then, assuming independence among the failure modes, the system reliability $R(t)$ is

$$R(t) = \prod_{i=1}^{n} R_i(t) \tag{2.35}$$

$R_i(t)$ is the probability that the i^{th} failure mode does not occur before time t, therefore $R(t)$, is the probability that none of the n failure modes occurs before time t. Let $\lambda_i(t)$ be the failure rate function for the i^{th} failure mode,

$$R(t) = \exp\left[-\int_0^t \lambda(t')\,dt'\right] \tag{2.36}$$

where $\lambda(t) = \sum_{i=1}^{n} \lambda_i(t)$. This is an important result stating that the hazard rate function for the system is determined by summing the hazard rate functions of the n independent failure modes.

2.6.3.1 Failure Modes with CFR Model

In a system consisting of n independent, serially related components each having a constant failure rate λ_i, we have from equation 2.36 that

$$\lambda(t) = \lambda = \sum_{i=1}^{n} \lambda_i \tag{2.37}$$

and

$$R(t) = \exp\left[-\int_0^t \lambda dt'\right] = \exp[-\lambda t] \tag{2.38}$$

where

$$\text{MTTF} = \frac{1}{\lambda} = \frac{1}{\sum_{i=1}^{n} \lambda_i} = \frac{1}{\sum_{i=1}^{n} 1/\text{MTTF}_i}; \qquad \text{MTTF}_i = \frac{1}{\lambda_i} \tag{2.39}$$

In other words, the system itself will have an exponential failure time (CFR model).

2.6.4 Serial Systems

Components in a system may be connected to one another either in a serial or a parallel configuration. In series all components must function for the system to function. In a parallel, or redundant configuration, at least one component must function for the system to function. Since reliability is a probability, system reliability R_s may be determined from the component reliabilities in the following way. Imagine a series system of two components (Figure 2.3)

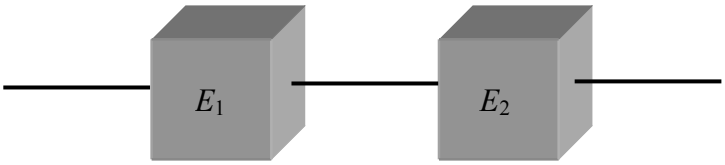

FIGURE 2.3 - Series System

where E_1 = the event that component 1 does not fail

E_2 = the event that component 2 does not fail

then ,

$P(E_1) = R_1$ and $P(E_2) = R_2$

where R_1 = the reliability of component 1

R_2 = the reliability of component 2

Therefore $R_s = P(E_1 \cap E_2) = P(E_1)P(E_2) = R_1(R_2)$ assuming that the two components are independent. In words, in order for the system to function, both component 1 and component 2 must function. Generalizing to n mutually independent components in series,

$$R_s(t) = R_1(t) \times R_2(t) \times \cdots \times R_n(t) \leq \min\{R_1(t), R_2(t), \ldots, R_n(t)\} \tag{2.40}$$

The system reliability can therefore be no greater than the smallest component reliability. Because of this equation, it is important for all components to have a high reliability, especially if the system contains a large number of components. If each component has a constant failure rate of λ_i, the system reliability is given by

$$R_s(t) = \prod_{i=1}^{n} R_i(t) = \prod_{i=1}^{n} \exp(-\lambda_i t) = \exp\left(-\sum_{i=1}^{n} \lambda_i t\right) = \exp(-\lambda_s t) \tag{2.41}$$

where $\lambda_s = \sum_{i=1}^{n} \lambda_i$.

2.6.5 Parallel Systems

Two or more components are in parallel, or redundant, configuration if all units must fail for the system to fail. If one or more units operate, the system continues to operate. System reliability for n parallel and independent components is found by taking

1 minus the probability that all *n* components fail. To see this imagine two components in parallel (Figure 2.4), then

$$\begin{aligned} R_s &= P\left(E_1 \cup E_2\right) = 1 - P\left(E_1 \cup E_2\right)^C = 1 - P\left(E_1^C \cup E_2^C\right) \\ &= 1 - P\left(E_1^C\right)\left(E_2^C\right) = 1 - \left(1 - R_1\right)\left(1 - R_2\right) \end{aligned} \tag{2.42}$$

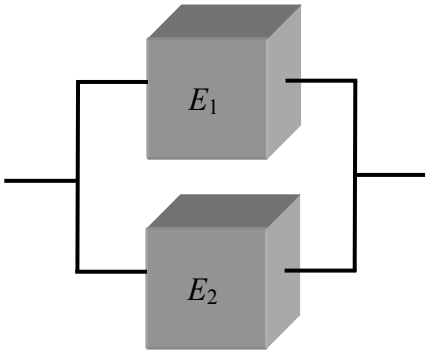

FIGURE 2.4 - Parallel System

Generalizing,

$$R_s\left(t\right) = 1 - \prod_{i=1}^{n}\left[1 - R_i(t)\right] \tag{2.43}$$

It is always true that

$$R_s(\mathrm{t}) \geq \max\{R_1(\mathrm{t}), R_2(\mathrm{t}), \ldots, R_n(\mathrm{t})\} \tag{2.44}$$

since $\prod\left[1 - R_i\left(t\right)\right]$ must be less than the failure probability of the most reliable component. For a redundant system consisting of all CFR components,

$$R_s\left(t\right) = 1 - \prod_{i=1}^{n}\left[1 - e^{-\lambda_i t}\right] \tag{2.45}$$

where λ_i, = the failure rate of the i^{th} component.

2.6.6 Reliability Analysis Techniques

McCalley [17] describes four techniques commonly used in the reliability analysis of SPS. These techniques are not exclusive for SPS reliability assessment. They are used widely in engineering reliability analysis.

2.6.6.1 Failure Mode and Effect Analysis (FMEA)

A FMEA is a technique that is designed to identify failure modes. Known as a "bottom-up" method, FMEA starts with a detailed list of all components with the system. A system can be analyzed one component at a time or the system can be divided into subsystems and modules as required. The steps involved in the process are

1. break the system down into subsystems
2. list all components
3. for each component, list all failure modes
4. for each failure mode,
   - list its effect on the next higher subsystem or system, and its failure rate
   - list the severity of the effect
5. when the next higher subsystem is the highest system, stop; otherwise, consider the next higher subsystem as a component, and return to (3).

The output of this process is a list including component name, failure mode, failure rate, and failure effect. However, this technique is poor at identifying combinations of failures that cause critical problems. Since each component is reviewed individually, failures due

to combination of components are not addressed. Common cause failures are rarely identified since they require more than one component failure. FMEA can be used an initial step to identity failure modes for Markov modeling [17].

2.6.6.2 Network Modeling

Many systems used in industry can be modeled through the use of simple networks. Network modeling (or reliability block diagrams) is used to perform a system integrity analysis through representing the system as a number of functional boxes interconnected to show the effect of each box on the overall system. The resulting networks show components in series, in parallel, or in combination configurations. The key step in the process of reliability modeling is to convert from a physical system into a network model.

2.6.6.3 Fault Tree Analysis

Another useful tool in a system reliability analysis is fault tree analysis. It is a graphical design technique that provides an alternative to reliability block diagrams. It is broader than a reliability block diagram and differs from reliability block diagrams in several respects. It is a top-down, deductive analysis structured in terms of events rather than components. The focus is on faults rather than reliability. All failures are faults, but not all faults may be considered failures. One advantage of this approach is that failures are usually easier to define than non-failures and there may be far fewer ways in which a failure can occur, in contrast to the numerous ways in which non-failures can occur [31].

The focus is usually on a significant failure or a catastrophic event, which is referred to as the top event and appears at the top of the fault tree diagram. The qualitative analysis consists of identifying the various combinations of events that will cause the top event to occur. This may be followed by a quantitative analysis to estimate the probability of occurrence of the top event.

2.6.6.4 Markov Modeling

Markov modeling involves definition of all mutually exclusive success/failure states in a system. These are represented by labeled circles. The system can transition from one state to another whenever a failure or a repair occurs. Transitions between states are shown with arrows and are labeled with appropriate failure or repair probability. With time modeled in discrete increments, calculations can be made showing the probability of being in each state for each time interval. Since some states represent system success, the probabilities of these states are added to obtain either system reliability or system availability as a function of time.

Markov modeling can incorporate independent and common cause failures, partial and full repairs, maintenance, and diagnostic coverage [17]. Most importantly, it provides that all of these features can be modeled as a function of time. This is in contrast to probability methods which provide steady state results and are accurate only for short repair times and low failure rates.

3 INTELLIGENT POWER ROUTERS

Researchers at University of Puerto Rico at Mayagüez proposed the development of a model for the next generation power network using a distributed concept based on scalable coordination by an Intelligent Power Router (IPR). The goal is to show that by distributing network intelligence and control functions using the IPR, the system will be capable of achieving improved survivability, security, reliability, and re-configurability [5].

The proposed system has a control scheme that can be detached from central control sites, and delegated to intelligent power routers (IPRs) that are strategically distributed over the entire over power delivery networks, possibly at key substations or transmission centers, managing existing redundant paths used to carry power from one of more producers to a given consumer. The routers will have embedded intelligence into them allowing the power router to switch power lines, shed load based on a priority scheme, activate auxiliary or distributed generation, isolate power region of the energy delivery network to prevent system cascade failures and receive/broadcast local state variable information to and from other routers. The ability to exchange information of the routers will allow coordination among themselves to reconfigure the network, even when the designated principal control center of the system has collapsed due to a natural or man-made disaster [5].

The proposed approach borrows from computer networks, where data can be moved between distant nodes via data routers. In the event of a component or system failure, the IPRs will make local decisions and coordinate with other routers to bring the system, or part of it, back into an operational state. For example, a metropolitan area can be divided into several sectors, each one served by at least two routers. These routers can then be connected to a second layer of routers that are in charge of controlling power delivery on the scale of regions formed by two or more sectors. These, routers can in turn connect to a group of backbone routers that are directly connected to the power generators. It is not intended that the IPRs will substitute current control protocols if there are no contingencies. However, under normal operating conditions, the IPRs would provide additional information on system status to the central energy management system. The IPR will allow the system to operate in degraded operation during major contingencies.

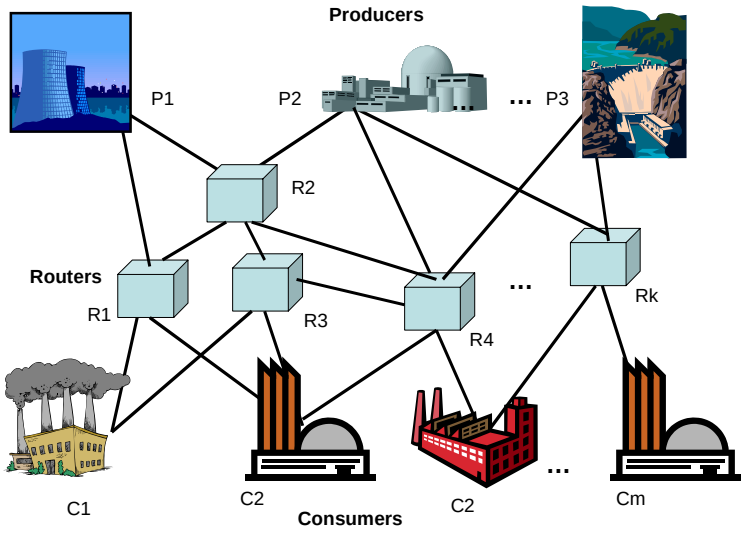

FIGURE 3.1 - Power system with IPRs

3.1 Power System Operation with IPRs

Figure 3.1 presents the envisioned system. Generation units P_1, P_2,…, P_n are connected via the power network with consumers C_1, C_2,…, C_m. The producers and the consumers are connected via a series of power lines and intelligent power routers, R_1, R_2,…, R_k that take on the role of controlling the routing of power over their lines when a major system disturbance occurs [5].

Basically, the routers are the intelligence of the network, capable of adjusting controllable system variables to meet unexpected system disturbances. More importantly, the routers will re-configure the network in the event of a high risk operating condition or a component or system failure. Figure 3.1 shows each IPR controls a series of input lines that bring power from either a power generator or another source possibly under the control of a different router. Also, each router controls a series of output lines transporting power to a consumer or serving as power sources to another power node that again may be controlled by a different router. Therefore, the routers are organized in a network providing multiple redundant power paths between producers and consumers. An important key to the design is the fact that to a given IPR, it should be irrelevant whether its inputs come from power producers or other IPR. In Distributed Systems terminology, this hierarchy is often called a **Peer-to-Peer** system (P2P) or a mesh [5].

The information collected by IPRs regarding the power flow through its power lines is going to be used to make local decisions on how to re-route power in the event of

changes in the amount of power moving along the lines, which might be caused by failures, changes in power generation or demand. Also, these routers may warn that emergency power sources are needed on-line to meet the power demands of the network in the event of a failure or unexpected demands. Finally, the routers might implement policies to bring down portions of the system or make some islanding in order to avoid further damage and maintain service to critical loads.

This approach is a departure from state-of-the-art schemes because the power network has the infrastructure to react to changes in a decentralized and autonomous fashion. The power network has enough redundancy, e.g. the existence of more than one means for accomplishing a given function [32], and intelligence to find alternate paths to deliver power to the loads. The goal is to survive failures, and returns critical loads to an acceptable level of operation. To achieve this, the approach reduces the risk associated with single-points of failures by using the IPR a mechanism to operate the system following a distributed control scheme.

3.2 IPR Components

The operational relationship of IPR subsystem is shown in Figure 3.2. The three subsystems are Computer Hardware, Software, and Power Hardware. The computer hardware will do the CPU functions and communications between sensors and other IPRs. Software will execute decisions based on the information collected from sensors.

The power hardware will switch, and control the power flow commanded by the decisions taken by the software.

3.2.1 Software

The Intelligence section (i.e. software) consists of the algorithm which will make and execute decisions, while the IPR operates. The intelligence section will control the switching device of the IPR depending on the network status. Network status is monitored locally via sensors and regionally through the data router communication exchange capability. Decisions of the intelligence section will be based, at least initially, on network status and pre-established contingency tables. We need to assess the software reliability to establish IPR reliability.

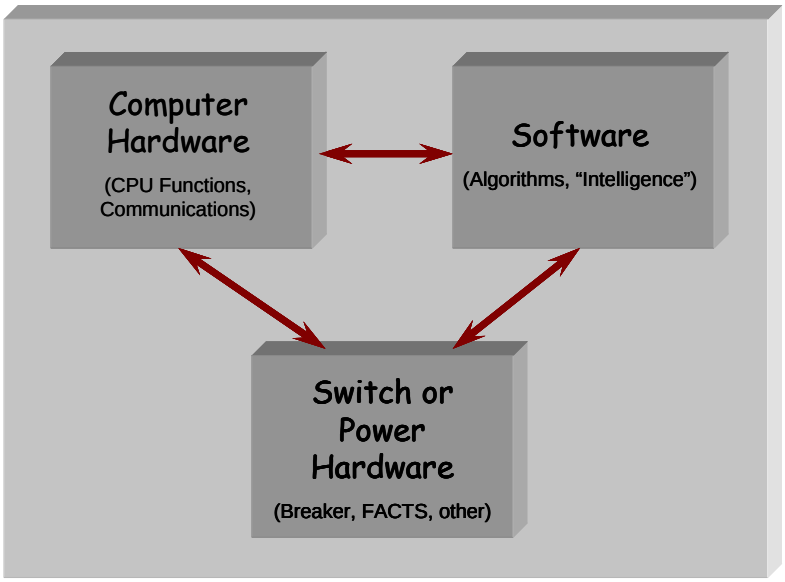

FIGURE 3.2 - Basic operational relationship of IPR major subsystems

There are two important concepts in measuring software reliability [33], [34]. First, the rate at which software fails is a function of execution time, which is a measure of software processing time (CPU time), generally expressed in terms of CPU-seconds or CPU-hours. There are times when CPU time (and hence execution time) cannot be measured directly. However, under appropriate conditions, execution time can be approximated in other ways. If the use of the CPU is relatively constant for example, then elapsed (or calendar) time multiplied by average utilization is a good approximation to execution time. In another instance, if the mix of types of items being processed is relatively constant, then execution time is relatively proportional to the number of items processed. The important point to make here is the modeling and analysis of software reliability is done in the execution time domain.

Second, the operational profile plays a large role in how frequently the software fails. An operational profile is the set of all the input states to the software together with the frequency with which they will occur in normal operation by the customer. Basically, the operational profile specifies how a customer will use the software product in his or her operating environment.

Models play an important role in estimating and analyzing software reliability. Software reliability models generally have the following two components [33].

- The execution time component (relates the failure of software to execution time) properties of the software being developed, properties of the development

environment, and properties of the operating environment. There are two general classes of models related to the execution time component:

  - reliability growth models (reliability improves with execution time). These models are particularly applicable during system test because the removal of faults reduces the rate at which failures occur.
  - constant reliability models (reliability does not change with execution time). These models are suitable after the product is introduced in the field when no fault removal is generally occurring.

- The calendar time component, which relates the passage of calendar time to execution time and the number of failures that have occurred.

