2004

Adaptive wide area protection of power systems

Jiang Huang
Iowa State University

Adaptive wide area protection of power systems

by

Jiang Huang

A dissertation submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Major: Electrical Engineering (Electric Power)

Program of Study Committee:
S. S. Venkata, Major Professor
Vijay Vittal
James McCalley
Govindrasu Manimaran
William Q. Meeker, Jr.

Iowa State University

Ames, Iowa

2004

Graduate College
Iowa State University

This is to certify that the doctoral dissertation of

Jiang Huang

has met the dissertation requirements of Iowa State University

Signature was redacted for privacy.

Major Professor

Signature was redacted for privacy.

For the Major Program

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

Studies of major blackouts reveal that power system protection devices have contributed to a majority of system disturbances. This leads to efforts of improving protection philosophy.

Analysis shows that conventional protection relies on coordination among stand-alone relays to obtain a dependability-biased component-protection scheme. Whereas it is more desirable and also feasible nowadays for an integrated approach to both component and system protection, provided modern relays possessing the ability of sharing information and applying intelligence in decision-making.

This dissertation proposes the adaptive protection concept for wide area systems. The scope of the research includes identifying and developing the desired architecture, intelligent algorithms and communication needs that facilitate the protection system to avoid and reduce the impact of system emergencies.

The purpose of this research work is to conceptualize and nurture adaptive protection concept for wide area systems, and to conduct feasibility studies to make this concept practically viable. Several case studies are conducted to show the effectiveness of the proposed adaptive protection scheme. In addition, voltage stability, which is a classic wide area problem, can be alleviated with the proposed concept. Steady state and transient simulation studies provided encouraging results. The detailed decision-making algorithms are simulated in several examples for validation of the concept.

CHAPTER 1. INTRODUCTION

The need to improve protection philosophy emerged with recent post-mortem studies of major blackouts. It was found that power system protection devices have contributed to a majority of system disturbances. False and undesired operations of these devices play an important role in initiating and propagating cascading events (Phadke, Horowitz, & Thorp, 1999; Taylor, 1999; Taylor & Erickson, 1997). A CIGRÉ study found that 27% of bulk power system disturbances resulted from false trips of the protection system (1995). An analysis of 17-year data provided in the North American Electric Reliability Council (NERC) reports (1995) revealed that 63% of major disturbances are protection-related.

A part of the responsibility for these problems lies in the nature and history of protection designs. Classical or component protection systems currently in vogue rely on individual relays to initiate switching actions to rapidly and reliably isolate a faulted portion of a local sub-system. This protection philosophy was formed more than 70 years ago (Sidhu et al., 2002). These systems were conceived to assure the "dependability" of fault isolation at the expense of false trips. The primary intent of this philosophy is to minimize damage to system components and is appropriate when a system is in a normal operating state. However, if a system is under stress, for example, due to outages or excessive loading, additional switching to isolate faults will cause further stress that may contribute to widespread system failures. If the switching is due to a false trip, or an undesired trip, then the protection system contributes to system failures. That is, system "security" is compromised.

A major advance in protection development was the introduction of System Protection Schemes (SPS) to expand the protection philosophy from a component level to a system level. SPS was intended to preserve the security of the system under specific conditions such as loss of synchronism from generators (Begovic et al., 2001). Functionally SPS makes use of signals from both system control and protection systems to assure "secure" system operation. However, based on the industry experience, SPS itself introduces unnecessary operations (Anderson & LeReverend, 1996). Furthermore, installing SPS as an additional layer of a dedicated scheme at the base of existing protection system could lead to complex coordination problems. This in turn could lead to conflicting protection decisions.

Therefore, SPS may not be best suited to close the gap between system protection and component protection.

An additional difficulty for proper protection is that a problem in the protection system can remain undetected under normal conditions. Such a "hidden failure" has been defined as *"a defect such as a component failure, inappropriate setting or incorrect external connection that remains undetected until some other system event causes the hidden failure to initiate a cascading outage"* (Phadke, Horowitz, & Thorp, 1995). A frequently cited example of a hidden failure is a failed fault detector or communication link in a directional comparison-blocking scheme that causes a relay to open a breaker inappropriately in the event of a fault on the adjacent line. Following a fault in a stressed power system, quite frequently hidden failures in protection systems would cause additional false trips. This tripping of additional facilities may start a chain reaction, evolving to catastrophic failures. Recent research work quantified the influence of hidden failures and supervising protection systems (Phadke, 2002). Among all suggested countermeasures, improving protection design to reduce the impact of hidden failures is of the greatest interest (Phadke, 2002).

Deregulation of electric utilities is another motivating factor to examine the current protection philosophy. Organizational restructuring of power systems calls for integration of conflicting protection requirements of competing entities, e.g. system operators, transmission system owners, and power producers. Thus, protection schemes originally designed for a vertically integrated system may not be appropriate for electric companies operating under deregulated environment (Phadke et al., 1999).

As power systems become more closely linked and heavily stressed, protecting them from both sustained faults and abnormal events requires an integrated approach to protection system design (Horowitz & Phadke, 1992). There is no doubt of the superiority of microprocessor relays over its analogue alternatives. They possess major advantages such as accurate extraction of the fundamental voltage and current components through filtering, functional benefits resulting from multi-processor design and extensive self-monitoring, etc. (Aggarwal & Johns, 1997). However, all these factors have not led to a major leap in speed, sensitivity and selectivity of the entire protection system. This is so because digital relays so far are simply replicates of their antecedents, or at the most, combination of several function

modules. Evaluating conventional relays, two constraints during the age when they were developed are noticed. Firstly, information was not shared among relays so each relay was using only a fraction of all information available. Secondly, the ability of each relay to process large amount of data was limited, by both the computation speed and the algorithms.

To combat the existing problems in various relay operation and meet the emerging power grids requirements, protection engineers have a considerable arsenal of new capabilities. New sensors, especially phasor measurement units (PMUs), provide fundamentally new functionalities (Denys, Counan, Hossenlopp, & Holweck, 1992). Utilities are busy installing new, high bandwidth communications systems for both business and operations, systems that also provide new capability for protection (Taylor, 2000). High-speed computation facilities provide the needed impetus. And computer-based relays provide the desired new logic for complex decision-making (Phadke & Thorp, 1993). Artificial Intelligence (AI) approaches are introduced for integrating extensive, redundant but imprecise data into intelligent decisions (Aggarwal & Johns, 1997). With the availability of these rapidly developing technologies, it is possible to gather critical and extensive information in real-time. This in turn will aid in assessing system vulnerability as quickly as possible. At the same time, improvements of power system equipment lead to an increase in operation limits (Wan, McCalley, & Vittal, 1999; Lachs, 2001). Increased transmission and generation capacity enables more flexibility in protection design and settings. In order for power grids of tomorrow to withstand catastrophes, it is highly desirable for the protection system to be adaptive based on system-wide considerations. An overall adaptive wide area protection design with both inherent dependability and security is now feasible. The performance of digital relays is to be substantially improved if new infrastructure and intelligent approaches fitting the technology available is adopted.

The purpose of this research work is to conceptualize and nurture adaptive protection concept for wide area systems, and to conduct feasibility studies to make this concept practically viable. The scope includes identifying and developing the desired architecture, algorithms and communication needs that facilitate the protection system to avoid and reduce the impact of system emergencies. The goal is to achieve a balance between dependability and security of the protection even under the occurrence of hidden failures in real time.

Several case studies are conducted to show the effectiveness of the proposed adaptive protection scheme. In addition, voltage stability, which is a classic wide area problem, can be alleviated with the proposed concept. Steady state and transient simulation studies provided encouraging results. The detailed decision-making algorithms are simulated in several examples for validation of the concept. Finally, the main contributions of this research work are identified.

CHAPTER 2. LITERATURE REVIEW

Two parts of work were conducted in reviewing the literature related to adaptive wide area protection and emergency control. One focused on the concept and development of adaptive protection. The second effort was to develop an annotated bibliography.

2.1 Adaptive Protection

The concept of "adaptive protection" has become commonly associated with many different proposals. For example, a relay system might adjust its bias to solve the problem in protection system design of skewing toward dependability rather than security. With computer relays connected to a communication system, one can imagine the bias being shifted toward secure operation during system stress due to component outages, impending storms, or heavy loading. Such a shift may be accomplished by adjusting the relay settings to alter the reach of relays. One can also adjust time delays or rely on backup relays. The system could then return to dependable operation when the period of stress has passed.

As a partial test of this concept, it has been shown that rapid calculation of new relay settings to maintain coordination in the event of system changes is possible. Jampala, Venkata and Damborg (1989) demonstrated the complete coordination of overcurrent relay settings for a 38-bus, 61-line system in 6 seconds using the supercomputers of 1988. While this is a small system, it was also shown that the relays that must be reset to maintain coordination in the event of topological changes are restricted to the neighborhood of the change (Ramaswami, Damborg, & Venkata, 1990). That is, in at least some cases, the extent of the required adaptation is limited.

Various definitions of adaptive protection have been used in the literature. Jampala et al. (1989, p.178) referred to *"the ability of the protection system to automatically alter its operating parameters in response to changing network conditions to maintain optimal performance."* The IEEE Power System Relaying Committee (PSRC) gave its definition (1993, p.975) of an adaptive function as one that *"automatically adjusts the operating characteristics of the relay system in response the changing power system conditions."* A more general definition (Horowitz, Phadke, & Thorp, 1988, p.1436) of adaptive protection is

given as *"a protection philosophy which permits and seeks to make adjustment to various protection functions in order to make them more attuned to prevailing power system conditions."*

Except for slight differences, all definitions suggest:

- Automatically altering, on-line, the protection system settings, functions and characteristics. This suggestion implies the need for computing and transmitting new operating parameters from a central site. Digital relays make on-line changes possible. An expanded communications system is required for realization.
- Finding optimal, condition dependent relay settings, i.e. settings that will result in the most desirable operation instead of a conventional trade-off between conflicting requirements, such as dependability and security, or for different load conditions.

A survey of adaptive protection literature between 1988 and 2002 is summarized in Table 2.1. Most striking here is the progression from basic concepts to those of wide area protection and control.

Table 2.1 Developments of adaptive protection concepts, 1988-2002

Time period	Summary of contributions
1988-1990	Basic concepts of adaptive protection Rapid coordination calculation experiments Subsystem and localization studies
1991-1993	Digital relaying systems Specific adaptive relaying examples Use of synchronized phasor measurements Surveys of industrial practice and wishes
1994-1996	Identify relays as major blackouts contributors Special purpose adaptive applications Identify concept of hidden failures Discussion of on-line coordination
1997-1999	Additional applications: auto reclosure, transformer protection Additional techniques: agents, decision trees Experiments with wide area concepts
2000-2002	Classify mechanism of hidden failures Experiments with new strategies in regional back-up protection

Recent studies of wide area control measures for avoiding or minimizing the impact of system disruptions have made liberal use of protection components. Hence, they should be

considered, at least in part, as extensions of the protection system. Most of them rely on switching action as a result of decisions based on measurements collected over a wide geographical area and the response depends on the system operating state. These are clear examples of adaptive protection. The studies reviewed in this section will serve to illustrate the point.

Two related papers by EPRI (1997) and Rovnyak, Taylor, and Thorp (1997) studied the ability to use phasor measurements distributed over the Western Electricity Coordinating Council (WECC, the previous WSCC) system to control otherwise unstable disturbances. The EPRI report (1997) examined preferred locations for the Phasor Measurement Units (PMU) as well as the communication networks necessary to collect the system phasor measurements at a central site. The study also investigated the stabilizing ability of rapid changes in HVDC transmission for selected contingencies on the WECC system, a control that may be possible as a result of the phasor measurements. Rovnyak et al. (1997) expanded the arsenal of controls and explored decision trees as a mechanism for making the control decisions that would be required to dispatch such control signals. It was found that, using a 176-bus model of the WECC system, an instability patterned on a 14 December 1994 disturbance could have been stabilized through a combination of generator tripping, HVDC flow adjustment, and load shedding distributed throughout the WECC system. In particular, the load shedding actions occurred at 16 buses distributed from the Pacific Northwest to Southern California. Of significance to protection system design is the breaker action due to load shedding and, perhaps, generator tripping. Since these actions were initiated 0.1 second (100 ms) after the event, the demands on the communication and control system were significant.

Researchers at Hydro-Quebec studied persistently troublesome instabilities on their system, ones that were uncontrollable with local controls alone (Kamwa, Grondin, Asber, Gingras, & Trudel, 1999). They found from simulation studies that the system could be stabilized with load modulation using signals derived from a mix of local information and global, i.e. phasor measurements at remote locations. The sensitivity of load-modulation-controller performance to communication time delays was examined and found to be an

important issue. Depending on the controller design, otherwise stable transients would become unstable if signal delays were as small as 250 ms.

Finally, Electricite de France (Faucon & Dousset, 1997; Houry & Faucon, 1999) reported on studies conducted for a "defense plan" in Southern France in the event of instabilities. If an out-of-step condition is detected, the plan is to isolate appropriate regions and adjust the balance of generation and loads in each island to sustain stable operation. The scheme involves detecting the instability at a central site using phasor measurements and sending trip signals to lines to accomplish the area isolation, and to loads to balance with the area generation. Their studies indicated that control action must be initiated within 1.3 seconds and they estimated that it could be accomplished in 1.07 seconds. The satellite communication system consumed 690 ms of this interval for wide area communications.

It can be observed from these studies that rapid switching actions, including adaptive islanding, load shedding and generator tripping, are beneficial in maintaining synchronism in unstable situations. Such use of the protection system over a wide area places very demanding requirements on the communication and control system. Faucon and Dousset (1997) analyzed these requirements and suggested they could be accomplished within the 1.3 seconds required. Other cases examined were more demanding requiring control action in as short an interval as 0.1 second. In a later chapter the time required for gathering data, making decisions and effecting control over a wide area is studied. It is estimated to be less than 200 ms using modern communication technology.

2.2 Bibliography on Adaptive Wide Area Relaying

An annotated bibliography was developed in this research. It covers various topics related to adaptive wide area relaying in the last 14 years and contains 81 entries. In this section the different categories of topics are listed for better understanding of the research work.

2.2.1 Advances in Protection

Local and regional protection techniques development is the most direct category that this research is involved. On one hand the rich resource of protection principle, algorithm and

practice advances provide the arsenal for detailed relay design improvement. On the other hand the topics in this category are confined by traditional protection philosophy.

- Local protection
  - Component protection
  - Automatic coordination
  - Adaptive autoreclosure
- SPS

2.2.2 *Wide Area Protection & Hidden Failures*

As new problems were found and as new needs emerged, new concepts were discussed in this category. So far the study of wide area protection and hidden failures is at the conceptual stage in the sense that no details, such as wide area protection architecture, system requirements considering the existence of hidden failures, or practical models and study approaches of hidden failures were proposed. Nevertheless, the discussion broadened the sight of protection engineers and intrigued more research interest.

2.2.3 *Relevant New Techniques*

These are new techniques in areas other than protection itself. They are, however, appealing for possible adoption in future relaying systems.

- Measurements
  - Sensors
  - Measuring algorithms
- Countermeasures in control
- Communications

2.2.4 *Artificial Intelligence Applications*

The brief introduction of Artificial Intelligence and its application in power system and protection are provided for the purpose of comparing existing AI approaches. The feasibility of applying various AI techniques to adaptive wide area protection algorithms was probed.

2.2.5 System Study

Profound understanding of system behavior with current protection is gained through post-mortem study of wide area disturbances conducted by other researchers.

- Voltage stability study
- Angular stability study

The annotated bibliography, along with a broad literature review, provides the researcher a solid base for adaptive wide area protection study and design.

CHAPTER 3. ADAPTIVE WIDE AREA PROTECTION DESIGN

The primary purpose of this chapter is to discuss various facets of adaptive wide area protection systems in order to generate thought-provoking ideas from protection engineers. The block diagram shown in Fig. 3.1 is to provide a quick overview of the proposed concept. From this diagram one can discern that there are many issues that need to be considered and implemented. In Section 3.1, two operating modes of adaptive protection are first defined. The relative issues on risk of security versus dependability for protection schemes are presented in Section 3.2. By analyzing the nature of the protection system, a new paradigm to view the overall protection architecture is offered and consequently the limitations of current protection systems are exposed in Section 3.3. The main contributions of SPS in combating problems of traditional component protection are introduced in Section 3.4. At the same time, it is also pointed out that SPS has its own limitations in meeting the needs of wide area protection systems. These observations motivated the author to propose new adaptive protection architecture for wide area power system protection. The hardware and logical details of this new and revolutionary architecture are proposed in Section 3.5. To realize the proposed architecture, decision-making algorithms for adaptive relaying are examined in detail in Section 3.6. Finally both single-phase and three-phase adaptive reclosure are briefly probed in Section 3.7 to complete the adaptive wide area protection design.

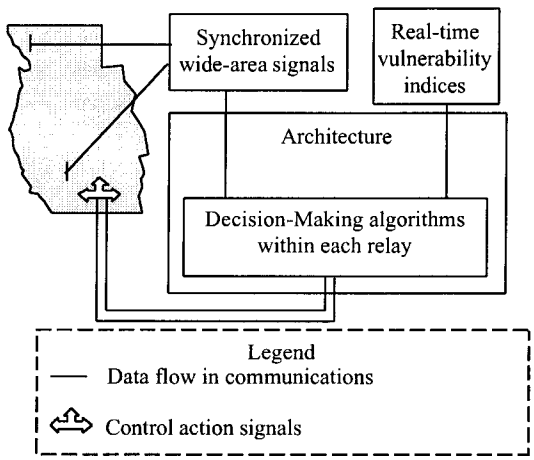

Figure 3.1 Conceptual block diagram of adaptive wide area protection

3.1 Two Forms of Adaptive Protection: Preventive and Emergency

Two different operating modes under which the protection system is required to respond are identified for the purpose of adaptive protection design. One mode anticipates vulnerabilities and positions the system to be more robust in the event of a threat. This first mode is called *Preventive Adaptive Protection* in which the protection system's characteristics are altered when the system is under stress. For example, the relay might adjust parameters by itself during heavy loading to guard against the impact of hidden failures. These changes are made before any fault but with the intent that, should such an event occur, the possibility and impact of any unnecessary operation of protection devices on the system would be minimal.

Another mode is *Emergency Adaptive Protection* in which the protection system reacts to an emergency by taking additional actions to restrict the impact of a relay unnecessary operation. For example, if a fault occurs and a hidden failure results in unnecessary line outages, a system-wide instability could occur. However, if corrective action were taken quickly and adaptively, a large outage may be avoided. This more ambitious response mode might identify a developing emergency and respond to diminish its impact, e.g. create islands with balanced generation and load in the event of a transient or dynamic instability.

Under the *Preventive Adaptive Protection* mode, there is adequate time for conducting off-line stability and risk analysis of the entire system. Therefore proper control measures are chosen to preserve the system security. In contrast, *Emergency Adaptive Protection* has a more critical response time requirement so the design of its architecture, algorithms and communications all need thorough assessment before being adopted. In this research more effort is devoted to the design of *Emergency Adaptive Protection*. These two operational modes are examined and discussed in detail in Chapter 5 based on the simulation of six cases via the proposed approach on a 179-bus equivalent test system.

3.2 Risk of Security versus Dependability for Power System Protection

It is observed that the prohibitive cost of wide area blackouts requires a philosophical shift from conventional "component protection" to "system protection", and from *"dependability"* to *"security"* of relay operation when a system is under stress (Phadke et al., 1999). In this section the balance of security versus dependability for power system protection is discussed to examine the intuitive observation stated above.

The reliability of a protection system has two aspects: *dependability* and *security.* Being "dependable" requires the protection system to operate correctly for all the faults for which it is designed to operate. If it fails to operate successfully when required then its dependability is lost. Being "secure" requires the protection system to operate only when it is intended to do so. Unnecessary or false tripping of any relay is identified as the loss of security.

A relay design can achieve the balance between dependability and security, for example, by tuning the relay sensitivity. Higher sensitivity usually leads to the tendency of relay false tripping due to the inevitable noise in the measurements. On the other hand, lower relay sensitivity may result in slow action or even possible failure to trip. In real life the design and configuration of protection schemes can be complicated and random failures of the relay parts may affect the relay behavior unexpectedly, thus the relationship between dependability and security may be very complex and difficult to study. In general, enhancing one measure would mean decreasing the other (Blackburn, 1998).

Traditionally the probability of protection systems "false tripping" is higher than that of their "failure to trip". This situation is acceptable for a grid with many alternative paths for power to flow from generators to loads. Intuitively it is reasonable because with multiple redundancies in the system, the loss of a component, say a transmission line, would not have severe impact on the system integrity and no customers are affected. However, when the system is critically loaded, or if it is experiencing contingencies, the relays can not afford to falsely trip and the philosophy of leaning to dependability is no longer appropriate (Horowitz & Phadke, 1992).

To decide the relay reliability bias between dependability and security, it is necessary to compare the impact of "false tripping" with that of "failure to trip". In the real world "failure to trip" of a primary relay usually ends up with isolation of the fault by backup relays. If it is a local backup, the impact is likely to be minimal. On the other hand if it is a remote backup then it will de-energize a larger portion of the system and therefore poses more threats to the system integrity. There are other factors that could also adjust the impact of a relay operation significantly, such as hidden failures and the social cost of blackouts. Therefore the decision on the balance of dependability versus security is a complex issue needing a careful examination and introspection. In the following examples, the author attempts to provide a simple risk analysis of protection systems operation to demonstrate that the balance between dependability and security varies as the system operating status changes. Firstly the composite risk of the protection system unreliability is defined and then each term is analyzed numerically.

Let A be the event of a relay tripping successfully.

B be the complement of A.

F denote a fault on a protected component, or referred to as the environment with hazard.

NF denote the complement of F.

Therefore A n NF denotes the unconditional event of "relay false tripping" (the same as a mis-operation or an unnecessary operation).

Similarly B n F denotes the unconditional event of relay "failure to trip".

R (A n NF) denotes the risk of relay false tripping.

R (B n F) denotes the risk of relay failure to trip.

P (A n NF) denotes the probability of relay false tripping.

P (B n F) denotes the probability of relay failure to trip.

C (A n NF) denotes the cost of relay false tripping.

C (B n F) denotes the cost of relay failure to trip.

Events A and B are assumed to be mutually exclusive, therefore dependent[1].

[1] Although Anderson (1999, p.1009) discussed the case of "events that are independent and disjoint (the same term as mutually exclusive)" , it is almost meaningless unless at least one of the two events is an empty set. This

The composite risk R from the two modes of relay failure, namely, false tripping and failure to trip is given by:

$$R = R(A \cap NF) + R(B \cap F)$$
$$= C(A \cap NF) * P(A \cap NF) + C(B \cap F) * P(B \cap F) \quad (3.1)$$

3.2.1 Risk versus Cost Analysis

Equation (3.1) forms the basis for risk analysis. It can be observed from this equation that the overall risk of a protective operation to the system has contributions from both probability of each unreliable mode and its corresponding cost to the system. The following examples provide a very basic and simplified analysis on the "risk versus cost" facet and the risk analysis from the probability point of view is discussed in Subsection 3.2.2. The examples are intended to illustrate the instinctive observations instead of systematically analyzing the risk of protection systems, which is beyond the scope of this research.

3.2.1.1 Example 1: protection of a single component

In this example two typical schemes of a two-relay protection system that protects a single component such as a generator or a transmission line, are compared. The first one considers a series layout which requires two-out-of-two for the successful protective operation and the second one applies a parallel logic requiring one-out-of-two for the successful protective operation.

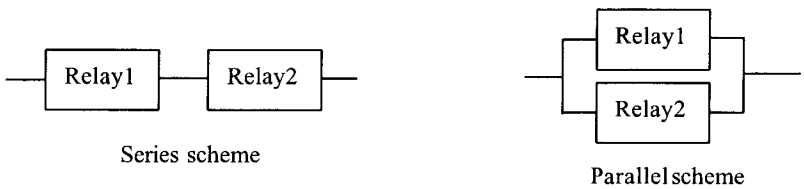

Figure 3.2 Two typical schemes of a two-relay protection system

---

is because non-empty mutually exclusive events are dependent. The reasoning of this statement is briefly listed as below:

For mutually exclusive events E1 and E2, P (E1 n E2) = 0;
For independent events E1 and E2, P (E1 n E2) = P (E1) * P (E2);
For non-empty events E1 and E2, P (E1) ? 0 and P (E2) ? 0, so P (E1) * P (E2) ? 0.

Therefore non-empty events A and B cannot be both independent and mutually exclusive. This conclusion is straightforward to understand since being mutually exclusive means that both events cannot occur simultaneously. In other words, if one event happens the other can not happen. This way the occurrence of one event has a great effect on the occurrence probability of the other. Thus the events are dependent.

The series scheme is more secure but less dependable than the parallel one.

Extending the notations in equation (3.1), define:

A_{series} and B_{series} as the events of tripping and not tripping, respectively, of the series protection scheme;

$A_{parallel}$ and $B_{parallel}$ as the events of tripping and not tripping, respectively, of the parallel protection scheme;

a_1 and b_1 as the events of tripping and not tripping, respectively, of relay 1;

a_2 and b_2 as the events of tripping and not tripping, respectively, of relay 2;

$P(a_i \mid NF)$ and $P(b_i \mid F)$ as conditional probabilities of "relay i false tripping" and "relay i failure to trip", respectively, where i = 1, 2;

$C(A \text{ n } NF)$ as the cost to the grid due to the protection scheme false tripping, assuming that the protection scheme internal layout makes no difference on the protection failure cost to the grid, or $C(A_{series} \text{ n } NF) = C(A_{parallel} \text{ n } NF) = C(A \text{ n } NF)$;

$C(B \text{ n } F)$ as the cost to the grid due to the protection scheme failure to trip, similarly assuming $C(B_{series} \text{ n } F) = C(B_{parallel} \text{ n } F) = C(B \text{ n } F)$.

The composite risk of the two protection schemes can be expressed as:

$$\begin{aligned} R_{series} &= C(A \text{ n } NF) * P(A_{series} \text{ n } NF) + C(B \text{ n } F) * P(B_{series} \text{ n } F) \\ &= C(A \text{ n } NF) * \{P(a_1 \mid NF) * P(a_2 \mid NF) * [1 - P(F)]\} + C(B \text{ n } F) * \{[P(b_1 \mid F) + P \\ &\quad (b_2 \mid F) - P(b_1 \mid F) * P(b_2 \mid F)] * P(F)\} \end{aligned} \tag{3.2}$$

$$\begin{aligned} R_{parallel} &= C(A \text{ n } NF) * P(A_{parallel} \text{ n } NF) + C(B \text{ n } F) * P(B_{parallel} \text{ n } F) \\ &= C(A \text{ n } NF) * \{[P(a_1 \mid NF) + P(a_2 \mid NF) - P(a_1 \mid NF) * P(a_2 \mid NF)] * [1 - P(F)]\} + \\ &\quad C(B \text{ n } F) * [P(b_1 \mid F) * P(b_2 \mid F) * P(F)] \end{aligned} \tag{3.3}$$

To simplify the case, the two relays are assumed to be identical. It is assumed that for each relay, the conditional probabilities of "relay false tripping" and "relay failure to trip" remain constant under different power system stress level (Anderson, 1999). Using the same data as Anderson (1999) did, $P(a_1 \mid NF) = P(a_2 \mid NF) = 0.05$, $P(b_1 \mid F) = P(b_2 \mid F) = 0.025$ and $P(F) = 10^{-4}$, equations (3.2) and (3.3) yield:

$$R_{series} = 2.5 * 10^{-3} * C(A \text{ n } NF) + 5 * 10^{-6} * C(B \text{ n } F)$$

$$R_{parallel} = 9.7 * 10^{-2} * C (A \text{ n } NF) + 6.3 * 10^{-8} * C (B \text{ n } F)$$

Obviously, the values of C (A n NF) and C (B n F) will determine the better scheme in term of minimal composite system.

- When C (A n NF) < $5.2 * 10^{-5}$ * C (B n F), $R_{series} > R_{parallel}$, which means the secure series logic scheme has a higher overall risk[2];
- When C (A n NF) > $5.2 * 10^{-5}$ * C (B n F), $R_{series} < R_{parallel}$, which means the same pro-security series scheme has a lower overall risk than the dependable parallel one.

To compare the risk of these two protection schemes, real costs of protection failures to the grid need to be explored further. Anderson (1999) claims that C (A n NF) << C (B n F). He argued that for a synchronous generator, the cost of an adverse tripping of a relay could be thousands of dollars. It is for the purchase of replacement energy at a higher cost. While the permanent damage to the generator could even mean millions of dollars if the relay fails to protect it. This assumption is true for lightly loaded to normal conditions due to the fact that there is always spinning reserve from other generators so adverse tripping of a generator is not catastrophic to the power grid. However, if the grid is already highly stressed to the extent of being (N-1) insecure, losing one more generator may lead to loss of synchronism, system islanding and extensive blackout, resulting in catastrophic conditions. In such a case, C (A n NF) could also reach millions of dollars or even more. Consequently the cost of "relay false tripping" would become comparable to that of "relay failure to trip" for stressed power grids. Thus the more secure relay scheme would have lower overall risk and becomes more preferable.

We point out that the results of this example are driven largely by the extreme events, specifically the extreme undependable failure mode, i.e., the two-relay failure to trip and the extreme insecure failure mode, i.e., the two-relay false tripping. An important assumption

[2] In general, when comparing any two protection schemes S1 and S2, when C (A n NF) * [P (A_{S1} n NF) - P (A_{S2} n NF)] < C (B n F) * [P (B_{S2} n F) - P (B_{S1} n F)], where the subscripts of S1 and S2 indicate these two schemes, $R_{S1} < R_{S2}$, suggesting scheme S1 is better than scheme S2 in the sense of overall risk of relay failure.

underlying this example is that the extreme undependable failure mode is constant with system stress, but the consequence of the extreme insecure failure mode changes significantly with system stress. Specifically, the consequence of the extreme undependable failure mode is given as 2C(G)+C(N-2); for the unstressed case, this is 1,000,020, and for the stressed case, 1,002,000. In terms of order of magnitude, this is effectively no change. In contrast, the consequence of the extreme insecure failure mode is given as C(N-2); for the unstressed case, this is 20, and for the stressed case, 2000, a difference of 2 orders of magnitude. As a result (given that probabilities are constant with increasing stress), we see

- virtually no change in risk of the extreme undependable failure mode (0.487583001 to 0.488065703)
- a change in risk of the extreme insecure failure mode of 2 orders of magnitude (0.190106 to 19.03029)

Reasoning for the above stated assumption is based on a perception that

- the extreme insecure failure would result in possible load interruption, whereas the cost of load interruption certainly varies with the load level drastically, and that
- the consequence of the undependable failure mode changes less drastically with system stress because the extreme undependable relay failure would cause equipment damage due to the presence of the high fault currents, plus the load interruption.