The passage of calendar time depends on the consumption of resources such as processing cycles on a computer system as a function of execution time and number of failures. During system test, other resources such as testers' time in detecting failures, and developers' time in locating and fixing the underlying faults, come into play in relating calendar time to execution time and number of failures.

3.2.2 Power Hardware

The switching device of an IPR can be a high voltage circuit breaker, FACTS (Flexible AC Transmission Systems), or another switching device capable of controlling the power flow in the transmission/distribution lines. The failure modes of the power hardware can be obtained from historical data. To simplify our study, we will only use circuit breaker information. Circuit breakers are mechanical switching devices mainly

used to protect the electric system. According to the operational features, the major failure modes of circuit breakers in service are [2], [35]-[38];

a) Failure in the closed position

b) Failure to close

c) Failure to close properly

d) Failure to stay closed, i.e., unintended trip

e) Failure in the open position

f) Failure to open

g) Failure to open properly

h) Failure to stay open, i.e., unintended close

A “major failure” is defined as “complete failure of a circuit breaker which causes the lack of one or more of its fundamental functions”; this results in an immediate change in the power system operating condition, or else results in mandatory removal from service for nonscheduled maintenance (intervention necessary within 30 minutes). The failure modes are as numerous as the types of designs. Obvious things would be broken mechanical parts, incorrectly manufactured parts, excessively worn parts, excessive corrosion, inadequate lubrication, gummy lubrication, incorrect adjustment, and things of this sort.

3.2.3 Computer Hardware

The data router section will handle the communication between IPR. The data router of an IPR will be basically the same data routers used in internet/Ethernet applications. They have to communicate the status of the network and useful data obtained by the system sensors (PT's, CT's, etc.) for the intelligence section to analyze and take appropriate action. For simplicity in our analysis we assume the sensors to be fully reliable. Data will be transmitted-received between IPR via wireless connection, fiber optic, dedicated line, or the most appropriate method depending on the topology of the area. To reduce communication problems every router should be able to "talk" with many routers as possible and be able to broadcast the status of the other routers. For example the communication link between two routers (R_A and R_B) can be interrupted, but this does not mean that these routers have failed if router R_B is linked to routers R_C, R_D, and R_E, which at least one of them, R_D for example, is also linked to R_A. If every router has the ability to "talk" with multiple routers and broadcast their status, then R_A will know the actual status of R_B thanks to R_D. The reliability of some Ethernet system commonly used in power substations and control centers to monitor and control a power system is discussed in [39]. The author shows that the availability of a redundant router system that operates any breaker in a substation can be as high as 99.9986% or an equivalent of 0.123 hours of downtime per year. MTBF (mean time between failures) is a measure of how reliable a product is, commonly used by data routers manufacturers to predict the reliability of their products

3.3 Configuration

The probability method of calculating system reliability measures the continuity of service rather than its quality by examining various conditions which must exist for power to flow in series and parallel combinations of system components. There are four assumptions when predicting reliability using above methods and others:

1. System components operate in a state of availability or unavailability.
2. Failures are independent.
3. For a series system, all of its components must be available for the whole system to be available.
4. For a parallel system, all of its components must fail for the whole system to fail.

Figure 3.3 shows possible functional configurations for the internal components of an IPR. Figure 3.3(a) shows the basic series configuration. If any of the internal components fail the IPR will fail. We assume that the probability of failure of each component (software, data router, and breaker) is independent of each other. Figures 3.3(b), (c), (d) and (e) introduce a redundant path for the software, router, and software-router respectively. If the main path fails, there is an auxiliary path allowing the IPR to maintain full functionality. We do not provide a redundant path for the breakers because we assume the cost of power breakers to be much higher than that of software or routers. Because of this economic constraint IPR will probably be implemented using existing breakers and switching devices. However, most substations layouts has available a breaker redundancy. In fact, it will increase the reliability of the IPR, so it will not affect

negatively our analysis. To avoid diminished reliability due to the inclusion of the additional IPR subsystems the IPR design can include a "by-pass" function, where the IPR will use only the breaker (such as today's protective systems) in the event of a full loss of intelligence and communications. We do not consider this configuration in the calculations that follow.

3.4 Example

In Chapter 2 we reviewed important concepts of reliability theory. Reliability is defined to be the probability that a component or system will perform a required function for a given period of time when used under stated operating conditions [31]. It is the probability of non-failure over time. These concepts are the basis of our work. Let

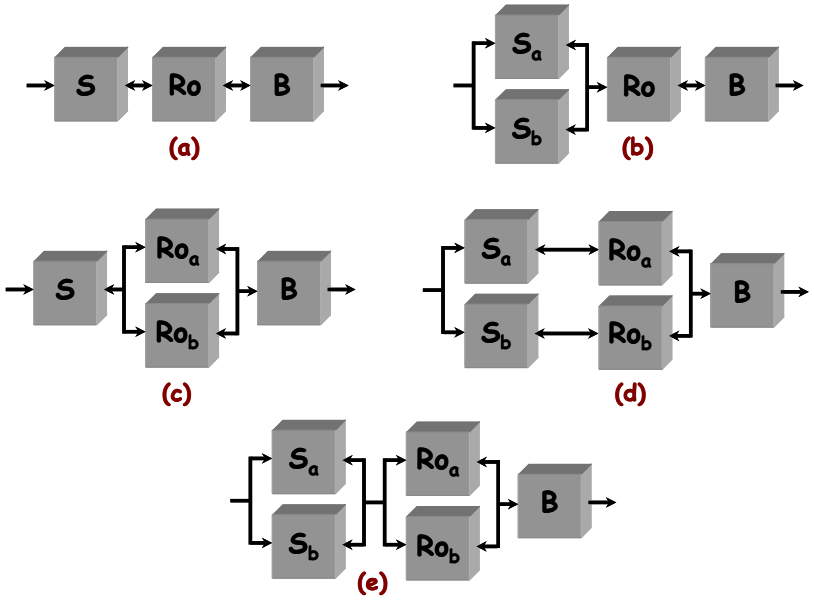

FIGURE 3.3 - IPR internal configurations

R = successful IPR operation = Reliability (3.1)

B = successful Circuit Breaker operation (3.2)

$\overline{B}$ = unsuccessful Circuit Breaker operation (3.3)

Ro = successful Router operation (3.4)

$\overline{Ro}$ = unsuccessful Router operation (3.5)

S = successful Software operation (3.6)

$\overline{S}$ = unsuccessful Software operation (3.7)

then IPR reliability for the series configuration shown in Figure 3.3(a) is

$$R = S \times Ro \times B \tag{3.8}$$

The IPR reliability for the configuration shown in Figure 3.3(b) is obtained by first calculating the reliability of the elements in parallel, then multiplying by the reliability of the series elements,

$$S = 1 - \overline{S}_a \, \overline{S}_b \tag{3.9}$$

thus,

$$R = S \times Ro \times B = \left(1 - \overline{S}_a \overline{S}_b\right) \times Ro \times B \tag{3.10}$$

The IPR reliability for the configuration shown in Figure 3.3(c) is obtained in the same way.

$$Ro = 1 - \overline{Ro}_a \, \overline{Ro}_b \tag{3.11}$$

thus,

$$R = S \times Ro \times B = S \times \left(1 - \overline{Ro}_a \, \overline{Ro}_b\right) \times B \tag{3.12}$$

The systems of Figure 3.3(d) and 3.3(e) combine series-parallel or parallel-series configurations to achieve a stronger redundancy. The IPR reliability for the configuration shown in Figure 3.3(d) is obtained first calculating the reliability of the series elements in top and bottom paths, then calculating the reliability of the ones in parallel

$$R_{\text{top}} = S_a \, Ro_a \tag{3.13}$$

$$R_{\text{bot}} = S_b \, Ro_b \tag{3.14}$$

$$\overline{R}_{\text{top}} = 1 - R_{\text{top}} = 1 - S_a \, Ro_a \tag{3.15}$$

$$\overline{R}_{\text{bot}} = 1 - R_{\text{bot}} = 1 - S_b \, Ro_b \tag{3.16}$$

then,

$$\begin{aligned} R_{\text{t/b}} &= 1 - \overline{R}_{\text{top}} \, \overline{R}_{\text{bot}} = 1 - (1 - S_a \, Ro_a) \times (1 - S_b \, Ro_b) \\ &= 1 - (1 - S_b \, Ro_b - S_a \, Ro_a + S_a \, Ro_a \, S_b \, Ro_b) \\ &= S_b \, Ro_b + S_a \, Ro_a - S_a \, Ro_a \, S_b \, Ro_b \end{aligned} \tag{3.17}$$

thus,

$$\begin{aligned} R &= R_{\text{t/b}} \times B \\ &= (S_b \, Ro_b + S_a \, Ro_a - S_a \, Ro_a \, S_b \, Ro_b) \times B \end{aligned} \tag{3.18}$$

Finally, the IPR reliability for the configuration shown in Figure 3.3(e) is obtained calculating first the reliability of the elements in parallel

$$S = 1 - \overline{S}_a \, \overline{S}_b \tag{3.19}$$

$$Ro = 1 - \overline{Ro}_a \, \overline{Ro}_b \tag{3.20}$$

thus,

$$R = S \times Ro \times B = \left(1 - \overline{S}_a \overline{S}_b\right) \times \left(1 - \overline{Ro}_a \overline{Ro}_b\right) \times B \tag{3.21}$$

System redundancy is obtained in two ways. Each component comprising the system may have one or more parallel components, or the entire system may be placed in parallel with one or more identical systems. The first case is referred to as low-level redundancy, and the second is referred to as high level redundancy [31]. Assuming that the intelligence and data router of an IPR forms a subsystem then, Figure 3.3(d) is representative of high-level redundancy, and Figure 3.3(e) of low-level redundancy. It will be shown below that the reliability of the low-level redundancy is greater than the reliability of the high-level redundancy [31]. Intuitively, this result can also be argued on the basis of the observation that both the low-level and the high-level redundant system will fail if either both components *S* fail or both components *Ro* fail. However, the high-level redundant system, Figure 3.3(d), may also fail if one *S* and one *Ro* fail, provided they fail on separate paths. Therefore, the high-level redundant system has additional failure modes.

To complete our example, reliability estimates of each component are needed. From [36] we have that "major failure per breaker year" estimate is 0.00672 for single-pressure high-voltage breakers above 63 kV (all voltages, from years 1988-1991). The reliability of high-voltage breakers can be calculated using (2.32)

$$R(t) = e^{-\lambda t}$$

assuming a constant failure rate (exponential failure distribution) [31]. Working with a one year period, the estimate for breakers reliability is $R(1) = B =$ 0.99330, or 99.330% of confidence.

From [39] we obtain the average MTBF of Ethernet routers to be 9.5 years, and for a price multiplier of 25, they are available with a 35 years MTBF. The reliability can be calculated from MTBF indices using (2.29)

$$R(t) = e^{-\frac{t}{MTBF}}$$

again, assuming a constant failure rate. For a one year period, the reliability found is $R(1) = Ro = 0.90009$ for a 9.5-years MTBF, or $R(1) = Ro = 0.97183$ for a 35-years MTBF.

Estimation of software reliability is not an easy task. To make a good estimate we need the total of code lines, loops, the frequency of each loops, the execution time, failure rate, fault density, etc. The software for an IPR is not available, so an estimate of its reliability is not possible. However, we assume a reliability of 0.95 and 0.99 in our example. We believe that these values are conservative, i.e. pessimistic since the controlling software on an IPR will no be extremely complex and its decisions will be based on pre-established contingency tables. The configurations with redundant software possibly will have two different algorithms that do the same procedures. If the two software are identical, there is a chance that in the event that software "*A*" (S_a) fails the

software "*B*" (S_b) will fail too when it comes to backup software "*A*" since both will have the same "bug".

Using equations 3.8, 3.10, 3.12, 3.18, and 3.21 to obtain the reliabilities of the configurations shown in Figure 3.3(a), (b), (c), (d), and (e) respectively, with $S = 0.95$, $Ro = 0.90009$, and $B = 0.99330$, we have

(a) $R = S \times Ro \times B = 0.95 \times 0.90009 \times 0.99330 = 0.84936$

(b) $R = \left(1 - \overline{S}_a \overline{S}_b\right) \times Ro \times B = (1 - (1 - 0.95)^2) \times 0.90009 \times 0.99330 = 0.89182$

(c) $R = S \times \left(1 - \overline{Ro}_a \overline{Ro}_b\right) \times B = 0.95 \times (1 - (1 - 0.90009)^2) \times 0.99330 = 0.93422$

(d) $R = (S_b\, Ro_b + S_a\, Ro_a - S_a\, Ro_a\, S_b\, Ro_b) \times B$

$= (0.95 \times 0.90009 + 0.95 \times 0.90009 - 0.95^2 \times 0.90009^2) \times 0.99330$

$= 0.96393 \times 0.99330 = 0.97244$

(e) $R = \left(1 - \overline{S}_a \overline{S}_b\right) \times \left(1 - \overline{Ro}_a \overline{Ro}_b\right) \times B$

$= (1 - (1 - 0.95)^2) \times (1 - (1 - 0.90009)^2) \times 0.99330 = 0.98093$

As said before, reliability is defined as the probability that a system (component) will function over some time period *t*, and it can be expressed as $R(t) = P\{T \geq t\}$, where *T* is a random variable of the time to failure of the system. If we define

$$F(t) = 1 - R(t) = P\{T < t\} \tag{3.22}$$

then, $F(t)$ is the probability that a failure occurs before time *t*. $F(t)$ is referred as the cumulative distribution function (CDF) of the failure distribution, and is normally used

when failure probabilities are being computed [31]. Using equation 3.22 the failure probabilities for each IPR configuration becomes:

(a) $F = 1 - R = 1 - 0.84936 = 0.15064$

(b) $F = 1 - 0.89182 = 0.10818$

(c) $F = 1 - 0.93422 = 0.06578$

(d) $F = 1 - 0.97244 = 0.02756$

(e) $F = 1 - 0.98093 = 0.01907$

Table 3.1 summarizes the results of reliabilities and failure probabilities for each configuration of Figure 3.3. The results show, as expected, that non-redundant configurations have lower reliabilities, or higher failure probabilities. Introducing redundancy in at least one of the components, the reliability of the system increases considerably, and reduces the probability of failure. The configurations shown in Figure 3.3(d) and 3.3(e) achieved the highest reliabilities. Also, the increase in reliability in these two configuration with the router of 35-years MTBF $\{Ro = 0.97183\}$ is not considerable, so the 25 times price increase may not be justified. A closer look to these reliabilities also proves that a system with low-level redundancy, configuration in Figure 3.3(e), has higher reliability than a system with high-level redundancy, configuration in Figure 3.3(d).

The reliability of the each IPR configuration is lower than the reliability of the breaker alone. We expect these results because the reliability in a series system will be

less than the lowest reliability of its components. All our IPR configurations reduce to a series configuration. The only way that the reliability of IPR can be greater than the reliability of the breaker is if we provide a redundant path to the breaker. The classical methods do not capture properly the increase in the reliability of a power system when a special protection scheme (SPS) is included. The next chapter analyzes the increase in reliability using the Risk Assessment approach for a system with and without IPRs.

TABLE 3.1 - Reliabilities and Failure Probabilities of IPR Configurations

IPR Configuration	$S = 0.95$ $Ro = 0.90009$ $B = 0.99330$		$S = 0.95$ $Ro = 0.97183$ $B = 0.99330$		$S = 0.99$ $Ro = 0.90009$ $B = 0.99330$		$S = 0.99$ $Ro = 0.97183$ $B = 0.99330$	
	R	*F*	*R*	*F*	*R*	*F*	*R*	*F*
(a)	0.84936	0.15064	0.91705	0.08295	0.88512	0.11488	0.95567	0.04433
(b)	0.89182	0.10818	0.96291	0.03709	0.89397	0.10603	0.96522	0.03478
(c)	0.93422	0.06578	0.94289	0.05711	0.97355	0.02645	0.98259	0.01741
(d)	0.97244	0.02756	0.98745	0.01255	0.98152	0.01842	0.99187	0.00813
(e)	0.98093	0.01907	0.99003	0.00997	0.98329	0.01671	0.99241	0.00759

4 RISK ASSESSMENT

The previous chapters discussed the two main methods used in a power system assessment. In [18] the steps involved in a deterministic method are summarized. These are:

1. Develop a base case model of the power system and identify the critical parameters.
2. Develop a contingency list for each critical parameter.
3. Identify the most limiting credible contingency, or contingencies, for each critical parameter.
4. Identify the limit for each critical parameter as the level where system performance following the most limiting contingency first violates minimum operating reliability criteria.

The criterion for judging operating point acceptability is then based on the identified limit. Thus, an operating point beyond this limit is unacceptable [18]. In the mean time, one of the IEEE Standard definitions for risk is the "product of probability and consequence". The Risk Assessment or Risk-Based Security Approach (RBSA) starts from the deterministic approach in those steps 1 and 2. However, the risk-based security approach differs from the deterministic approach in the following way: “whereas the deterministic approach develops limits based on the most severe contingencies, the risk-based security approach develops limits based on a composite measure computed from a risk contribution from all contingencies in the list, where risk is the product of probability

and consequence" [18]. In other words, the risk-based security approach analyzes all contingencies, and not only the most severe.