When the cost of equipment which is considered constant is usually much larger than that of a load interruption, the overall cost of relay undependable failure varies insignificantly with system load level.

This simple example shows that the protection reliability bias between dependability and security of different relay schemes under different operational conditions can be analyzed by the probability and cost of different modes of protection failure. This analytical approach may be generalized to a large power system, although the procedure could be complex and challenging. Normally the operation condition of a grid is required to be (N-1) secure, as the stress going up, the grid becomes less secure. There is a certain point at which

the grid becomes (N-1) insecure. It is therefore desirable to identify the grid stress level and to adjust the protection system behavior accordingly.

Based on the result of this simple example, one might conclude that, for highly stressed power grids, we should bias protection systems more towards security than for lightly loaded systems needing higher dependability. This might be the case, but before reaching a strong conclusion to this effect, it is necessary to examine at least two additional questions.

- To what extent should protection bias be driven only by the extreme events?
- To what extent do failure probabilities vary with system stress?

We believe that our above analysis provides an excellent springboard for investigating these additional questions.

3.2.1.2 Example 2: protection of two components

In this example, the same risk analysis approach as in previous subsection is applied to compare different schemes for the protection of two components. Two sets of two-relay protection schemes same as those in the previous example are installed to protect two components, such as generators or transmission lines. The two sets of protection schemes are either both series layout to create a pro-security scheme or both parallel as a pro-dependability setting.

When the protected components are electrically far away from each other, neither protection scheme is able to see the fault occurring nearby the other component. The operation of each protection scheme depends only on the prevailing condition of the neighborhood of its own protected component and the relays characteristics. That is, the behavior of the two sets of protection schemes is assumed to be independent. Tables 3.1 through 3.3 show the calculation of probability and risk in this independent case. Table 3.1 provides the probability data and formulas used for the calculation that follows. The following data used are again borrowed from Anderson (1999):

a, representing protection conditional false tripping probability;

b, representing protection conditional failure to trip probability;

p, representing power grid fault rate.

Tables 3.2 and 3.3 calculate the risks of the pro-security scheme and the pro-dependability scheme under different grid conditions. In an (N-2) secure grid the cost of (N-2) contingency is relatively low (assumed to be $0 in Table 3.2) comparing to the cost of damaging the facility (assumed to be $1,000,000 in Table 3.2). Therefore the overall risk of all 12 unreliable modes of the more secure protection scheme (9.88 in Table 3.2) is higher than that of the pro-dependability scheme (0.125 in Table 3.2). Whereas when the grid is (N-2) insecure the cost of (N-2) contingency can be quite high (assumed to be $10,000 in Table 3.3), leading to a different comparison of the risks of the two protection schemes[3]: pro-security scheme 9.94 and pro-dependability scheme 95.4 in Table 3.3. The conclusion from this example is similar to that from Example 1 -- highly stressed power grids would need the protection system biased more towards security than lightly loaded systems towards dependability.

Table 3.1 Probabilities of relay operations

	Probability formulas	one relay	series scheme (of two relays)	parallel scheme (of two relays)
Protection conditional false tripping	a	0.05	0.05*0.05=0.0025	0.05+0.05-0.05*0.05=0.0975
Protection conditional failure to trip	b	0.025	0.025+0.025-0.025*0.025=0.049375	0.025*0.025=0.000625
Protected component fault rate	p	0.0001	0.0001	0.0001
Protection unconditional false tripping	a * (1-p)	0.049995	0.00249975	0.09749025
Protection unconditional failure to trip	b * p	0.0000025	4.9375E-06	6.25E-08
Protection normal	(1-a) * (1-p)	0.949905	0.99740025	0.90240975
Protection correct tripping	(1-b) * p	0.0000975	9.50625E-05	9.99375E-05

Table 3.2 Risk of protection operations with the grid (N-2) secure

	formulas	2 series schemes: secure	2 parallel schemes: dependable
assumed cost of (N-2) contingency ($)	C(N-2)	0	0
assumed cost of damaging the equipment ($)	C(G)	1.00E+06	1.00E+06
risk of 2 schemes false tripping	C(N-2)*a*(1-p)*a*(1-p)	0	0

[3] The cost to the system of a contingency varies greatly with many factors such as different types of contingency and system operating conditions. In this case, assuming the cost of (N-1) contingency is zero, the threshold cost of (N-2) contingency is $1,024. That is, as long as the cost is below $1,024, the risk of the pro-security scheme is higher than that of the pro-dependability one. If the cost of (N-1) contingency is actually larger than zero, the threshold cost of (N-2) contingency is even smaller.

risk of 1 scheme false tripping, 1 correct tripping, (2 cases)	2*C(N-2)*a*(1-p)*(1-b)*p	0	0
risk of 1 scheme false tripping, 1 failure to trip, (2 cases)	2*[C(N-2)+C(G)]*a* (1-p)*b*p	0.024685031	0.012186281
risk of 1 scheme correct tripping, 1 failure to trip, (2 cases)	2*[C(N-2)+C(G)]*b*p*(1-b) *p	0.000938742	1.24922E-05
risk of 2 schemes failure to trip	[2*C(G)+C(N-2)]*b*p*b*p	4.87578E-05	7.8125E-09
(N-2) cases overall risk	sum	0.025672531	0.012198781
assumed cost of (N-1)contingency($)	C(N-1)	0	0
risk of 1 scheme false tripping, 1 normal (2 cases)	2*C(N-1)*(1-a)*(1-p)*a*(1-p)	0	0
risk of 1 scheme normal, 1 failure to trip, (2 cases)	2*C(N-1)*(1-a)*(1-p)*b*p	9.85E+00	1.13E-01
(N-1) cases overall risk	sum	9.85E+00	1.13E-01
summing all 12 cases	sum	9.88E+00	1.25E-01
cost of normal condition ($)	C(N)	0	0
2 schemes normal	C(N)*(1-a)*(1-p)*(1-a)*(1-p)	0	0
2 schemes correct tripping	C(N-2)*(1-b)*p*(1-b)*p	0	0
1 scheme correct tripping, 1 normal (2 cases)	2*C(N-1)*(1-a)*(1-p)*(1-b)*p	0	0
summing all 16 cases	sum	9.88E+00	1.25E-01

Table 3.3 Risk of protection operations with the grid (N-2) insecure but (N-1) secure

	formulas	2 series schemes: secure	2 parallel schemes: dependable
assumed cost of (N-2) contingency ($)	C(N-2)	1.00E+04	1.00E+04
assumed cost of damaging the equipment ($)	C(G)	1.00E+06	1.00E+06
risk of 2 schemes false tripping	C(N-2)*a*(1-p)*a*(1-p)	0.062487501	95.04348845
risk of 1 scheme false tripping, 1 correct tripping, (2 cases)	2*C(N-2)*a*(1-p)*(1-b)*p	0.00475265	0.194858637
risk of 1 scheme false tripping, 1 failure to trip, (2 cases)	2*[C(N-2)+C(G)]*a* (1-p)*b*p	0.024931882	0.012308144
risk of 1 scheme correct tripping, 1 failure to trip, (2 cases)	2*[C(N-2)+C(G)]*b*p*(1-b) *p	0.00094813	1.26171E-05
risk of 2 schemes failure to trip	[2*C(G)+C(N-2)]*b*p*b*p	4.90016E-05	7.85156E-09
(N-2) cases overall risk	sum	0.093169163	95.25066786
assumed cost of (N-1)contingency($)	C(N-1)	0	0
risk of 1 scheme false tripping, 1 normal (2 cases)	2*C(N-1)*(1-a)*(1-p)*a*(1-p)	0	0
risk of 1 scheme normal, 1 failure to trip, (2 cases)	2*C(N-1)*(1-a)*(1-p)*b*p	9.85E+00	1.13E-01
(N-1) cases overall risk	sum	9.85E+00	1.13E-01
summing all 12 cases	sum	9.94E+00	9.54E+01
cost of normal condition ($)	C(N)	0	0
2 schemes normal	C(N)*(1-a)*(1-p)*(1-a)*(1-p)	0	0
2 schemes correct tripping	C(N-2)*(1-b)*p*(1-b)*p	9.03688E-05	9.9875E-05
1 scheme correct tripping, 1 normal (2 cases)	2*C(N-1)*(1-a)*(1-p)*(1-	0	0

	b)*p		
summing all 16 cases	sum	9.94E+00	9.54E+01

When the two sets of protection schemes are installed on components that are electrically close, for example on adjacent lines, they may react to the same fault or disturbance. Thus their operations are no more independent. It is complex to precisely study the dependent events without going into excessive details of the relay location, protection principle, fault type, fault location, etc. In Table 3.4, it is assumed that the two sets of protection schemes are installed so close that the fault zones they can detect are the same.

Table 3.4 Risk of protection operations for fully dependent case, with the grid(N-2) secure

	formulas	2 series schemes: secure	2 parallel schemes: dependable
assumed cost of (N-2) contingency ($)	C(N-2)	0	0
assumed cost of damaging the equipment ($)	C(G)	1.00E+06	1.00E+06
risk of 2 schemes false tripping	C(N-2)*a*(1-p)*a	0	0
risk of 1 scheme false tripping, 1 correct tripping, (2 cases)	2*C(N-2)*a*(1-b)*p	0	0
risk of 1 scheme false tripping, 1 failure to trip, (2 cases)	2*[C(N-2)+C(G)]*a*b*p	0.0246875	0.0121875
risk of 1 scheme correct tripping, 1 failure to trip, (2 cases)	0	0	0
risk of 2 schemes failure to trip	0	0	0
(N-2) cases overall risk	sum	0.0246875	0.0121875
assumed cost of (N-1)contingency($)	C(N-1)	0	0
risk of 1 scheme false tripping, 1 normal (2 cases)	2*C(N-1)*(1-a)*(1-p)*a	0	0
risk of 1 scheme normal, 1 failure to trip, (2 cases)	2*C(N-1)*(1-a)*b*p	9.85E+00	1.13E-01
(N-1) cases overall risk	sum	9.85E+00	1.13E-01
summing all 12 cases	sum	9.88E+00	1.25E-01
cost of normal condition ($)	C(N)	0	0
2 schemes normal	C(N)*(1-a)*(1-p)*(1-a)	0	0
2 schemes correct tripping	0	0	0
1 scheme correct tripping, 1 normal (2 cases)	2*C(N-1)*(1-a)*(1-b)*p	0	0
summing all 16 cases	sum	9.88E+00	1.25E-01

The conclusion again is the same as that from previous analysis. In Table 3.4 which represents the (N-2) secure condition, the more secure scheme has a higher overall risk, whereas things are reversed under the (N-2) insecure condition. The table for the (N-1)

secure but (N-2) insecure case is omitted since the formulas and data are almost the same as the ones in Table 3.4. The only difference is that in the (N-2) insecure table, the cost of (N-2) contingency is set as $10,000 instead of $0 as in Table 3.4. This leads to the same result as in Table 3.3, with the risks of the two schemes being 9.94 and 95.4, respectively. As one can expect, if an even higher cost of grid collapse is assumed, say, $100,000, the advantage of the pro-security scheme would be much more apparent, with a risk of 10.5 compared to 953 of the more dependable scheme.

3.2.2 Risk versus Probability Analysis

The factors contributing to the risk of relay failures are the probabilities of different failure modes and the corresponding cost to the grid. In Subsection 3.2.1, the variation of the overall risk is substantially credited to different failure costs under different operating conditions. This is because in the risk analysis it is assumed that for each relay, conditional probabilities of "relay false tripping" and "relay failure to trip" remain constant under different power system operational conditions. Recent work has shown that this assumption needs slight adjustment since the probabilities of relay failures also change under different operation conditions (Seegers et al., 2001; Wang & Bollen, 2001). It is shown that the probability of some relays "false tripping" in a stressed grid is higher than that in a lightly loaded grid, but the probability of their "failure to trip" in a stressed grid is lower than that in a lightly loaded grid.

The impact of loading level on relay false operations in steady state is summarized as follows:

- The protection design and relay setting philosophies are to avoid influence between protection and grid loadability. There are some relays with the operation principle immune to loading levels (Seegers et al., 2001):
  - Current differential relays are almost completely immune to increased load on a protected line. As the load current increases, the spurious differential current caused by finite CT accuracy will increase, but at the same time, the restraining current will increase as well. The percentage characteristic ensures relay stability for any amount of overload.

- Phase comparison relays respond to phase relation between the currents at all the terminals of a protected line. As the load current increases, the relationship of the phase angles of the currents at the line terminals remains consistent thereby preventing false tripping.

- It has been observed by other researchers that some relays are inherently susceptible to load level impact due to their operation principle (Seegers et al., 2001; Wang & Bollen, 2001):
  - The overcurrent relays may operate unnecessarily because of measurement inaccuracy during high current situations, such as cold load picking up;
  - Different distance relay characteristics will exhibit different responses to loading. In general, distance replays are less susceptible to the impact of steady state loading levels, whereas transient currents may cause false operations.

The potential impact of disturbances on protection systems is also studied and summarized in Table 3.5 (Wang & Bollen, 2001).

Table 3.5 Power system disturbances and corresponding impacts on protective relays*

Disturbance type	Undervoltage	Overcurrent	Impedance	Overvoltage
Voltage transient	V	X	X	V
Current transient	X	V	X	X
Voltage swell	X	X	X	V
Voltage sag	V	V	V	X
Voltage fluctuation	V	X	V	V
Short-time overload	X	V	V	X

* Legend of the impact level: X -- minor or no impact; V -- potential impact.

In summary, based on the work quoted, the impact of loading on relay false operations shows that the conditional probability of false tripping, P (A | NF) of some relays could change under different operation conditions. This variation would contribute to the overall risk of the protection system unreliability. To gain more perspective, assume relays are designed and set to operate with a proper balance between security and dependability in reducing the overall risk to the system. When the grid is highly stressed, the probability of relay false tripping becomes even higher. With all other factors remaining the same, shifting the relay reliability towards security is necessary to preserve utmost security of the system.

Thus the conclusion is that the relays should be shifted more towards security under stressful loading conditions. Table 3.6 provides a numerical explanation of this conclusion. The data are from the aforementioned Example 1. The only difference is that the value of conditional false tripping probability (a) in Table 3.6 is considerably higher than that in Example 1. Comparison of Table 3.6 with Example 1 shows that the change in the relay conditional false tripping probability alone may have apparent influence on the overall risk of protection failures.

Table 3.6 Risk influenced by the change in probability

	formulas	one relay	series scheme of two relays (secure)	parallel scheme of two relays (dependable)
conditional false tripping	a	0.06	0.0036	0.1164
conditional failure to trip	b	0.025	0.049375	0.000625
fault rate	p	0.0001	0.0001	0.0001
unconditional false tripping	a*(1-p)	0.059994	0.00359964	0.11638836
unconditional failure to trip	b*p	0.0000025	4.9375E-06	6.25E-08
normal	(1-a)*(1-p)	0.939906	0.99630036	0.88351164
correct tripping	(1-b)*p	0.0000975	9.50625E-05	9.99375E-05
cost of false tripping	C(N-1)	52	52	52
cost of failure to trip	C(G)	1.00E+06	1.00E+06	1.00E+06
overall risk	C(N-1)*a*(1-p)+C(G)*b*p		5.12468128	6.11469472

3.3 Nature of the Protection System

The protection philosophy needs improvement as researchers have realized in recent years (Phadke et al., 1999). In this section, the author examined the nature of protection so the weak point of relaying system performance can be identified. The goal of this analysis is to lay the ground for proposing the adaptive protection in sections 3.5 through 3.7.

Considering the overall protection design in power system, there are two aspects involved that can be decoupled to a certain extent. One is the *individual relay mechanism* at the micro level and the other is the *protection system scheme* at the macro level. The characteristic differences of the two are listed below for further comparison and analysis:

- *Individual relay mechanism* implies the theory, principle, or decision-making algorithm of each relay.

- It reflects the functional relationship of output signals and input signals in the form of curves, tables or formulas.
- It relies more on the scientific information, e.g. studies of short circuit, stability and disturbance propagation.
- The techniques have always developed to produce better relay mechanisms, from over-current relays to differential relays, from distance relays to traveling wave relays.

- *Protection system scheme* is the strategy with which all relays are organized and the way in which they cooperate and coordinate with each other.
  - The major concern in *protection system scheme* is the coordination between primary protection and backup protection.
  - The detailed decision-making mechanism inside the relay is considered as a black box at this level; only the output signals and their interaction matter.
  - It has been more of an art than science. Therefore it needs to be reconsidered in a theoretic and mathematical way.

As one can realize from de-coupling these two logic levels, more study focusing on improving the *protection system scheme* is needed for a potential leap in relay system enhancement.

The reason of protection being "dependable" rather than "secure" can be analyzed from this layered point of view. The origin of this inherent limitation of component protection may trace back to the natural evolution of *protection system scheme* during the past seventy years (Sidhu et al., 2002). The features of *protection system scheme* as it is adopted presently are summarized as below:

- All relays are self-contained in the sense that they implement the measurements and logic individually, and trigger output actions independently which are tripping signals sent to circuit breakers;
- Unreliability of protection is unavoidable due to part failures including hidden failures etc. The strategies for combating it are different for the two aforementioned aspects of reliability:

- Dependability is enforced by multiple redundancies of relays. Designated backup relays can backup primary relays locally or in the immediate region of adjacent one or two buses;
- Security is considered less of a problem in the protection history. Occasionally when a specific relay tends to falsely trip excessively, an additional series supervisory relay is deployed to form a more secure tripping decision.

- Since many relays, both primary and backup, may control the same tripping device in a logically parallel way, coordination among relays is realized by using fixed discrete time delay steps;
- There is uncertainty in each decision-making step because of inevitable noise from measurements, insufficient/erroneous information etc. But each relay generates deterministic tripping or no-tripping decisions. Uncertainty is expressed by simply applying margins in relay settings.

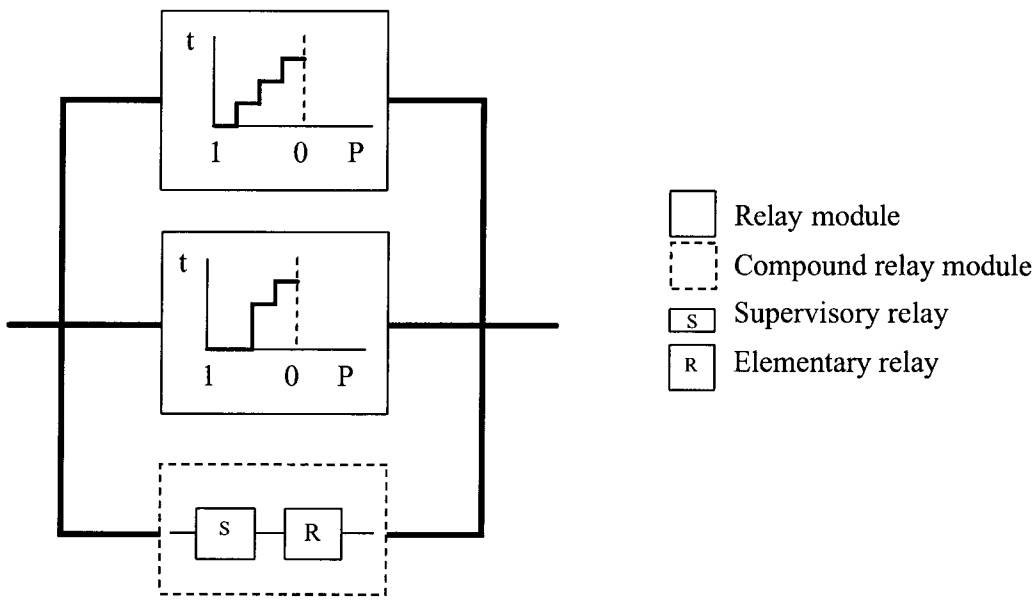

Figure 3.3 Logic diagram of existing protection system scheme for one protected component

Above is the *protection system scheme* that protection engineers recommended many decades ago (Sidhu et al., 2002). The logic used for protecting a power system device is shown in Fig. 3.2. It has been a smart and inexpensive model of the physical phenomena based on the techniques at that time. But more requirements as well as problems are

emerging. This invokes the thoughts that today might be the time for establishing a more advanced scheme. The new scheme is expected to be based on developing techniques, not only in the domain of power systems, but also in mathematics, control theory, computer science, communication applications, sensor and measurement techniques, and many breakthroughs in related areas.

3.4 An Intermediate Solution: SPS

Protection design philosophy has been slowly but obviously changing. The improvement is in the sense of shifting the bias from local protection to regional protection, from assuring dependability to pursuing security.

A major advancement was the introduction of System Protection Scheme (SPS) to expand the protection philosophy from a component level to a system level. According to NERC (2002, p.2), SPS is defined as *"an automatic protection system (also known as a remedial action scheme) designed to detect abnormal or predetermined system conditions, and take corrective actions other than and/or in addition to the isolation of faulted components to maintain system reliability. Such action may include changes in demand, generation (MW and Mvar), or system configuration to maintain system stability, acceptable voltage, or power flows. An SPS does not include (a) underfrequency or undervoltage load shedding or (b) fault conditions that must be isolated or (c) out-of-step relaying (not designed as an integral part of an SPS)."* The distinctiveness of this concept is that the purpose of protection is no longer confined to assuring the safety of power system components.

There has been a clarification of the acronym of SPS:

> System Protection Scheme (SPS) is the common name used when the focus for the protection is on the power system supply capability rather than on a specific equipment. SPS was earlier the acronym for Special Protection Scheme, with basically the same meaning as System Protection Scheme is today [1.1]. The word 'special' is nowadays replaced by 'system', since it is more relevant to describe this type of protection. (Karlsson et al., 2000, p.147)

Today there are thousands of SPS installed all over the world (Karlsson, et al., 2000). Strictly speaking, no two SPS are exactly the same due to their individual and problem-

specific design. Basically they are classified as two types: centralized and distributed. From the mechanism of their sensing, they can also be classified into two types: event-based and response-based. The pros and cons for both types have been discussed in length (Karlsson, et al., 2000).

One major contribution of various SPS is to incorporate more input signals to control and protection systems. This means more degrees of freedom are available through advanced technologies in the area of measurement and communications. Some typical inputs are listed as follows (Begovic, et al., 2001):

- Active power flows in the network
- Voltage magnitude and reactive power flows
- Angles between buses
- Impedance
- Resistance and rate-of-change of resistance
- Frequency
- Rate of change of frequency
- Spinning reserve
- Cold reserve
- Inertia constant H
- Load
- Weather/season
- Relays and breaker status

Also practical algorithms are required to process all data efficiently. Another achievement of SPS is the growth of the set of available control actions over the past years (Begovic, et al., 2001):

- Out-of-step relaying
- Load shedding

- Controlled power system separation
- Generation dropping
- Fault clearing
- Fast valving
- Dynamic braking
- Generator voltage control
- Capacitor/reactor switching and static VAR compensation
- Load control
- Supervision and control of key protection systems
- Voltage reduction (actions of OLTC transformers: blocking; reducing the voltage set-point)
- Phase shifting
- Tie line rescheduling
- Reserve increasing (temporary reactive power overload of synchronous machines)
- Generation shifting
- HVDC power modulation

But it was reported that quite a few of SPS operations resulted in unwanted tripping of the systems. These unnecessary operations are not frequent, or even rare over the SPS in-service time span. However, compared to the also infrequent correct operation occasions they are noteworthy (Anderson & LeReverend, 1996). This indicates that the SPS needs a thorough review.

Furthermore, SPS brings more complexity (Nielsen, Coultes, Gold, Taylor, & Traynor, 1988). Expanding or modifying dedicated "system protection" on top of existing protection systems would cause more and more coordination problems. Because component and system protection are designed differently and installed separately to control the same set of power system components. The SPS may control several protection devices in different

established relay schemes at different locations and with various settings. Without proper coordination, SPS can cause conflicts with conventional protection. For example, transfer trip signal from SPS and local tripping decision may be different; remote load shedding and local load shedding may differ both in time delay, amount and steps. There is no standard practice of overriding/blocking between commands from the two.

Therefore an additional layer of "system protection" network made of dedicated system protection devices is not a perfect modification to the established protection system structure. A more desirable design to close the gap between component protection and system protection would be an integrated protection system.

The work accomplished thus far in adaptive protection implies that flexibly tuning existing protection devices for both component protection and system protection is feasible. The same set of devices implementing the jobs of both component protection and system protection would circumvent the aforementioned coordination complexity. Under different operation conditions, the bias towards security or dependability is changing and balanced. For example, dependability is preferable during light load conditions because of larger system margin and less probability of cascading events. An adaptive relay should be able to take both local component sensing and remote system sensing into decision making to fulfill both requirements. Thus tuning between different modes discretely or continually enables one overall design. This is based on the tenability or intelligence of computer relays. At present dedicated SPS can be considered as a transit period of patching system protection functions to existing component protection systems, before mature adaptive protection network is widely adopted.

3.5 Proposed Architecture

3.5.1 Hardware Architecture

As the capabilities of relays expand and new technologies are introduced, it is important to understand how adaptive protection can be extended into preventive and emergency control. One could think of three layers of hierarchical hardware needed for wide area protection. The lowest level of a distributed control system for local protection occurs at the relay level. A "relay" could be a simple classical relay, a modern digital relay, or an

Intelligent Electronic Device (IED). IED is defined by IEEE (1994, p.8) as *"any device incorporating one or more processors with the capability to receive or send data/control from or to an external source (e.g., electronic multifunction meters, digital relays, controllers)"*. At each relay location, modern technology transforms the sensor, relay and breaker into a switch with sophisticated computation and multiple input variables. The middle layer at the substation level contains many such units, each able to operate independently but also capable of being interconnected through a substation computer. They realize protection for small regional systems. Finally, at the highest level, each substation is interconnected with neighboring substations for line protection but can also be connected with a central computer for wide area protection and control.

As a result, future substation protection and switching control systems will resemble those in Fig. 3.4, which is a modification of the substation control system described in the previous stage of the research (Damborg, Kim, Huang, Venkata, Phadke, 2000). The figure of hardware architecture illustrates the substation configuration and the information flow both inside of and between substations.

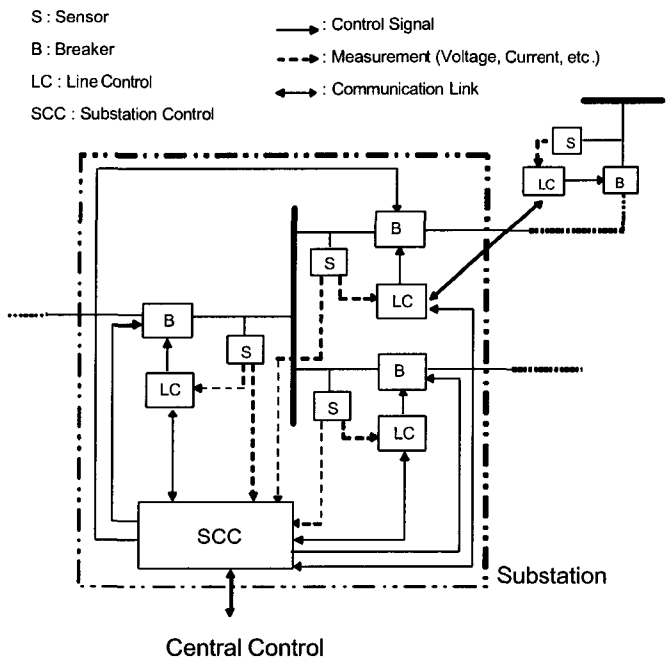

Figure 3.4 A coordinated wide area protection and control system

In Fig. 3.4, each line-end is equipped with sensors (S), a line controller (LC) and breakers and actuating circuitry (B). Sensors include conventional ones as voltage transformers (VTs) and advanced ones as phasor measurement sensors. The line controller is the successor to the modern computer relay, sometimes referred to as the adaptive relay in this document. In addition to a local control for each breaker, there is a Substation Coordination Controller (SCC) that receives signals from each sensor at the substation and can control each breaker at the substation. This extra level of substation logic allows for breaker action based on the state of all lines and bus bars at the substation. In the present context SCC could be a module implemented in local SCADA computer, or an individual device installed in the substation. Since the SCC-controlled set of breakers overlaps with the LC-controlled set of breakers, coordination among SCCs and LCs is needed. To enable the coordination, a local network with specific communication protocols is expected. The SCC and LCs are connected to the same local network so information can be easily shared, including measurement from sensors and system indices from high-level modules etc. Wide area control can be accomplished by communication between the SCC and a Central Controller. The Central Controller coordinates wide area protection actions with all substations.

The role of this system is to monitor and control all the breakers in the substation. Through monitoring, the system will provide alerts in the event of breaker/relay failures, including hidden failures when possible, and will assure proper settings for coordination. The system will also be given an active role to change settings upon command in preventive mode, and to coordinate all breakers at the substation to isolate faults based on both local and remote information in the emergency mode. An example would be to de-energize a minimal portion of a substation in the event of a breaker failure that may affect multiple lines.

This system will be a major element in a wide area control system that involves protection devices. It must communicate with immediate neighbors for rapid tripping of far-end line faults and for redundant relays coordination. It must also communicate with the central control system for truly wide area emergency management.

While each end of each transmission line must be protected by the operation of a relay/breaker system, the SCC can provide a coordinated response of all breakers at a

substation. LCs can as well coordinate with each other through communication and distributed decision-making. Further, these substations can be interconnected throughout a system to provide coordinated system response. This system can take advantage of enhanced computation (at relays, in substations and centrally) and modern communications to respond not only to faults but also to threats such as unusual loading or weather. Through a network of substation controllers the protection/control system is organized over a wide area.

3.5.2 *Functional Architecture*

In Section 3.5.1, controllers are proposed to coordinate all switching actions. This section discusses how all the bgical functions are organized and cooperate with each other. It is within the scope of the logic *protection system scheme* defined in Section 3.3. Contrary to existing protection system scheme that is summarized in Section 3.3, a new one is proposed for integrating component and system protection:

- Relays are not completely self-contained in the sense that they implement the measurements individually, but independent logic and output actions of tripping breakers are restricted to primary protection functions;
- Relay backup function is realized mutually among relays without intentional time delay, with information from peer relays through communications among the networked relays both locally and remotely;
- Since many relays may control the same tripping device in parallel logic, coordination is realized at a higher decision level through communications or at the peer level through coordinated distributed decisions;
- Uncertainty is expressed by each relay, thus the output of each relay is a pair of tripping decision and the corresponding certainty value, or a set of such pairs;
- The higher-level decision controller is able to process more input, supervising and tuning other relays and making inference decisions during emergencies.

To summarize the proposed functional architecture of adaptive protection, the features are listed in Table 3.7. The corresponding functions as they exist presently are also provided in this table for comparative purposes.

The assumption in the proposed architecture is that the backup functions rely heavily on latest communications and computer technologies, which provide more information for the decision-making process. Therefore, incorrect operations resulted from complex system behavior such as hidden failures, and noisy measurements could be harnessed. System-wide information like the vulnerability index can also be incorporated to decision-making procedure for the consideration of stability maintenance. It is believed that the proposed protection philosophy results in higher speed in backup operations by eliminating the intentional time delay in exchange for a shorter communication time delay. At the same time, fall back solutions for failure of communication links need to be figured out. It is to be stressed that primary protection is expected to remain the same for both current and future schemes. It is also worth mentioning that this is an open structure so more new developments can be easily incorporated if any further technique improvements are available.

The author is aware that *"A growing number of protective schemes are primarily designed for improving power system stability or enhancing system security. These schemes ... are safeguards designed to alter or preserve the system structure, security, or connectivity"* (Anderson, 1999, p.853). However, this research does not intend to design A SCHEME for the purpose of maintaining system stability. Instead, a change of protection philosophy always with the consideration of stability in mind is the goal of this research.

Table 3.7 Protection system functional architecture: current and future

	Current	Future (Proposed)
Functionality	Self-contained: • Individual measurements and logic • Independent output actions	Not completely self-contained: • Individual measurements • Dependent decision-making logic and output actions
Redundancy	Relays can backup other relays locally or remotely (one or two adjacent busses)	• Backup functions are realized mutually among networked peer relays • Information from peer relays is shared through communications among the networked relays both locally and remotely
Coordination	• Parallel logic of "OR" • More than one stage of time delay in each relay	• At a higher decision level or at distributed decision-making level • Realized through communications • Without intentional time delay
Uncertainty	Implicitly represented by applying margins to form conservative settings. It is more of art than science.	Explicitly expressed by each relay: the output of each relay is a pair of fault location/tripping decision and the corresponding certainty value, or a set of such pairs
Supervision	• Provided for a specific relay tending to falsely trip • An extra supervisory relay is deployed to form a compound relay module • Tripping decision is given from logically serial control of "AND"	• Provided for all networked relays • Peer relays can supervise mutually at no extra effort • The higher-level decision controller is able to process more input, supervising and tuning other relays and making inference decisions during emergencies

3.6 Decision-Making Algorithms

As summarized in Section 2.1, all of definitions of adaptive protection are suggesting on-line altering of relay settings (Damborg et al., 2000). This feature works well under the preventive mode of system operation. However, under the emergency mode, there is no time to reset and validate relay settings. The relays should make decisions almost instantaneously based on real-time operational conditions of the power system. That is to say, the adaptive feature needs to be implemented within the relay decision-making algorithm. In company with architectural improvements described in the previous section, it is the addition of intelligence into the decision-making process that distinguishes adaptive protection from traditional protection schemes and exhibits the potential power for the future.

3.6.1 Existing Algorithms

A protective relay is usually required to make a correct decision in a very short time. Therefore, the decision-making algorithm should be effective, fast, and versatile to include various system operating conditions. On the other hand, it is usually difficult to choose a simple criterion that accommodates the large numbers of possible system conditions (topology, load level, etc.) and incidents for relay settings. Therefore an algorithm that incorporates every criterion into a manageable computation burden is needed. In the following, a single-criterion decision algorithm and two multiple-criteria decision algorithms are described as existing algorithms before the new algorithm is proposed.

3.6.1.1 Single-Criterion Decision Algorithm

In most existing relays, the decision-making algorithm is the characteristic function in the form of a curve with threshold(s). The function has 0/1 as the output, which is dependent on input signals and their derivatives. As an example, Fig. 3.4 gives the illustration of such a function for a three-zone distance relay. The difference between Bus2 and the reach of Zone1 is the setting margin, the conservative solution to uncertainties. The advantage of the single-criterion decision algorithm is its simplicity and low cost. But it is not suitable for incorporating more than one decision-making criterion.

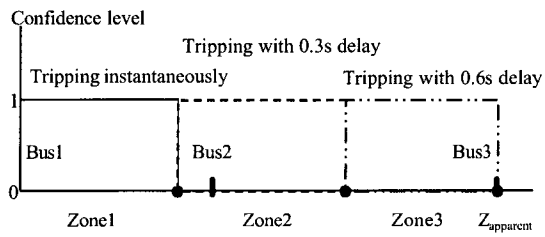

Figure 3.5 Example of tripping logic in a deterministic distance relay

3.6.1.2 Multiple-Criteria Decision Algorithms

When more than one criterion is involved in making the final decision of a relay operation, a multiple-criteria decision algorithm is applied to achieve more reliable output. Each relay characteristic function represents one criterion. Redundant relay characteristic functions participate in the final decision-making. Two existing multiple-criteria decision

algorithms are discussed below for illustrative purposes. It is not an exhaustive list of algorithms that protection schemes adopt.

- Simple Voting

From more than one 0/1 output from relay characteristic functions, simple voting such as n out of m (n<m) can make the final decision. Examples of extreme conditions for simple voting are serial and parallel settings, i.e. "AND" and "OR" voting, which are used in most secure and backup conditions, respectively. This is very similar to the figure in a recent paper by Phadke, which thoroughly explores the adaptive protection concept for hidden failures (2002). In this algorithm, increased hardware investment is the price for a more reliable decision. The additional computational burden is manageable because only the simple logic of "AND" and "OR" are involved. However, the improvement in reliability is also limited since a simple voting scheme cannot reflect the difference of relays. Due to the nature of different types of relaying principles (e.g. overcurrent, current differential, etc.), the accuracy of measurement and correctiveness of the judgments from different relays may be different. Therefore, their voting rights are not necessarily equal.

- Voting with Weighting Factors

Pre-defined, adjustable weighting factors for each relay within the backup scheme are introduced and claimed working well for more reliable protection (Tan, Crossley, Kirschen, Goody, Downes, 2000). The decision-making process is that the 0/1 output from each relay is multiplied by suitable weighting factors, then added up and compared to a certain threshold to produce the final output. The advantage of this algorithm is that unequal weighting factors reflect the relative importance of different relaying principles. The limitation is that predefined weighting factors cannot reflect real-time relay conditions.

Summarizing all existing algorithms, it is noticed that none of them is able to reflect the inherent uncertainty relays encounter. This topic is studied in the following section.

3.6.2 Application of Fuzzy Theory in Modeling Uncertainties

3.6.2.1 Uncertainty Study

"So far as the laws of mathematics refer to reality, they are not certain. And so far as they are certain, they do not refer to reality."

--Albert Einstein

Mathematical modeling of physical systems is often complicated by the presence of uncertainties. Protective relay algorithms, for example, entail uncertainties in the process of measuring, communication and calculation, etc. The presence of uncertainties impacts the validation of the relay tripping decision. Even though significant effort has been made to incorporate uncertainties into relay models, a systematic approach instead of intuitive solutions has not been presented.

The author believes that the discussion of uncertainties, where they are from and the approaches to hedge their impact provides insight into the source of the problem. Further, it can lead to the solutions as proper algorithms to model uncertainties.

The basic approach of protection devices is to define equipment status by identifying voltage and current waveform patterns. This could be difficult if uncertainties are present and not modeled quantitatively. Uncertainties come from both measurement collected and settings predefined therefore virtually inevitable. Numerous researches have been conducted in identification of the key sources of uncertainty (Aggarwal & Johns, 1997). Here are some examples of the source of uncertainties:

- Operation condition changes: load/generation/topology
- Various network configurations
- Different fault condition
- Inaccuracies caused by measuring equipment and noise introduced by EMI
- Possible missing of information
- Approximation in relay settings and coordination trade off
- Existence of hidden failures in protection systems, with various failure modes (Phadke et al., 1995)

Ronen (1988), a physicist showed that uncertainties are inherent in nature, or more correctly in the way the nature is observed. "Uncertainty principle" and "Complementary Principle" introduced in 1920s legitimated the role of uncertainties in physics. Uncertainties are introduced by fragmentation of nature. It is the way human learns by isolation of small

parts of nature to deal with each part separately. The introduction of "system concept" is based on the assumption that influence from the surroundings is perfectly known which is not absolutely correct.

Uncertainties are brought in by measurement, which is interference between the measurement device and the system. It can be corrected to some extent, but not completely. New techniques are applied to reduce uncertainty in measurement, for example, PMU, by providing precise phasor information, could potentially aid in a more efficient relay decision making.

However, the existing architecture and algorithms of relays have not made the most of the currently available information. For problems where data are limited and where simplifying assumptions have been used, as in a relay, a robust algorithm that models uncertainty appropriately thus reducing the uncertainty in decisions is of key importance.

3.6.2.2 Comparing Probability Theory with Fuzzy Theory in Modeling Uncertainties

It has been realized that there are uncertainties in our universe. Or rather, absolute certainty is rare. In particular, uncertainty comes from missing/incomplete and/or imprecise/incorrect information. And imprecision is an inherent property of the world external to an observer.

Technically capturing the characteristics of the uncertainty plays an important role in decision making procedure. Only an algorithm robust enough to incorporate various uncertainties possesses the greatest likelihood of success in the real world. The existing relays adopt an approach of "threshold margins" for representations of measurement imprecision and "wait and see" for all possible erroneous decisions resulting from data and devices imperfection. This research makes an effort in promoting a more systematic algorithm for quantification of uncertainty than this primitive mixture of "art and science". Before elaborating the proposed application of fuzzy theory in adaptive relaying, it is worthwhile to compare the relationship of fuzzy theory and another more widely used approach in uncertainty modeling, probability theory.

Probability theory and fuzzy sets are currently among the most visible mathematical frameworks allowing conceptualization of uncertainty. It is true that *"One of the most*

controversial issues in uncertainty modeling and information sciences is the relationship between probability theory and fuzzy sets" (Dubois & Prade, 1993, p.1059).

This is because there have been quite some similarities, mix-ups and misunderstandings between the two. The fuzziness and probability are orthogonal concepts that characterize different aspects of human experience. If probability is an objective approach then fuzziness is the subjective way to represent the uncertainty.

Probability theory is a mathematical framework to represent the likelihood of phenomena with uncertain outcomes. Statistical or random uncertainties are inherent in the physical world and have been studied thoroughly for centuries. So far the best accepted approach in modeling it is the probabilistic theory.

Another category of uncertainty arises in human cognition process, including information extraction and reasoning. For example, in Section 3.2 it is observed that for a highly stressed power grid the protection should bias more towards security than towards dependability under normal conditions. Implementing such philosophy in relays would introduce the problem of quantifying the concepts of "highly stressed", "more towards security", "towards dependability" and "normal conditions". The perception phenomenon can be neither characterized nor measured using statistical theory. The mathematical modeling and management of this cognitive uncertainty is by fuzzy set theory.

The fuzzy set theory has been started in late 60's (Zadeh, 1965). Although related to probability, fuzziness is a different concept. Fuzziness is a type of deterministic uncertainty. It describes the *event class ambiguity.* Fuzziness measures the *degree* to which an event occurs, not whether it occurs. The amorphous intelligence of fuzzy theory emulates the efficient and robust process of the brain, featuring aggregation of continuous distribution of attributes and relative grades of information (Kosko, 1990).

While membership grades can be determined with probability densities in mind, there are other interpretations as well not in agreement with frequencies or probabilities calculus.

In fact, from a mathematical perspective, fuzzy sets and probability exist as parts of a greater generalized information theory and are among many formalism methods for representing uncertainty (Klir, 1992). In essence, fuzzy logic and probability theory are the most powerful tools to overcome the imperfection in information system. Fuzzy logic is

mainly responsible for representation and processing of vague data. Probability theory is mainly responsible for representation and processing of randomness. The following table clarifies the differences between the two theories (Tizhoosh, 1997).

Table 3.8 Differences between fuzzy logic and probability theory

Probability Measure	Membership Function
Arouses from the question whether or not an event occurs	Arouses from the question to what degree an event occurs
Assuming the event class is crisply defined	Assuming the event class is ambiguously defined
Before an event happens	After the event happened
Assuming the law of non contradiction holds	When the law of non contradiction is violated, hence it can cope with inconsistency
Calculates the probability that an ill-known variable x ranging on U hits the well-known set A	Calculates the membership of a well-known variable x ranging on U hits the ill-known set A
Randomness	Vagueness
	Modeling linguistic variables and used in inference processes
Measure Theory	Set Theory
Domain is 2U (Boolean Algebra)	Domain is [0,1]U (Cannot be a Boolean Algebra)

Probability and fuzzy sets are already jointly used in several domains of applications, and it provides a richer uncertainty modeling environment. A fuzzy probability extends the traditional notion of a probability when there are outcomes that belong to several event classes at the same time but to different degrees. According to Dubois and Prade (1993, p.1066), *"...instead of considering probability and fuzzy sets as conflicting rivals, it sounds more promising to build bridges and take advantages of the enlarged framework for modeling uncertainty and vagueness they jointly bring us to."*

It is important to note that neither fuzziness nor probability govern the physical processes in nature. They are brought in by humans to compensate for their own limitations. Detailed theoretical discussion of the relationships between fuzziness and probability may be found in the reference (Dubois, 1993).

3.6.2.3 Advantages of Fuzzy Set Theory

Fuzzy set theory simulates human intelligence in trading off between significance and precision. It is a convenient way to map an input space to an output space. As Lotfi Zadeh, who is considered to be the father of fuzzy logic, once remarked: *"In almost every case you can build the same product without fuzzy logic, but fuzzy is faster and cheaper"; "As complexity rises, precise statements lose meaning and meaningful statements lose precision"* (The MathWorks Inc., 1995).

- Fuzzy logic is conceptually easy to understand.

The mathematical concepts behind fuzzy reasoning are as simple as common sense. What makes fuzzy nice is the "naturalness" of its approach instead of any far-reaching complexity. It is based on natural language which is convenient and efficient. Since fuzzy logic is built atop the structures of qualitative description used in everyday language, it is easy to use. Therefore applying fuzzy theory in protection is straightforward for relay engineers who have been working this art on both science and intuition.

- Fuzzy logic is tolerant of imprecise data.

The function of relays is designed to make precise decisions based on imprecise, even erroneous or missing information. Actually fuzzy theory is one of the most efficient ways in modeling uncertainty in decision making process.

- Fuzzy logic can flexibly model nonlinear functions of arbitrary complexity.

Protection is a highly nonlinear function, highly relying on people experience. While fuzzy set theory can match any set of input-output data. It can be built on the experience of experts. It is also easy to layer more functionality on top of fuzzy modules. So by applying fuzzy logic to relays, people are still in control of the decision-making module. Microprocessor relays have made this flexibility a unique advantage over traditional relays.

There are other Artificial Intelligence (AI) tools which lend themselves very well to the area of power system protection, such as Expert Systems (ES), Fuzzy Logic systems (FL), and Artificial Neural Networks (ANN). Among them, ES has been mostly restricted to problems with less stringent time response requirement, like off-line relay settings and

coordination. According to IEEE PSRC G-4 report submitted by Kezunovic, et al. (1999, p.35), "Expert Systems are well suited to smaller problem domains that have narrow fields of expertise." In the complex environment like wide area protection, it is very difficult to narrow down the scope of the ES. ANN with the ability of mapping complex and highly non-linear input/output patterns provides an attractive solution to some of the long-standing problems in protection, like phase-selection. But the difficulties in application to protection come from its excessive dependence on training data set. This is particularly not suitable for restructing utilities since the system is not running as it was designed. Therefore simple intelligence algorithms such as fuzzy logic are proposed for adaptive protection in wide area. FL is considered a powerful tool in relay decision-making since it is much closer in spirit to human thinking and natural language than traditional logic systems. Its mechanism of simplifying complexity ensures real-time response, which is the key requirement for relay applications.

3.6.3 Proposed Algorithm: Voting with Real-Time Intelligent Factors

To ensure real-time response of the adaptive protection system, modeling aforementioned uncertainty without sacrificing speed is necessary. More over, modern relays are required to perform advanced functions. The bias of security and dependability needs to be adjusted in real time; relay decision may base on multi-criteria with various weighting factors. Therefore, voting with real-time intelligent factors, such as a fuzzy factor is proposed.

As an example, a fuzzy distance relaying function is represented in Fig. 3.5. Instead of making 0/1 decisions with time delays as shown in Fig. 3.4, fuzzy decisions with real-time confidence level membership functions are made almost instantaneously. The curves of each relay characteristic function are set according to power system parameters, pre-calculated contingency analysis, and even experience. The settings could be modified according to real-time relay conditions. For example, failures in relay self-checking or outdated input signals would decrease its confidence level. Each relay sends out multiple decisions and the corresponding confidence level values. Multiple redundancies of relay make it possible to estimate the fault status even with part of the information missing. After collecting all relevant information, a voting scheme is realized in the relay by computation and ranking of

confidence values for each decision. When the result with the highest ranking is greater than a certain threshold, corresponding action is taken immediately by the relay. And other peer relays are informed of the operation. The setting of the threshold can be tuned according to real-time system conditions, such as a vulnerability index. Thus the bias towards security or dependability can be shifted continuously within a reasonable region. In practice, the characteristic function of an adaptive rely may be multi-dimensional and quite complex. It incorporates more input signals than $Z_{apparent}$ only. Fig. 3.5 is just for the purpose of concept illustration and comparison with Fig. 3.4.

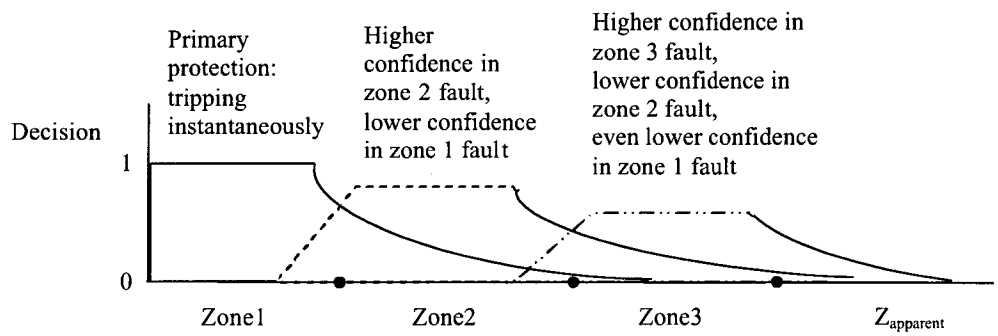

Figure 3.6 Example of characteristic function in a fuzzy distance relay

For primary protection, the action of tripping breakers is usually taken directly because a normal primary protection function has the decision confidence level of higher than the threshold. For backup functions with the confidence level less than the threshold, the final judgment is left to a relay with more information from other relays on the communication network. This relay could be local or remote, peer relay or higher-level intelligent controller, or even the same primary relay after getting enough information from other relays. No time delay is introduced on purpose. The only delay is from the communication time among relays. Thus a fault is cleared as fast as possible, after a well-informed decision is reached. The forming of the final decision is slower than that of traditional primary relays but it is believed to be more proper. Additional redundant information will hopefully contribute to making a proper final decision. Consequently, there is less probability of false tripping of the relays.

This algorithm could be viewed as a more general form of existing algorithms presented in Section 3.6.1. The additional computation expense of this algorithm varies. For

individual relay characteristics, the procedure of fuzzification could be a membership function calculation if there is a close form expression, or through a simple table look-up. For the final decision-making it might be simple arithmetic computation followed by defuzzification at a certain threshold. The total calculation time is probably able to be limited to within 10 ms (Kezunovic, et al., 1999).

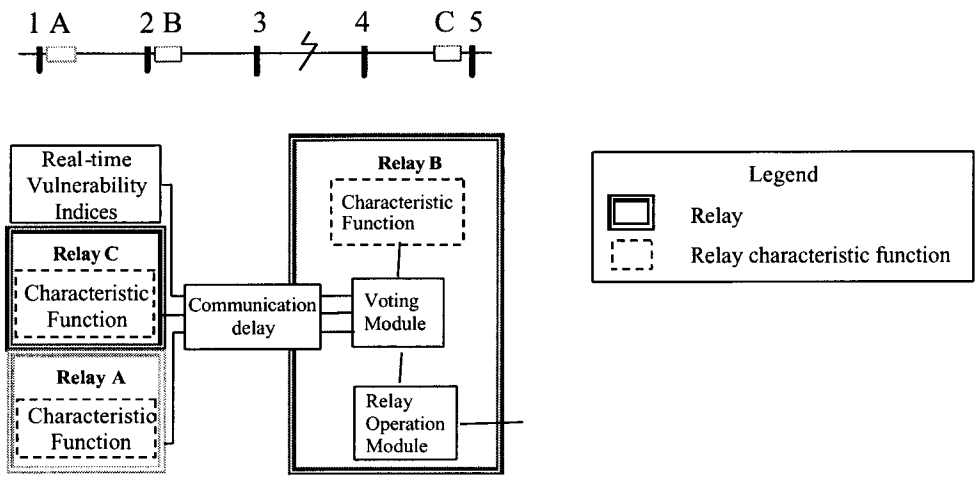

Figure 3.7 Logic diagram of the proposed protection system for one protected component

Through a simple example, the proposed architecture and algorithm of the intelligent voting scheme is illustrated for a small five-bus power system. Fig. 3.6 shows how one relay on the network processes a backup protection function with the aid from peer relays. Assume that there is a fault between bus 3 and bus 4. The primary protection at one side or both sides of the two buses fails to sense the zone 1 fault. This extreme condition may happen due to hidden failures, either in relay settings or the relay hardware (Phadke, 2002). Backup relays A, B and C all see the fault remotely with different confidence levels as indicated in Fig. 3.7, labeled as Z_A, Z_B and Z_C. Assuming relay B measures the apparent impedance Z_B in zone 2, which is the line between bus 3 and bus 4, with a confidence value of 0.7. Also Z_B could mean a fault in its zone 1, which is the line between bus 2 and bus 3, with a confidence value of 0.55. The threshold is set to 1. Thus relay B by itself cannot make a firm decision. However, intelligent information collected from relays A and C could help relay B to make a proper decision adaptively. In relay B, after collecting signals from the peer relays, the computation result is the confidence value for "fault between bus 3 and bus 4" greater than

the threshold. Instantaneous tripping signal is sent to breakers at bus 3 and bus 4 to trip the faulted portion of the system. If only one side of the line between bus 3 and 4 is affected by hidden failures, the backup function for the failed protection would have similar process. It is reasonable to believe that the proposed architecture and algorithms can be effectively applied to reduce the impact of hidden failures. Implementation of the algorithm in MATLAB environment is demonstrated in Chapter 5.

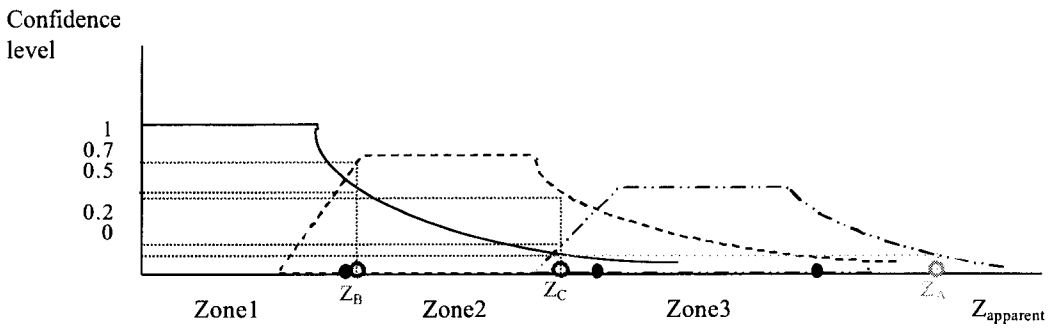

Figure 3.8 Example of tripping logic in a fuzzy distance relay

3.7 Adaptive Autoreclosure

It is well known that the majority of faults in overhead lines are temporary in nature (Blackburn 1998). Accordingly autoreclosure schemes are applied to transmission and distribution systems as an effort to maintain transfer power to the maximum extent. Both fast and delayed reclosing following fault clearing have positive effect on system stability and synchronism, thus preserving the continuity of supply and improving grid reliability (IEEE PSRC, 1992).

However, autoreclosure practice can also pose problems towards equipment safety and system stability. Major threats come from the possibility of second shock by reclosing to a permanent fault or a temporary fault but before a sufficient time for fully de-ionizing the fault path. Since the present practice of automatic reclosure is essentially employing a "trial and error" approach without differentiating fault types and fault conditions, there is no control over the risk of second shock. Therefore autoreclosure schemes have been mostly used when temporary faults play an important role but the consequences of reclosing into a

permanent fault is not prohibitive (Anderson, 1999). Thus in some utilities reclosing is not widely adopted in EHV transmission systems.

Nevertheless, it is imaginable that with new techniques available to discriminate temporary faults and to determine the proper time to reclose, autoreclosure would be used more widely and efficiently. Furthermore, considering the possible existence of inadvertent relay operations, it is more sensible to apply reclosing to avoid unnecessary loss of system connectivity. The challenge, however, lies in how to differentiate a real fault or a false alarm. This is where the intelligence of the relay comes into play in preserving the security of the system (Anderson, 1999).

There is one more consideration in the issue of autoreclosure. It is the practice of three-phase tripping versus single-phase tripping. Three-phase tripping is more adopted in the North America, even for one-phase-to-ground faults. Although there are some EHV schemes having single-pole reclosing, it is not a dominant practice in the US. In other areas, such as China and Russia, single-phase tripping and reclosing is used for single-phase faults. Generally three-phase tripping is simple and safe, whereas single-phase tripping and reclosing enhances the system security (IEEE PSRC, 1992).

In summary, the issues that an autoreclosure scheme needs to ascertain are whether to reclose the circuit breakers, which phase(s) to reclose and precisely when to reclose. New techniques, referred to as adaptive autoreclosure techniques, are developed to address these questions and are briefly introduced in the following text.

- Distinguishing between permanent and transient faults

The concept of adaptive reclosure was firstly studied in 1980s to distinguish between temporary and permanent faults for single-phase switching cases (Ge, Sui, & Xiao, 1989). The method is based on an analysis and comparison of coupling voltages in both steady and transient states on the opened phase during reclosing dead time, which is the period following the tripping operation.

A number of approaches have followed to address this subject. One is Artificial Neural Network (ANN)-based scheme for single-phase adaptive reclosure. The circuit breaker control system is created on features extracted from the characteristic voltage waveforms that developed on the opened phase during the secondary arc period. It has been

observed that with many factors affecting these waveforms, e.g. line configuration, pre-fault loading, fault location, fault point on wave, source parameters, or even atmospheric conditions, the relationship between these factors and the voltage is very complex. The neural network is trained by sufficient data from fault simulation and can recognize certain situations to give a good reclosure decision. The test results demonstrate the ability of the ANN approach to be used as an attractive and effective means of realizing an adaptive autoreclosure scheme (Fitton, Dunn, Aggarwal, Johns, & Bennett, 1996).

Other than artificial intelligent methods, numerical approaches using high-frequency fault transient components have also been presented both in the spectral and time domain (Djuric & Terzija, 1995; Radojevic, Terzija, & Djuric, 2000). The faulted phase voltage is modeled as a serial connection of fault resistance and arc voltage. Line terminal voltage and current data are processed using the Fast Fourier Transform (FFT) and arc voltage is estimated through Least Error Squares Technique. Moreover, Li et. al have introduced an approach in identifying arcing faults by processing high frequency current transient using the wavelet transform (Li, Dong, Bo, Chin, & Ge, 2001).

Adaptive reclosure for three-phase switching has been hard to implement because the fault arc extinguishes soon after a three-phase tripping of the line. Some researchers found the solution from the power line carrier communication signals (Huang, Li, & Li, 2002). The transmission channel for carrier current restores quickly after the line tripping. Therefore the propagation of carrier current is affected by the fault spot, if still existing. By analyzing the high frequency signal produced by carrier current transmitter and its communication channel of carrier protection, fault characteristics can be identified.

- Deciding the reclosing time

The effectiveness in maintaining power system stability is largely determined by the speed with which autoreclosure can be achieved (Johns, Song, & Aggarwal, 1993). The present reclosure schemes usually adopt a fixed dead time before reclosing (Blackburn, 1998). This is the simplest way and can be very inefficient. To avoid unsuccessful reclosure or unnecessarily long dead time, adaptively calculated dead time could contribute to the system stability drastically.