The main difference in the two approaches resides not in the methods used to obtain the results. Instead, the main difference in the two approaches resides in the criterion used to judge operating point acceptability. Whereas one uses a deterministic criterion (stable or unstable for most severe contingency under worst-case disturbance scenario), the other uses a criterion based on probability and consequence (composite risk level from all contingencies). Therefore, the RBSA extends the deterministic approach. One of the appeals of this approach is ease of transition for system operators; the change is transparent to the operators except for new graphs and tables [18].

4.1 Benefits of RBSA

RBSA offers various benefits compared to traditional methods. For system operators this approach is appealing because it is easier to understand numerical values in terms of money (in the case that the impact has been measured in economic costs) rather than a simple index. It can bridge economics and security because the method measures the economic consequence of an uncertainty weighted by its probability of occurrence. Therefore, it is a means to explicitly include security in ordinary economic decision-making problems. The other benefits of the RBSA, aside of the economic-security bridge, are [16]:

- *A leading indicator*. The basic application of the risk index is to use available information to decide "now" in preparation for a condition that is minutes, hours, weeks, or years into the future.
- *Risk as a Function of Operating Condition.* Results of RBSA are provided so as to illustrate the functional dependence of risk on pre-contingency operating conditions that operators are able to monitor, understand, and control.
- *Risk is assignable*. Because risk is computed for each security problem, each contingency, and each component, it is easy to identify components or conditions causing it and incurring it.
- *Composite Risk*. The risk computation reflects the composite effect of all contingencies and all resulting security problems, resulting in a measure of the overall security level of the region.
- *Cumulative Risk*. Risk can be calculated for each operating condition, and summation over all time instances provides a cumulative risk assessment over the specified time period.
- *Risk Preferences*. RBSA provides the capability to manage security based on the decision maker(s) preference regarding risk exposure.

In measuring risk, it is essential that we differentiate between an outcome and a decision. An outcome is an unavoidable result of a decision. Based on this, we can classify transmission reinforcement, unit commitment, economic dispatch, and load interruption as decisions. The outcomes of these decisions are the effects on the circuits. These effects, which include equipment damage and equipment unavailability, are

random because they are heavily dependent on weather and on loadings, the randomness of the latter caused mainly by uncertainties in demand and equipment outages. The RBSA is in terms of the probability and monetary impact of these effects, given a decision. Calculation of the risk index has the distinct advantage of providing a uniform basis of comparing various decisions. In comparison, reliability evaluation of circuit overload, using a load interruption-based index like LOLP, requires that the load interruption policy remain fixed throughout the study. The problem with this approach lays in the elimination a degree of freedom in the decision space, and because there is no guarantee that the programmed load interruption policy is the same as the one that will actually be used [19].

4.2 Risk Assessment Procedure and Example

In [25] and [40] McCalley and Fu developed a seven-step procedure for risk quantification applied to a system with and without SPS (specifically for a generation rejection scheme). This procedure will be used to apply it for a system with and without IPRs.

4.2.1 Collect Information

First of all, is necessary to have a good knowledge of the system to be analyzed and the operational layout of the protection system to be used. The latter has been already done in Chapter 3. For our analysis we are going to use the 179-bus equivalent of the

western region of the United States (WSCC/WECC). It has a total of 179 buses, 263 lines, 29 generator, and 104 loads. Table 4.1 summarizes the load/generation case totals.

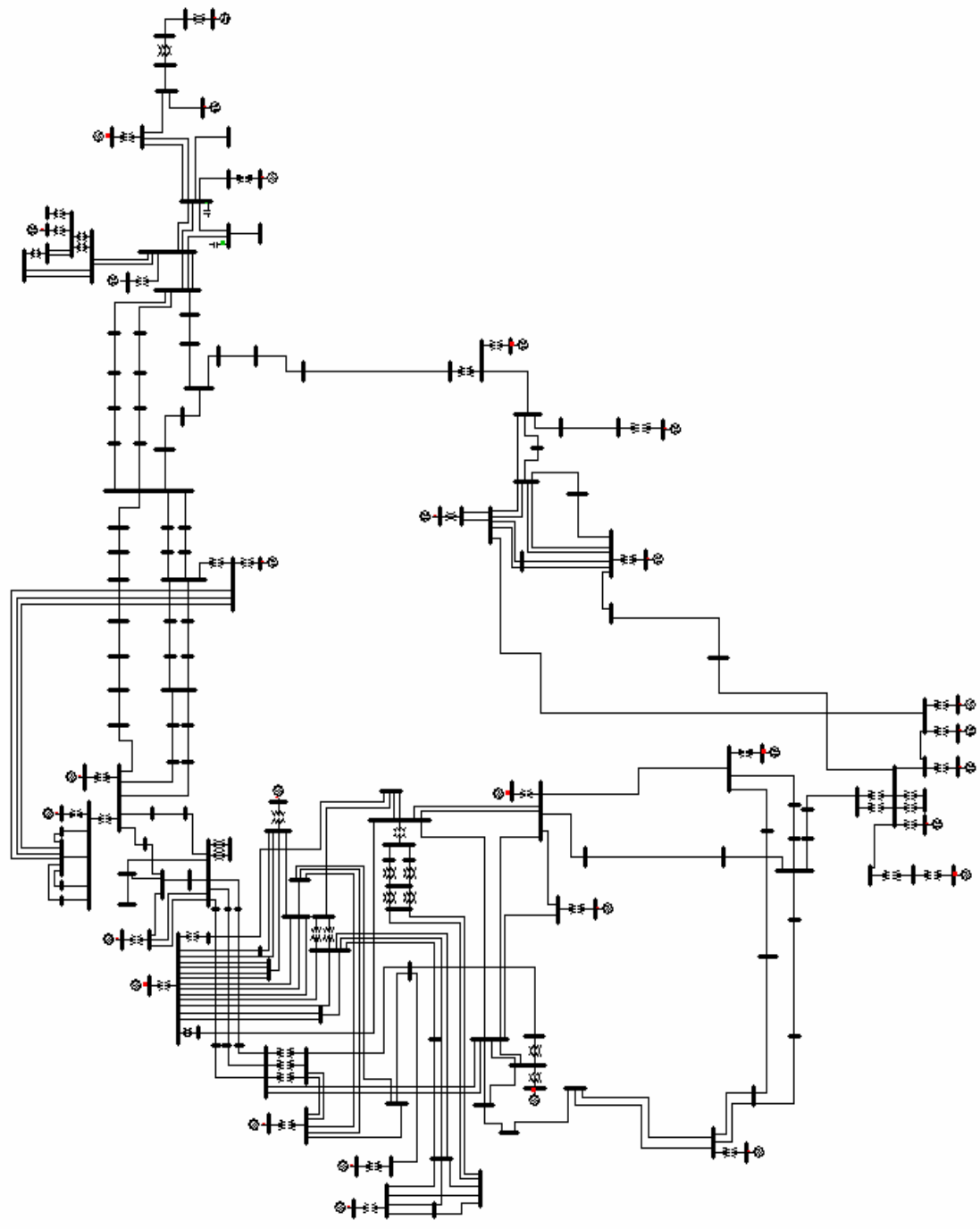

FIGURE 4.1 - WSCC 179-bus System

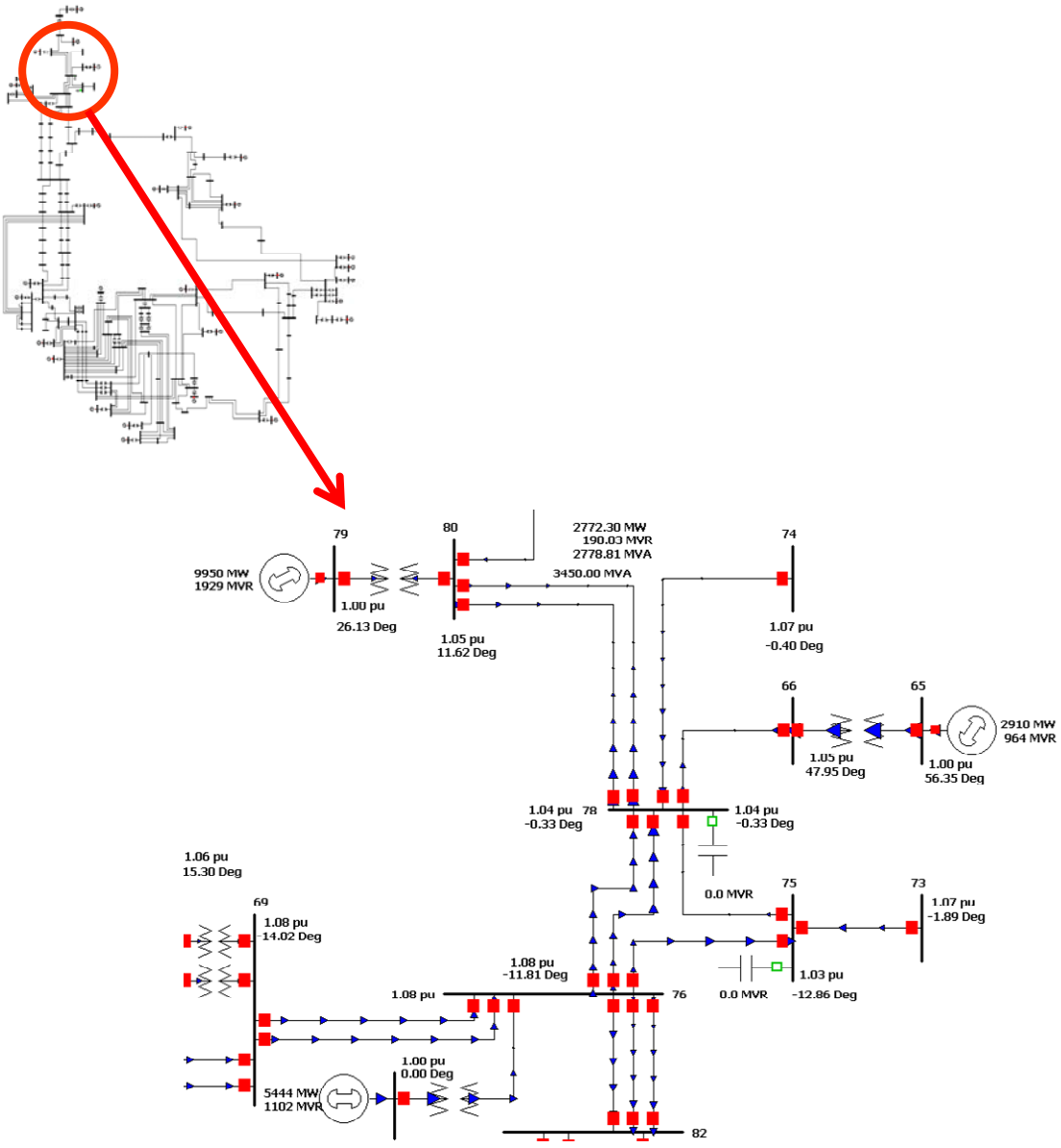

FIGURE 4.2 – Study Zone

TABLE 4.1 - Case Totals for 179-bus System

	MW	**MVar**
Load	61007	16095
Generation	61680	14284
Shunts	-	-4896
Losses	672	3085

In [41] a contingency set that leads the system to a voltage collapse is analyzed. The initial contingency corresponds to a three phase fault in line $L_{76\text{-}82}$. This contingency is followed by a line tipping between buses 76 and 78, then another tripping between buses 78 and 80. We modified this set because we figured out that only a simultaneous or successive outage of lines $L_{76\text{-}78}$ and $L_{78\text{-}80}$ is necessary to start a voltage collapse due an insufficiency of reactive power in that zone (Figure 4.3, dark areas). To alleviate this problem buses B_{75} and B_{78} need a VAR compensator of 350 and 450Mvar respectively. The proposed IPR for this case will monitor these lines, and connect the compensators promptly or sequentially (to minimize problems like inrush currents, etc.) in the event of one line outage to prevent a system collapse if the other line go out-of-service too. Figure 4.4 shows the components of the IPR. In this case, two (2) breakers will share the same software and router. It is assumed that line sensors are fully reliable, but they can be introduced in the analysis without further complication.

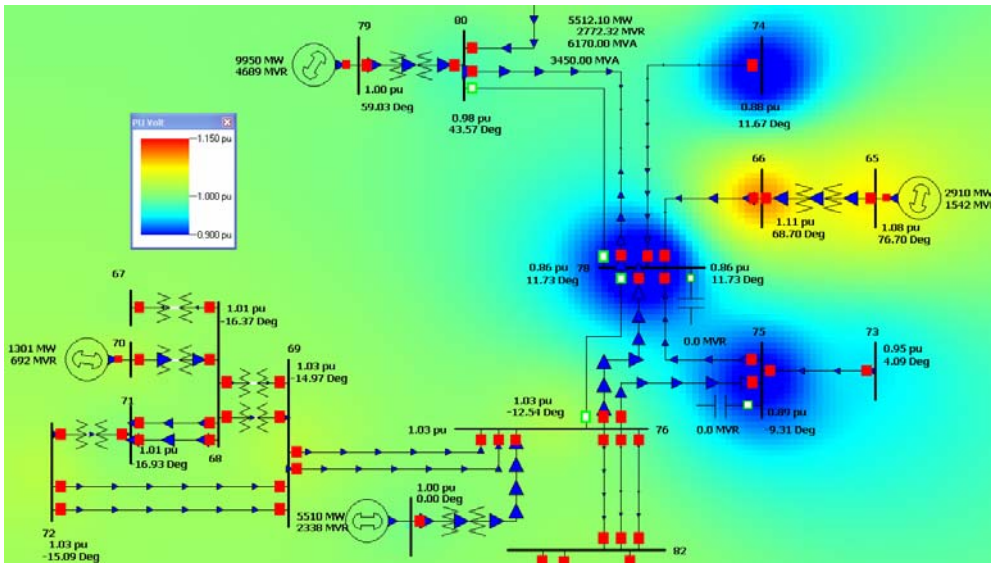

FIGURE 4.3 - Voltage Contour (snap shot) of voltage collapse

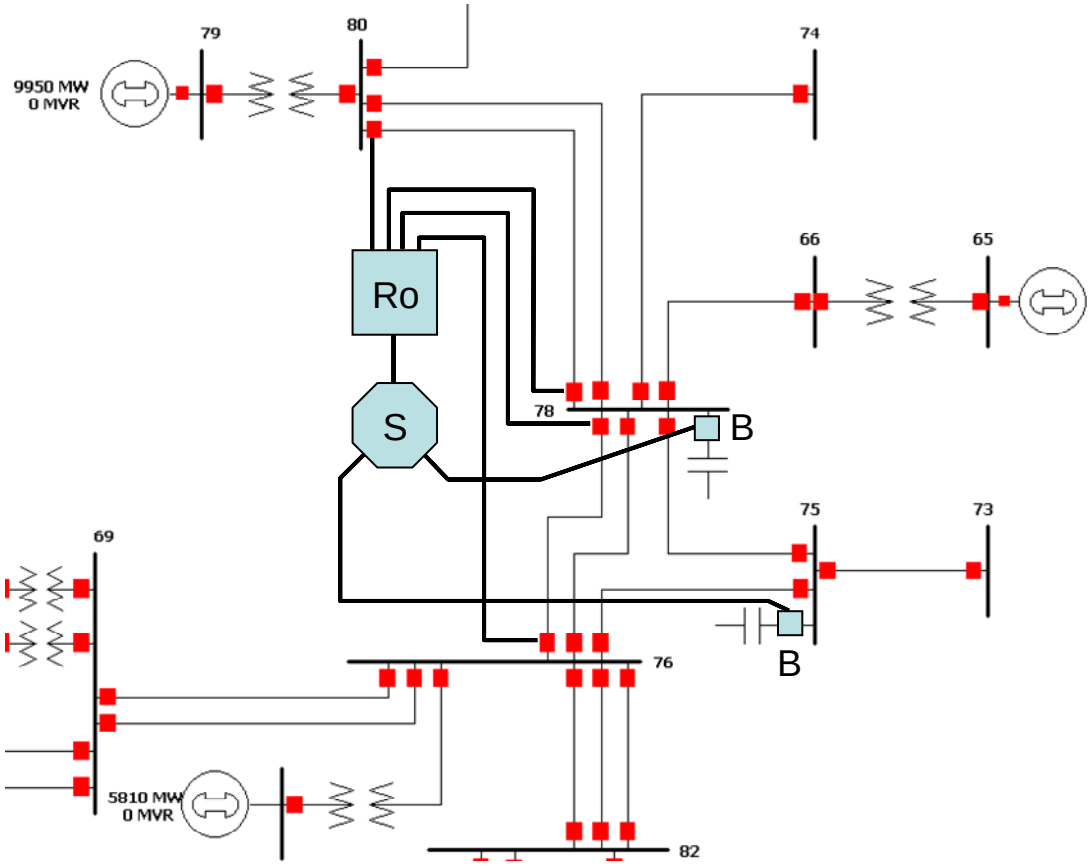

FIGURE 4.4 – IPR layout

Let:

- F_j: event there is a fault on circuit j ($L_{76\text{-}78}$, $L_{78\text{-}80}$) $j = 1, 2, \ldots, N_C$
- N_C: number of critical circuits
- N_T: total number of events considered in the study
- E_i: initiating events $i = 1, 2, \ldots, N_C, N_C+1, N_C+2, \ldots N_T$
  - The first N_C event correspond to "N-1" outage,

$$E_i = \overline{F_1} \cap \overline{F_2} \cdots \overline{F_{i-1}} \cap F_i \cap \overline{F_{i+1}} \cdots \overline{F_{N_C}}$$

- The N_C +1 event correspond to no fault,

$$E_{N_C+1} = \overline{F_1} \cap \overline{F_2} \cap \cdots \cap \overline{F_{N_C}}$$

- Events E_i, $i > N_C$+1 correspond to simultaneous outage of two or more circuits

- K: system collapse event
- X: pre-contingency operating point
- T: IPR switching event
- $Risk(\cdot)$, $I(\cdot)$, $P(\cdot)$: risk, impact, and probability of a event, respectively.