There are two parts of the time determination process involved. One is to precisely define the secondary arc extinction time in the case of transient faults. Some work in adaptive autoreclosure has introduced the measure of adjusting dead times according to arc extinction times (Sang-Pil, Chul-Hwan, Aggarwal, & Johns, 2001; Tuan, Hadj-Said, Sabonnadiere, & Feuillet, 2000). However, although the secondary arc extinction time provides a good indication of when to reclose, reclosure of the circuit breakers immediately following arc extinction will normally result in a re-strike of the fault. This is because a further finite time is required to allow the fault arc path to deionize fully, so that the transmission line may withstand the full system voltage on re-energization. It has been identified that the length of this additional delay period after secondary arc extinction is definite and does not vary with the line length, characteristic of fault or voltage level (Websper, Johns, Aggarwal, & Dunn, 1995). Therefore the optimal reclosure time can be determined by applying this deionization time in conjunction with adaptive autoreclosure techniques.

- The role of single-phase tripping and auto-reclosing

Single-phase autoreclosure (SPAR) is quite extensively used in long-line applications in China and Europe. It involves tripping only the faulted phase for single-phase earth faults. SPAR takes advantage of the fact that the most frequent faults in overhead transmission lines are phase-to-ground unsymmetrical faults. The representative statistics show that the percentage of single-phase-to-ground faults would be 70% for HV and 93% for EHV/UHV lines (IEEE PSRC, 1992).

Since only the faulted phase is tripped during the fault, approximately 50% of transmission capacity is still retained via the two healthy phases, the switching overvoltages and shaft torsional oscillations of thermal units are reduced. Other benefits of single-phase tripping and auto-reclosing include improving transient stability and system reliability, as well as cost effective (IEEE PSRC, 1992). From the industry experience the practice of SPAR has redefined the optimal response to line fault.

The effectiveness of single pole autoreclosure in wide area disturbances has been noticed. For example, the famous WECC 2 July 1996 outage was initiated by a transient B-phase fault at the Kinport-Jim bridge 345kV line. If single-phase tripping and reclosing was adopted, a successful B-phase reclosing may have avoided further cascading. Suggestions

have been made to revise NERC reliability criteria to accommodate single-phase tripping and autoreclosing to avoid cascading outages and raise the system stability level in real operational practice (Liu, 1998).

- Distinguishing relay false operations from real faults

The methods aforementioned for distinguishing between permanent and transient faults can also be applied to identify relay false operations. Furthermore, the author would suggest applying the "voting with real-time intelligent factors scheme" described in Section 3.6 to determine the confidence level of the existence of a real fault. With information from all connected relays both before the tripping operation and afterwards, plus the system recommended reliability bias index, the adaptive relay is more likely to make better and informative reclosure decisions than under the traditional isolated conditions.

In general, adaptive autoreclosure techniques can offer many advantages over conventional schemes in improving power system stability and reliability. adaptive autoreclosure leads to high percentage of high-speed successful reclosures after the optimum dead time, or no reclosure onto permanent faults. This, in turn contributes to reducing damaging shocks and voltage dips, longer circuit breaker life, better supply quality and stability, and faster sympathy trip response, etc. (Fitton & Gardiner, 1995; IEEE PSRC, 1992). Therefore adaptive autoreclosure is considered a feature that adaptive wide area protection would encompass.

In this chapter, a new concept on adaptive wide area protection for power system is proposed and various related topics are discussed. The architecture and algorithms are explored at the conceptual level, leaving practical design and validation to Chapter 5. Communication that is required to support this proposed adaptive wide area protection is discussed in the following chapter.

CHAPTER 4. COMMUNICATIONS REQUIREMENTS FOR ADAPTIVE WIDE AREA PROTECTION

Communications have always been important in power system protection and control. Early protection systems have in fact included their own dedicated communication channels, such as power line carrier and microwave, which are considered as a part of the whole relaying scheme (Blackburn, 1998).

It is obvious that high speed and reliable communication is necessary to realize the proposed adaptive protection scheme described in Chapter 3. For this reason, the communication systems that are currently available are briefly introduced and evaluated, with the intention of adoption some for utilization in the proposed protection design.

In this chapter, communication media and protocols that are required for the proposed protection design are examined. The time needed for communication procedure in adaptive wide area protection is estimated. To meet the requirements of speed, reliability and intelligence for communication protocols, profiles of existing communication protocols are promoted. However, limitations of current protocols are identified and possible modifications are suggested.

4.1 Transmission Media

Telecommunication is the transfer of information across a distance. To support the transmission, there must be a transmitter, at least one receiver, and some physical medium in between. There are a number of options in selecting the transmission technique. Basically a data transmission system can be either wired or wireless. That is, the signal is either guided through a transmission medium or unguided between antennas. In this section, major communication techniques are briefly reviewed.

The electromagnetic spectrum of transmission media is shown in Fig. 4.1. According to Stallings (2000), when choosing a communication medium, the key concerns are maximum data rate and distance between repeaters. Hence, these parameters of mainstream transmission media are summarized and compared in Table 4.1 (Stallings, 2000). All data are for digital communications and the number may change over the time since new technologies

are emerging everyday. It is just to give the reader a rough feeling in comparison of the capacity and distance of popular transmission media.

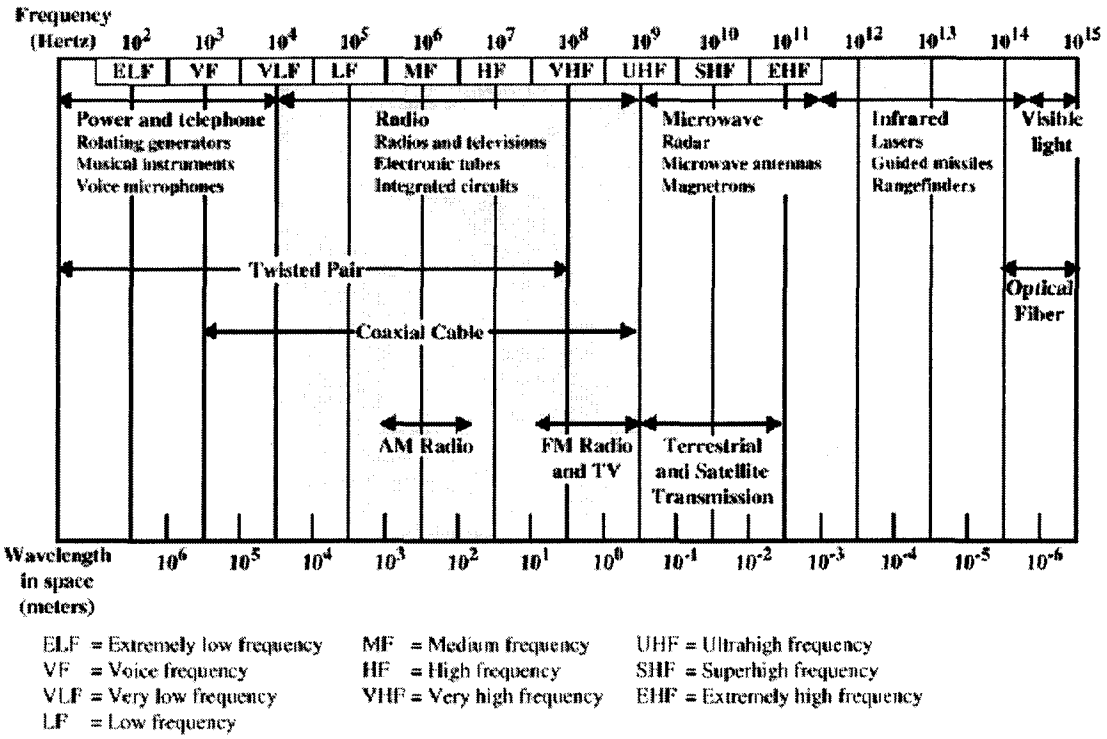

Figure 4.1 Electromagnetic Spectrum for Telecommunications (Stallings, 2000)

Table 4.1 Digital capacity and distance of transmission media

		LAN data rate (bps)	WAN data rate (bps)	repeater distance (km)
Guided media (wire)	Twisted pair	600 M	4 M	1-3
	Coaxial cable	500 M		1-10
	Fiber optics	1G -1T		10-100
Unguided media (wireless)	Terrestrial Microwave	N/A	50M	2-40
	Satellite Microwave	N/A	36M-72M	N/A

4.1.1 Guided Transmission Media (Stallings, 2000)

- Twisted-pair

Twisted-pair is two independently insulated wires twisted around one another. One wire carries the signal while the other wire is grounded and absorbs signal interference.

Many of twisted-pair wires are usually bundled into cables. Twisted-pair cable is widely used by older telephone networks and modern local-area networks (LANs). It is cheap and easy to work with, yet susceptible to interference and noise.

- Coaxial cable

It is a type of wire that consists of a center wire surrounded by insulation and then a grounded shield of braided wire. The shield minimizes electrical and radio frequency interference. Coaxial cabling is the primary type of cabling used by the cable television industry and is also widely used for local computer networks.

- Fiber optic cables

This is a technology that uses glass (or plastic) threads (fibers) to transmit data. A fiber optic cable consists of a bundle of glass threads, each of which is capable of transmitting messages modulated onto light waves by laser or LED. Fiber optics has the following advantages over traditional metal communications lines, besides greater bandwidth and longer distance:

1. Data can be transmitted digitally rather than analogically.
2. Fiber optic cables are less susceptible than metal cables to interference due to its electromagnetic isolation.
3. Fiber optic cables are much thinner and lighter than metal wires.

The main disadvantage of fiber optics is that the cables are expensive to install. In addition, they are more fragile than wires and are difficult to split.

4.1.2 Wireless Transmission (Stallings, 2000)

- Terrestrial microwave systems

Microwave systems transmit voice and data through the atmosphere as high frequency radio waves. Use of a certain frequency generally requires Federal Communications Commission (FCC) licensing. The focused beams of microwave are directional and cannot bend around corners or around the earth's curvature. They need direct line-of-sight so there must be an unobstructed view between the transmitter and the receiver at relay stations. Disruptions of the microwave usually occur due to heavy fog and rain.

- Satellite microwave systems

It is a microwave system using the satellite as a relay station. The satellite contains many communications channels and receives both analog and digital signals from earth stations. Satellite receives signals on one frequency, amplifies or repeats and transmits signals on another frequency.

- Broadcast radio

The major difference between microwave and broadcast radio transmission is that the broadcast radio is omni-directional, having signal spreads in all directions and can be received by many antennas, while microwave is intended for point-to-point transmission only. In other words, the broadcast radio can transmit data to many destinations at the same time. This characteristic has limited the use of broadcast radio in power system protection and control due to security considerations.

4.1.3 Comparison among Twisted Pair, Coaxial Cable, and Optical Fiber

The coaxial cable has higher data rate and bandwidth than that of twisted pair. The repeater spacing of twisted pair and coaxial cable is similar. However, the fiber optics has superior performance compared with twisted pair and coaxial cable, both in bandwidth and the repeater spacing. When the environment is susceptible to electromagnetic interference, both twisted pair and coaxial cable may have reliability problem, where the fiber optics stands out due to no electrical coupling in the transmission mechanism.

4.1.4 Comparison between Microwave and Optical Fiber

When choosing from optics and microwave communication it is needed to consider the different characteristics of these two media. The bandwidth and repeater spacing parameters are compared in Table 4.1. Obviously fiber optics has the advantage in both parameters. For its physical condition, fiber optics is not affected by the electromagnetic interference and has higher security. However, fiber optics is possibly knocked down by a storm or it may be difficult to change the routing physically. On the other hand, the microwave is transmitted through the air therefore easier to be detected so its security is relatively low. But it is easier for it to change the configuration even to point-to-multipoint broadcast.

4.2 Estimation of Communication and Control Times

The concept of adaptive protection as envisioned in Fig. 3.4 depends on the speed with which the adaptive relays can identify and analyze an emergency as well as the speed with which remedial control action can be effected. Therefore the proposed protection system must be supported by a fully developed, high-speed data communications system. Utilities are installing high speed LANs interconnecting all components in substations. Also optical fiber networks with appropriate protocols and dedicated links to connect the substations with central controllers are expected. Many utilities are already installing such networks, both for their internal use and to establish additional business providing communications services.

The current time estimate for the total process of adaptive protection is shown in Table 4.2. It includes data collection, communication, and control action after fault initiation.

Table 4.2 Estimated times for adaptive protection actions

Activity	Time	Ref.
Sensor processing	5 ms	(Dutta & Dutta Gupta, 1992)
Transmission of information to central controller	10 ms	(Li, Yates, Doverspike, & Dongmei, 2001)
Processing incoming message queue	10 ms	(Li et al., 2001)
Analysis and decision	100 ms	(Faucon & Dousset, 1997)
Transmission of control signal	10 ms	(Li et al., 2001)
Operation of local device	50 ms	(Blackburn, 1998)
Total	185 ms	

The time for sensors to process data and the time for devices to operate are well understood and documented in the literature (Dutta & Dutta Gupta, 1992; Blackburn, 1998). The times required for the other activities are more difficult to determine. The estimate of communication time is based on the assumption that utilities will have complete fiber optic networks available with dedicated channels provided as needed for high priority communication and control signals. Hence, for short messages, the communication time depends almost entirely on the propagation speed along fiber cables at 124,138 miles/sec. (Li et al., 2001). This estimate is based on a distance of 1000 miles plus some delay time for intermediate nodes (0.3 ms per node). Whether there is a node delay depends on the protocols used. The computation time for making control decisions varies greatly with the hardware and software. The estimate is consistent with that used by the EDF defense plan (Faucon & Dousset, 1997). The conclusion is that 200 ms should be adequate to accomplish

the data collection, communication, and control action after fault initiation. If the computation time is estimated as around 10ms (Kezunovic, et al., 1999), the total time needed is less than 100ms.

For preventive control, this speed is adequate. For emergency control, the proposed adaptive relays are expected to be faster than conventional backup relays. The normal operational requirement of several milliseconds for primary protection functions can still be met. Furthermore, the back-up functions in the proposed scheme can provide faster and more appropriate decisions under different operating conditions.

4.3 Requirements for Intelligence

More than speed issues discussed above, the proposed design of protection systems needs sophisticated consideration of communication protocol improvements. Similar to established protection system architecture, there are overlaps among sets of breakers controlled by each relay. This is the basic concept of redundancy for reliable protective operation. Therefore, coordination among relays is needed. An advantage of the proposed architecture over the existing one is that all relays are networked so utilizing proper communication for coordination is possible and flexible. Previously, each relay had to independently apply different duration of time delays, with the only intention of waiting for other relays' possible operation. Yet for adaptive relays, more knowledge of data from other relays provides necessary information for a delay-free coordination. To perform effective coordination through communications, the protocol is expected to be high-speed, reliable, fault-tolerant, and intelligence-enabled. It is to be accomplished for both local and wide area communications.

The communication protocols require intelligence because the purpose of the communication is no longer pure data gathering. More structured functions are expected from communication procedures. For example, in the application of generators shifting power output to relieve line overloading, a central strategy sends out query messages to get all related generators and load information for negotiation. After a certain number of negotiation iterations, generator shifting actions are taken at different places and line loads are correspondingly reduced. This is a typical preventive control case, since a local

overloading may potentially lead to a large-area disturbance and unintentional islanding as it happened in the recent blackout in the U.S. on August 14, 2003 (U.S./Canada Power Outage Task Force, 2003). In such a case the communication protocol should enable flexible data structure, negotiation functions, and intelligent decisions for effective control and protection of the system.

To support high-performance intelligent relay operations over the network, legacy communication protocols (Modbus, DNP3.0, and IEC 870-5) may not be well suited to emerging practices. Three main features need to be changed:

- Legacy protocols are points-list oriented, which means they have fixed data format and possess a heavy documentation burden. As a contrast, object-oriented protocols are self-descriptive thus expandable, making intelligent applications possible.
- Legacy protocols are optimized for slow serial data connections due to the history and technology confinements. Nowadays, wide bandwidth data transfer necessitates high-performance LAN and WAN protocols.
- Legacy protocols are based on the assumption of master-slave architecture. But the information exchange among relays calls for peer-to-peer communication protocols, which becomes the key function in the proposed architecture.

4.4 Features and Discussion of UCA™

With the background of the emerging need for developing open communication architecture for IED communication in substations, EPRI launched the Utility Communication Architecture (UCA™) project in 1986 (IEEE, 1999; IEEE PSRC, 2003). It is a standards-based approach to utility communications. The objective of the project was to meet the requirements of a wide range of utility performance criteria, while maintaining consistency at the device and data levels to reduce wide-scale integration costs.

As stated in sections 4.2 and 4.3, the requirement of the proposed adaptive protection to the communication system is stringent in speed, reliability and intelligence. It is obvious that the legacy communication protocols in power system protection and control are not able to meet the requirement. Therefore UCA™ is briefly introduced in this section and the

possibility of adopting it for adaptive wide area protection system is evaluated. This section does not have the intent to give a whole picture of UCA™. Instead, only relay-related topics are discussed. The references (IEEE, 1999; IEEE PSRC, 2003) provide a better overview and more details about UCA™.

In the past several years, UCA™ has been adopted as an international standard of IEC 61850. The technical specifications of each version of UCA™ represent a consensus of expert opinion at the time of publication. However, this work is still being continued through the standardization process by a number of organizations and modifications are very likely.

UCA™ 2.0 was developed as the result of several pilot projects launched in 1993 and 1994 (IEEE, 1999). Within the UCA™ 2.0 framework,

- Profiles are recommended with suites of Open System Interconnection (OSI) layered protocols. Within each profile, a set of commercially available high-speed communication protocols is adopted.
- The definition of the data and control functions made available by the device is known as the device object model. The standardized device data and methods models are defined in Generic Object Models for Substation and Feeder Equipment (GOMSFE), which describes the format, representation, and meaning of utility data. The self-descriptive object models in GOMSFE assure device interoperability.
- The device models make use of a set of Common Application Service Models (CASM) to describe the communication behavior of the devices. A standard mapping of these services onto the UCA application layer protocol, Manufacturing Message Specifications (MMS), when used in conjunction with the device models, completely specifies the detailed interoperable structure for utility field devices.

The major benefits of employing UCA are briefly summarized:

- Multi-vendor interoperability: The use of standard device-service-protocol mapping completely specifies the detailed interoperable structure and open data access for utility field devices.
- Self-description of devices: detailed object-orientated device models were developed to support the basic functionality of each device class. The use of named variables in device models, as opposed to anonymous point lists in legacy protocols, greatly reduces planning, commissioning, documentation costs, and installation problems. Hence validation of the mapping of SCADA database entries with field device values becomes extremely simple.
- Independent functional structure: layered approach enables the isolation of device models from the underlying network protocol, and the ability of utilities to choose the media/link combination that best meets their cost/benefit range.
- Saves 40% capital costs and 15%-30% recurring costs (IEEE PSRC, 2003): the savings in costs are through application of one set of common standards and ease of maintenance.
- Benefits of the Ethernet LAN which is within UCA profiles:
  - reduction of conventional wiring
  - parallel operation
  - shared resources
  - shared redundancy
  - availability of off-the-shelf diagnostics and network management products
- Expandability: The devices hardware and applications are free from technical obsolescence and can expand incrementally. Both utility and vendors can incorporate future communications innovations while maintaining their existing implementations.
- Security: UCA allows secure access by "foreign" utilities to specific systems and customers, while keeping them isolated from the details of the network and device infrastructure.

Generic Object Oriented Substation Event (GOOSE) is one of the basic global models defined in GOMSFE for reporting relay IED input and output signals. In the following subsections, GOOSE functions and performance are evaluated for adoption in the proposed adaptive protection system.

4.4.1 Generic Object Oriented Substation Event (GOOSE)

It is the development of IED that results in the possibility of direct network access to field devices, as well as more processing being performed at the end device. In contrast to the conventional master/slave communication, there emerges the need for arbitrary pairs of IEDs, or peers, to manage communication mutual information. GOOSE is designed to address peer-to-peer communications issues of protective relay IEDs. In general, this type of communications

- Is mission sensitive and time critical,
- Supports variable time contact closures, and
- Must be highly reliable.

Accordingly the operation mechanism of GOOSE is designed as follows:

- Distributed decision making: the decision of the appropriate action to GOOSE messages, and the action to take should a message time out due to a communication failure, are determined by local intelligence in the IED receiving the GOOSE message.
- Multicast: The target speed of UCA time-critical messages is identified as 4 ms for simple binary state information. To meet the stringent time requirement for GOOSE messages, the communication mode of multicast is chosen for sending the same message to multiple devices simultaneously. The work model is known as "publisher/subscriber", in which sending device publishes the message and any device interested in is programmed to subscribe to it.
- Repeated and unacknowledged transmission: IEDs are required to initiate a GOOSE message whenever the status changes. As long as the output is stable the

same message keeps retransmitting to the network. The retransmission intervals range from several milliseconds to one minute and can be configured.

- Time to live ("hold time"): the message (status) will expire after the hold time expires, unless the same status message is repeated or a new message is received.
- IED status reporting: To ensure that all associated IEDs will know the current status of their peers, the status of each IED is transmitted in the following way:
  - A newly activated IED will send current status as an initial GOOSE.
  - Any IED can request a specific IED's status at any time.
  - All IEDs will send out their status message on a periodic basis.

Table 4.3 Common components required for GOOSE

	Name	Description	DataType[4]
header	Sending IED	Unique name of the device sending IED	IDENT
	t	Time stamp of the GOOSE message	BTIME6
	SqNum	Message sequence number	INT16U
	StNum	Event sequence number	INT16U
	HoldTim	Hold time is the time that a particular message is held before it is canceled	INT16U
	BackTim	Back time is the time since the last event	INT16U
	PhsID	Identifies faulted phases	INT16U
DNA		Protection Dynamic Network Announcement[5]	BSTR64
UserSt		User status is a group of 128 bit pairs defined by the utility or vendor	BSTR256

The format of the GOOSE message is standardized in UCA 2.0. Table 4.3 includes the common components used to facilitate the GOOSE class object.

[4] The UCA standard data types are defined as following (IEEE, 1999):
IDENT: VSTR65, identifies a Data Object or subcomponent of a Data Object within the scope of the server
VSTRn: Printable ASCII text string—1 to n characters
BTIME6 Number of ms since midnight and days since 1 January 1984 - 6 Octets
INT16U Unsigned integer—16 bits
BSTRn: Bit string—"n" bits

[5] Protection DNA is a single 64-bit message that conveys all required protection scheme information regarding an individual IED. In this message each bit pair is uniquely assigned to one feature of the protection scheme; the four states corresponding to the bit pair values are defined as a standard. By this means protection DNA in a GOOSE message reports the status of all components in the IED to its peers per the enrollment list.

4.4.2 Wide Area GOOSE (WAG)

The function of WAG is time-critical communication over an extensive area, for example, relay transfer tripping. Moreover, WAG is intended to form a foundation for "next generation power system control" (IEEE PSRC, 2003). Therefore the performance in speed and traffic control is of vital importance. In a wide area network, multicast GOOSE messages are bridged rather than routed among substations for the sake of speed. Benchmark tests show that Ethernet bridging over Synchronous Optical NETwork (SONET) only adds 1ms to the propagation timing (IEEE PSRC, 2003). Thus the total time delay of a GOOSE message would include 4 ms of GOOSE time, 1ms of bridging time plus the fiber delay, which is typically 5 μs/km. This means that a GOOSE message can be sent over 1000 km in 10 ms. This communication delay represents the best that can be achieved based on present day techniques. It is acceptable for today's remote protection and control requirement as long as the traffic load is under control. However, concerns for WAG performance due to message clogging do exist and will be discussed in the following subsection.

4.4.3 Limitations and Modifications

GOOSE of UCA 2.0 meets most of the requirements of the proposed adaptive protection for communication architecture. However, there is still concern with the practical use of GOOSE in the future.

4.4.3.1 Object Model Considerations

GOOSE is based upon the asynchronous reporting of an IED's outputs status to other peer IEDs (IEEE, 1999). The design principle is such that the associated IEDs receiving the message use the information contained therein to determine what the appropriate protection response is for the given state. Thus the status of each IED contributes to the decision-making of enrolled peer IEDs and information is shared.

The protection Dynamic Network Announcement (DNA) bit pairs of GOOSE were originally designed to facilitate connection among devices through the definition of "standard" bits. In UCA 2.0, there are 26 bit pairs defined in the 64-bit protection DNA for 26 identified features of a protection scheme, e.g. the 2^{nd} bit pair is assigned to the status of "lock out" while the 6^{th} bit pair is assigned to the status of "send transfer trip" (IEEE, 1999).

However, the ability of today's IED to provide multiple component protection made such standard assignments limiting. On one hand, one bit pair, or four values for different states of each feature was designed for digital output of relays and might be inadequate in the foreseeable future. The data structure of next generation IEDs feature could be more complex than simple digital signals. It could be the protection device status with its corresponding "confidence level" as proposed in Section 3.6. Therefore the communication standard should not limit itself to digital value exclusively. On the other hand, even if a specific IED does not have a certain feature, it is standardized to fill every bit of the reporting message. This leads to waste of both communication bandwidth and processing time. The truth is, the definition of GOOSE is wrapping a point-list in a self-descriptive message.

The limitation has been realized soon after the publication of UCA 2.0. As a result, the DNA bits now have become user-definable (IEEE PSRC, 2003). However, interoperability would be infeasible if DNA bits are totally user defined. If protocol converters are needed for GOOSE communication, UCA would be a practically vain effort in communication standardization. Instead of loosing control of the standardization process, a self-descriptive object-oriented data model would solve the problems of both expandability and interoperability.

The author proposes a GOOSE DNA structure to include an additional DNA header for each feature state reported in the GOOSE message. The DNA header is of the data type of INT16U. Within this DNA header the first 12 bits are for the identification number of relay features, which are defined in the standard, e.g. 245 (000011110101) can be defined as the "fault detection with fuzzy factor" as proposed in Section 3.6. The DNA header has the capacity of 4096 protection scheme features. The remaining 4 bits in the header are to indicate the length in bit of the state value that follows. Thus the maximum length of the DNA payload is 16 bits, or maximum of 65536 states. This length indicator enables variable length of states for different protection features, which is a must for complex object models. The principle of DNA header is that the definition of each feature identification number, its corresponding state format and meaning are standard and publicized among users and vendors. Table 3.12 gives an example of a part of the DNA in a GOOSE message.

Table 4.4 A part of the protection DNA in a GOOSE message reflecting one feature of the protection scheme

DNA header		payload		
000011110101	0010	1	0	1
Identification number of a specific protection feature: fault detection with fuzzy factor	3 bits following	the state format and meaning defined: 1: true for "in-zone fault"; 01: with a "confidence level" of 0.5		

The advantages of the proposed data model include enabling transferring complex data objects without loosing interpretability, flexibility in message length so less waste in bandwidth. In the mean time, adding the DNA header would slightly increase the communication overhead. Transferring a GOOSE message of standard 26 bit pairs without the optional user status part, as defined in UCA 2.0, involves a payload ratio[6] of 7% within the application layer protocol. While the same information transferred as the proposed model involves a payload ratio of 5%. The decrease in the percentage of useful data transferred is not significant.

4.4.3.2 Performance Considerations

When the communications among IEDs involve reporting time-critical messages, the real-time response speed requirement could be very critical, e.g. 2 ms for one-way transfer on substation LAN (McDonald, Cáceres, Borlase, & Janssen, 1998). Simulations and benchmark testing during earlier phases of the Substation Initiative Demonstration Project have proved that 100 Mbps Fast Ethernet and/or switched Ethernet would meet requirements for protection commands over the substation LAN (IEEE PSRC, 2003). The testing was carried out with typical IED counts under disaster overload conditions caused by simultaneous faults. The results show that Ethernet with an intelligent switcher is at least as fast as legacy hardwired configuration under different loading scenarios and with multiple events in parallel. It is also promising that the development of Gigabit Ethernet and 10 Gigabit Ethernet would facilitate higher speed communication, by which the stringent protection and control time requirements are becoming easier to meet.

[6] For the purpose of comparing two object models difference in the DNA data block, the payload ratio is calculated as the ratio of DNA state information block over overall message including headers, although actually part of the in formation in the header can be considered as payload as well.

On the other hand, the concern about the network performance still exists. Theoretically, to ensure communications have the speed so that relays can derive fault isolation decisions, the response times for data transfer must be deterministic and repeatable. Some protocols have deterministic time delay, e.g. token ring (IEEE 802.5), token bus (IEEE 802.4). But all token protocols have too much overhead for a high-speed network. Meanwhile, the most popular high-speed LAN configurations, 10M Ethernet (IEEE 802.3) and 100M Ethernet (IEEE 802.3u, y), which are among UCA profiles, are not protocols with deterministic delay. The mechanism of collision detection has no guarantee to predict data transfer delay. So a shared medium network is associated with variable communications latency. The "best effort" protocol quality of service (QOS) lacks message arrival and processing assurance. In addition, Ethernet does not support priority data transfer. Coexistence of mission-critical control signals with non-mission-critical data causes more variation in the QOS. And the repeated GOOSE messages add even more challenges to the network load and device processing. In practice if no effective congestion control mechanism is in action to manage the network traffic, unacceptable transmission delay or even packet loss are potential risks in the multicast GOOSE transmission.

UCA has made major efforts in assuring network performance and making up for the holes in the service. In order to ensure consistent and repeatable data delivery times, collisions are to be eliminated. UCA 2.0 provides two options for LAN connection: shared hub and switch. Network collision problems can be solved to some degree with switches. To further minimize collisions among messages, the refresh interval between the IED repeat messages is parameterized and randomized. Furthermore, hardware message filtering and prioritization in each IED can address device overload concerns by giving priority to mission-critical messages. Each receiving IED can use back time to set appropriate local times associated with the original state even if intervening messages were lost.

Still it is realized that caution must be taken in device design for UCA GOOSE to be effective as a method to send mission-critical data throughout the network (IEEE PSRC, 2003). All layers of all devices on the network must make sure that their functioning and malfunctioning will not overload the network or device buffers and delay the control messages.

The performance of GOOSE messages, in particular WAG, is susceptible to possible failures in traffic control. It is more of a problem for WAN communications because all WAG messages are sent to the WAN without filtering. To aggravate the situation, TCP/IP, which is recommended by UCA, does not support priority data transfer. The best effort data transfer is too primitive for protection applications since it leads to unreliable transfer and unpredictable turnaround delay. Only dedicated link/connection has the possibility to fulfill requirements raised by wide area protection and control applications. So far the only resort of avoiding clogging the network is by "taking caution" in all implementation of WAG schemes not to send too many GOOSE messages. This sounds dangerous because only one malfunctioning or malicious device without this required caution is enough to paralyze the entire wide area network. Even without considering the extreme cases, eliminating non-essential GOOSE traffic would be a challenge in the wide area network. Hence, guarding-devices for network management or built-in mechanism of the protocol is needed to ensure the performance of WAG. In the future, the solution might be UCA adopting other high speed communication protocols that guarantees deterministic time delay.

CHAPTER 5. ADAPTIVE PROTECTION FOR ENHANCING SYSTEM SECURITY

In this chapter, several cases are studied to demonstrate the effectiveness of the proposed relaying concept in enhancing system security. Transient simulation is conducted on a 179-bus test system for the purpose of validation of the adaptive protection scheme. The detailed decision-making algorithms are simulated in two examples to show the protection system achieving the balance between dependability and security.

5.1 Test System

The 179-bus test system used in these study cases is based on the interconnection in the western United States shown in Fig. 5.1. It is displayed on a background that outlines the represented geographical area. Compared to the actual system, this test system uses many equivalents. While the names of actual substations are used, it is cautioned that the system operation discussed here does not necessarily represent the actual system behavior.

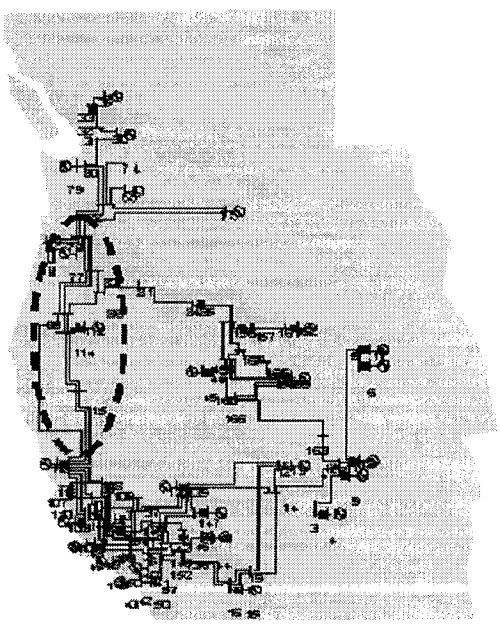

Figure 5.1 A 179-bus Test System

The base case for the study has the generation of 61,411 MW and 12,330 Mvar that corresponds to a high summer peak. During such times, there is a heavy north to south flow through the area along the left of the system that is carried by both the Pacific DC Intertie (not shown in the figure) and parallel AC circuits (circled in the dashed oval). The focus has been on this region in developing examples of system problems that would result from relay operations.

A detail of the test system, consisting of the portion of Fig. 5.1 inside the dashed oval, is shown in Fig. 5.2. This segment consists of the high voltage AC system that is parallel to the Pacific DC Intertie and is a critical portion of the system during high loading. Faults that result in the loss of multiple circuits here lead to instabilities affecting large segments of the western system. The simulations have been performed using ETMSP from the PSAPAC 5.0 software package supplied by EPRI.

5.2 Examples of Preventive Adaptive Protection

In this section, three examples are provided to show how altering the behavior of the protection system in a preventive mode can meet the grid requirement. The adaptive protection shifts to a more "defensive" posture when the system is deemed vulnerable. Two of these examples involve protection unnecessary operations. Unnecessary relay operations frequently result from hidden failures. It is presumed that regardless of how much effort is expended to test the protection system to ensure that it will operate properly, some hidden failures are inevitable. Hence adaptive behavior of the protection system to reduce the impact of such failures is desirable.

5.2.1 Example 1 – Blocking Sympathy Trip

Consider a three-phase permanent fault on line 83-114(1) near bus 83 as shown in Fig. 5.2. Normal operation of the protection system would clear both ends of the line using current differential relaying or instantaneous Zone 1 operation at bus 83 and a transfer trip signal to bus 114. The resulting transient is stable.

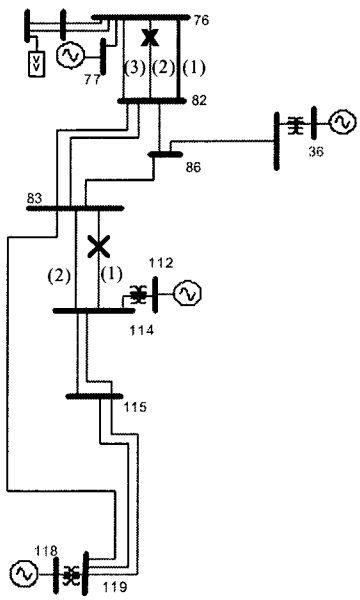

Figure 5.2 A critical portion of the test system

One type of hidden failures identified in the literature (Phadke et al. 1995) occurs in transfer trip systems involving directional-comparison blocking. If such a system were employed here, the relays in the unfaulted parallel circuit 83-114(2) would see the fault but would be inhibited from tripping by the blocking signal. However, if a hidden failure were to occur in this blocking system, the parallel circuit 83-114(2) would trip as well. The loss of both of these circuits results in an unstable, cascading transient in which 14 generators have tripped in 4.28 seconds due to loss of synchronism. The resulting blackout extends over most of the southwestern United States.

This instability is illustrated in Fig. 5.3 where the test region of Fig. 5.1 is represented by a surface. The elevation of points on that surface represents angular differences in generation near those points. All values are smoothed to create a continuum. The shape of the surface in the figure indicates that all generators in the southwest (the dark region) are tripped off as a result of the system instability.

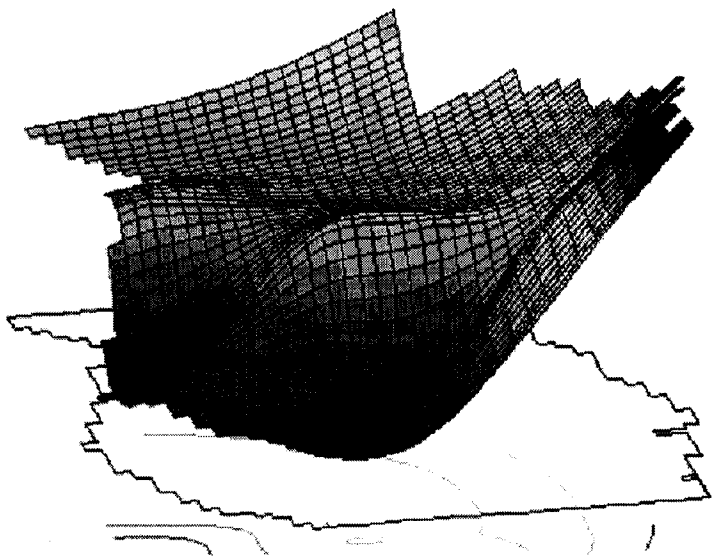

Figure 5.3 Generator angle contour of unstable system without adaptive protection

It is hypothesized that a preventive adaptive protection system might combat this situation. With knowledge that the system is vulnerable to such failures during periods of high loading, the system could decide to deactivate the transfer trip system during such times and rely on zone 2 relaying to clear the far end of the faulted line. The result is still stable although with higher amplitude transients in generator angles. Fig. 5.4 displays the contour of angle differences for this scenario, which is stable. Fig. 5.5 illustrates the motion of the angle of the generator at bus 112 in the normal case where there is no hidden failure in the protection system, and both ends of the line are cleared in 50 ms, with the adaptive case where the near end is cleared in 50 ms and the far end in 350 ms. As expected, the angle oscillations are larger in the adaptive case but an instability has been avoided in the event of the hidden failure hypothesized above. With an adaptive protection system like that suggested in Fig. 3.4, such a change in relaying strategy could be implemented quickly whenever the system vulnerability is judged to be too high.

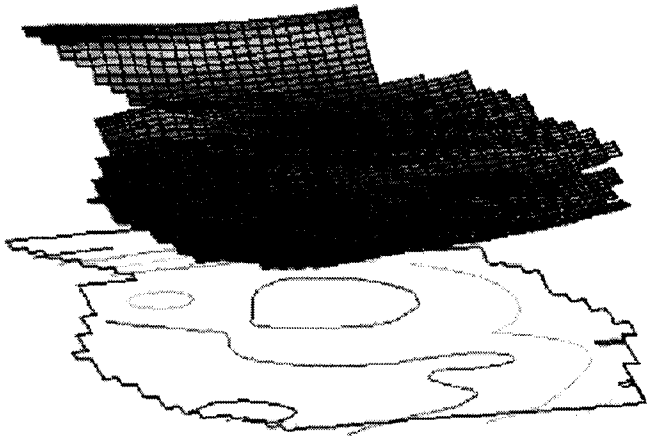

Figure 5.4 Generator angle contour of stable system due to adaptive protection

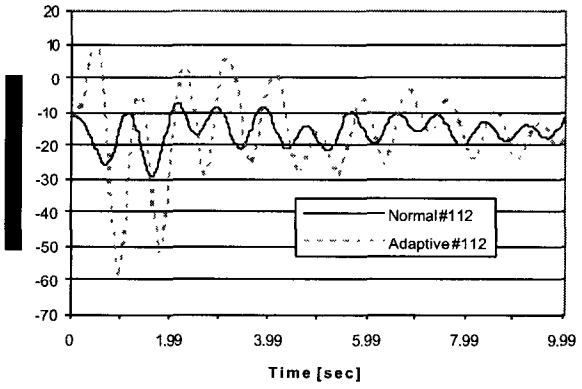

Figure 5.5 Generator angle transient at bus 112

5.2.2 Example 2 - Avoiding Emergency under Heavy Load

When the system is stressed, actions taken by protective relays could result in severe consequences even if these actions are suitable for normal operating conditions. Consider the Critical Clearing Time (CCT) of a three-phase fault on the second line between John Day and Grizzly, 76-82(2), at a point 25% from John Day (Fig. 5.2). In this portion of the Pacific AC Intertie, three parallel 500-kV transmission lines carry the north-south flows in parallel with the DC intertie.

In Table 5.1, a uniform system real load increase of 1.5% results in a line flow increase of 56% at 76-82(2). The CCT becomes impractically short (<50 ms) since a fast circuit breaker needs 50-70 ms to open (Blackburn, 1998).

Table 5.1 System sensitivity to load levels

	Pre-fault line flow through 76-82 (2)	Line 76-82 (2) CCT	System behavior
Base case	864 MW	160 ms	Stable
1.5% increase in system P	1,349 MW	<50 ms	Severe oscillations on parallel line (1) &(3), up to 2 GW per line

One solution to this difficulty is to extend the CCT by shedding load immediately after the fault. Simulation shows that, by simultaneously shedding 2% of system P and clearing the faulted line, the CCT is greater than 120 ms, which is a practical operating time. This load-shedding scheme is necessary only for heavily loaded conditions. Therefore the adaptive protection system could be switched to a preventive mode with a load-shedding scheme armed when this stressed system condition is detected.

5.2.3 Example 3 – Short Term Overloading

This example again considers a fault on line 76-82(2) with system loading as in the base case. If a hidden failure were to exist on line 76-82(1), such as a failure of a directional relay or zone 2 delay timer, the fault could trip both circuits leaving only line 76-82(3) in service. Specifically, with all lines in service, the current in line 76-82(3) is 0.5 kA. But the current increases to a steady state of 2.3 kA, following a transient peak of 3.5 kA, if the other two lines are out. This third line may trip on overload resulting in system islanding if its relays were not set to anticipate this eventuality. Similar events happened many times in history (NERC, 2003).

Preventive adaptive protection can be employed to avoid such a catastrophe by modifying relay settings in advance. The triggering factor would be the heavy loading condition. If the relays are reset to allow a transient peak of 3.5 kA for 2.5 seconds and a

steady state current of 2.3 kA which is below the 500kV line thermal limit[7], the system will remain stable. That is, when heavy loading occurs, the adaptive protection scheme could switch to higher overload current and longer overload tripping delay settings to maintain system stability during emergencies.

Another solution would be having responsive mechanism in the adaptive relaying. By incorporating the real-time information of both load level and topology, the relay decision-making procedure at line 76-82(3) can override the normal settings to hold up higher and longer transient and load current. The details of algorithms implementation of this example is shown in Section 5.4.

In summary, examples 1, 2, and 3 are simple illustrations of how the system of Fig. 3.4 can lead to a more defensive protection system in times of stress and vulnerability. In each case, the control available within the substation and central controllers, coupled with high-speed communication and computer controlled switching devices allow new control logic to be implemented. This new logic adjusts the protection system behavior prior to a disturbance to avoid an otherwise catastrophic failure.

5.3 Examples of Emergency Adaptive Protection

The system of Fig. 3.4 would be used in an emergency mode as well as in a preventive mode. That is, if the communication and control operations can be accomplished rapidly enough, it would be possible for the protection system to respond to an emergency by analyzing the problem and operating the appropriate protection components to avoid a catastrophic failure. In Section 4.2 it was estimated that the time required for detecting a problem, analyzing that problem and executing the appropriate control is on the order of 100~200 ms. The available time is determined for executing the proper control in different scenarios as shown in the examples below.

---

[7] The actual current-temperature relationship of bare overhead lines can be calculated given the weather conditions (IEEE 1993). The maximum allowable conductor temperature is normally selected so as to limit either conductor loss of strength due to the annealing of aluminum or to maintain adequate ground clearance. When these effects are considered, it is common to use a higher maximum allowable conductor temperature for transient thermal rating calculations than for steady-state thermal rating calculations. For fault calculations, the maximum allowable temperature is normally close to the melting point of the conductor material (Walker et al., 1982).

The portion of the system in Fig. 5.2, which is the most sensitive to failures, is repeated as Fig. 5.6 with specific breakers indicated. All examples concern a permanent three-phase fault between Malin, bus 83, and Summer, bus 86, at a point 10% from Summer as shown in Fig. 5.6. Allowing for breaker actuation time, normal relay action would clear both ends of the line with breakers A and B within about 50 ms. The cases considered involve a failure in the transfer trip system so that breaker B at Malin, 83, fails to clear that end of the line. With this failure of B, the system will resort to a backup-relaying scheme. Thus it is likely that all lines at Malin would trip using zone 2 of distance relays[8]. As a result, breakers C, D, E, F, and G would all open in 250~350 ms, depending on the relay time delay and breaker actuation time. This breaker action disrupts the entire AC corridor and, for this heavily loaded base case, the system is unstable and rapidly loosing synchronism.

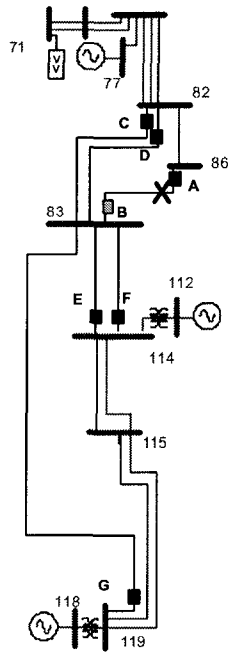

Figure 5.6 A critical portion of the test system with breaker identities shown.

Three examples in this section will show how the adaptive protection system of Fig. 3.4 can avoid this instability. Each relies on rapidly gathering information on line flows and breaker status from the Malin and all neighboring substations. Then the adaptive relays

[8] All six lines are assumed to be connected to a single bus section. Other bus configurations may behave differently.

identify the problem and take the remedial action described in the example. In all cases the speed required of the adaptive protection system is studied. That is, how much is enough time for the protection system to respond to the event before the system becomes unstable and the opportunity to avoid catastrophic failure is lost. Hence, for each example, the maximum time available is found for the remedial action to be accomplished, a time that depends on system loading and event sequence.

5.3.1 Example 4 –Recovery through Reclosure

The circuit breaker controllers must analyze the information available on the fault to identify the corrective action required. This mechanism can be realized in a centralized manner at the control center or distributed in each adaptive relay. In the centralized approach the Central Controller collects information from the affected substations through high-speed communications. The measurement of CTs on the six lines at Malin would be able to detect which line is carrying the major fault current out of the bus. If there were doubt, voltage and current information from the neighboring buses could be compared to identify the faulted line. Additional information would be available from a sequence of events recorder detecting the timing of breaker A relative to the others. Assuming breaker B is operational, the remedial action is to open breaker B and reclose the breakers on the five unfaulted lines. Such a group of remedial action commands are sent again through the communication channels that connect the substations and the control center. Thus the system recovers through proper reclosure actions. The distributed approach requires all adaptive relays at these six lines connected to the same network so they can share information in a peer-to-peer manner. By exchanging the measurement data and performing proper analysis built in each relay, the same set of decisions can be reached by each adaptive relay individually.

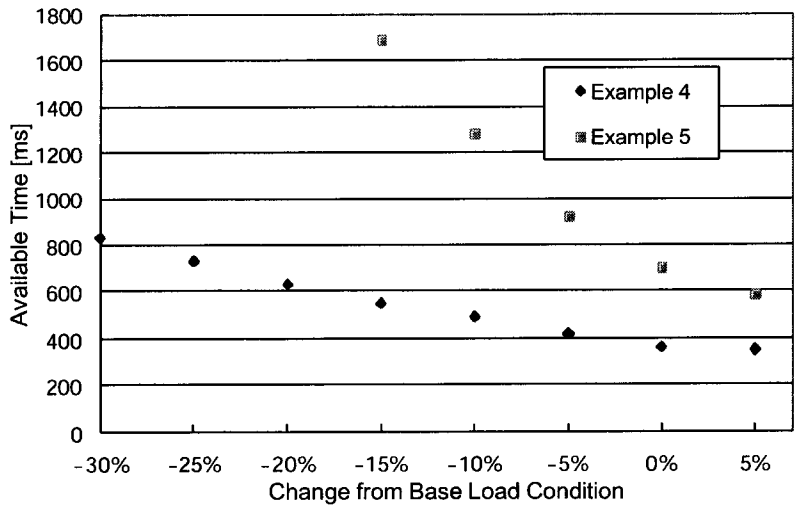

Figure 5.7 The time available for remedial actions

The time available for this corrective action to maintain synchronism is examined through simulation. The lower set of data points, labeled "Example 4" of Fig. 5.7 summarizes the results for 8 cases, each at different load levels identified by the change from the base case. The base case represents the already heavily loaded system described before. In fact, a 10% increase in system loads leads to a failure of the power flow to converge. Hence the cases from a 5% increase down to a 30% decrease from the base case are explored. All load adjustments are applied uniformly at all load buses. The time available between the occurrence of the fault and the necessary reclosure action varies between 360 and 830ms. The results show that even for heavy loading conditions the time available for adaptive protection to take remedial actions is adequate. The only concern is the proper coordination between the adaptive controller and traditional backup relays. This issue is addressed in the following example.

5.3.2 Example 5 – Adaptive Backup Relaying

The relaying failure scenario of this example is the same as that of Example 4. The differences are in the response of the protection system. Specifically, all traditional back up relaying is assumed to be overridden by adaptive back relaying. The practical approach can be having the Central Controller supervising and managing traditional relays, blocking if necessary, or replacing traditional relays with adaptive relays as backup. Same as in Example

4, breaker A opens in 50ms, because the primary functions operate instantaneously. Breaker B fails to operate due to the fault detector failure. In the centralized setup, Zone 2 in traditional backup relaying is blocked or delayed by the Central Controller so the other lines at Malin remain energized. In the distributed setup, each adaptive relay at the five unfaulted lines reaches the no-tripping decision based on information collected over the wide area. Upon assessing the status of the system, breaker B is opened either by the Central Controller command or the adaptive relay at breaker B, without any disruption of the other lines. This assessment depends on information from all connected relays sensing the fault and appropriate logic. The logic would include algorithms that can incorporate data uncertainty and incompleteness such as voting schemes with fuzzy techniques. With modern computation and communication technology, this decision process takes no more time than a normal backup relay. The implementation of this procedure is simulated in Section 5.4.

The upper set of data points in Fig. 5.7, labeled "Example 5", indicates the time available for this adaptive backup relaying action for different system loads. The system is stable even if breaker B remains closed for loads that are 20% less than the base case. Of course, the fault currents are of concern and breaker B would be opened as quickly as the adaptive protection system could manage. The times displayed in Fig.4.7 represent the maximum time available for system stability. The results show that the time available is even more than that of the corresponding conditions in Example 4.

5.3.3 Example 6 – The Effect of a Temporary Reduction of Power Flow

In Example 4, where breakers C through G must be reclosed and breaker B opened, the time available for remedial action is quite short for high load levels. Even though the time available is longer than 200 ms, which is estimated to be required, it is to be explored whether the available time could be extended by temporarily reducing the flow through the affected lines. Since this portion of the Western U.S. system is parallel to the Pacific DC Intertie, it is possible shifting some load rapidly to that system, perhaps very temporarily. Indeed, the DC intertie is not used for such purposes and such a shift may be inappropriate for various operational reasons. However, other mechanisms for flow reduction may be possible since the shift can be very temporary if maintaining synchronism is the only concern.

For example, it may be possible to divert flow through some other part of the system or even shed some load for a brief period.

The Pacific DC Intertie (PDCI) connects the Cellio Station, bus 71, with the Sylmar Station in the Los Angles area, spanning a distance of 1,361 km. Fig. 5.6 shows the terminal at bus 71 but the Sylmar Station is outside the area shown. While studying the controls for power flow on this line is beyond the scope of this research work, it is believed that flow can be altered very rapidly as is the case in other electronic controls.

Fig. 5.8 plots the time available when the system is loaded as in the base case and the DC flow is increased by 1000, 2000, or 3000 MW. The available time increases from 360 ms in the base case to 430 ms for a 3000 MW increase in DC flow. In these studies, it is assumed that the flow diversion occurred at the same time as the remedial switching action. That is, in the case where the DC flow was increased by 2000 MW, the system could wait a maximum of 410 ms to divert that flow and accomplish the breaker switching.

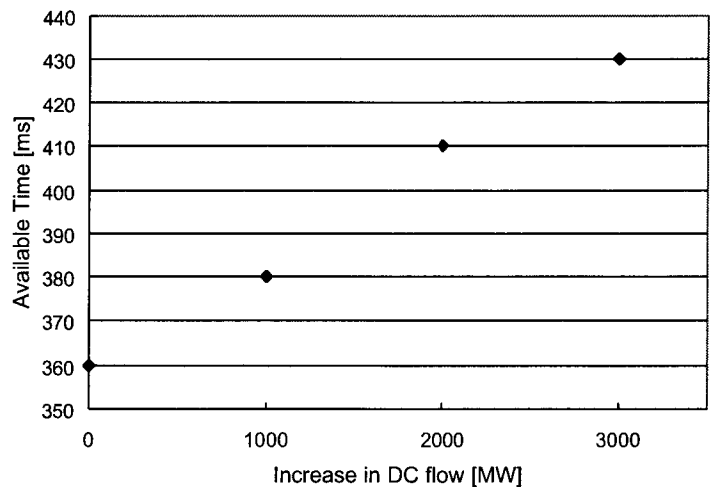

Figure 5.8 The time available for remedial actions after changing of HVDC flow

It was also studied how rapidly the DC flow could be restored to its original value and maintain synchronism. Fig. 5.9 illustrates the result for the case of a 2000 MW transfer to the DC line for the base case as well as 5% changes above and below the base case. The lower data points are a repeat of the result in Example 4 with no load diversion. The middle data points are the time available when there is a 2000 MW diversion and the upper data points

identify the minimum time, from the time of the fault that the dc flow can be returned to its initial value.

For example, when the loading is 5% above the base case, the available time is increased to 410 ms providing the DC flow is also increased by 2000 MW at that same time. That is, the DC flow increase gains 50 ms before action is required and the flow need be maintained for only an additional 440 ms or until 850 ms from the time of the fault.

Again, it is not clear that such operation is feasible on the present DC system or any other but it illustrates some of the important interactions of the system components during faults. It is known that the PDCI is capable of transmitting up to 3100 MW in normal operation and 3650 MW for ten-minutes (Elliott, Lavier, Kuehn, & Kuechler, 1999).

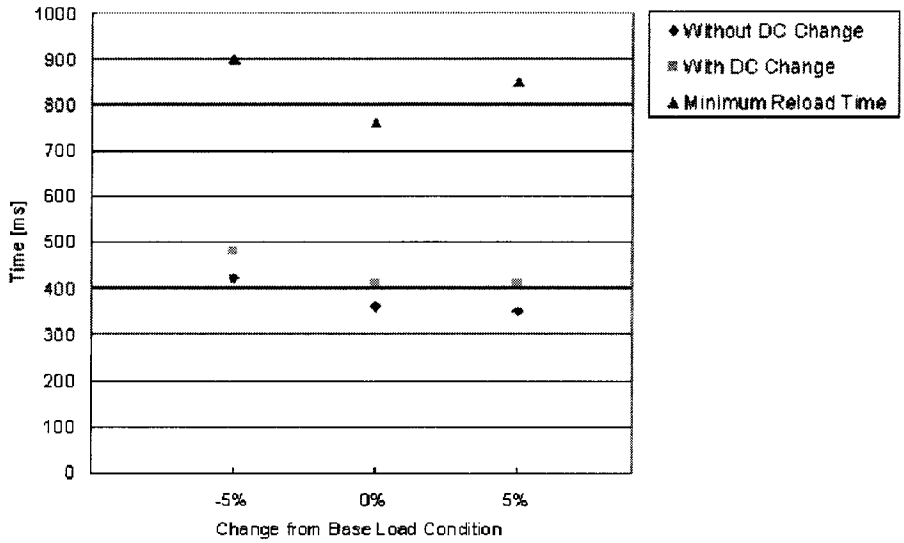

Figure 5.9 Time available for remedial action after increasing DC flow by 2000 MW

5.4 Algorithms Implementation

The examples provided in this section are to implement the internal logic of adaptive wide area relays proposed in Section 3.6. The basic idea is to equip intelligent relays with real-time wide area information through appropriate communication channels. The input signals are for indicating the system vulnerability and relay reliability bias. They can come from real-time system monitoring, off-line analysis programs or simply from loading conditions and topology information. Within the adaptive relay, the decision-making module incorporates much more input signals than does a conventional relay to make more

intelligent protection decisions. In the examples here the author applies fuzzy set inference mechanism to the decision-making logic module. However, more possibilities of other implementation, such as multi-agent systems could also be explored.

The procedure of implementing the algorithms in the following two examples is summarized as three steps:

Step1. Creating and editing Fuzzy Inference Systems (FIS) in MATLAB's Fuzzy Logic Toolbox. This is the core of the proposed adaptive relay intelligence.

Step2. Building the test transmission system in MATLAB's Power System Blockset, with the FIS module built in step 1 as the control mechanism of the adaptive relay.

Step3. Testing the system behavior under different fault conditions in the block diagram simulation environment of Simulink.

5.4.1 Implementation of Example 3 in Section 5.2.3

The first example is to implement the adaptive relay logic in Example 3 in Section 5.2.3. Consider a permanent fault on line 76-82(2) with a hidden failure on line 76-82(1) as shown in Fig. 5.2. Both circuits would trip leaving only line 76-82(3) in service. Then the conventional protection of line 76-82(3) may trip on overload or Zone 3 of the distance relay, resulting in system islanding.

Previous research carried out by the author employed preventive protection setting change to avoid this catastrophe. If the relays are reset to allow a transient peak of 3.5 kA and a steady state current of 2.3 kA, the system will remain stable. However, although heavy load can be detected in advance and serves as the criterion of switching relay settings, relay unnecessary operations and hidden failures are not foreseeable. An ideally intelligent or adaptive protection system should be able to alter its behavior according to real-time data which reflect both power grid vulnerability and the situation of peer relays. A possible implementation of such an adaptive relay operating in emergency mode is illustrated in this example.

In Fig. 5.10 the portion of interest in Fig. 5.2 is modeled in Simulink. The simplified power grid includes four buses (Bus1 as the equivalence of the system in the north, 76, 82, Bus4 as the equivalence of the system in the south), one source connected to Bus1, one load connected to Bus4, and five transmission lines in between. The three parallel transmission

lines connecting bus 76 and 82, denoted as line1, line2 and line3, are the objects of study in this case.