4.2.2 Identify initiating events

An initiating event can be a line outage, a generator tripping, load dropping, etc. The purpose of this step is to identify the set of initiating events that are going to be part of our analysis. If we want to calculate the system risk with and without IPR it is necessary to include the events which activate the IPR. However, if we want the system total risk, all initiating events need to be included.

In our study, the outages of lines $L_{76\text{-}78}$ and $L_{78\text{-}80}$ induce a voltage collapse of the system. Both outages become our basic events. It implies that our study has four initiating events ($2^2 = 4$).

Basic events: F_1, loss of line $L_{76\text{-}78}$

F_2, loss of line $L_{78\text{-}80}$

Initiating Events E_1, loss of line $L_{76\text{-}78}$

E_2, loss of line $L_{78\text{-}80}$

E_3, no outage

E_4, loss of both lines

4.2.3 Identify Risk Sources

The purpose of the IPR in our study is to connect the VAR compensators for the prevention of a voltage collapse. Usually, the risk in a SPS comes from hardware or software failure, a faulty design logic, or human error. In this example only hardware and software failure is assumed to be the source of risk. The operation of an IPR is classified into one of the following categories:

1. IPR works correctly in a contingency $(T \cap E_i)$ $\quad i = 1, 2, \ldots N_C, N_C+2, \ldots N_T$
2. IPR does not work correctly in a contingency $\left(\overline{T} \cap E_i\right)$
3. IPR acts when there is no contingency $\left(T \cap E_{N_C+1}\right)$. A failure.
4. IPR does not act and there is no contingency $\left(\overline{T} \cap E_{N_C+1}\right)$. A situation established only to achieve completeness in the mathematical formulation of the problem.

According to these categories, the risk for the system with IPR comes from three sources:

Source 1. IPR fails to work in a contingency. The power system may or not may collapse depending on the pre-fault operating condition.

Source 2. IPR works promptly and correctly, the system will no collapse. Depending on the assessment, zero or non-zero impact will occurs.

Source 3. IPR works unnecessary when there is no outage. Zero or non-zero impact will occur depending on the assessment.

4.2.3.1 Risk Model Development

The risk of an event E_i, i = 1, 2, … which causes IPR to act or system collapse K, given that the system is at X operating point is denoted $Risk\left(\left(K \cup T\right) | X\right)$. For simplicity, from now on the dependence on X will not be explicitly showed in the notation. It is understood that the risk assessment is operating point dependant. Then, the risk is given by

$$Risk\left(K \cup T\right) = \sum_{i=1}^{N_T} Risk\left(E_i\right) = \underbrace{\sum_{i=1}^{N_T} P\left(K \cap \overline{T} \cap E_i\right) \times I\left(K \cap \overline{T} \cap E_i\right)}_{source\#1} + \underbrace{\sum_{i=1}^{N_T} P\left(T \cap E_i\right) \times I\left(T \cap E_i\right)}_{source\#2\&3} \tag{4.1}$$

The first term is caused by source one, where there is a system collapse, while the second term is caused by sources two and three when there is no collapse. The term $P\left(K \cap \overline{T} \cap E_i\right)$ is the probability of IPR failure $\overline{T}$, resulting in a system collapse K. using conditional probability this term can be expressed as,

$$P\left(K \cap \overline{T} \cap E_i\right) = P\left(\overline{T} \cap E_i\right) \times P\left(K \mid \left(\overline{T} \cap E_i\right)\right) \tag{4.2}$$

4.2.4 IPR Reliability Assessment

Chapter 3 discussed the failure rate and reliability of each IPR's components, and the reliability of an IPR as a "whole" was calculated. However, for the following assessment is only necessary the failure rate of each component. We choose Markov modeling to perform reliability assessment, because its flexibility, it can incorporate independent and common failures, partial and full repairs, etc, and all of these features can be modeled as a function of time. As Section 2.6.6.1 mentioned, FMEA (Failure Mode and Effect Analysis) can be an initial step for Markov modeling. McCalley and Fu [40] recommended the following steps in a SPS evaluation if FMEA and Markov methods are used: 1) describe the system, 2) complete FMEA, 3) develop Markov model, 4) simplify Markov Model, and 5) calculate state probabilities.

4.2.4.1 Describe the system

The IPR diagram is shown in Figure 4.4, and it has been already discussed in Section 4.2.1. The IPR will respond to four initiating events: outage of line $L_{76\text{-}78}$ or $L_{78\text{-}80}$, no outage, or the outage of both lines. The probability formulation for each event is summarized in Table 4.2.

TABLE 4.2 - Initiating events probabilities

Event	Line Outage	Probability
E_1	$L_{76\text{-}78}$	$P(E_1) = P(F_1)P(\overline{F_2})$
E_2	$L_{78\text{-}80}$	$P(E_2) = P(\overline{F_1})P(F_2)$
E_3	none	$P(E_1) = P(\overline{F_1})P(\overline{F_2})$
E_4	$L_{76\text{-}78}$ and $L_{78\text{-}80}$	$P(E_1) = P(F_1)P(F_2)$

4.2.4.2 Complete system level FMEA

In this step all the IPR components are identified and listed. For each component, all failure modes and system effects should be identified. In our case, each IPR component (*Ro*, *S*, and *B*) can have two modes: 0-working, 1-failure. Before to continue, we must characterize the failure mode for each component:

B: 0, the breaker switch properly

1, the breaker does not close

Ro: 0, the router communicates properly

1, the router does not send any information

S: 0, the software works properly

1, the software takes an incorrect (opposite) decision

TABLE 4.3 - FMEA list

Component	Failure Mode	Failure rate λ (per year)	Failure rate λ (per day)
Router	1	0.10526	$\lambda_1 = 0.000288392$
Software	1	0.05129	$\lambda_2 = 0.00014053$
Breaker	1	0.00672	$\lambda_3 = 0.0000184110$

These values of Table 4.3 were obtained from the MTBF, MTTF or the annual failure for each component (literature). The failure rate of the router (λ_1) was obtained from its MTBF of 9.5 years. The daily rate of the software (λ_2) was calculated from the assumed reliability of 0.95 and converted to the failure rate per year of 0.05129. Finally, the failure rate of the breaker (λ_3) was obtained from literature.

4.2.4.3 Develop the Markov Model

First, the states need to be defined. There are represented by the combination of states of all system components. The IPR shown in Figure 4.4 will have 16 states ($\underbrace{2}_{R}\times\underbrace{2}_{S}\times\underbrace{2}_{B}\times\underbrace{2}_{B}=2^4=16$), because we are considering only two modes (working and failure). Since it has four components, each state will have four digits (d_1 d_2 d_3 d_4), each one corresponding to R, S, B_1 and B_2 respectively. The development of a Markov model starts from a state in which all components are successful, usually numbered as zero, then follow the rule: "for any successful state, list all failure rates for all successful components" [40]. Then, the sixteen states obtained are

0000	0001	0010	0011
0100	0101	0110	0111
1000	1001	1010	1011
1100	1101	1110	1111

Some states are identical (e.g., 0010 and 0001), since both breakers play the same role in the system. Merging these identical states, the resulting states are:

S_0 – 0000	S_1 – 0001, 0010
S_2 – 0011	S_3 – 0100
S_4 – 0101, 0110	S_5 – 0111
S_6 – 1000	S_7 – 1001, 1010
S_8 – 1011	S_9 – 1100
S_{10} – 1101, 1110	S_{11} – 1111

Here S_0, S_1, … S_n represents a state space of the IPR, where S_p is a set of mutually and exhaustive states. Then each step can be classified in the following categories based on the response of each estate to system input events:

- C_1: If there is an active signal (*AS*, initiating event), the IPR works properly. If there is an inactive signal (*IS*, initiating event) IPR works unnecessary.
- C_2: If there is an *AS*, the IPR works properly. If there is an *IS*, IPR does not switch (works properly).
- C_3: If there is an *AS*, the IPR does not work properly. If there is an *IS*, IPR works unnecessary.
- C_4: If there is an *AS*, the IPR does not work properly. If there is an *IS*, IPR does not switch (works properly).

For example, S_9 (1100), is classified in C_1 because when there is an *AS* the router remains "quiet" since it is in failure mode, the software takes the opposite decision (failure) based in the last operational point received (just before the failure of the router,

e.g. no outages), so it switches the capacitors resulting in a successful IPR operation. However, if the signal is inactive *IS* the same situation occurs: the router remains "quiet" since it is in failure mode, the software takes the opposite decision, so it switches the capacitors resulting in a unnecessary IPR operation. The other states can be classified as follows

$$C_1: S_9$$

$$C_2: S_0$$

$$C_3: S_3, S_4, S_{10}$$

$$C_4: S_1, S_2, S_5, S_6, S_7, S_8, S_{11}$$

The resulting Markov chain is given by the next Figure.

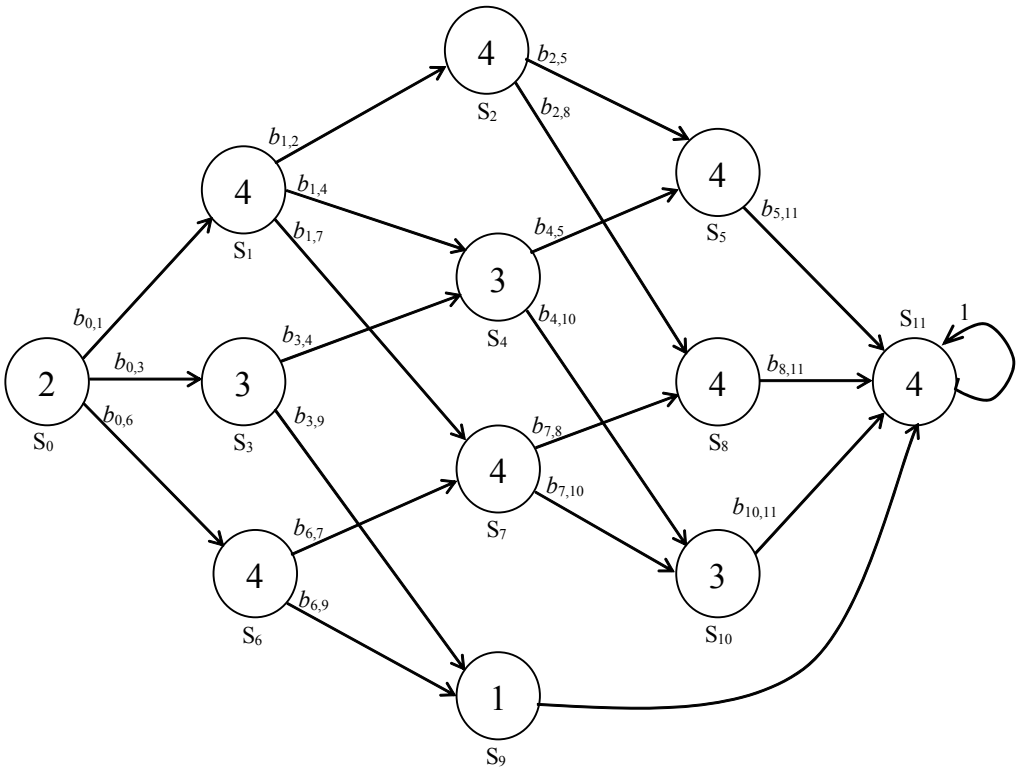

FIGURE 4.5 - Markov Chain

4.2.4.4 Simplify the Markov Model

Since our model is quite small, is not necessary to reduce it further. Nonetheless, the steps to reduce a Markov model are discussed. First of all, two concepts are used before the steps, and these are:

- A transition state is a state that has non-zero entry transition probability from other state(s) and non zero exit transition probability to other state(s).
- An absorbing state is a state that has a 1.0 transition probability to itself.

Then, the reduction steps are as follows:

1. Merge absorbing state belonging to the same class. Entry transition probabilities are added.
2. For each absorbing state, eliminate all preceding states that a) are in the same class C_k as the absorbing state: b) have only one exit transition probability. Add the entry probabilities as the entry probabilities to the absorbing states.
3. Merge all transition states in the same class C_k that have identical transition probabilities to common states. Entry probabilities are added. Exit probabilities remain the same.

4.2.4.5 Calculate State Transition Probabilities

The failures of the IPR components are assumed to have an exponential distribution, therefore the PDF of component failure is $f(t) = \lambda e^{-\lambda t}$, where λ stands for

the failure rate per unit interval. The probability that a component fails before time t is given by

$$F(t) = \int_0^t \lambda e^{-\lambda t} dt = 1 - e^{-\lambda t} \approx \lambda t \tag{4.3}$$

Where the approximation improves as λt gets small. With this mode, a $n + 1$ by $n + 1$ transition matrix B is obtained, where b_{pq} (p, q = 0, 1, …n) indicates the probability that the system transfers from S_p to S_q, and n stands for the number of states. Basically, we are approximating a continue Markov chain as a discrete chain.

Assuming a probability list at initial time $t = t_0$ is:

$$P_L^{(0)} = \left(P\left(S_0'(t_0)\right) \cdots P\left(S_n'(t_0)\right) \right) \tag{4.4}$$

and after m intervals, the probability list using the Chapman-Kolmogorov equations is:

$$P_L^{(m)} = \left(P\left(S_0'(t_m)\right) \cdots P\left(S_n'(t_m)\right) \right) = P_L^{(0)} \times B^m \tag{4.5}$$

The elements in the probability list $P_L^{(m)}$ provide the probability that the system is in state S_p' after m time intervals. Then

$$\begin{aligned}
P(C_1) &= \sum P\left(S_p'\right) \qquad S_p' \in C_1 \\
P(C_2) &= \sum P\left(S_p'\right) \qquad S_p' \in C_2 \\
P(C_3) &= \sum P\left(S_p'\right) \qquad S_p' \in C_3 \\
P(C_4) &= \sum P\left(S_p'\right) \qquad S_p' \in C_4
\end{aligned}$$

We can abbreviate the transition which exits from each state as follows,

$$
\begin{aligned}
b_0 &= 1 - b_{0,6} - b_{0,3} - b_{0,1} & \qquad b_6 &= 1 - b_{6,9} - b_{6,7} \\
b_1 &= 1 - b_{1,7} - b_{1,4} - b_{1,2} & \qquad b_7 &= 1 - b_{7,10} - b_{7,8} \\
b_2 &= 1 - b_{2,8} - b_{2,5} & \qquad b_8 &= 1 - b_{8,11} \\
b_3 &= 1 - b_{3,9} - b_{3,4} & \qquad b_9 &= 1 - b_{9,11} \\
b_4 &= 1 - b_{4,10} - b_{4,5} & \qquad b_{10} &= 1 - b_{10,11} \\
b_5 &= 1 - b_{5,11}
\end{aligned}
$$

where

$$
\left.\begin{matrix} b_{0,6} \\ b_{1,7} \\ b_{2,8} \\ b_{3,9} \\ b_{4,10} \\ b_{5,11} \end{matrix}\right\} \approx \lambda_1 \qquad
\left.\begin{matrix} b_{0,3} \\ b_{1,4} \\ b_{2,5} \\ b_{6,9} \\ b_{7,10} \\ b_{8,11} \end{matrix}\right\} \approx \lambda_2 \qquad
\left.\begin{matrix} b_{1,2} \\ b_{4,5} \\ b_{7,8} \\ b_{10,11} \end{matrix}\right\} \approx \lambda_3 \qquad
\left.\begin{matrix} b_{0,1} \\ b_{3,4} \\ b_{6,7} \\ b_{9,11} \end{matrix}\right\} \approx 2\lambda_3
$$

are the transition probabilities approximated with (4.3) for t = 1 day. Arranging these probabilities, the following state transition matrix (B) is obtained:

$$
B = \begin{pmatrix}
b_0 & b_{0,1} & 0 & b_{0,3} & 0 & 0 & b_{0,6} & 0 & 0 & 0 & 0 & 0 \\
0 & b_1 & b_{1,2} & 0 & b_{1,4} & 0 & 0 & b_{1,7} & 0 & 0 & 0 & 0 \\
0 & 0 & b_2 & 0 & 0 & b_{2,5} & 0 & 0 & b_{2,8} & 0 & 0 & 0 \\
0 & 0 & 0 & b_3 & b_{3,4} & 0 & 0 & 0 & 0 & b_{3,9} & 0 & 0 \\
0 & 0 & 0 & 0 & b_4 & b_{4,5} & 0 & 0 & 0 & 0 & b_{4,10} & 0 \\
0 & 0 & 0 & 0 & 0 & b_5 & 0 & 0 & 0 & 0 & 0 & b_{5,11} \\
0 & 0 & 0 & 0 & 0 & 0 & b_6 & b_{6,7} & 0 & b_{6,9} & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & b_7 & b_{7,8} & 0 & b_{7,10} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & b_8 & 0 & 0 & b_{8,11} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & b_9 & 0 & b_{9,11} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & b_{10} & b_{10,11} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}
$$

$P(S_p(t_0))$ provides the probability that the system is in state p at time $t = t_0$. In time $t = t_0$ every component is assumed to be working properly. Therefore

$$\begin{aligned} P_L^{(0)} &= \left(P\left(S_0\left(t_0\right)\right) \quad P\left(S_1\left(t_0\right)\right) \quad \cdots\cdots P\left(S_{11}\left(t_0\right)\right)\right) \\ &= \left(1 \quad 0 \quad \cdots \quad 0\right) \end{aligned} \tag{4.6}$$

After m time intervals from time $t = t_0$ the probability is

$$\begin{aligned} P_L^{(m)} &= \left(P\left(S_0\left(t_m\right)\right) \quad P\left(S_1\left(t_m\right)\right) \quad \cdots\cdots P\left(S_{11}\left(t_m\right)\right)\right) \\ &= P_L^{(0)} \times B^m \end{aligned} \tag{4.7}$$

The elements in the probability list $P_L^{(365)}$ provide the probability that the system is in state S_p after 365 time intervals, i.e. one year, because the time interval is chosen to be one day. Substituting the failure rate in the transition matrix, and using (4.7) gives:

$$\begin{aligned} P_L^{(365)} = P_L^{(0)} \times B^{365} = \big(&8.4363\times10^{-1} \quad 1.1382\times10^{-2} \quad 3.8283\times10^{-5} \\ &4.4420\times10^{-2} \quad 5.9760\times10^{-4} \quad 2.0044\times10^{-6} \\ &9.3678\times10^{-2} \quad 1.2602\times10^{-3} \quad 4.2264\times10^{-6} \\ &4.9178\times10^{-3} \quad 4.3588\times10^{-5} \quad 2.2602\times10^{-5}\big) \end{aligned}$$

Since S_1 correspond to category C_1, S_0 to C_2, and so on, the probabilities for each category are,

$$P(C_1) = P(S_9) = 4.9178 \times 10^{-3}$$
$$P(C_2) = P(S_0) = 8.4363 \times 10^{-1}$$
$$P(C_3) = P(S_3) + P(S_4) + P(S_{10}) = 4.4420 \times 10^{-2} + 5.9760 \times 10^{-4} + 4.3588 \times 10^{-5} = 4.5061 \times 10^{-2}$$
$$P(C_4) = P(S_1) + P(S_2) + P(S_5) + P(S_6) + P(S_7) + P(S_8) + P(S_{11})$$
$$= 1.1382 \times 10^{-2} + 3.8283 \times 10^{-5} + 2.0044 \times 10^{-6} + 9.3678 \times 10^{-2} + 1.2602 \times 10^{-3} +$$
$$4.2264 \times 10^{-6} + 2.2602 \times 10^{-5} = 1.0639 \times 10^{-1}$$

4.2.5 Impact Assessment

The impact associated with IPR failure to connect the VAR compensators resulting in a system collapse is denoted as $I\left(K \cap \overline{T} \cap E_i\right)$. If the information is available, we can include redispatch, startup cost, re-energization of lines, etc. If the IPR connect the VAR compensators the impact associated is denoted as $I\left(T \cap E_i\right)$. This impact is non-zero too, because there is a possible operational cost involved. However, the impact of the operation of such system should be much less that loosing the whole power system, or part of it.

The problem in our study is that there is no available (at that time) enough information to do an accurate economic impact assessment of the WCSS 179-bus system. Instead, we will do an estimate on the generation lost.

Vittal in [42] study the islanding phenomenon in the 179-bus system. From this reference, the system can be split in 2 or 3 areas. As part of our research we studied the

179-bus system and found out that is possible to split the system in five islands based on the following criteria:

- Load/generation balance
- Minimum set of interconnection lines (ties)

The next Table summarizes the generation and load for each island as a percentage of the total system. Figure 4.6 shows the island created based in the previous criteria. The studied contingency is located in zone **1a**. From Table 4.4 we know that the generation in that area is about 28,535 MW and the load is approximately 25,839 MW. If we assume that its islanding system (maybe another specialized IPR) is working properly, only the generation in zone **1a** will be lost in the event of a voltage collapse.

In [43] Billinton analyzes the economic cost of non-supply of different customer sectors based on a CIGRE report (TF 38.06.01). The report includes surveys done in Australia, Canada, Denmark, Great Britain, Greece, USA, and other countries. Figure 4.7 shows a comparison of economic sectors and their damage functions. Using this information, and assuming a certain load distribution between sectors we can estimate the customer impact depending the duration of the outage. For example, if we assume an outage duration of 10 hours the estimated cost is 60, 150, 50, and 10 $/kW for residential, commercial, industrial, and agricultural customers respectively. Then, the 25,839 MW of zone **1a** can be distributed in the following way:

- 40% - Residential load
- 25% - Commercial load
- 30% - Industrial Load

- 5% - Agricultural load

The estimated cost of interruption for all residential customers is about $620 millions (0.4 × 25,839,000 × 60 = $620,136,000). The same procedure results in estimated cost of $969 millions for commercial customer, $388 millions for the industry, and $13 millions in agriculture. The total customer loss exceeds the $1.99 billion mark. The utilities have an impact associated to redispatch of generation units, re-energization or lines, exchange of faulted components, the income loss of un-served load, etc. Since we do not have available the operational costs of the WSCC, we will estimate only the income loss of the un-served load. Assuming an average cost of 0.10 $/kWh, the income loss suffered by utilities is approximately $25.8 millions (25,839,000 × 0.10 × 10). Then, the total economic impact due to the loss of zone **1a** is $2.02 billions.

TABLE 4.4 - WSCC 179-bus generation and loading per area

Area name	Buses	Generators	Generation [MW]	% of Total Generation	Loads	Load [MW]	% of Total Load
1a	39	5	28534.59	46.2620879	10	25838.7	42.3531089
1b	18	4	5530	8.9655869	19	4748.5	7.78343097
1c	13	10	7020	11.3812694	39	5818.7	9.53763289
2a	42	4	5883	9.5378929	16	8821.5	14.4596265
2b	67	6	14712.7	23.8531628	20	15780.4	25.8662007
Totals	179	29	61680.29	100	104	61007.8	100

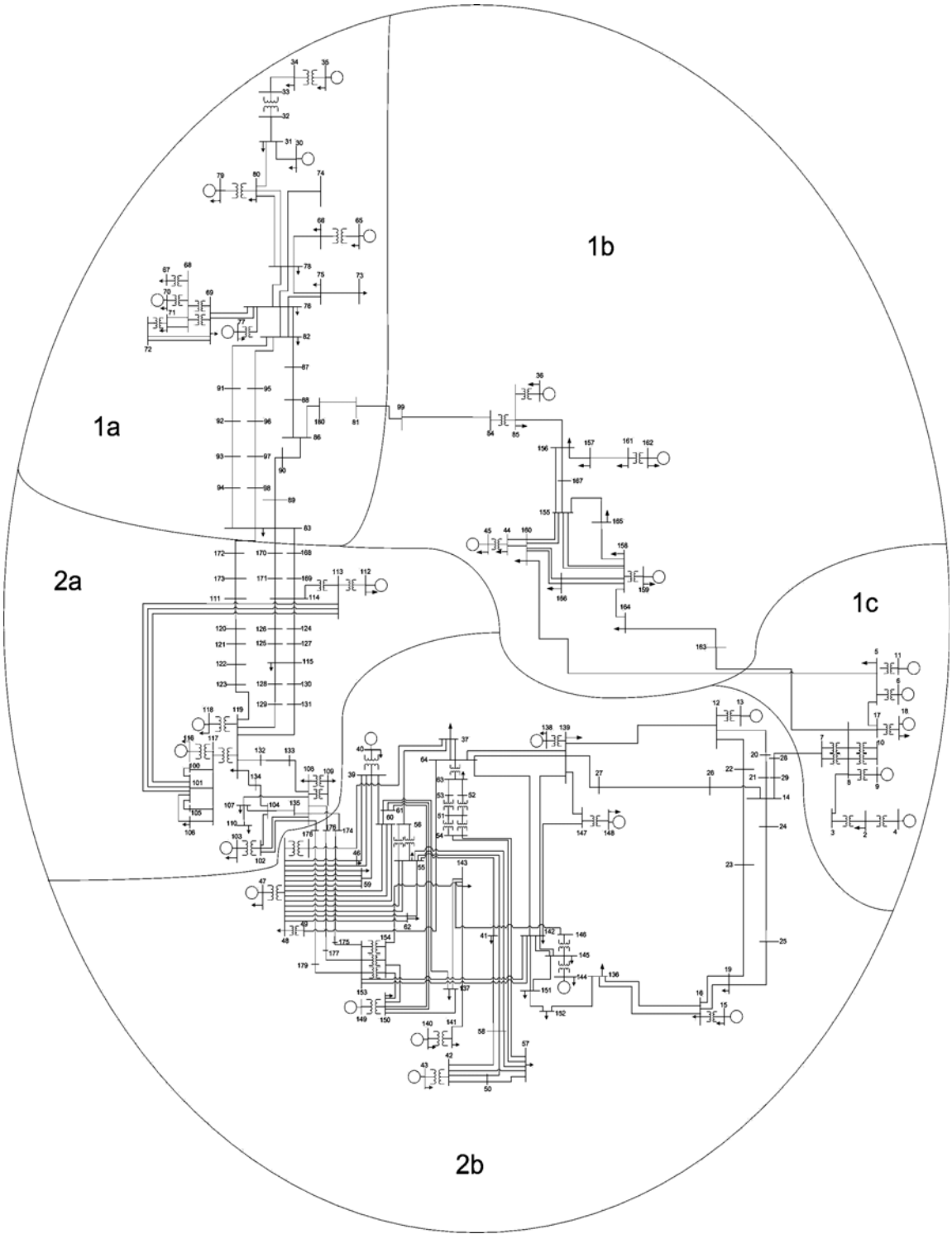

FIGURE 4.6 - WSCC 179-bus areas

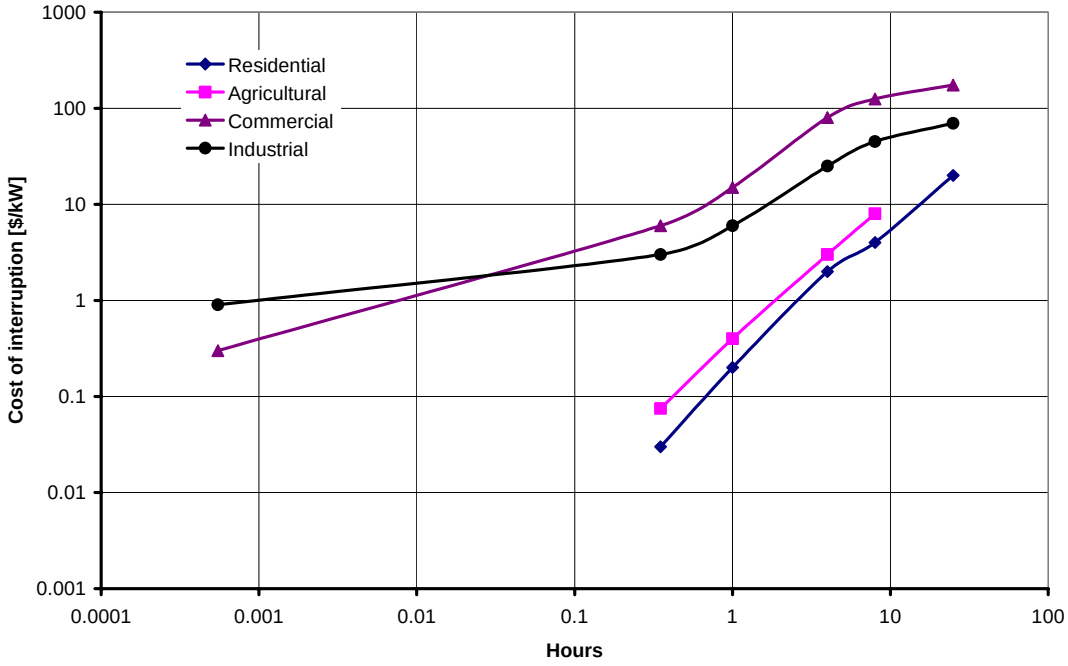

FIGURE 4.7 - Customer damage functions - comparison of economic sectors [43]

4.2.6 Evaluate Risk

First of all, we need to calculate $P(T \cap E_i)$ and $P(\overline{T} \cap E_i)$ for use in equations 4.1 and 4.2. Since $S = S_0, S_1, S_2, \ldots S_{11}$ represent a state space of the IPR, where S_p is a set of mutually and exhaustive states, then

$$\begin{aligned} P(E_i \cap T) &= P\left((E_i \cap T) \cap (S_0 \cup S_1 \cup S_2 \cup \cdots \cup S_n)\right) \\ &= \sum_{p=0}^{n} P(E_i \cap T \cap S_p) \\ &= \sum_{p=0}^{n} P(T \mid (E_i \cap S_p)) P(E_i \cap S_p) \end{aligned} \tag{4.8}$$

Since E_i is independent of S_p, $P(E_i \cap S_p) = P(E_i)P(S_p)$, or more clearly, the occurrence of a line outage is independent of the state of the IPR. Then

$$P\left(E_i \cap T\right) = \sum_{p=0}^{n} P\left(T \mid \left(E_i \cap S_p\right)\right) P\left(E_i\right) P\left(S_p\right) \tag{4.9}$$

and

$$P\left(E_i \cap \overline{T}\right) = \sum_{p=0}^{n} P\left(T \mid \left(E_i \cap S_p\right)\right) P\left(E_i\right) P\left(S_p\right) \tag{4.10}$$

Based on the state space of the categories C_k, in where the original state space have been condensed, we have

$$P\left(E_i \cap T\right) = \sum_{k=1}^{4} P\left(T \mid \left(E_i \cap C_k\right)\right) P\left(E_i\right) P\left(C_k\right) \tag{4.11}$$

$$P\left(E_i \cap \overline{T}\right) = \sum_{k=1}^{4} P\left(\overline{T} \mid \left(E_i \cap C_k\right)\right) P\left(E_i\right) P\left(C_k\right) \tag{4.12}$$

where,

$$\begin{aligned} P(E_i) &= P(F_j) \prod_{g \neq j} P(\overline{F}_g) \ , \qquad j = i \\ &= (1 - e^{-\lambda_j}) e^{\sum_{g \neq j} \lambda_g} \end{aligned} \tag{4.13}$$

This probability is obtained assuming that the fault process on a line is a homogeneous Poisson process [40], since F_1, F_2, … F_n are independent of each other. Each basic event E_i belongs to a group either active (*AC*) or inactive (*IN*). The active input is that one which warns the IPR to connect the compensators, and the inactive input is that one which not activates the IPR. Given the basic input events, E_i and C_k, the system output is determined. Then, the conditional probability terms in equations 4.11 and 4.12 is 0 or 1, as expressed below,

$$E_i \subset AC \rightarrow \begin{cases} P\left(T \mid \left(E_i \cap C_k\right)\right) = \begin{cases} 1 & k = 1,2 \\ 0 & k = 3,4 \end{cases} \\ P\left(\overline{T} \mid \left(E_i \cap C_k\right)\right) = \begin{cases} 1 & k = 3,4 \\ 0 & k = 1,2 \end{cases} \end{cases}$$

$$E_i \subset IN \rightarrow \begin{cases} P\left(T \mid \left(E_i \cap C_k\right)\right) = \begin{cases} 1 & k = 1,3 \\ 0 & k = 2,4 \end{cases} \\ P\left(\overline{T} \mid \left(E_i \cap C_k\right)\right) = \begin{cases} 1 & k = 2,4 \\ 0 & k = 1,3 \end{cases} \end{cases}$$

For example, given that there is no outage (E_3) which is supposed to be an *IN*, and the IPR has an unnecessary switching action (C_1 or C_3), then the probability of a switching action given that event E_3 occurred and it is in state S_3, S_4, S_9, or S_{10} (which belong to C_1 or C_3) is one $\{P\left(T \mid \left(E_3 \cap C_1\right)\right) = 1$, or $P\left(T \mid \left(E_3 \cap C_3\right)\right) = 1\}$.