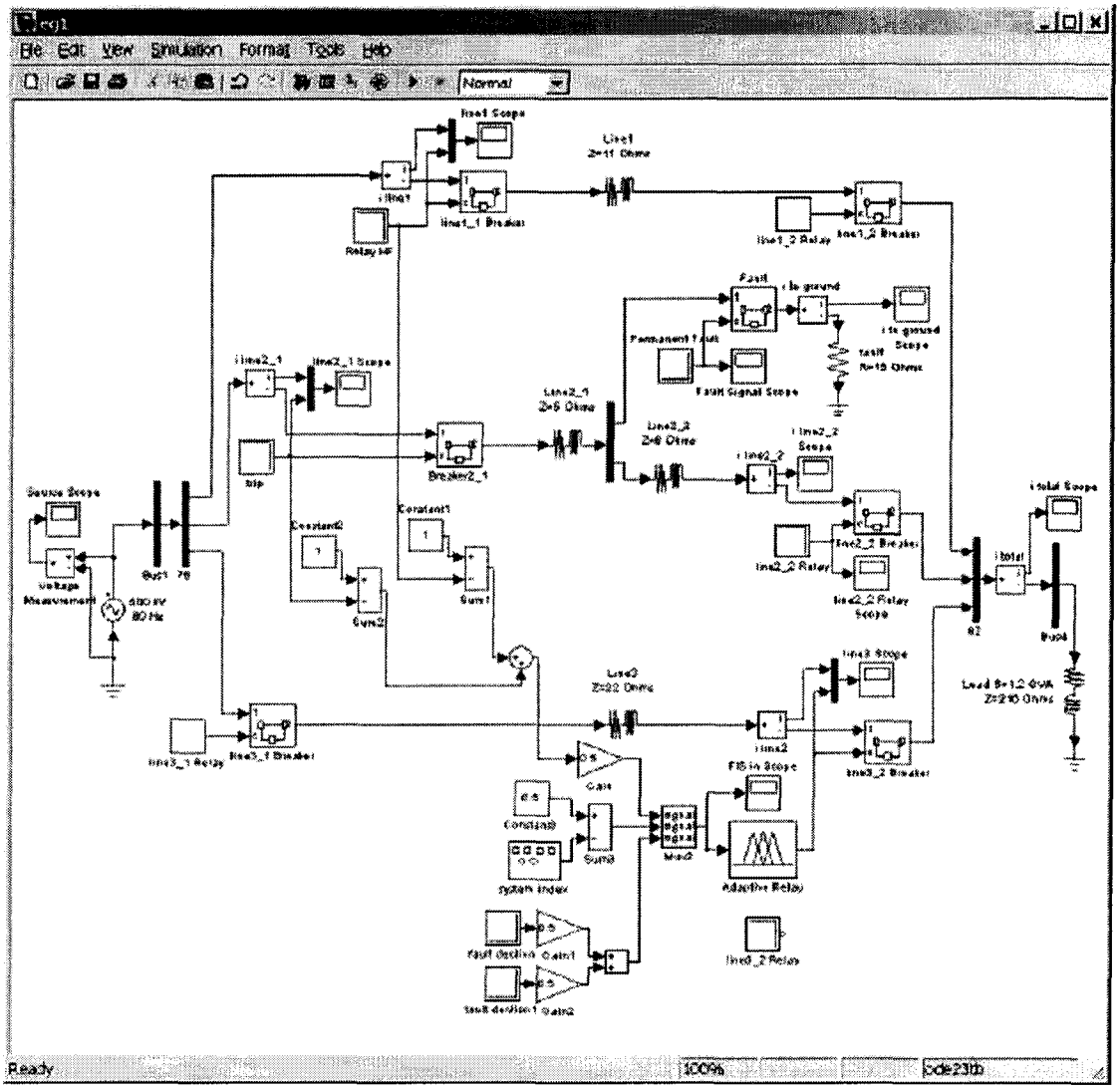

Figure 5.10 Three parallel lines between bus 76 and 82 are modeled in Simulink

The sequence of events starts with a fault on line2 at t = 2 cycles, with the fault signal shown in Fig. 5.11. The fault is cleared correctly by relays at both sides of line2, at t = 6 cycles. In Fig. 5.12 the current through line2 is recorded, varying from the normal load of 0.9 kA to the fault current of over 20 kA and ends up with zero. Assume the existence of a hidden failure on line1 such that line1 opens inadvertently at t = 6 cycle too as recorded in

Fig. 5.13. This situation resembles the initial event of many real-world disturbances, e.g. 1996 WSCC voltage collapse. It leaves line3 with an unusual high post-fault current. Under normal circumstances, such a high current should have tripped line3. Fig. 5.14 exhibits the phenomenon of lines3 tripping by Zone 3 backup relay after 0.6 second time delay. Thus the whole north to south AC corridor is disconnected and the load current is interrupted.

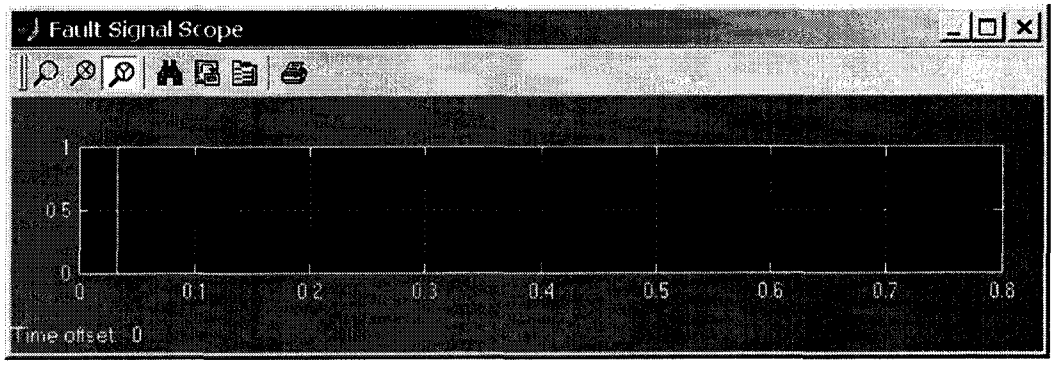

Figure 5.11 Fault occurs on line2 at t = 2 cycles

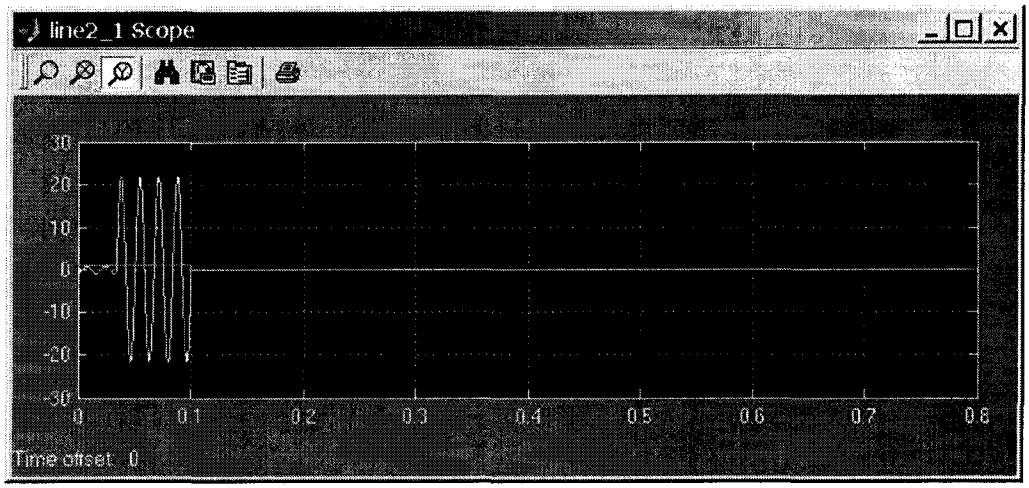

Figure 5.12 Line2 current and relay signal: fault cleared at t = 6 cycle

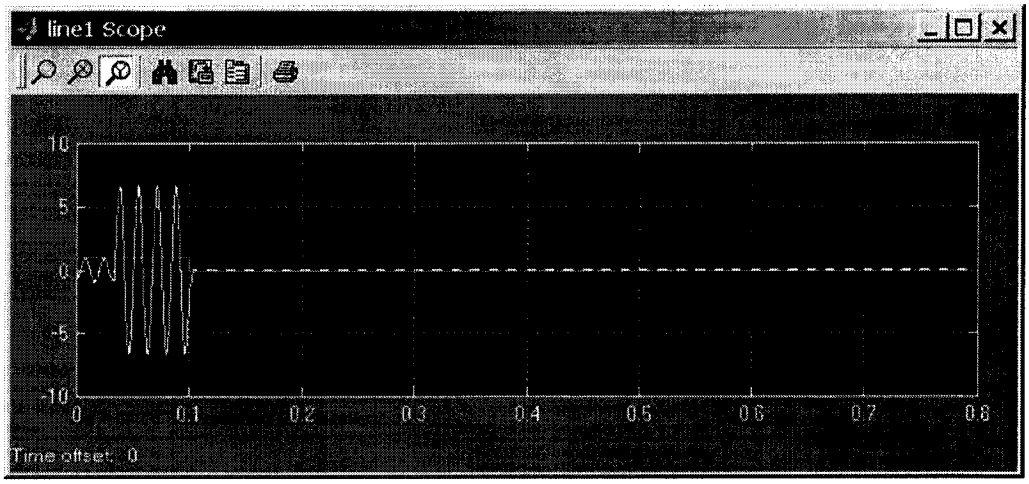

Figure 5.13 Line1 current and relay signal: relay trips incorrectly at t = 6 cycle

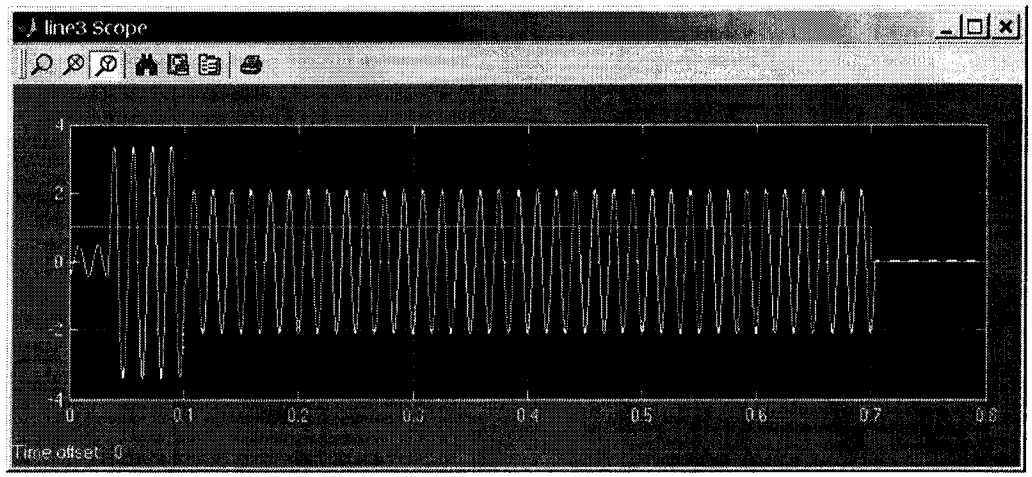

Figure 5.14 Line3 current with conventional distance relay: protection operation at t = 42 cycles

However, for a stressed system with both heavy load and all alternative paths lost, line3 should be able to contribute to the system integrity by sustaining higher current for longer as long as the current itself does not exceed the thermal limit of the facilities. In this specific example the conductor of line3 is required to carry 2.3 kA of post-fault current, corresponding to 2 GVA of line load, which is below the stead-state thermal limit of 500kV transmission lines (Walker et al., 1982). Even for a more aggressive case when the post-fault current exceeds the conductor thermal limit, considering the thermal time constant[9], there is still enough time for the adaptive protection to analyze the situation and initialize appropriate

[9] Conductor thermal time constant is the time for the conductor temperature to reach 63% of its final value. The value of thermal time constant is usually more than 10 minutes (IEEE 1993).

actions other than tripping line3, such as reclosing the unfaulted line2 to save the system from falling apart. Fig. 5.15 shows the implementation of line3 adaptive relay applying the fuzzy inference system (FIS) to make operation decisions. The decision-making module of the relay incorporates wide area information, such as system loading indices (variable name "SysIndex") and the percentage of parallel facilities lost (variable name "NumPrlTrp"), to evaluate the need of intentional overloading. By assigning proper membership functions to all input and output signals (Fig. 5.16, 5.17, 5.18, 5.20) and designing inference rules (Fig. 5.19) according to system study, expertise or even common sense, the mechanism is able to make intelligent decisions within the order of millisecond (Fig. 5.21).

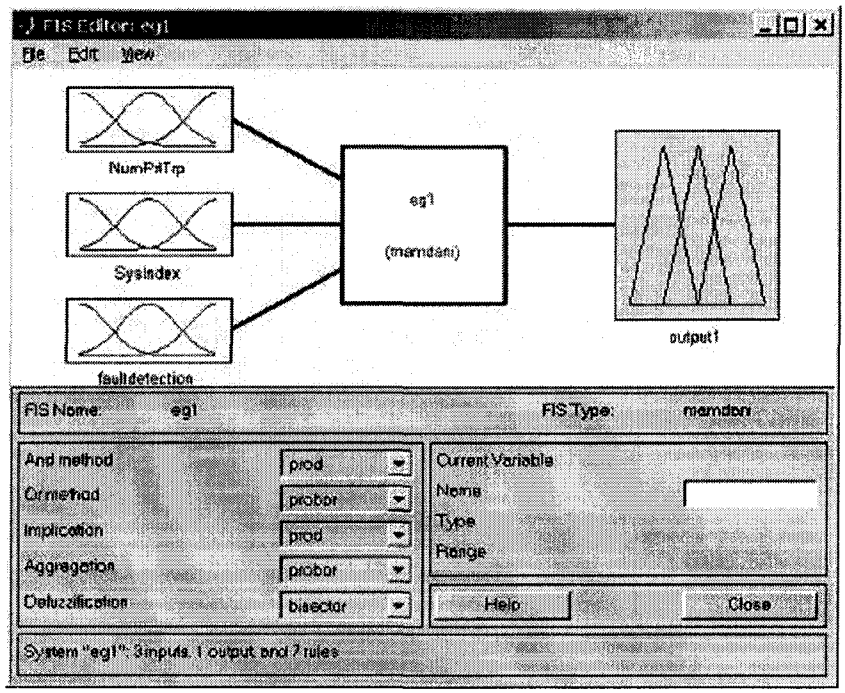

Figure 5.15 Fuzzy Inference System of adaptive relay on line3

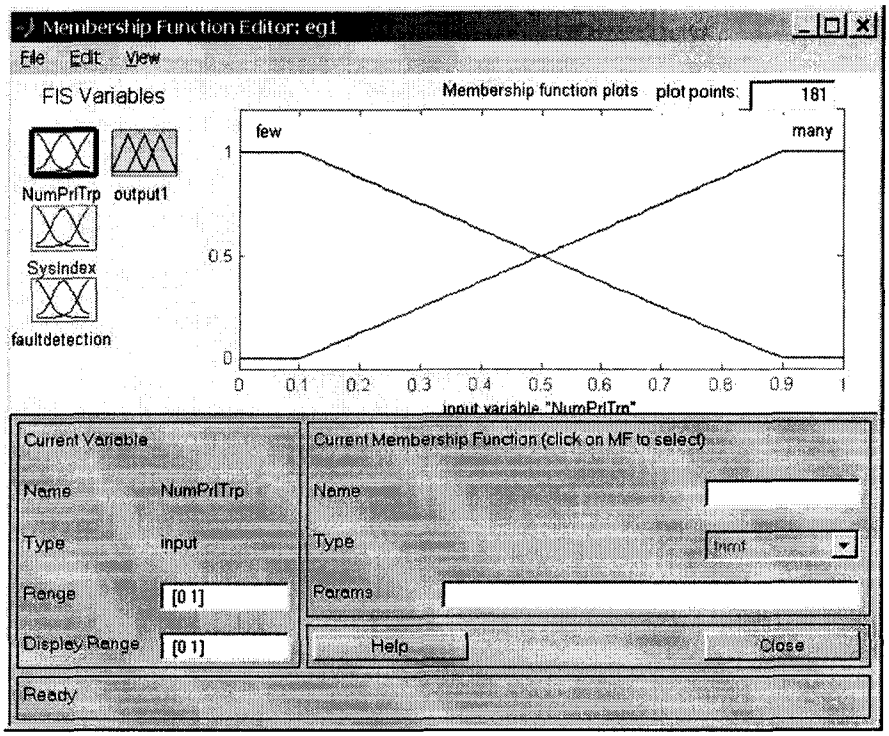

Figure 5.16 Membership functions of the input signal " percentage of parallel facilities lost"

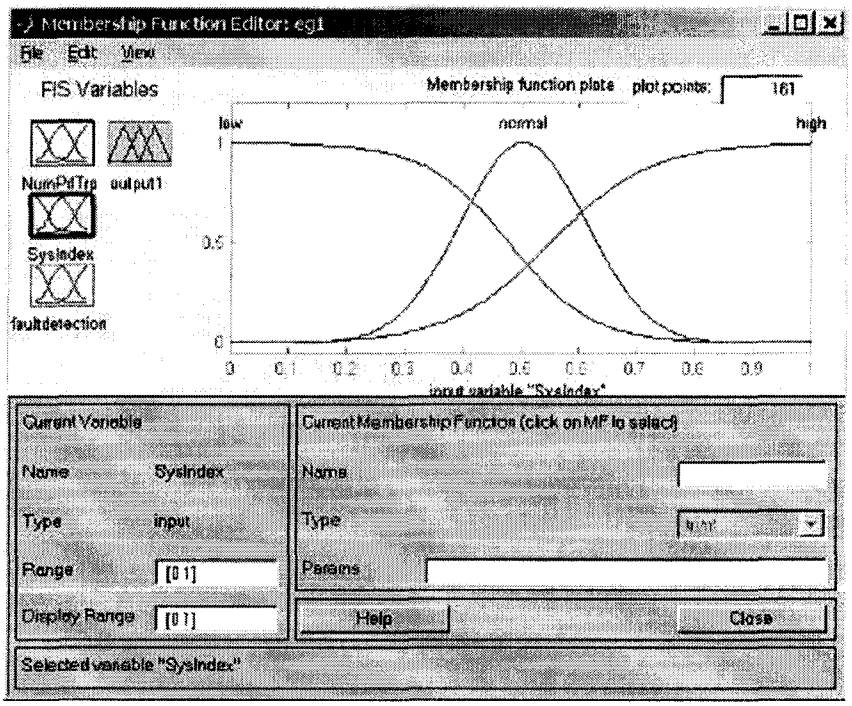

Figure 5.17 Membership functions of the input signal " system loading index"

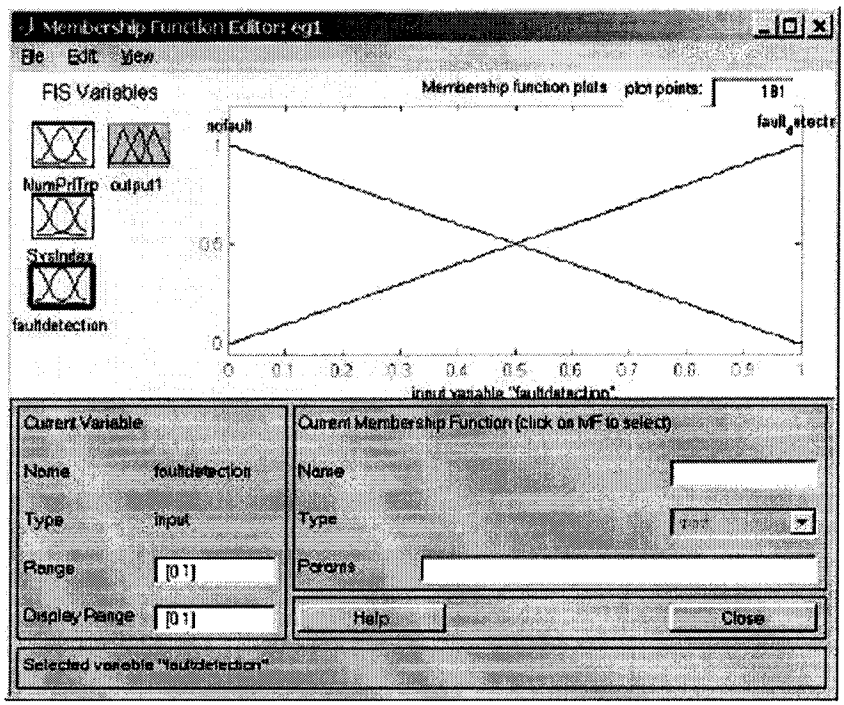

Figure 5.18 Membership functions of the input signal " confidence of a local fault detected"

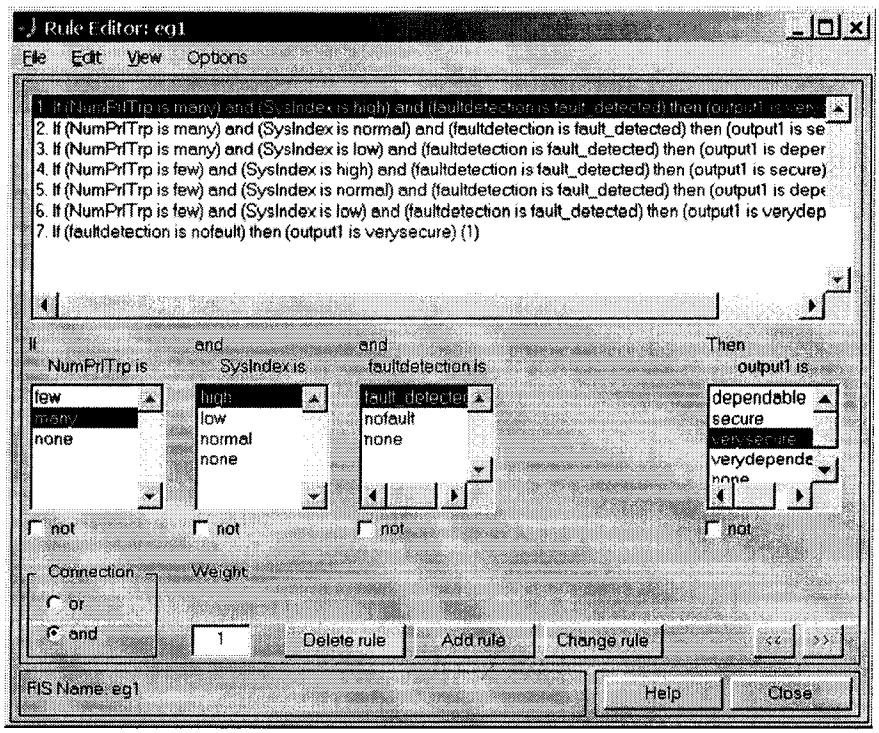

Figure 5.19 FIS rules

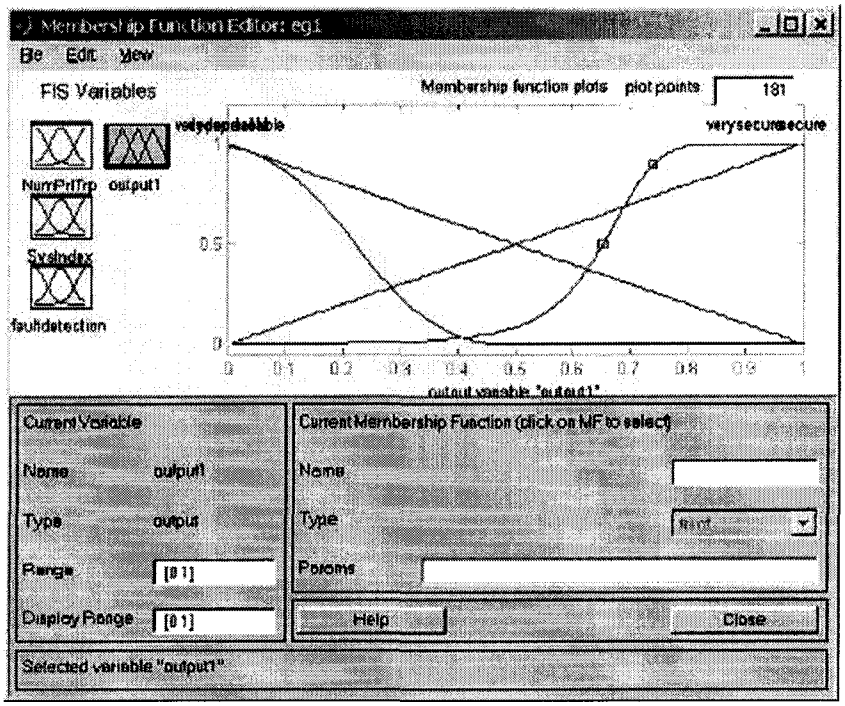

Figure 5.20 Membership functions of the output signal " bias of tripping decisions"

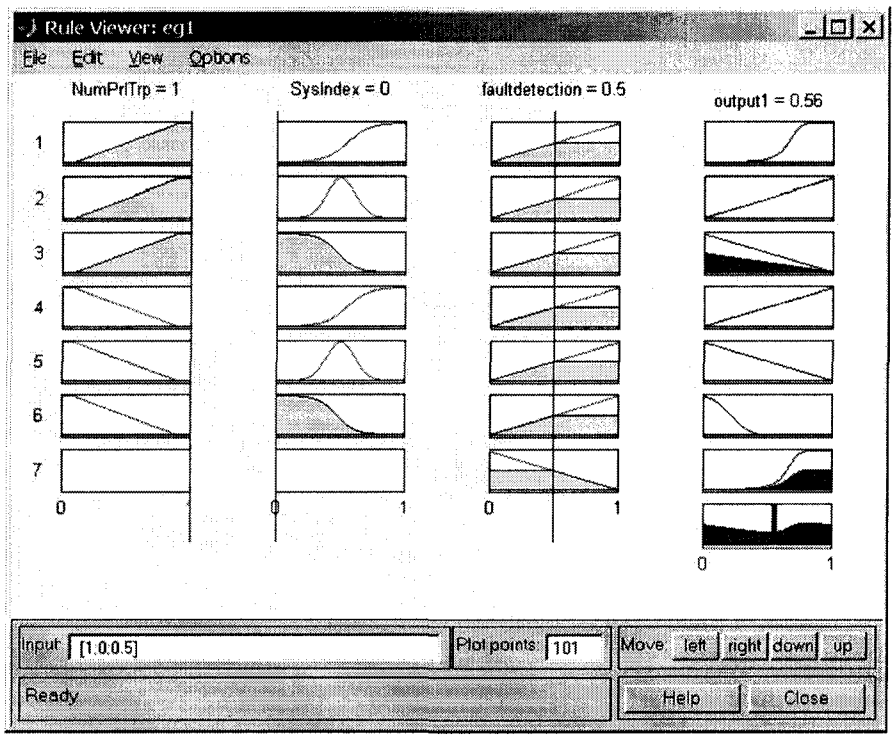

Figure 5.21 Inference procedure snapshot

The inference procedure snapshot in Fig. 5.21 shows the action of input signal fuzzification, aggregation and output defuzzification. While in Fig. 5.22 and 5.23 the variation of input and output are recorded over time. In Fig. 5.22, the uppermost yellow line reflects the condition of line1 and line2 by showing the percentage of parallel facility tripped, which is critical topology information to the decision of line3. More topology data, both local and remote ones, can be incorporated in similar input signals via appropriate communications. The middle cyan line represents the confidence level of fault detection of the relay. This is a variable with a value between 0 and 1 instead of a firm digital value 0 or 1 as in traditional relays because in real life many factors affect the assertion of the existence of a fault. Among these factors are fault type, fault location, relay condition etc. The purple slope represents the fluctuating system loading index. Comparing Fig. 5.22 to Fig. 5.23, it is clear to see the impact of all input signals on the decision of the adaptive relay. The relay does not trip at t = 42 cycles as the conventional relays would do because of relatively high system demand and high percentage of parallel facilities lost.

Other combinations of input signals can be simulated and finely tuned according to experts' experience and operation requirements. The idea of this design is to show that relays can tune the operation bias continuously based on the level of system stress and vulnerability. The logic shown above adjusts the protection system behavior during a disturbance to avoid an otherwise catastrophic failure.

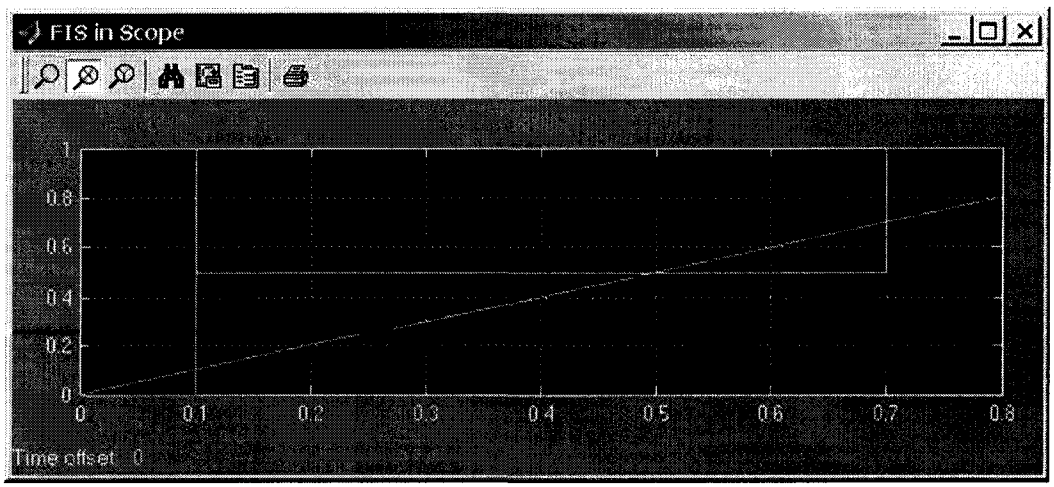

Figure 5.22 Input signals of the adaptive relay

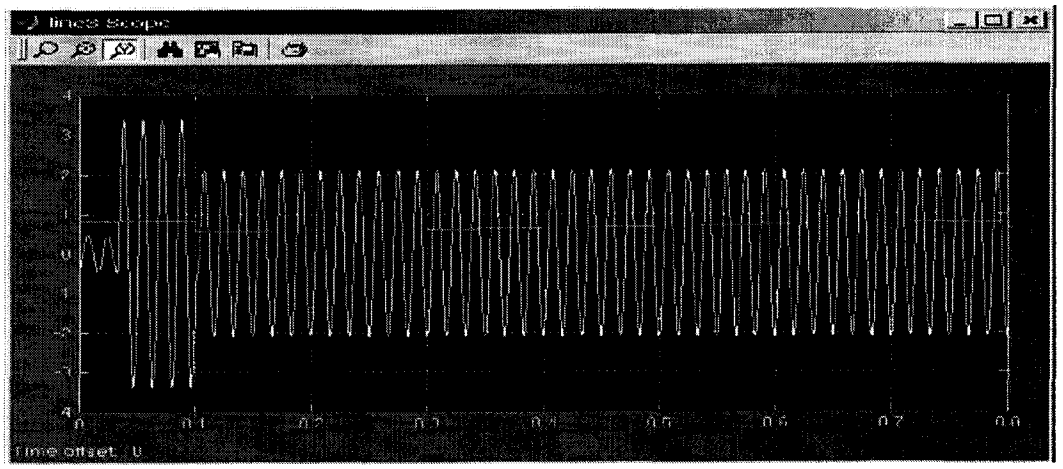

Figure 5.23 Current through line 3

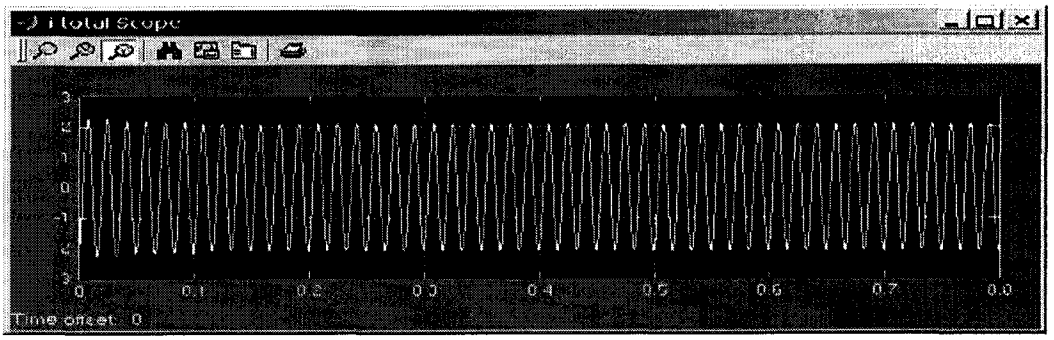

Figure 5.24 Load current not interrupted

5.4.2 Implementation of Example 5 in Section 5.3.2

A permanent fault between bus 83 and 86, as well as protective relay A through L are shown in Fig. 5.25 for this example. Normally circuit breakers A and B are supposed to clear both ends of the line within 4 cycles. When relay A has a defect such that breaker A at bus 83 fails to open that end of the line, the traditional system will resort to a remote backup-relaying scheme, resulting in disruption of the entire AC corridor and the system rapidly loosing synchronism.