Assuming a constant failure rate $\lambda = 4.58 \times 10^{-5}$ [outages/year] for both lines [40], is found that,

$$P\left(F_i\right) = 1 - e^{-\lambda} = 4.5799 \times 10^{-5} \qquad i = 1,2$$
$$P\left(E_1\right) = P\left(E_2\right) = P\left(F_1\right)P\left(\overline{F}_2\right) = \left(1 - e^{-\lambda}\right)e^{-\lambda} = 4.5797 \times 10^{-5}$$
$$P\left(E_3\right) = P\left(\overline{F}_1\right)P\left(\overline{F}_2\right) = e^{-2\lambda} = 9.9991 \times 10^{-1}$$
$$P\left(E_4\right) = P\left(F_1\right)P\left(F_2\right) = \left(1 - e^{-\lambda}\right)^2 = 2.098 \times 10^{-9}$$

The probabilities $P\left(T \cap E_i\right)$ and $P\left(\overline{T} \cap E_i\right)$ required in equations 4.1 and 4.2 are:

$$P(E_1 \cap T) = P(E_1)\left[P(C_1) + P(C_2)\right] = 3.8861 \times 10^{-5}$$
$$P(E_1 \cap \overline{T}) = P(E_1)\left[P(C_3) + P(C_4)\right] = 6.9358 \times 10^{-6}$$
$$P(E_2 \cap T) = P(E_2)\left[P(C_1) + P(C_2)\right] = 3.8861 \times 10^{-5}$$
$$P(E_2 \cap \overline{T}) = P(E_2)\left[P(C_3) + P(C_4)\right] = 6.9358 \times 10^{-6}$$
$$P(E_3 \cap T) = P(E_3)\left[P(C_1) + P(C_3)\right] = 4.9974 \times 10^{-2}$$
$$P(E_3 \cap \overline{T}) = P(E_3)\left[P(C_2) + P(C_4)\right] = 9.4993 \times 10^{-1}$$
$$P(E_4 \cap T) = P(E_4)\left[P(C_1) + P(C_2)\right] = 1.7799 \times 10^{-9}$$
$$P(E_4 \cap \overline{T}) = P(E_4)\left[P(C_3) + P(C_4)\right] = 3.1767 \times 10^{-10}$$

To find the risk, the conditional probability in equation 4.2 is needed: $P\left(K \mid \left(\overline{T} \cap E_i\right)\right)$. From simulations, is known that the probability of collapse given that occurred event E_3 or E_4 and there is no tripping action of the IPR is 0 and 1 for E_3 and E_4 respectively. However, for events E_1 and E_2 the probability is not known.

4.2.6.1 Probability of Voltage Collapse

Sobierajski [44] developed a method to obtain a probability of voltage collapse for a given branch, based on the line *P-Q* curve. The procedure of this method is summarized as follows.

The transmission line or the power transformer can be characterized by its reactance X_L and susceptance B_L. The resistance R_L may be neglected and assume that there are known the voltage magnitude V_F at sending node and the active and reactive at receiving node.

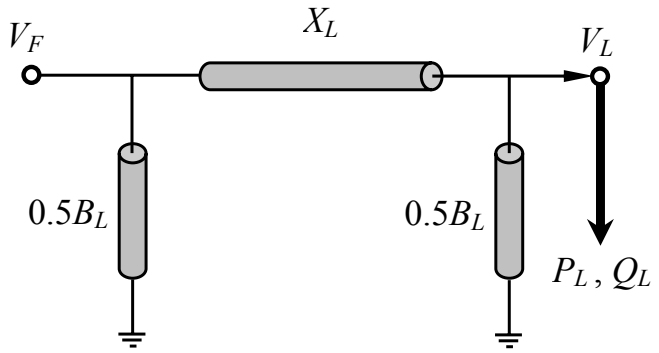

FIGURE 4.8 - Line diagram

Power load P_L and Q_L are dependent on voltage magnitude V_L and angle δ at the receiving node, so we obtain the following load flow equations for P_L, Q_L load treated as positive values

$$-P_L \frac{V_F V_L}{X_L} \sin\delta \tag{4.14}$$

$$-Q_L + 0.5B_L V_L^2 = \frac{V_F V_L}{X_L} \cos\delta + \frac{V_L^2}{X_L} \tag{4.15}$$

Substituting $e_L = V_L \cos\delta$ and $f_L = V_L \sin\delta$ we obtain

$$P_L = -\frac{V_F V_L}{X_L} f_L \tag{4.16}$$

$$Q_L = \frac{V_F}{X_L} e_L - \left(\frac{1}{X_L} - 0.5B_L \right) \left(e_L^2 + f_L^2 \right) \tag{4.17}$$

All consideration may be made in per unit (p.u.). We may choose the base voltage as $V_b = V_F$ and the base power as

$$S_b = \frac{V_F^2}{X_L} \tag{4.18}$$

We should be careful to change the system p.u. values to its nominal values before selecting computing S_b as the new base. Additionally the line charge coefficient may be introduced as

$$c = 1 - \frac{X_L B_L}{2} \tag{4.19}$$

The value of the charge coefficient c depends on the value of branch susceptance B_L. In the case of a transformer, $B_L < 0$ and $c > 1$. In the case of a line, $B_L > 0$ and $c < 1$. If branch susceptance is neglected $B_L = 0$ and then $c = 1$. Dividing both sides of equations 4.16 and 4.17 by S_b we obtain the following load flow equations in per unit

$$P = -f \tag{4.20}$$

$$Q = e - c\,(e^2 + f^2) \tag{4.21}$$

where $P = P_L / S_b$ - active load in p.u. , $Q = Q_L / S_b$ -reactive load in p.u., $e = e_L / V_F$ - the real part of voltage in p.u., $f = f_L / V_F$ - the imaginary part of voltage in p.u..

The P and Q values that give singular solution of load flow equations are associated with the zero determinant of Jacobian matrix. These P-Q values create the P-Q boundary curve of load flow solution. We can find the form of the P-Q boundary curve by the detailed analysis of load flow equations. After linearization of equations 4.20 and 4.21 we obtain

$$\begin{bmatrix} \Delta P \\ \Delta Q \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 - 2ce & -2cf \end{bmatrix} \begin{bmatrix} \Delta e \\ \Delta f \end{bmatrix} \tag{4.22}$$

The determinant of Jacobian matrix of 4.22 equals

$$D = 1 - 2ce \tag{4.23}$$

hence

$$e = \frac{1 - D}{2c} \tag{4.24}$$

For zero determinant $D = 0$ we have

$$e = \frac{1}{2c} \tag{4.25}$$

Substituting (4.25) into the formula of reactive bus load (4.21) we have as follows

$$Q = \frac{1}{2c} - c\left(\frac{1}{4c^2} + P^2\right) \tag{4.26}$$

Hence, the *P*-*Q* boundary curve of load flow solutions for a transmission line has the following formula

$$Q = -cP^2 + \frac{0.25}{c} \tag{4.27}$$

Let P and Q load be random variable, uniformly distributed between their maximal and minimal values, like Figure 4.9

$$P_{\min} \le P \le P_{\max}$$

$$Q_{\min} \le Q \le Q_{\max}$$

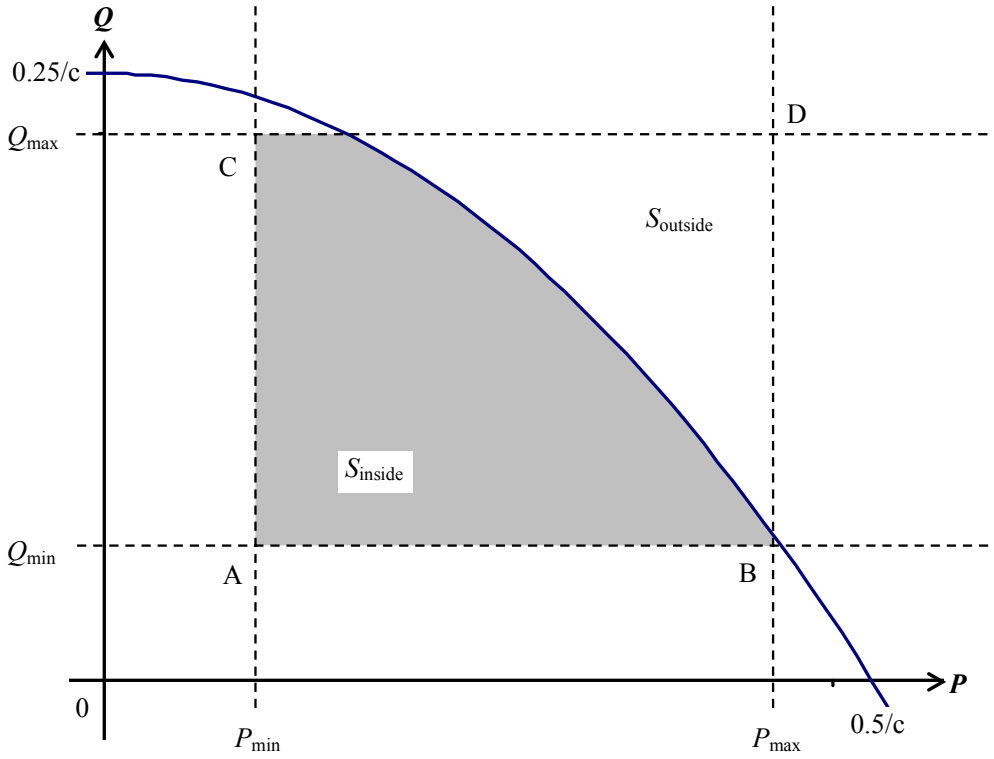

FIGURE 4.9 - *P*-*Q* Curve

The probability of the branch voltage collapse is obtained using the geometrical definition of probability

$$p_{VC} = \frac{S_{outside}}{S} = 1 - \frac{S_{inside}}{S} \tag{4.28}$$

where S means the area of ABDC rectangular

$$S = (P_{\max} - P_{\min})(Q_{\max} - Q_{\min}) \tag{4.29}$$

and S_{inside} is the area placed inside the *P*-*Q* upper curve. The solution of branch load flow equations exists only inside the *P*-*Q* curve, i.e. for *ABC*. There is no solution for the points outside the *P*-*Q* curve, i.e. for *BCD* area.

The base load can be treated as the minimal values

$$P_{\min} = P_o \text{ and } Q_{\min} = Q_o \tag{4.30}$$

According to Figure 4.9 the maximal value of P and Q can be calculated using the formula of the P-Q curve

$$P_{\max} = \sqrt{-\frac{Q_{\min}}{c} + \frac{0.25}{c^2}} \tag{4.31}$$

$$Q_{\max} = -cP_{\min}^2 + \frac{0.25}{c} \tag{4.32}$$

The area of ABC can be computed using the definite integral formula

$$\begin{aligned} S_{ABC} &= \int_{P_{\min}}^{P_{\max}} \left(-cP^2 + \frac{0.25}{c} - Q_{\min} \right) dP \\ &= \left(-\frac{c}{3} P^3 + \frac{0.25}{c} P - Q_{\min} P \right) \Bigg|_{P_{\min}}^{P_{\max}} \\ &= -\frac{c}{3} \left(P_{\max}^3 - P_{\min}^3 \right) + \left(\frac{0.25}{c} - Q_{\min} \right) \left(P_{\max} - P_{\min} \right) \end{aligned} \tag{4.33}$$

Finally, the probability of voltage collapse is

$$p_{VC} = 1 - \frac{S_{ABC}}{S} = 1 - \frac{-\frac{c}{3} \left(P_{\max}^3 - P_{\min}^3 \right) + \left(\frac{0.25}{c} - Q_{\min} \right) \left(P_{\max} - P_{\min} \right)}{\left(P_{\max} - P_{\min} \right) \left(Q_{\max} - Q_{\min} \right)} \tag{4.34}$$

Tables 4.5 and 4.6 summarize the numerical values in the procedure to obtain the probability of voltage collapse for the events E_1 and E_2. Figure 4.10 shows the *P-Q* curve of event E_1.

TABLE 4.5 - Original and New bases/p.u. values for the initiating events

Event	Line	Original Bases		Original Per unit values			New Bases		Power Flow	
		S_b [MVA]	V_F [kV]	V_F	X_L	B_L	S_b [MVA]	V_F [kV]	P [MW]	Q [MVar]
E_1	$L_{78\text{-}80}$	100	500	1.03266	0.00820	1.30000	13004.72	516.33	2772.37	463.20
E_2	$L_{76\text{-}78}$	100	500	0.91528	0.02316	1.71520	3617.17	457.64	950.83	434.13

TABLE 4.6 - Probability of voltage collapse for the initiating events

Event	Line	c	Minimum PF values [p.u.]		Maximum PF values [p.u.]		S	S_{ABC}	p_{VC}
			$P_{\min}$	$Q_{\min}$	$P_{\max}$	$Q_{\max}$			
E_1	$L_{78\text{-}80}$	1.00500	0.21317	0.03562	0.46052	0.20309	0.04142	0.02325	0.43881
E_2	$L_{76\text{-}78}$	0.97629	0.26287	0.12002	0.37330	0.18861	0.00758	0.00401	0.47107

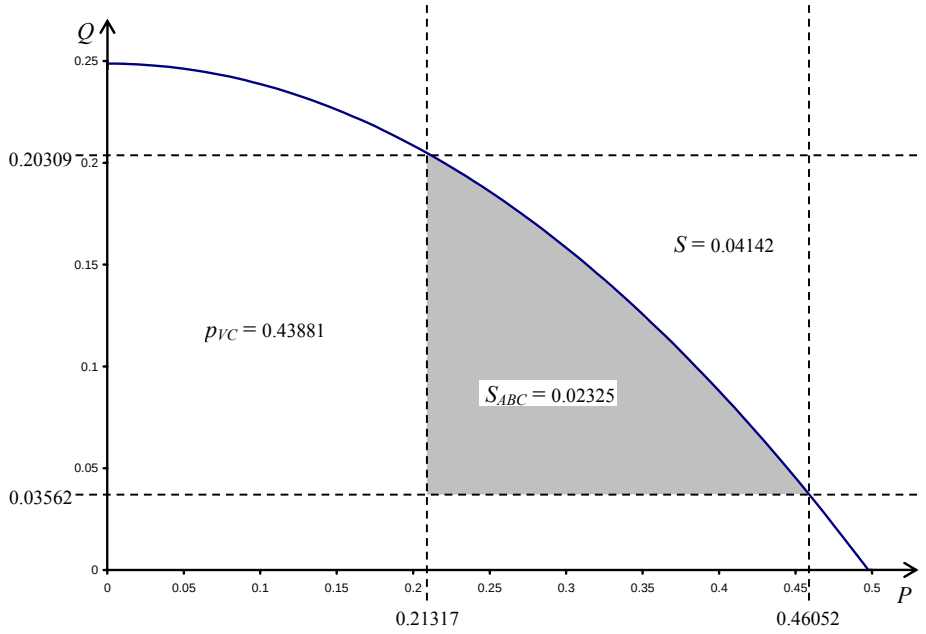

FIGURE 4.10 - *P-Q* Curve for event E_1

Now we have the probability values needed to complete the risk assessment. Finally, we have to assign the impact for each event. As discussed before, the estimated economic impact is about \$2.02 billions. The impact of a VAR compensator can be neglected since the cost of using/connecting a VAR compensator is much lower compared to the economic impact.

4.2.6.2 Impacts

1. $E_1 \cap T$: $L_{76\text{-}78}$ outage, IPR connects compensators

$$I\left(E_1 \cap T\right) = 0$$

2. $E_1 \cap \overline{T}$: $L_{76\text{-}78}$ outage, IPR does not connect compensators

$$I\left(E_1 \cap \overline{T} \cap K\right) = \$2,015,441,000$$
$$I\left(E_1 \cap \overline{T} \cap \overline{K}\right) = 0$$

3. $E_2 \cap T$: $L_{78\text{-}80}$ outage, IPR connects capacitors

$$I\left(E_2 \cap T\right) = 0$$

4. $E_2 \cap \overline{T}$: $L_{78\text{-}80}$ outage, IPR does not connect compensators

$$I\left(E_2 \cap \overline{T} \cap K\right) = \$2,015,441,000$$
$$I\left(E_2 \cap \overline{T} \cap \overline{K}\right) = 0$$

5. $E_3 \cap T$: No line outage, IPR connects capacitors

$$I\left(E_3 \cap T\right) = 0$$

6. $E_3 \cap \overline{T}$: No line outage, IPR does not connect compensators

$$I\left(E_3 \cap \overline{T}\right) = 0$$

7. $E_4 \cap T$: $L_{76\text{-}78}$ and $L_{78\text{-}80}$ outage, IPR connects compensators

$$I\left(E_4 \cap T\right) = 0$$

8. $E_4 \cap \overline{T}$: $L_{76\text{-}78}$ and $L_{78\text{-}80}$ outage, IPR does not connect compensators

$$I\left(E_4 \cap \overline{T} \cap K\right) = \$2,015,441,000$$
$$I\left(E_4 \cap \overline{T} \cap \overline{K}\right) = 0$$

4.2.6.3 Risk Results

Then, from equation 4.1 we have

$$\sum_{i=1}^{N_T} Risk\left(E_i\right) = \sum_{i=1}^{N_T} P\left(K \cap \overline{T} \cap E_i\right) \times I\left(K \cap \overline{T} \cap E_i\right) + \sum_{i=1}^{N_T} P\left(T \cap E_i\right) \times I\left(T \cap E_i\right)$$
$$= \sum_{i=1}^{N_T} P\left(K \mid \left(\overline{T} \cap E_i\right)\right) \times P\left(\overline{T} \cap E_i\right) \times I\left(K \cap \overline{T} \cap E_i\right) + \sum_{i=1}^{N_T} P\left(T \cap E_i\right) \times I\left(T \cap E_i\right)$$

$$Risk\left(E_1\right) = Risk\left(K \cap \overline{T} \cap E_1\right) + Risk\left(T \cap E_1\right)$$
$$= P\left(K \cap \overline{T} \cap E_1\right) I\left(K \cap \overline{T} \cap E_1\right) + P\left(T \cap E_1\right) I\left(T \cap E_1\right)$$
$$= P\left(K \mid \left(\overline{T} \cap E_1\right)\right) P\left(\overline{T} \cap E_1\right) I\left(K \cap \overline{T} \cap E_1\right) + P\left(T \cap E_1\right) I\left(T \cap E_1\right)$$
$$= 0.43881\left(6.9358 \times 10^{-6}\right)\left(2,015,441,000\right) + 3.8861 \times 10^{-5}\left(0\right)$$
$$= \$6,134$$

The risk for events E_2, E_3, and E_4 is \$6584.9, \$0, and \$0.64024 respectively. Therefore, the total risk with IPR is:

$$Total\ Risk = \sum_{i=1}^{4} Risk\left(E_i\right) = Risk\left(E_1\right) + Risk\left(E_2\right) + Risk\left(E_3\right) + Risk\left(E_4\right)$$
$$= 6,134 + 6,584.9 + 0 + 0.64024$$
$$= \$12,720$$

To obtain the system risk without IPR, we should assume that the IPR activating events have zero probability ($T = 0$ and $\overline{T} = 1$). Then, the expression for a system without IPR according from equation 4.1 is

$$\begin{aligned}\sum_{i=1}^{N_T} Risk(E_i) &= \sum_{i=1}^{2} P(K \cap E_i) \times I(K \cap E_i) + P(E_4) I(E_4) \\ &= P(E_1) P(K \mid E_1) I(K \cap E_1) + P(E_2) P(K \mid E_2) I(K \cap E_2) \\ &\qquad + P(E_4) I(E_4) \\ &= 4.5797 \times 10^{-5} (.43881)(2,015,441,000) + 4.5797 \times 10^{-5} (0.47107)(2,015,441,000) \\ &\qquad + 2.098 \times 10^{-9} (2,015,441,000) \\ &= \$83,986\end{aligned}$$

4.2.7 Make Decision

The final step in the risk assessment it decide whether or not use IPR in the system. The given results favor the implementation of the IPR because of its lower system risk. Next chapter discuss further these results, and the final decision in our risk assessment.

5 DISCUSSION

In Chapter 3 we obtained estimated results of reliabilities and failure probabilities different IPR configurations. The results show, as expected, that non-redundant configurations have lower reliabilities, or higher failure probabilities. Introducing redundancy in at least one of the components, the reliability of the system increases considerably, and reduces the probability of failure. The configurations shown in Figure 3.3(d) and 3.3(e) attained the highest reliabilities. However, the reliability of the each IPR configuration is lower than the reliability of the breaker itself. We expect these results because the reliability in a series system will be less than the lowest reliability of its components. All our IPR configurations reduce to a series configuration. The only way to attain a higher IPR reliability than the breaker is if we provide a redundant path to the breaker. Does this mean that it is better to have only the breaker instead of the IPR? We believe not. A breaker will act based on local data, without regard to the system state outside its protection zone. The IPR, through its communication capabilities, will act based on local and regional data enhancing the system reliability. The classical methods do not capture properly the increase in the reliability of a power system when a special protection scheme (SPS) is included.

Risk Assessment approach provides us a method to capture the increase in reliability when a system has a SPS like an IPR. The results in Chapter 4 prove that. As seen, the risk is lower for the system with IPR. The main risk comes from events E_1 and E_2. In the case for the system with IPR both risks are similar, \$6,134 vs. \$6,584.9. The

slight difference is due to the higher probability of collapse of E_2, because the remaining line $L_{76\text{-}78}$ works more stressed than line $L_{78\text{-}80}$ in event E_1. The risk for E_3 is zero or near to zero because there is no outage, so the probability of a collapse due to the non-outage of both line is negligible. However, it is interesting to note that the risk for event E_4 is quite low too. It only showed a \$0.64 of risk. The main reason is the extremely low probability of the occurrence of a successive outage of both lines. It is also true for the system without IPR. For example, the probability of occurrence of one-line outage is 4.5797×10^{-5}. However, for a successive outage of both lines the probability drops to 2.098×10^{-9}. Nonetheless, there is a significant difference between the risk values for each system, \$12,720 vs. \$83,986. Although the results have [\$] units, we should not take these results as cost differences or savings since there is no accurate impact assessment. Is preferably to take this values as indicatives in the reliability improvement of the power system.

Is justified the inversion in an IPR? Noting that a data router can cost about \$20,000 (for a Cisco 7206VXR router), estimating the software development to cost \$30,000, and a high voltage circuit breaker about \$10,000, plus installation, the cost should not be more than \$100k. If we compare this cost with the potential loss of \$2.02 billions if the system collapses, the inversion of an IPR is negligible. It can be compared to spend half cent (0.5 ¢) of a \$100 bill, therefore it makes the IPR an attractive alternative.

The following Table shows the risk change in the system if IPR reliability measures vary. The most dramatic change occurs when the data router/computer hardware is changed from unit having 9.5 years MTBF to 35 years (with the software reliability fixed at 0.99), since the risk is reduced in a 58%. However, if we compare both values ($10,065 and $4,237.6) with the risk of the system without IPR, the risk change is not so dramatic. The risk with IPR for a router with 9.5 years is 12% of the risk without IPR, while with a router having a MTBF of 35 years the risk is only 5%. Is the investment in a more reliable data router is justified? Probably not, because the investment in a 35 years MTBF router is 25 times the price of a 9.5 MTBF router, and the gain (lower risk) in the system is only 7%. Figure 5.1 shows the decrease of the system risk due to the increase in the MTBF of the router. It verifies our assumption of not justify the investment in router of higher reliability. From this Figure we note slow decrease of risk from about a MTBF of 10 years or greater, however, the price increase steeply if we assume a linear function.

TABLE 5.1 – System Risk due to the variation of the IPR's components reliability

System	$S = 0.95$ MTBF = 9.5	$S = 0.95$ MTBF = 35	$S = 0.99$ MTBF = 9.5	$S = 0.99$ MTBF = 35
with IPR	$12,720	$7,366.4	$10,065	$4,237.6
without IPR	$83,986	$83,986	$83,986	$83,986

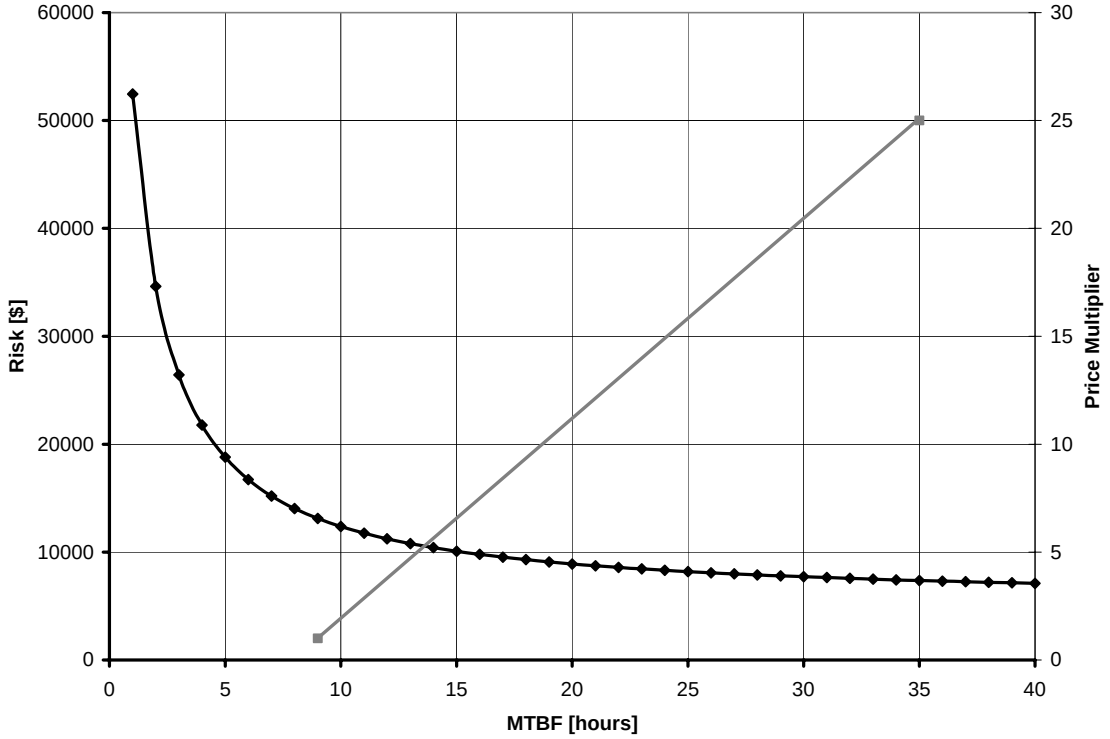

FIGURE 5.1 – System Risk vs. Data Router MTBF

As we can observe, the IPR increases the stability and security of the system at that generation/load level. Fu [40] shows in his dissertation that is possible for a certain operation points to have a system risk lower without the SPS than with it. The optimal point when the IPR is activated is known as the "arming point". This point is the area of intersection of the Generation vs. Risk curve for a system with IPR with the same curve for a system without IPR (Figure 5.2). Determining the arming point of the system can optimize the risk assessment since the system will work at the lowest risk level possible based on the operational point of the system.

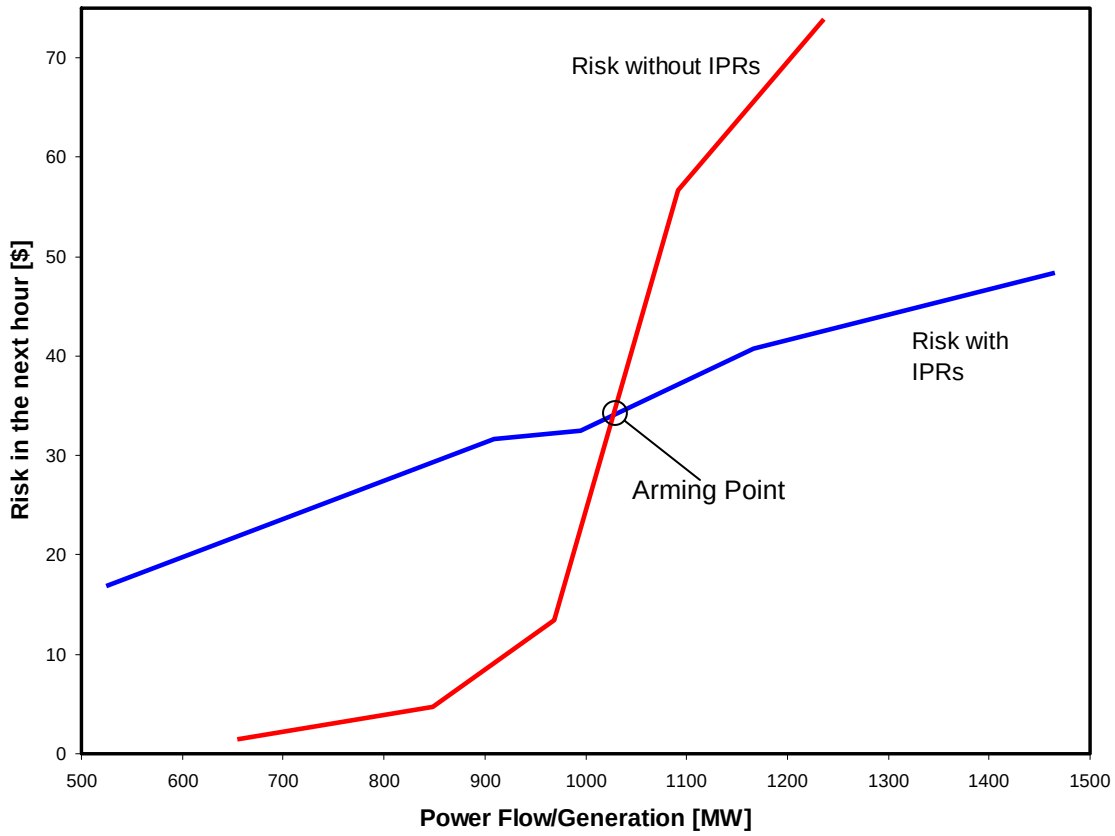

FIGURE 5.2 – Generation vs. Risk level curve for Arming Point Determination

6 CONCLUSION

We have estimated the reliability of an Intelligent Power Router (IPR) based on the failure probabilities of its primary subsystems; software, communications and switching element, and a variety of possible functional relationship between these subsystems. Since an IPR has not being built yet we have estimated the failure probabilities of its subsystems from our knowledge of existing similar systems, e.g. existing software, data routers and circuit breakers reliability estimates. As expected, the configurations that provide redundancy achieved the highest reliabilities and lowest failure probabilities. Due to the series configuration chosen the reliability of the IPR is smaller than that of the breaker alone. However, a breaker will act based on local data, without regard to the system state outside its protection zone. The IPR, through its communication capabilities, will act based on local and regional data enhancing the system reliability.

Risk Assessment approach provides us a method to capture the increase in reliability when a system has a SPS like an IPR. Our work demonstrated the IPR increases the stability and security of the system at that generation/load level. There is a significant difference between the risk for the power system with IPR and the system without it. The main risk in both cases comes from events E_1 and E_2. The reason is the low probability of the occurrence of a successive outage of both lines. Although the results have [$] units, we should not take these results as cost differences or savings since

there is no accurate impact assessment. Is preferably to take this values as indicatives in the reliability improvement of the power system.

Therefore, is the IPR investment justified? Yes. The cost of an IPR should not be more than $100k. If we compare this cost with the potential loss of $2.02 billions if the system collapses, the investment on an IPR is negligible, plus it will reinforce the reliability and security of the power system.

6.1 Future Work

The previous work presented the risk assessment applied to a system with IPR. It demonstrated the increase in the system's reliability due to IPR. However, there is enough room to enhance the assessment. To obtain better estimates it is necessary to:

- *Improve the impact assessment*. Obtaining the cost-generation functions for each unit, the cost of re-energization and/or replacement of damaged components, the customer (type) distribution, among other factors, will considerably improve the impact assessment on the WSCC.

- *If possible, do a sensitivity study*. Changing system parameters to learn how these changes affects the simulation results, and therefore the probability of voltage collapse, to observe the variations in the system total risk.

- *Obtain a loading vs. risk curve for a system with and without IPR*. It is essential to determine the optimal "arming point" of the IPR in order to attain the lowest risk possible at all operational points.

REFERENCES

[1] L. Goel, and C. Feng, “Well-being framework for composite generation and transmission system reliability evaluation”, IEE Proceedings on Generation, Transmission and Distribution, Volume146, Issue 5, Sept. 1999, pp. 528-534.

[2] A. Shaban, and A. Go, “A reliability and economic evaluation of a transmission system-I: Using frequency and duration of failure method”, Twenty-Fifth Southeastern Symposium on System Theory, March 1993, pp. 94-100.

[3] U.S.-Canada Power System Outage Task Force, “Interim Report: Causes of the August 14th Blackout in the United States and Canada”, November 2003.

[4] R. Billinton, and L. Goel, “Overall adequacy assessment of an electric power system”, IEE Proceedings Generation, Transmission and Distribution, Volume 139, Issue 1, January 1992, pp. 57-63.

[5] Agustín A. Irizarry-Rivera, Manuel Rodríguez, Miguel Vélez-Reyes, José R. Cedeño, Bienvenido Vélez, Efraín O'Neill-Carrillo, and Alberto Ramírez, "Intelligent Power Routers for Distributed Coordination in Electric Energy Processing Networks", Proceedings of the 2003 EPNES Workshop, Orlando, Florida, October 23-24, 2003.

[6] R. Billinton, and R. Allan, Reliability Evaluation of Power Systems, Plenum Publishing Corporation, 2nd edition, 1996.

[7] A.A. Irizarry-Rivera, Risk-based operating limits for dynamic security constrained electric power systems, PhD Dissertation., Iowa State University, Ames, Iowa, 1996, pp. 93.