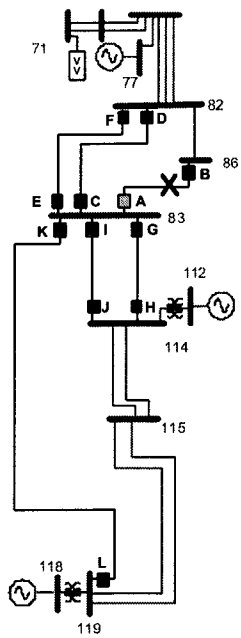

Figure 5.25 The test system with breaker identities shown

In this example it is assumed that all relays from A through L are adaptive ones instead of traditional distance relays. The simulation model built in Simulink is shown in Fig. 5.26. Seven buses (bus 82, 86, 83, 114, 115, 119, 118) and 11 transmission lines are modeled, as well as a source and a load. With FIS (Fig. 5.27) built into the adaptive relay, rules in Fig. 5.28 are executed. All input signals from local and remote relays are fuzzified by membership functions similar to the one that is shown in Fig. 5.29. The inference procedure is captured in Fig. 5.30 through 5.32.

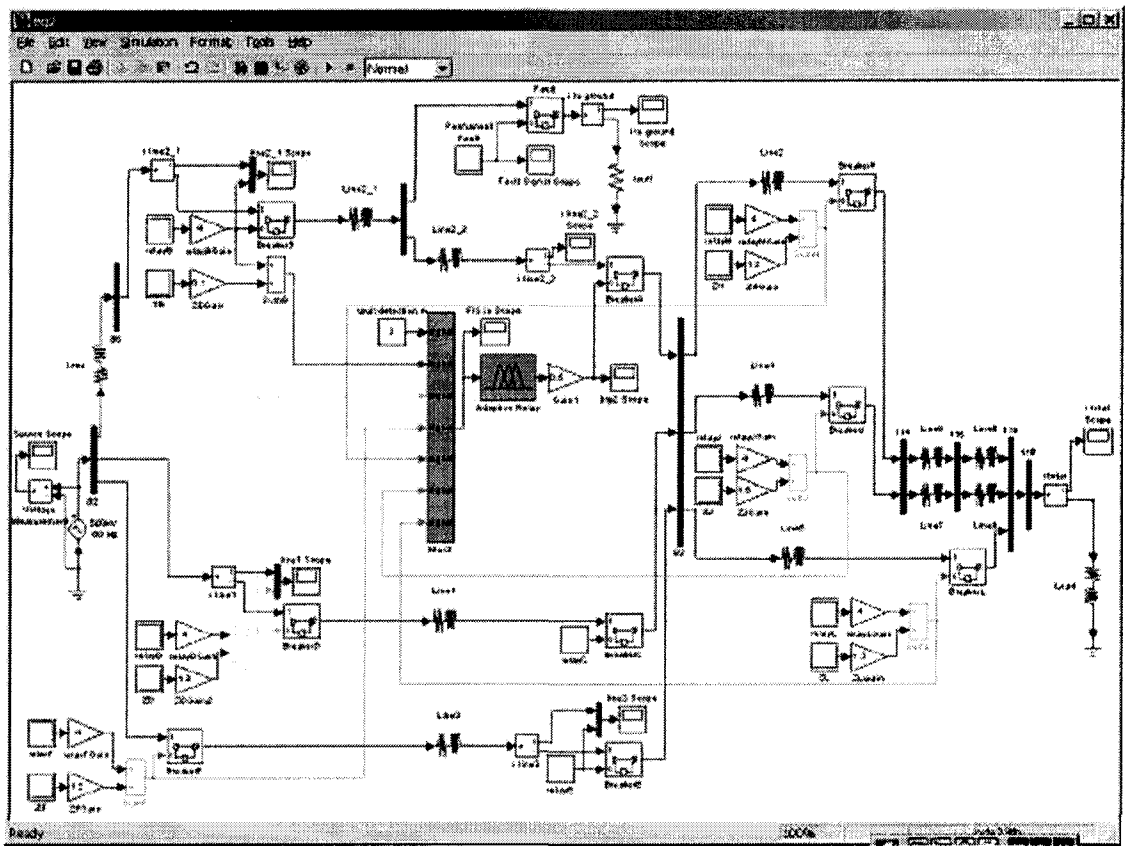

Figure 5.26 Simulink model of the test system

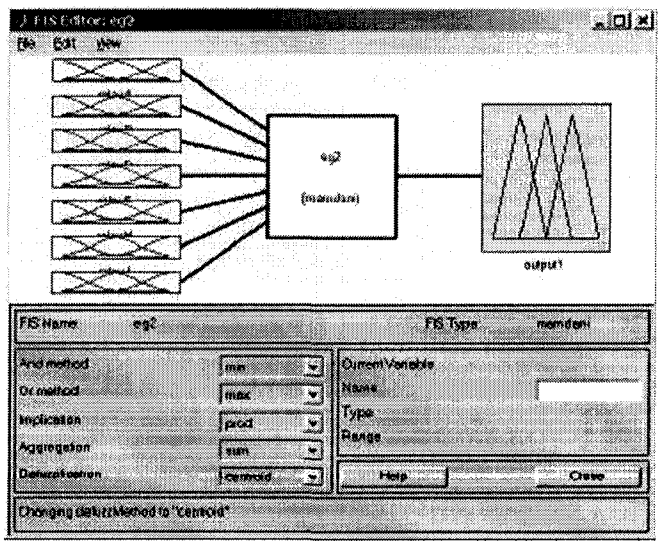

Figure 5.27 FIS properties

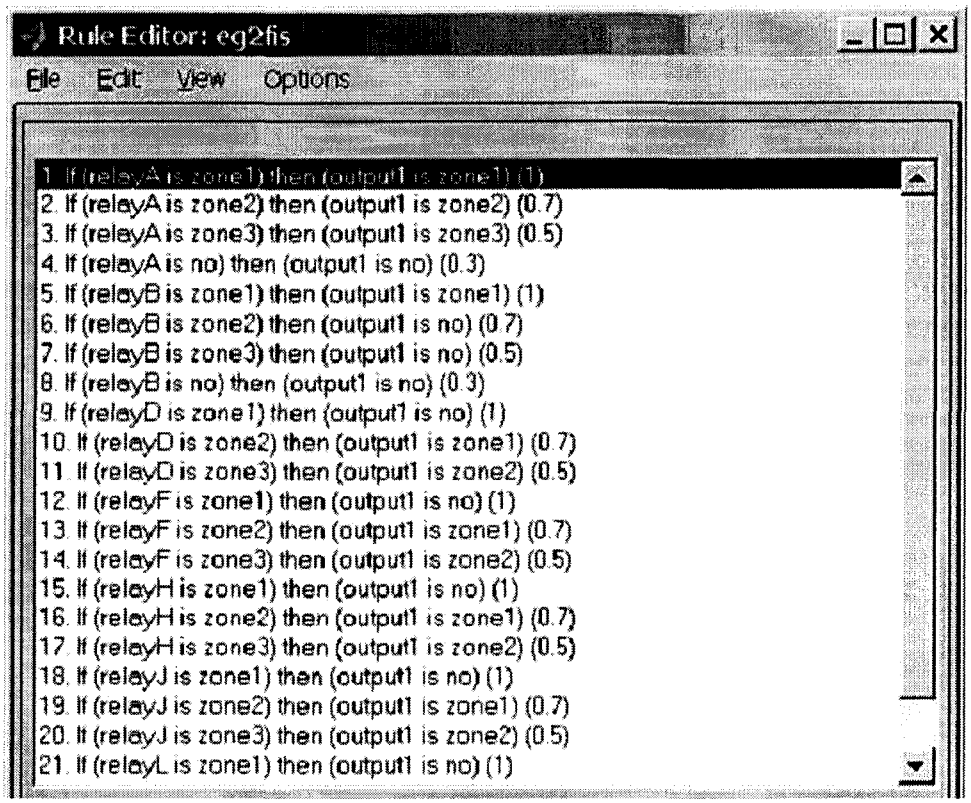

Figure 5.28 Rule view

The principle of adaptive relaying is to share information among peer relays as well as among system monitoring and control devices. Consequently the decision-making procedure of relay A is not merely a function of relay A, but of the system indices and its peer relays, both in the same substation and in neighboring stations, or even remotely if necessary. The rules shown in Fig. 5.28 are more complicated than a simple voting scheme. It is to incorporate multiple input signals with different weighting factors assigned. In real-time operation, the input signals from each relay are also functions of the fault detector measurement and the device condition of that relay. In the simulation, communication delays are considered random at the order of several cycles. This explains the dispersed arrival of input signals in Fig. 5.31.

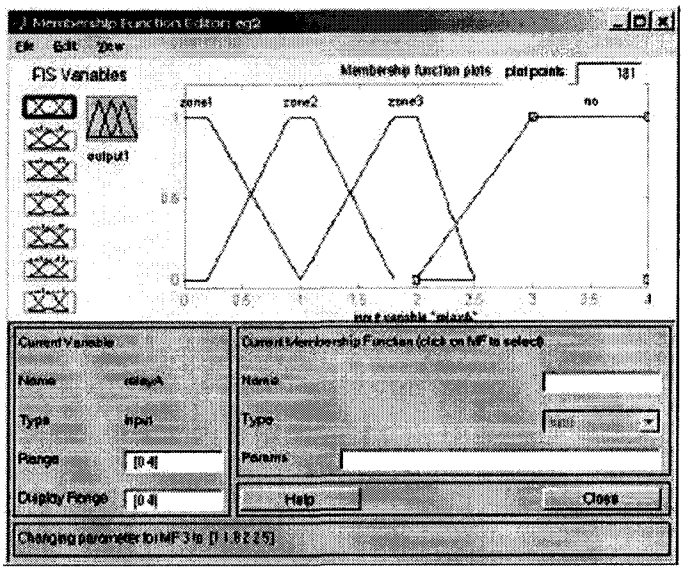

Figure 5.29 A typical membership function of a fuzzy distance relay

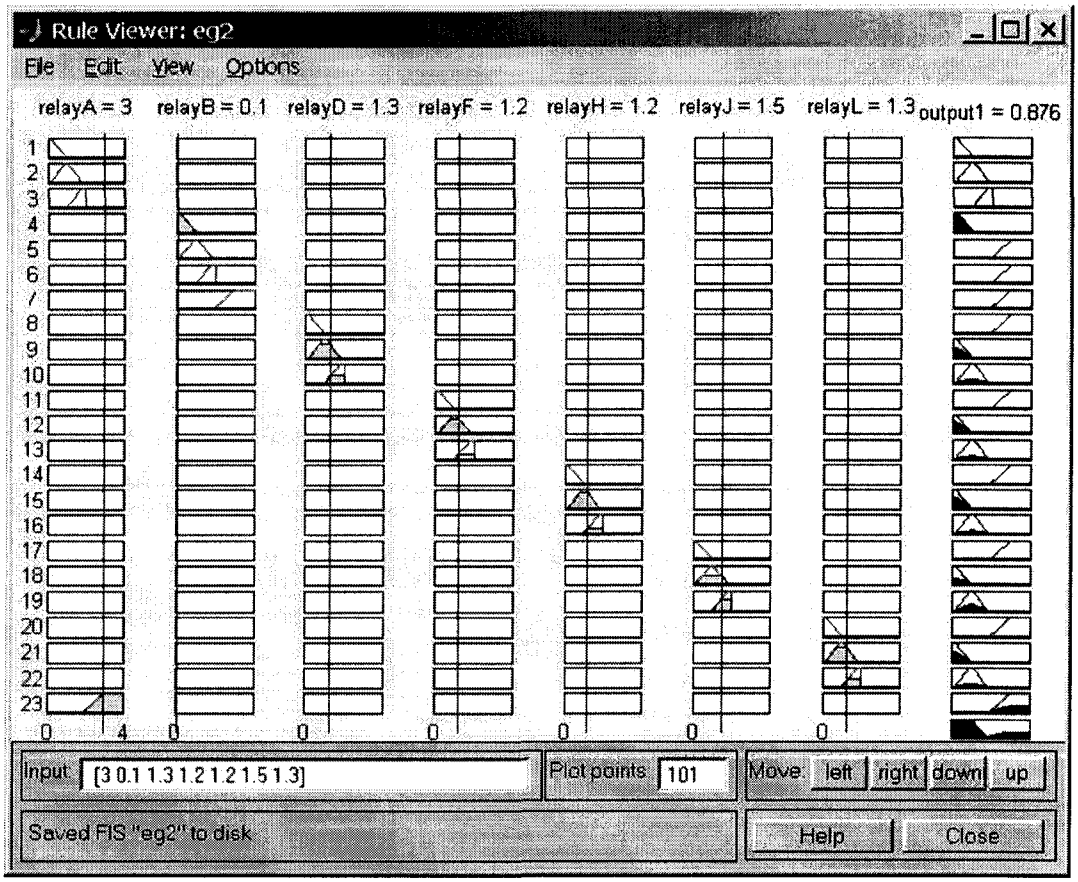

Figure 5.30 FIS inference procedure snapshot

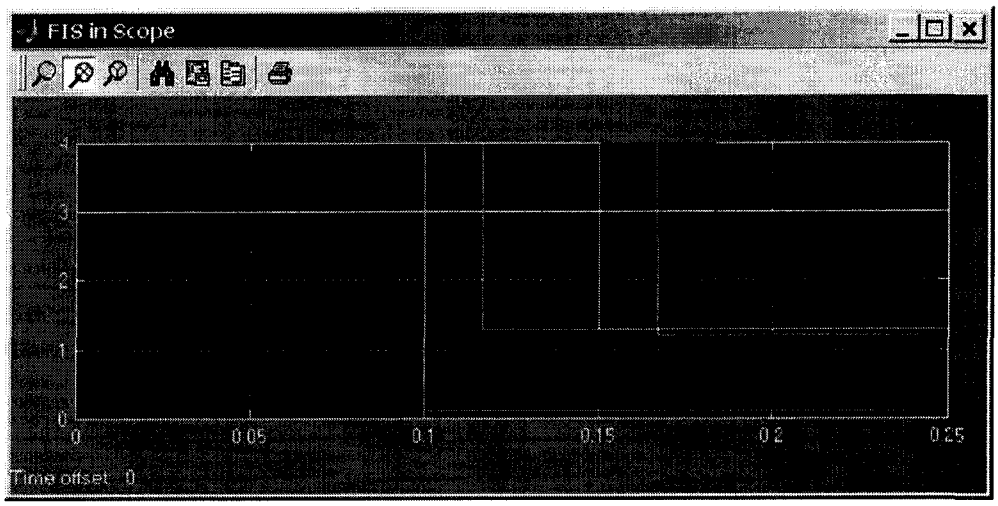

Figure 5.31 Input of FIS

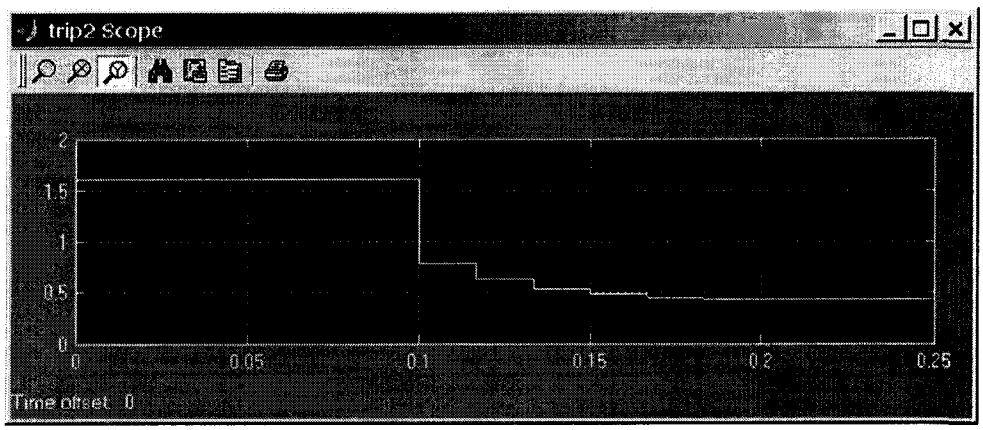

Figure 5.32 Output of FIS

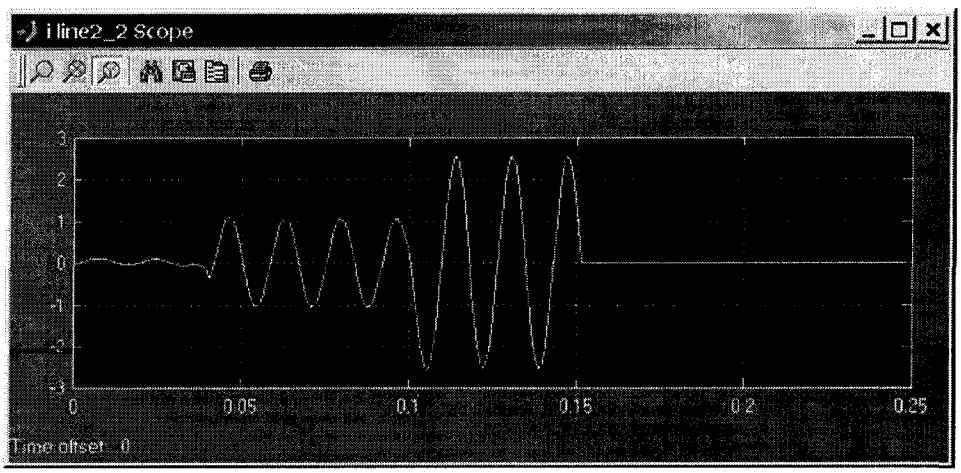

Figure 5.33 Current through breaker A

The simulation results display that with more and more information arriving to contribute to the decision of relay A (in Fig. 5.31), the confidence level of breaker A to stay closed becomes less and less (in Fig. 5.32). Upon assessing the status of the entire system, the adaptive relay A would reach the conclusion that the fault is within its protection zone while the fault detector at A is malfunctioning. Fig. 5.33 displays the result that breaker A is forced to open after the FIS output is less than a certain threshold. With appropriate logic implemented in modern computation and communication technology, this intelligent decision process takes less time than a normal backup relay. Therefore the backup functions at other lines would not operate so the other lines remain undisrupted.

In this section two examples of adaptive relay algorithm implementation are simulated in MATLAB and Simulink. They are simply to illustrate the proposed idea and validate the dynamic simulation of previous six examples. More realistic simulation would be needed if the prototype of an adaptive relay is being built.

CHAPTER 6. ADAPTIVE PROTECTION FOR MITIGATING VOLTAGE COLLAPSE

It was wide area disturbances leading to system collapse, in particular voltage collapse, that have drawn significant attention to the possibility of a revolution in protection philosophy. In this chapter the historical disturbance data are firstly reviewed to find the interrelationship between protective systems and the voltage collapse incidents. Adaptive wide area protection scheme proposed in previous chapters is then applied to mitigate system voltage collapse. The protection design is briefly described and demonstrated through an application to the WECC 179-bus equivalent system. The system simulations with and without the proposed adaptive protection scheme are presented on a comparative basis. The results exhibit the effectiveness of adaptive wide area protection in preventing the system voltage collapse. The results are summarized and discussed at the end of the chapter.

6.1 Analysis of Historical Data

The security of a bulk power system is threatened when it is loaded to its maximum capacity. Voltage instability and incorrect protective relay operations are two major interrelated phenomena that occur when the system is under stress, as illustrated in Fig.5.1. As reported in many voltage collapse incidents (NERC, 2003), slow clearing of a fault may lead to excessive drop of the system voltage to a threshold value from which the system cannot recover itself. Low bus voltages during high loading conditions tend to trip protective relays to further aggravate the situation. Similar phenomenon can be observed with generators. The lack of reactive power during heavy loading conditions may trigger field limiters and overload protection to trip the generators. This undoubtedly contributes to the system collapse.

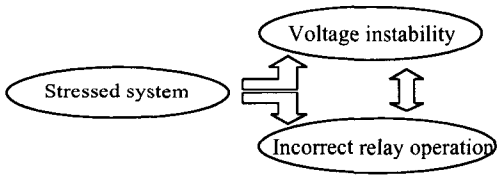

Figure 6.1 Demonstration of the aggravation loop

Two aspects of the interrelationship between voltage stability and protection are observed by studying historical voltage collapse incidents (Begovic, et al., 1993; Begovic, et al., 2001; Alsberg, 1996):

- Protection systems are mostly responsible in triggering voltage collapse. Table 5.1 summarizes the initializing events in some severe voltage instability incidents. It shows how relay unnecessary operations lead to cascade voltage disturbances in a given system.
- The occurrence of voltage instability poses additional challenges to protection systems. This is quite often for relays depending on measuring bus voltage. For example, the apparent impedance seen by low voltage buses with high load currents may fall into the protected zone of impedance relays and they may trip unnecessarily. This in turn may create unnecessary loss of system security

Table 6.1 Examples of initializing events in voltage-related incidents

1982	Belgium collapse started from six generators tripped by field limiter and overload protection (Begovic, et al., 1993).
1983	Swedish network failure was initiated by a 220kV line overload protection operation (Begovic, et al., 1993).
1987	Tennessee voltage collapse was caused by the slow clearing of a fault and the result of a voltage value low enough for cascading relay operations and stalled motors (Begovic, et al., 1993).
1989	Hydro Quebec disturbance was attributed to undesirable tripping of all SVCs on the HV network (Begovic, et al., 1993).
07/1996	WSCC voltage collapse began with parallel transmission line sympathy tripping (Alsberg, 1996).
08/ 1996	WSCC voltage collapse involved a faulty relay, exciters overload and overloading of a tie (Begovic, et al., 2001).

In order to have a quantitative understanding of the interrelationship between voltage stability and protection, historical data from NERC (2003) are summarized in Table 5.2. The goal is to identify the role of protection in voltage collapse and to examine the incorrect relay operations due to voltage collapses. All voltage-related disturbances are classified into the following two types according to their consequence and the time scale of evolution:

- *Emergency event,* which causes load shedding and customer interruption without advance warning, including "Interruption" and "Unusual Occurrence" defined by

NERC (2003). From the protection point of view, emergency events have more value for further study.

- *Foreseeable event,* which is more acceptable for customers, because either they receive adequate warning of the incident so they can respond appropriately, or customers reduce their respective load voluntarily. This type of event includes "Voltage Reduction", "Load Reduction/Demand Reduction", and "Public Appeal" again as defined by NERC. This category has little to do with protection therefore is ignored in later analysis.

Table 6.2 Voltage related disturbances and protection

Emergency event	Correct operation	9/30	30%	30/42	42/213
	False tripping	12/30	40%		
	Failure to trip	7/30	23%		
	Not protection-related	2/30	7%		
	(Voltage causing unnecessary operation)	(7/30)	(23%)		
Foreseeable event	Correct operation	2/12	17%	12/42	
	False tripping	0			
	Failure to trip	0			
	Not protection-related	10/12	83%		

As shown in Table 5.2, there were 42 voltage-related events among 213 NERC DAWG disturbances recorded from 1991 to 2000. From the protection point of view, the causes of these events are listed as "correct operation", "false tripping", "failure to trip" and "not protection-related". The study of these categories is to identify the role of protection in voltage disturbances.

On the other hand, the phenomenon of an abnormal system voltage triggering relay unnecessary operation is included in the category of "voltage causing unnecessary operation". The study of this category is to expose the second aspect of the relationship between voltage stability and protection as described in the beginning of this section.

Now examining the statistics given in Table 5.2, an obvious interrelationship between severe voltage disturbances and protection can be discerned by the high percentage of the following incidents:

- Incorrect relay operations contributing to emergency voltage-related large disturbances (63%)[10].
- Emergency voltage problems causing incorrect relay operations (23%).

Therefore the concept of adaptive wide area protection, which is an effective way of eliminating unnecessary operations under stressed conditions, is proposed as a solution to mitigate voltage collapse incidents.

6.2 Case Study

With the intelligence and adaptiveness, relay schemes proposed in Chapter 3 would be able to apply possible protection countermeasures to mitigate wide area problems, in particular voltage collapse. In general, these actions include temporary generator overloading, more secure transmission protection and reactive support.

In this section, the tuning of adaptive relays using real-time signals to yield secure system protection for a voltage collapse study is discussed. The purpose of maintaining transfer power and system stability is achieved by avoiding unnecessary relay operations.

A voltage collapse incident with and without the proposed adaptive protection is simulated on a large test system. The steady state PV curves that are obtained from the simulation mimic the operating condition change during contingencies.

6.2.1 Test System

The system selected for this study is the same WECC 179-bus equivalent system used in Chapter 4. The one-line diagram is shown again in Fig. 5.2, with four 500 kV buses circled: bus 2, bus 32, bus 37 and bus 73. The study is focused on these buses that are considered to represent the wide area system behavior. The reasons of choosing these four buses are:

- The voltage level of these four buses (500kV) reflect the bulk system voltage profile more accurately;
-

[10] This is the summation of " false tripping" (40%) and " failure to trip" (23%) of protection system.

- These four buses are scattered geographically so the entire interconnected system profile is well represented;
- The voltage at these four buses is more sensitive to the system load increase and thus ideally suited for this study. Fig.5.3 shows voltage change ratio for each bus under a load increase from the base case to the collapsing critical point.

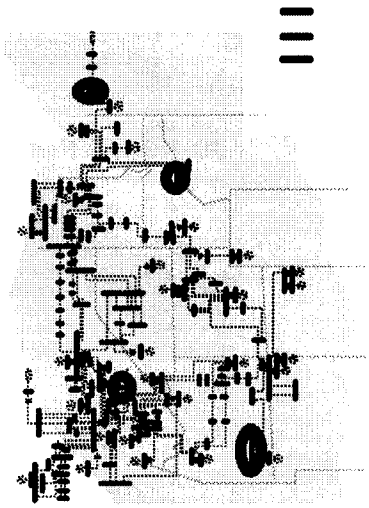

Figure 6.2 One-line diagram of WECC 179-bus equivalent system, with 4 buses circled.

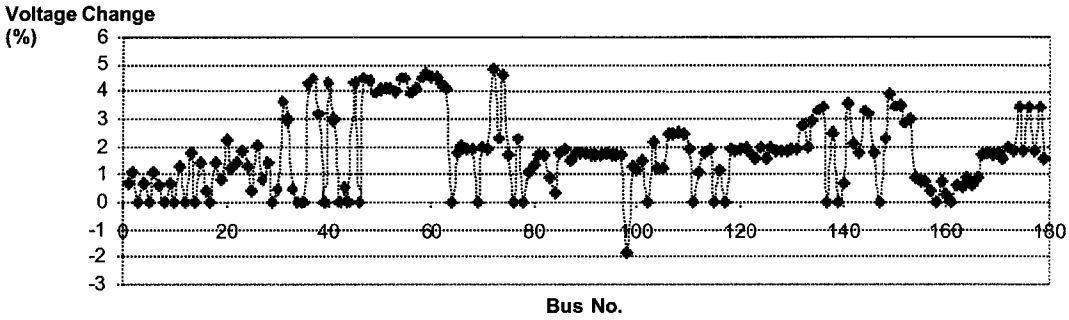

Figure 6.3 Percentage of voltage change for all buses from base case to critical point

To simplify the case, it is assumed that 450 Mvar SVCs are installed at the load center of bus 2. In real world this can be an aggregation set of distributed SVCs installed on a number of buses in the vicinity. Under normal operating conditions, 436.4 Mvar of SVCs are switched in at the load level of 60,785.4 MW to provide proper voltage support. In the following subsections the performance of the relays at bus 2 for SVC protection is examined to study the effect of protection on voltage stability.

6.2.2 Simulated Incident

The disturbance caused by geomagnetic storms during sunspot cycles is considered as a relay common mode failure in this study. Billinton and Allan (1992, p.353) gave the definition of a common mode failure as "an event having a single external cause with multiple failure effects which are not consequences of each other." A typical example would be one wide area disturbance, like a geomagnetic storm, causing more than one failures in protection systems. This situation is similar to the well-known March 13, 1989 outage that actually occurred in Hydro Quebec, in which hundreds of mis-operations of relays intended for SVC protection resulted in loss of power for the entire province (Kappenman & Albertson, 1990). It took only one-and-a-half minutes from the initial event to complete blackout (Kappenman, Zanetti, & Radasky, 1997). Such a short time frame of wide area disturbance has prohibited possible human operator intervention and forces the researchers to seek for improvements in protective relays (Chano et al., 1995).

As a result of perturbations in the earth's magnetic field during geomagnetic storms, induced voltage gradients occur along the earth surface. The resulting earth-surface potentials (ESPs) are in turn impressed between any two neutral points of grounded wye-connected transformers at both ends of a line. The quasi dc geomagnetically induced currents (GICs) produced by the ESP drives into half-cycle saturation of the transformer core. The asymmetrical saturation creates harmonic distortion which could trip many protective relays unnecessarily.