[8] R. Billinton, K. Rajesh, and M. Fotuhi-Firuzabad, “Probabilistic Methods Applied to Adequacy Assessment of Small Isolated Power Generating Systems”, PMaps ‘97, Vancouver, 1997.

[9] R. Billinton, and R. Karki, “Application of Monte Carlo simulation to generating system well-being analysis”, IEEE Transactions on Power Systems, Volume 14, Issue 3, August 1999, pp. 1172-1177.

[10] L.S. Low, and L. Goel, “Incorporating deterministic criteria in the probabilistic framework for composite generation and transmission systems**”,** IEEE Power Engineering Society Summer Meeting, Volume 4, July 2000, pp. 2069-2074.

[11] R. Billinton, and M. Fotuhi-Firuzabad, “Reserve capacity assessment in small isolated electric power generating systems”, Power Engineering Journal, Volume 10, Issue 2, April 1996, pp. 73-80.

[12] A. Abdulwhab, and R. Billinton, “Application of wellbeing concepts in short term generating unit preventive maintenance scheduling”, Canadian Conference on Electrical and Computer Engineering, Volume 1, May 2002, pp. 150-155.

[13] Guangbin Lian, and R. Billinton, “Operating reserve risk assessment in composite power systems”, IEEE Transactions on Power Systems, Volume 9, Issue 3, August 1994, pp. 1270-1276.

[14] Weihui Fu, Sanyi Zhao, J.D. McCalley, V. Vittal, and N. Abi-Samra, “Risk assessment for special protection systems”, IEEE Transactions on Power Systems, Volume 17, Issue 1, February 2002, pp. 63-72.

[15] D.J. Pearson, and V.G. Rose, “Risk assessment model for distribution system reliability”, 14th International Conference and Exhibition on Electricity Distribution, Volume 6, June 1997, pp. 38/1-38/4.

[16] J.D. McCalley, V. Vittal, and N. Abi-Samra, “An overview of risk based security assessment”, IEEE Power Engineering Society Summer Meeting, Volume 1, July 18-22, 1999, pp. 173-178.

[17] Fubin Liu, Yang Li, Yixin Ni, Guoqing Tang, and N. Leeprechanon, “A novel strategy of pricing for steady-state security in deregulated environment”, IEEE Power Engineering Society Winter Meeting, Volume 1, January 27-31, 2002, pp. 428-433.

[18] J.D. McCalley, A.A. Fouad, V. Vittal, A.A. Irizarry-Rivera, B.L. Agrawal, and R.G. Farmer, R.G., “A risk-based security index for determining operating limits in stability-limited electric power systems”, IEEE Transactions on Power Systems, Volume 12, Issue 3, August 1997, pp. 1210-1219.

[19] Y. Dai, J.D. McCalley, N. Abi-Samra, and V. Vittal, “Annual risk assessment for overload security”, IEEE Transactions on Power Systems, Volume 16, Issue 4, November 2001, pp. 616-623.

[20] V. Vittal, J.D. McCalley, V. Van Acker, W. Fu, and N. Abi-Samra, “Transient instability risk assessment”, IEEE Power Engineering Society Summer Meeting, Volume 1, July 18-22, 1999, pp. 206-211.

[21] A.M. Leite da Silva, J.L. Jardim, A.M. Rei, and J.C.O. Mello, “Dynamic security risk assessment”, IEEE Power Engineering Society Summer Meeting Volume 1, July 18-22, 1999, pp. 198-205.

[22] H. Wan, J.D. McCalley, and V. Vittal, "Increasing thermal rating by risk analysis", IEEE Transactions on Power Systems, Volume 14, Issue 3, August 1999, pp. 815-828.

[23] Weihui Fu, and J.D. McCalley, "Risk based optimal power flow", IEEE Power Tech Proceedings, Porto 2001, Volume 3, September 10-13, 2001, 6 pp.

[24] J.D. McCalley, V. Vittal, H. Wan, Y. Dai, and N. Abi-Samra, "Voltage risk assessment", IEEE Power Engineering Society Summer Meeting, Volume 1, July 18-22, 1999, pp. 179-184.

[25] J.D. McCalley, and Weihui Fu, "Reliability of special protection systems", IEEE Transactions on Power Systems, Volume 14, Issue 4, November 1999, pp. 1400-1406.

[26] P.M. Anderson, and B.K. LeReverend, "Industry experience with special protection schemes", IEEE Transactions on Power Systems, Volume 11, Issue 3, August 1996, pp. 1166-1179.

[27] J. Lua, "Probabilistic vulnerability assessment tool for surface ship under extreme dynamic loads", Applied Mechanics Department, A&T Engineering Technology Center, Ateon Company, 240 Oral School Road, Mystic, CT 006355-1208.

[28] Sheldon M. Ross, *Introduction to Probability Models*, Harcourt Academic Press, 7th edition, 2000, pp. 693.

[29] Athanasios Papoulis, *Probability, Random Variables, and Stochastic Processes*, McGraw-Hill, 3rd edition, 1991, pp. 666.

[30] Dimitri P. Bertsekas, and John N. Tsitsiklis, Introduction to Probability, Lecture notes, Course 6.041-6.431, Massachusetts Institute of Technology, Fall 2000, pp. 284.

[31] Charles E. Ebeling, An Introduction to Reliability and Maintainability Engineering, McGraw-Hill, 1st edition, 1997, pp. 486.

[32] "Definitions of terms for reliability and maintainability", Military Standard MIL-STD-721C, Department of Defense, Washington, DC, 20301.

[33] W.W. Everett, "Software reliability measurement", IEEE Journal on Selected Areas in Communications, Volume 8, Issue 2, February 1990, pp. 247-252.

[34] W.W. Everett, “Software component reliability analysis”, IEEE Symposium on Application-Specific Systems and Software Engineering and Technology, March 1999, pp. 204-211.

[35] A. Pons, A. Sabot, and G. Babusci, “Electrical endurance and reliability of circuit-breakers-common experience and practice of two utilities”, IEEE Transactions on Power Delivery, Volume 8, Issue 1, January 1993, pp. 168-174.

[36] C.R. Heising, A.L.J. Janssen, W. Lanz, E. Colombo, and E.N. Dialynas, “Summary of CIGRE 13.06 Working Group world wide reliability data and maintenance cost data on high voltage circuit breakers above 63 kV”, Industry Applications Society Annual Meeting, Volume 3, October 1994, pp. 2226-2234.

[37] C.R. Heising, “Worldwide reliability survey of high-voltage circuit breakers”, Industry Applications Magazine, Volume 2, Issue 3, May-June 1996, pp. 65-66.

[38] IEEE guide for diagnostics and failure investigation of power circuit breakers, IEEE Std C37.10-1995, September 23, 1996, pp. 55.

[39] G.W. Scheer, and D.J. Dolezilek, “Comparing the reliability of Ethernet network topologies in substation control and monitoring networks”, Schweitzer Engineering Laboratories, Inc.

[40] Weihui Fu, Risk assessment and optimization for electric power systems, PhD Dissertation., Iowa State University, Ames, Iowa, 2000, pp. 158.

[41] Mohamed A. El-Sharkawi, Presentation: “Modern Heuristic Optimization Techniques and Potential Applications to Power System Control”, Department of Electrical Engineering, University of Washington, Seattle, WA 98195-2500, elsharkawi@ee.washington.edu, http://cialab.ee.washington.edu

[42] V. Vittal, H. You, and Xiaoming Wang, “Slow coherency-based islanding”, IEEE Transactions on Power Systems, Volume 19, Issue 1, February 2004, pp. 483-491

[43] R. Billinton, “Economic cost of non-supply”, IEEE Power Engineering Society Winter Meeting, Volume 2, January 27-31, 2002, pp. 959-962.

[44] Sobierajski, K. Wilkosz, J. Bertsch, M. Fulczyk, and C. Rehtanz, “Prompt identification of weak transmission lines regarding voltage collapse”, Fifth International Conference on Power System Management and Control, No. 488, April 17-19 2002, pp. 285-290.

APPENDIX – A *MATLAB Code for Risk Calculation*

```
%-------------------------------------------------------------------------%
%%%%%        Enter the Reliabilty Indicators of IPR components        %%%%%
%%%%%            and convert them to Failure rate (per year)          %%%%%
%-------------------------------------------------------------------------%
L3=input('Enter the Failure rate (per year) of Breaker = ');
disp('     ')

Rsoft=input('Enter the Reliability (per year) expected of Software = ');
disp('     ')
L2=-log(Rsoft);

MTBF=input('Enter the MTBF (years) specified for Router/Computer = ');
disp('     ')
L1=1/MTBF;


%-------------------------------------------------------------------------%
%%%%%            Convert the Failure rate to a daily basis            %%%%%
%-------------------------------------------------------------------------%

Ld1=L1/365;
Ld2=L2/365;
Ld3=L3/365;


%-------------------------------------------------------------------------%
%%%%%            Calculate the transitions from each state            %%%%%
%-------------------------------------------------------------------------%

p1=1-Ld1-Ld2-2*Ld3;
p2=1-Ld1-Ld2-Ld3;
p3=1-Ld1-2*Ld3;
p4=1-Ld2-2*Ld3;
p5=1-Ld1-Ld2;
p6=1-Ld1-Ld3;
p7=1-Ld2-Ld3;
p8=1-2*Ld3;
p9=1-Ld1;
p10=1-Ld2;
p11=1-Ld3;


%-------------------------------------------------------------------------%
%%%%%                Calculate the transition matrix                  %%%%%
%-------------------------------------------------------------------------%

B=[p1   2*Ld3  0      Ld2    0      0      Ld1    0      0      0      0      0;
    0   p2     Ld3    0      Ld2    0      0      Ld1    0      0      0      0;
    0   0      p5     0      0      Ld2    0      0      Ld1    0      0      0;
    0   0      0      p3     2*Ld3  0      0      0      0      Ld1    0      0;
    0   0      0      0      p6     Ld3    0      0      0      0      Ld1    0;
    0   0      0      0      0      p9     0      0      0      0      0      Ld1;
    0   0      0      0      0      0      p4     2*Ld3  0      Ld2    0      0;
    0   0      0      0      0      0      0      p7     Ld3    0      Ld2    0;
    0   0      0      0      0      0      0      0      p10    0      0      Ld2;
    0   0      0      0      0      0      0      0      0      p8     0      2*Ld3;
    0   0      0      0      0      0      0      0      0      0      p11    Ld3;
    0   0      0      0      0      0      0      0      0      0      0      1];

Po=[1 0 0 0 0 0 0 0 0 0 0 0];

Pm= Po*(B^365);


%-------------------------------------------------------------------------%
%%%%%         Calculate the probability of each category (Ci)         %%%%%
%-------------------------------------------------------------------------%

C1=Pm(1,10);
C2=Pm(1,1);
C3=Pm(1,4)+Pm(1,5)+Pm(1,11);
C4=Pm(1,2)+Pm(1,3)+Pm(1,6)+Pm(1,7)+Pm(1,8)+Pm(1,9)+Pm(1,12);
```

```
%-------------------------------------------------------------------------%
%%%%%            Calculate Event and Collapse probabilities           %%%%%
%-------------------------------------------------------------------------%

Ld=0.0000458;
E1=(1-exp(-Ld))*(exp(-Ld));
E2=(1-exp(-Ld))*(exp(-Ld));
E3=exp(-2*Ld);
E4=(1-exp(-Ld))^2;

E1T=E1*(C1+C2);
E1Tn=E1*(C3+C4);
E2T=E2*(C1+C2);
E2Tn=E2*(C3+C4);
E3T=E3*(C1+C3);
E3Tn=E3*(C2+C4);
E4T=E4*(C1+C2);
E4Tn=E4*(C3+C4);

KE1Tn=0.438808567821; KE1=0.438808567821;
KE2Tn=0.471066713688; KE2=0.471066713688;
KE3Tn=0;
KE4Tn=1;


%-------------------------------------------------------------------------%
%%%%%                 Assing the impact for each Event                %%%%%
%-------------------------------------------------------------------------%

IE1T=0;
IE1TnK=2015441000; IE1K=2015441000;
IE1TnKn=0;

IE2T=0;
IE2TnK=2015441000; IE2K=2015441000;
IE2TnKn=0;

IE3T=0;
IE3TnK=0;
IE3TnKn=0;

IE4T=0;
IE4TnK=2015441000; IE4=2015441000;
IE4TnKn=0;


%-------------------------------------------------------------------------%
%%%%%                   Calculate the Risk with IPR                   %%%%%
%-------------------------------------------------------------------------%

RE1=KE1Tn*E1Tn*IE1TnK+E1T*IE1T;

RE2=KE2Tn*E2Tn*IE2TnK+E2T*IE2T;

RE3=KE3Tn*E3Tn*IE3TnK+E3T*IE3T;

RE4=KE4Tn*E4Tn*IE4TnK+E4T*IE4T;

R_IPRs=RE1+RE2+RE3+RE4


%-------------------------------------------------------------------------%
%%%%%                 Calculate the Risk without IPR                  %%%%%
%-------------------------------------------------------------------------%

R_woIPRs=E1*KE1*IE1K+E2*KE2*IE2K+E4*IE4


%-------------------------------------------------------------------------%
%%%%%                              END                                %%%%%
%-------------------------------------------------------------------------%
```

APPENDIX – B *MATLAB Code for Voltage Collapse Calculation*

```
%%%%%The workspace corresponding to this program must be loaded first%%%%%%
%                                                                          %
%               So7678D --|                                                %
%               So7880D   |---- Power Flow data for each contingency      %
%                  SoNO --|                                                %
%                                                                          %
%                V7678D --|                                                %
%                V7880D   |---- Bus voltage data for each contingency     %
%                   VNO --|                                                %
%                                                                          %
%                     Z ------- Line Impedance data                        %
%                    kV ------- Base Voltage of each bus                   %
%                                                                          %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%


%--------------------------------------------------------------------------%
%%%%%                      Select the desired Event                   %%%%%
%--------------------------------------------------------------------------%

disp('Which Event do you want to analyze?')
disp('       1 - No Outage')
disp('       2 - L76-78 Down')
disp('       3 - L78-80 Down')
disp('                      ')

G=input('Enter the desired Event = ');



VC=zeros(263,11);     %%%Creates a matrix to put the Voltage Collape values
Sold=100;


for n=1:263

   Zab=Z(n,4)+(Z(n,5))*i;   %%%Define Line Impedance
   B1=Z(n,2);               %%%Define the Sending Bus
   B2=Z(n,3);               %%%Define the Receiving Bus



%--------------------------------------------------------------------------%
%%%%%                Define the minimum P and Q values               %%%%%
%%%%%                 depending on the selected event                %%%%%
%--------------------------------------------------------------------------%

   if G==1
   Po=abs(SoNO(n,4));

   Qo=abs(SoNO(n,5));

   Vb=VNO(B1,2);

   else
       if G==2
              Po=abs(So7678D(n,4));

              Qo=abs(So7678D(n,5));

              Vb=V7678D(B1,2);
       else
           if G==3
                 Po=abs(So7880D(n,4));

                 Qo=abs(So7880D(n,5));

                 Vb=V7880D(B1,2);
           else
           end
       end
   end
```

```
%-------------------------------------------------------------------------%
%%%%%              Change the system base to the new base             %%%%%
%%%%%               and calculate the new p.u. quantities             %%%%%
%-------------------------------------------------------------------------%

   Zbold=((kV(B1,2))^2)/Sold;

   Zohms=Zbold*Zab;
   XLohms=imag(Zohms);
   BLold=Z(n,6)*Sold;

   Sbnew=((kV(B1,2)*Vb)^2)/XLohms;
   Zbnew=((kV(B1,2)*Vb)^2)/Sbnew;
   XL=XLohms/Zbnew;
   BL=BLold/Sbnew;

   C=1-((XL*BL)/2);                 %%% Calculate the charging coefficient


%-------------------------------------------------------------------------%
%%%%%               Calculate the maximun P and Q values              %%%%%
%%%%%                and Probability of Voltage Collapse              %%%%%
%-------------------------------------------------------------------------%

   Pmin=Po/Sbnew;
   Qmin=Qo/Sbnew;

   Pmax=sqrt(-Qmin/C+0.25/(C^2));
   Qmax=-C*(Pmin^2)+0.25/C;

   Sabc=-(C/3)*(Pmax^3-Pmin^3)+((0.25/C)-Qmin)*(Pmax-Pmin);
   S=(Pmax-Pmin)*(Qmax-Qmin);
   Pvc=1-Sabc/S;


%-------------------------------------------------------------------------%
%%%%%              Put all calculated values into a matrix            %%%%%
%-------------------------------------------------------------------------%

   VC(n,1)=n;
   VC(n,2)=B1;
   VC(n,3)=B2;
   VC(n,4)=C;
   VC(n,5)=Pmin;
   VC(n,6)=Pmax;
   VC(n,7)=Qmin;
   VC(n,8)=Qmax;
   VC(n,9)=Sabc;
   VC(n,10)=S;
   VC(n,11)=Pvc;

end


%-------------------------------------------------------------------------%
%%%%%                              END                                %%%%%
%-------------------------------------------------------------------------%
```