Therefore it is essential to take precautions to prevent or mitigate the effects of GICs on large interconnected power systems. However, the disturbance to the relays studied in this chapter is not restricted to GICs. In this study the incident is generalized as a common mode failure of relays leading to undesirable tripping of SVCs. Other triggering factors of similar common mode failures could be widespread harmonic distortion due to other reasons.

6.2.3 Base Case: No Disturbance

The PV curves of the test system are generated under the following assumptions:

- All loads increase at the same percentage level at each bus at the original power factor;

- Similarly, the system load increase is picked up by all generators at equal percentage level;
- The change in the system loss is picked by the slack bus.

The Continuous Power Flow (CPF) program developed at Iowa State University (Ajjarapu & Christy, 1992) is utilized to generate the PV curves required for the study. The system load margin is found to be 65,410.83 MW. This case reflects the pre-contingency condition of the system. It serves as the base case for the study. The results for this case are shown in Fig.5.8 to 5.11 (labeled as "base case") on a comparative basis for other two cases to follow.

6.2.4 Case 2: with Disturbance, Using Conventional Protection Scheme

Conventional SVC protection is provided by thermal overload relays, overcurrent relays, overvoltage relays, unbalance relays etc., generally referred to as SVC relays in this document. These relays are susceptible to false tripping due to the high harmonic levels (Chano et al., 1995). Improvements have been suggested to protect SVCs under these abnormal conditions (Bozoki, et al., 1996). However, most of the current relay schemes are designed to have an operation bias towards dependability. Each relay operates based on its own fault detection and any of the redundant relays can trip the protected SVC. Therefore with a common mode failure of all SVC relays, many SVCs would be disconnected unnecessarily, as shown in Fig. 5.4.

Due to the nature of the widespread disturbance, it is reasonable to assume that all SVC relays within the affected area initiate unnecessary tripping signals. Similar to the base case, the PV curves for the loss of SVCs are generated for this case using the CPF program. It is assumed that transient stability is maintained during the contingency. The simulation results show a much lower load margin of 60,964.99 MW compared to the base case. The PV curves of the four buses are shown in Fig. 5.8 through Fig. 5.11, labeled as "case 2".

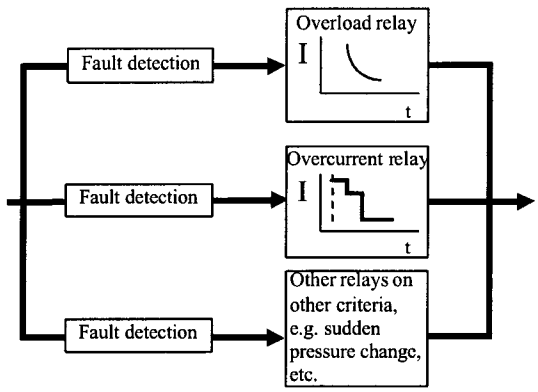

Figure 6.4 Logic diagram for existing SVC protection.

The dashed arrow in Fig. 5.8 shows the phenomenon of a voltage collapse. It indicates that there is no viable equilibrium point on the case 2 curve if the pre-contingency (base case) load level is between 60,964.99 MW and 65,410.83 MW. Thus conventional relay mis-operations contribute to voltage collapse. This is perhaps similar to what happened in Hydro Quebec in 1989 as identified in Table 5.1.

6.2.5 Case 3: with Disturbance, Using Adaptive Wide Area Protection Scheme

The effectiveness of the adaptive wide area protection to prevent voltage collapse is demonstrated here. The proposed protection scheme increases the load margin by adaptively and intelligently tuning the relays to a more secure status under highly stressed conditions.

The possible implementation of the adaptive protection can be made either distributed at several substations, or centralized at the energy control center.

The centralized decision-making architecture may adopt a hierarchical relay network. A large amount of relays at lower level have less authority for decision making thus need less intelligence. The high-level logic decision device in a control center has relay signals/breaker status of all circuits. It also monitors the system stress through various real-time/quasi real-time vulnerability indices. This well-informed high level controller coordinates tripping decisions among all SVC relays. Consequently the analysis within the high level relay enables it to trip the most likely faulted SVC first, updating measurements, and then to trip the next most likely faulted one if fault detection sustains. Such a central control device is more likely to find out there is no real SVC fault and what the relays see are just harmonics. Thus fewer SVCs will be disconnected.

In this study, only the distributed approach at the substation level is implemented. That is, the operation decisions are made within each relay, rather than coordinated by a central controller. Each adaptive SVC relay is connected to a peer-to-peer network. Fault detection is realized in each relay the same way as it is in existing SVC relays. The result of processed detection is sent to the network for information sharing. Subsequently each relay gathers real-time input signals and all signals contribute to the final decision of a relay.

The procedure is simulated using the MATLAB Power System Blockset and Fuzzy Logic Toolbox. In this study the author chose to apply a fuzzy inference mechanism for implementing the decision-making logic. However, other implementation schemes such as multiagent systems can also be explored.

The decision-making module in each relay is represented as a Fuzzy Inference System (FIS) as shown in Fig.5.5. It incorporates various input signals, including conventional relay fault detection results, signals from its peer relays installed over a wide connected area, and the Voltage Stability Index (VSI) into the decision-making procedure. The VSI, calculated on-line, shows the distance of the system to the critical point. The VSI is available from CPF as the ratio of $\left(-\frac{dP_T}{dV_j}\right)$, where P_T is the total system real power load and V_j is the voltage of the weakest bus (Ajjarapu & Christy, 1992).

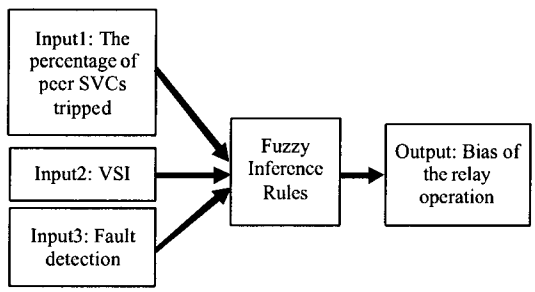

Figure 6.5 Fuzzy Inference System diagram for an adaptive relay.

Fig. 5.6 shows the membership functions of one of the adaptive relay input signals — the percentage of its peer SVCs disconnected. If this input signal is "bw", suggesting more SVCs are connected and working, this specific relay can afford to operate in a more dependable manner. However, when this input is "high", which means there are many SVCs over the wide area being tripped, the var support is insufficient. At this time stretching the

limit of this particular SVC to some extent might be a remedy for system integrity, while tripping one more SVC may severely threaten the system voltage stability. Thus the operation bias of this adaptive relay is tuned to security. This protection philosophy is beneficial in combating the situation of common mode relay failures. Similar membership functions of other input/output signals can be defined.

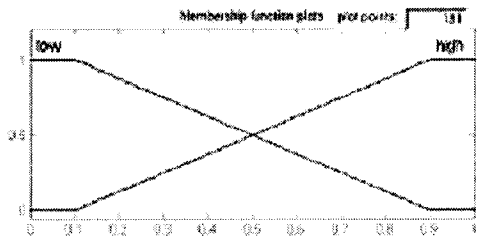

Figure 6.6 Membership functions of input1: the percentage of peer SVCs disconnected.

In each adaptive relay, all input signals are processed by membership functions. Then a series of weighted "if then" rules are applied for the inference procedure. The aggregated result is defuzzified to yield proper operating decisions. Thus the fuzzy inference mechanism can be able to make intelligent decisions within the order of milliseconds (Kezunovic, et al., 1999). The snapshot of the procedure is captured in Fig. 5.7.

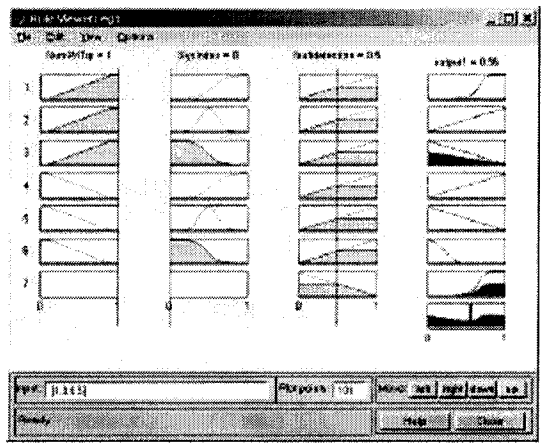

Figure 6.7 Inference procedure snapshot.

In the simulation all adaptive relays make the decision of not tripping. It is because of the high percentage of peer relays detecting the same fault, and the stress of the entire system. In real world, data error due to communication delays or noisy measurements may cause some relays to trip. But at least fewer SVCs will be disconnected than in the conventional standalone setting.

It is reasonable and even conservative to assume that only some of the SVCs are tripped, e.g. 256 Mvar at the starting load level of 60,785.4 MW. That is 180.4 Mvar remained in the system. With this var support, the load margin is restored to 65,396.36 MW. Compared with the base case load margin at 65,410.83 MW, the system is not severely deteriorated by partially tripping the SVCs with adaptive relays. The PV curves for this case are also shown in Fig. 5.8 through Fig. 5.11, labeled as "case 3". The solid arrow in Fig. 5.8 shows that the system settles down to a stable operating point after the disturbance. As long as the pre-contingency load level is less than 65,396.36 MW, the grid will be able to find a post-contingency stable operating point. That is, the system stays stable, assuming about one half of the relays in the adaptive SVC protection scheme operate as desired.

The purpose of this chapter is to demonstrate the application of adaptive relays in combating voltage collapse. Therefore the relay design details are not elaborated. The details of the adaptive protection architecture, algorithms, intelligent inference procedure, and communication requirements are covered in previous chapters.

6.2.6 Summary

Table 5.3 summaries the simulation results of the three cases for bus 2. It is shown that at the same load level, reactive power support is different for the cases due to different size of SVCs connected. From this table it is clear that adopting the adaptive relay concept could have saved the system integrity and thus possibly avoids events similar to the 1989 Hydro Quebec disturbance.

Table 6.3 The load center of bus 2 and system characteristic at different cases

	P at bus 2 (MW)	Q at bus 2 (Mvar)	Power factor at bus 2	Load margin (MW)
Base case	1,750.0	-56.0	0.999488 leading	65410.83
Case 2	1,750.0	380.4	0.97718 lagging	60,964.99
Case 3	1,750.0	200.0	0.993533 lagging	65,396.36

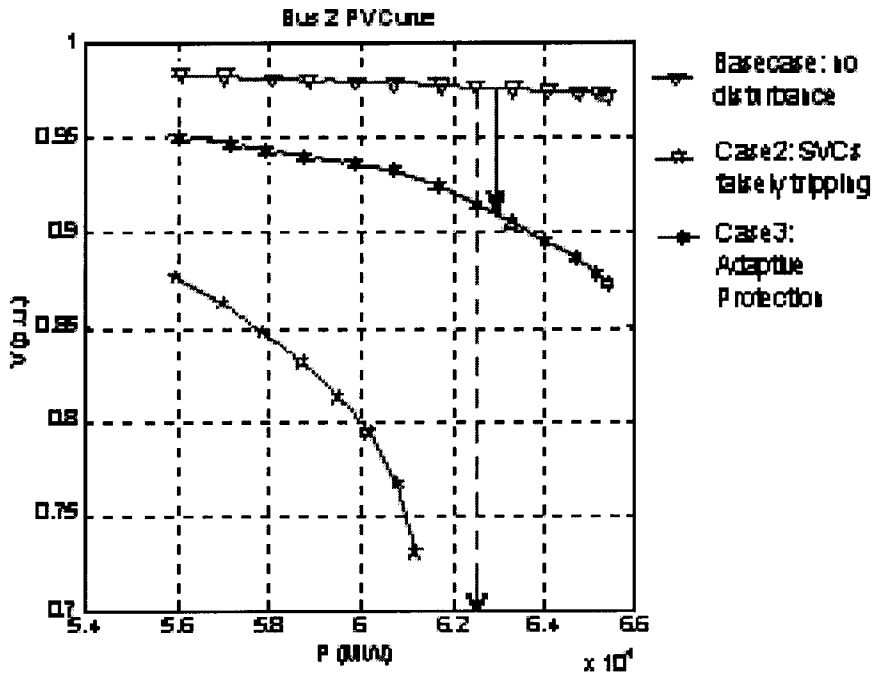

Figure 6.8 Bus 2 PV curves for three cases.

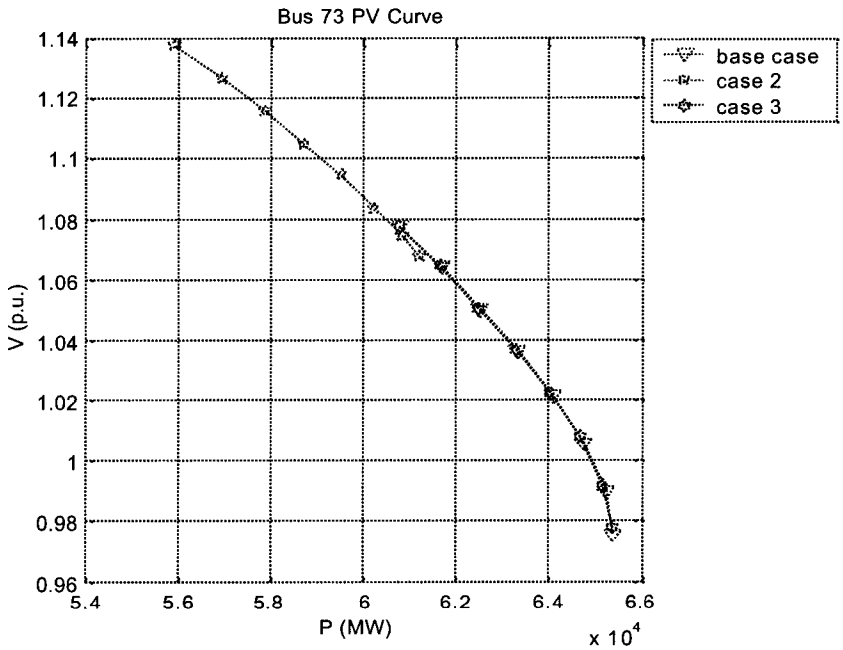

Figure 6.9 PV curves at bus 73 of three cases.

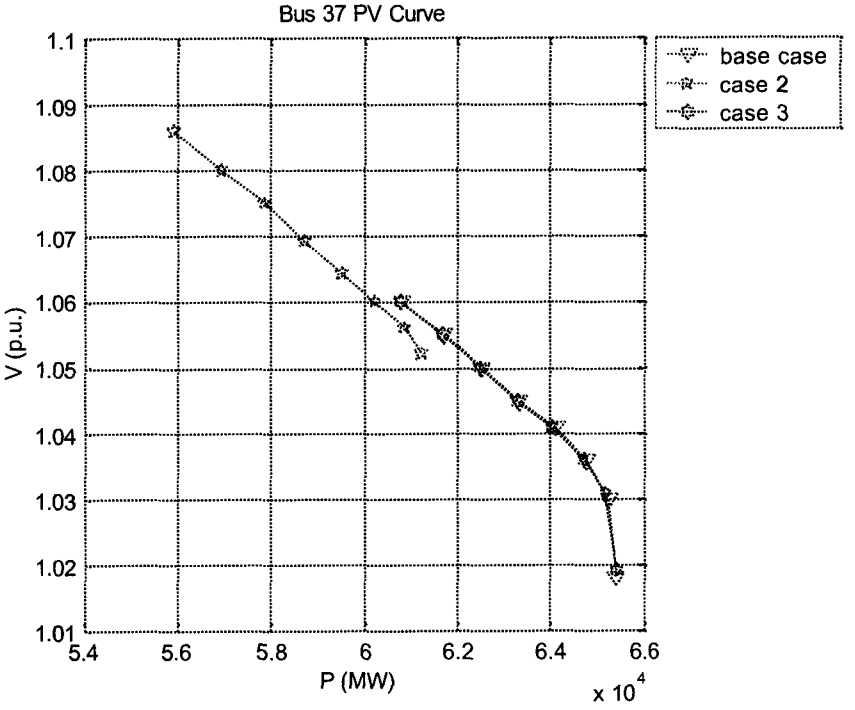

Figure 6.10 PV curves at bus 37 of three cases.

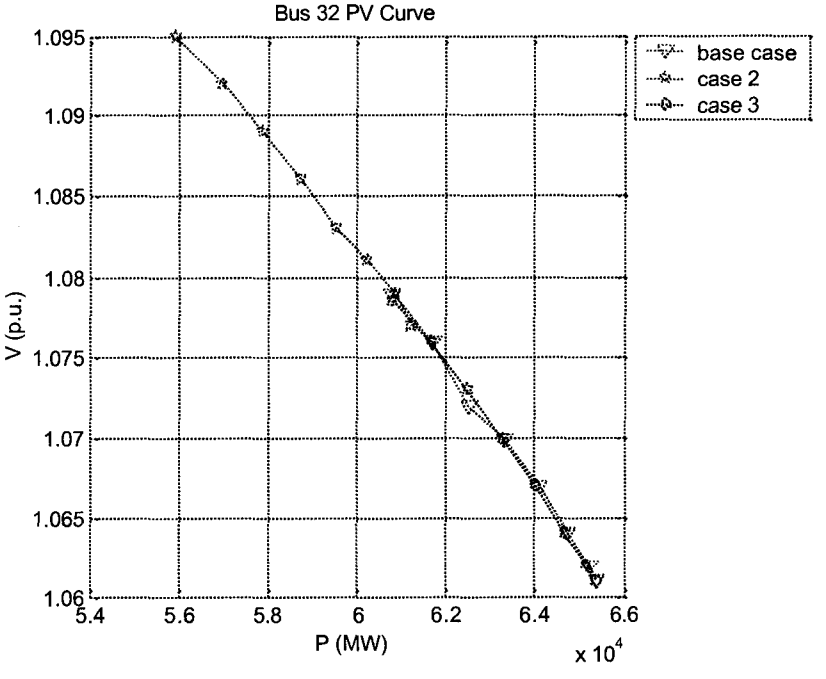

Figure 6.11 PV curves at bus 32 of three cases.

6.3 Conclusions and Future Work

The objective of this chapter is to demonstrate that the proposed adaptive protection can tune the bias continuously based on the level of system stress and vulnerability, as well as response from other peer relays. The logic described in chapter 3 adjusts the protection system behavior during a disturbance to avoid an otherwise catastrophic failure.

The example study described in this chapter is intended to demonstrate the effectiveness of the adaptive protection concept. Further work is needed in studying more complex voltage disturbance cases by using dynamic response curves rather than static curves as used in this study. Further, the proposed relay models should conform to the dynamic system performance.

CHAPTER 7. CONTRIBUTIONS

Through post-mortem studies of catastrophic failures it is realized that improvement of protection philosophy is needed for wide area system protection. It is because current protection schemes may contribute to major blackouts due to the tendency of component protection sacrificing security for dependability.

Adaptive protection based upon the latest technologies can combat emergencies involving faults that could otherwise lead to wide area disturbances. The concept is far from being well-accepted for the industry but it is consistent with the directions of technology development now underway.

This research work identifies the importance of improvements in the system architecture for adaptive wide area protection development. Based on rapid-developing technologies, an open architecture, intelligent algorithms and communications for adaptive wide area protection are proposed. It is shown that adaptive protection is able to fulfill requirements of both dependability and security. The proposed protection system, which performs timely adaptive actions based on system-wide considerations, is intended to empower future power grids to withstand wide area catastrophes. The examples cited are intended to illustrate the concept. Further work is needed to nurture the concept before it can be implemented in the industry. It remains to determine additional situations where rapid emergency response of the protection system is effective and to determine what controls are useful in such cases. It also remains to study applications and to evaluate this concept in a specific, operational system.

7.1 Major Contributions

The main contributions of this research work are as follows:

- Proposing a new concept on adaptive wide area protection for power systems
- Designing the over-all architecture of adaptive wide area protection system
- Demonstrating and validating the proposed adaptive wide area protection system architecture

- Developing practical intelligent algorithms for the proposed adaptive wide area protection
- Demonstrating and validating the proposed intelligent adaptive protection algorithms
- Providing design criteria for intelligent communications that are suitable for adaptive wide area protection system
- Promoting the adoption and modification of UCA ^{TM}
- Proposing the adoption of adaptive autoreclosure, in particular, single-phase tripping and reclosure in the practice of adaptive wide area protection

7.2 Publications

- J. Huang, S. S. Venkata, V. Ajjarapu, Z. Zhou, "Developing adaptive protection to mitigate voltage collapse," Proceedings of NAPS, 2003.
- J. Huang, S. S. Venkata, "Wide-area adaptive protection: architecture, algorithms and communications," Proceedings of CRIS Conference on Power Systems and Communications Infrastructures for the Future, Beijing, 2002.
- M. Kim, M.J. Damborg, J. Huang, S.S. Venkata, "Wide-Area adaptive protection using distributed control and high-speed communications," Presented in 2002 PSCC, Seville, Spain, Jun. 24-26, 2002.
- M.J. Damborg, S.S. Venkata, J. Huang, M. Kim, "Examples of adaptive transmission system protection using rapid communication and control," 2001 International Middle-East Power Systems Conference (MEPCON), 29 – 31 Dec. 2001, Cairo Egypt, 2001.
- M.J. Damborg, M. Kim, J. Huang, S.S. Venkata, A. G. Phadke, "Adaptive protection as preventive and emergency control," *Proceedings of IEEE Power Engineering Society 2000 Summer Meeting*, vol. 2, pp. 1208 –1212, 2000.

REFERENCES

R. Aggarwal, A. Johns, "AI for protection systems," K. Warwick, A.O. Ekwue, and R. Aggarwal (Eds.), *Artificial Intelligence Techniques in Power Systems*. Institution of Electrical Engineers, London, pp.123-142, 1997.

V. Ajjarapu, C. Christy, "The continuation power flow: a tool for steady state voltage stability analysis," *IEEE Trans. Power Systems*, vol.7, pp. 416-423, Feb. 1992.

C. Alsberg, "WSCC unfolds causes of the July 2 disturbance," *IEEE Power Engineering Review*, vol.16, iss.9, pp.5, 1996.

P. M. Anderson, B.K. LeReverend, "Industry experience with special protection schemes," *IEEE Trans. Power Systems*, vol. 11, iss.3, pp.1166-1179, 1996.

P. M. Anderson, *Power System Protection*, New York: McGRAW-HILL, 1999.

M. Begovic, et al., *System Protection and Voltage Stability*, IEEE PSRC Report, 1993.

M. Begovic, et al., *Wide Area Protection and Emergency Control*, IEEE PSRC System Protection Subcommittee Working Group C-6 Report, 2001 (84 pages).

R. Billinton, R. N. Allan, *Reliability Evaluation of Engineering Systems: Concepts and Techniques*, 2nd ed., Plenum Press: New York and London, 1992.

J. L. Blackburn, *Protective Relaying: principles and applications*, 2nd ed., New York: M. Dekker, 1998.

B. Bozoki, et al., "The effects of GIC on protective relaying," *IEEE Trans. Power Delivery*, vol.11, iss.2, pp.725 –739, Apr. 1996.

S.R. Chano, et al., "Static var compensator protection," *IEEE Trans. Power Delivery*, vol.10, iss.3, pp. 1224 -1233, Jul. 1995.

CIGRÉ (1995), An international survey of the present status and the perspective of long-term dynamics in power systems, CIGRÉ Task Force 38-02-08 Final Report.

M. J. Damborg, M. Kim, J. Huang, S. S. Venkata, A. G. Phadke, "Adaptive protection as preventive and emergency control," *Proceedings of IEEE Power Engineering Society 2000 Summer Meeting*, vol. 2, pp. 1208 –1212, 2000.

P. Denys, C. Counan, L. Hossenlopp, and C. Holweck, "Measurement of voltage phase for the French future defense plan against losses of synchronism," *IEEE Trans. Power Delivery*, vol. 7, no. 1, Jan. 1992, pp. 62-69,1992.

M. B. Djuric, C.V. Terzija, "A new approach to the arcing faults detection for fast autoreclosure in transmission systems," *IEEE Transactions on Power Delivery*, vol. 10, pp. 1793 -1798, 1995.

D. Dubois, H. Prade, "Fuzzy sets and probability: misunderstandings, bridges and gaps," *Proc. of the Second IEEE Inter. Conf. on Fuzzy Systems*, vol. 2, pp. 1059-1068, 1993.

P. K. Dutta, P. B. Dutta Gupta, "Microprocessor-based UHS relaying for distance protection using advanced generation signal processing," *IEEE Trans. on Power Delivery*, vol. 7, no. 3, pp.1121-1128, 1992.

F. E. Elliott, B. E. Lavier, W. P. Kuehn, A. Kuechler, "FEM-Study on converter transformer failures in the Celilo HVDC converter station," *IEEE Power Engineering Society 1999 Winter Meeting*, vol. 2, pp.1047 –1052, 1999.

EPRI, 'Synchronized Phasor Measurements for the Western Systems Coordinating Council," *EPRI Final Report TR-107908*, 1997.

O. Faucon and L. Dousset, "Coordinated defense plan protects against transient instabilities," *IEEE Computer Applications in Power*, vol. 10, no. 3, pp. 22-26, 1997.

D.S. Fitton, I.P. Gardiner, "Advantages for power system operation using a neural network based adaptive single pole autoreclosure relay," *IEE Colloquium on Artificial Intelligence Applications in Power Systems*, pp. 4/1 -4/7, 1995.

D.S. Fitton, R.W. Dunn, R.K. Aggarwal, A.T. Johns, A. Bennett, "Design and implementation of an adaptive single pole autoreclosure technique for transmission lines using artificial neural networks,", *IEEE Trans. on Power Delivery*, vol. 11, no. 2, pp. 748 –756, 1996.

Y. Ge, F. Sui, Y. Xiao, "Prediction methods for preventing single-phase reclosing on permanent fault," *IEEE Trans. on Power Delivery*, vol. 4, no. 1, pp 114 -121, 1989.

S.H. Horowitz, A.G. Phadke, and J.S. Thorp, "Adaptive transmission system relaying," *IEEE Trans. on Power Delivery*, vol. 3, no. 4, pp. 1436-1458, 1988.

S. H. Horowitz, A. G. Phadke, *Power System Relaying*, England: Research Studies Press Ltd., 1992.

M.P. Houry and O. Faucon, "Defense plans: Economic solutions for improving the security of power systems," *Control Engineering Practice*, vol. 7, no. 5, 1999.

Q. Huang, Y. Li, B. Li, "A new adaptive autoreclosure scheme to distinguish transient faults from permanent faults," *Proc. of PowerCon 2002, International Conference on Power System Technology*, vol.2, pp. 671 –674, 2002.

IEEE, "Standard for calculating the current-temperature relationship of bare overhead conductors," IEEE Std 738-1993, 1993.

IEEE, "IEEE standard definition, specification, and analysis of systems used for supervisory control, data acquisition, and automatic control," Std C37.1-1994, 1994.

IEEE, "IEEE TR1550 Utility Communications Architecture," ver. 2.0, *technical report*, 1999.

IEEE PSRC, "Single phase tripping and auto reclosing of transmission lines-IEEE Committee Report," *IEEE Trans. on Power Delivery*, vol.7, no. 1, pp. 182 –192, 1992.

IEEE PSRC, "Feasibility of adaptive protection and control," *IEEE Trans. on Power Delivery*, vol. 8, no. 3, pp. 975-983, 1993.

IEEE PSRC, *WG H-6 report draft*, 2003.

A.K. Jampala, S.S. Venkata, and M.J. Damborg, "Adaptive transmission protection: concepts and computational issues," *IEEE Trans. on Power Delivery*, vol. 4, no. 1, pp. 177-185, 1989.

A.T. Johns, Y.H. Song, R.K. Aggarwal, "Study of turbine-generator torsional oscillations with particular reference to adaptive autoreclosure," *Proc. of TENCON '93, IEEE Region 10 Conference on Computer, Communication, Control and Power Engineering*, vol.5, pp. 133 - 136, 1993.

I. Kamwa, R. Grondin, D. Asber, J.P. Gingras, G. Trudel, "Large-scale active-load modulation for angle stability improvement," *IEEE Trans. Power Systems*, vol. 14, no. 2, 1999.

J. G. Kappenman, V. D. Albertson, "Bracing for the geomagnetic storms," *IEEE Spectrum*, vol. 27, no. 3, pp. 27-33, 1990.

J. G. Kappenman, L. J. Zanetti, W. A. Radasky, "Geomagnetic storms can threaten electric power grid," *Earth in Space*, American Geophysical Union, vol. 9, no. 7, pp.9-11, 1997.

D. Karlsson, et al., 'Special Protection Schemes in power systems: modeling and analysis," *CIGRÉ Technical Committee Task Force 38.02.19*, 2000.

M. Kezunovic, et al., "Intelligent systems in protection engineering," *IEEE PSRC WG G4 final report*, 1999.

G. Klir, "Probabilistic vs. possibilistic," *Conceptualization of Uncertainty, Analysis and Management of Uncertainty: theory and applications*, B.M. Ayyub, M. M. Gupta, L. N. Kanal. (editors), pp. 13-25, Elsevier, 1992.

B. Kosko, "Fuzziness vs. probability," *International Journal of General Systems*, vol. 17, no. 1, pp. 211-240, 1990.

W.R. Lachs, "Maximizing rotor thermal capacity," *Proc. of the 2001 IEEE Power Engineering Society Winter Meeting*, vol. 1, pp. 205 –208, 2001.

G. Li, J. Yates, R. Doverspike, and W. Dongmei, "Experiments in Fast Restoration using GMPLS in Optical / Electronic Mesh Network," *Optical Fiber Communication Conference and Exhibit*, pp. PD34_1 -PD34_3, 2001.

Y. Li, X. Dong, Z.Q. Bo, N.F. Chin, Y. Ge, "Adaptive reclosure using high frequency fault transients," *IEE Proc. of Seventh International Conference on Developments in Power System Protection*, pp. 375 –378, 2001.

C.Q. Liu, "A discussion of the WSCC 2 July 1996 outages," *IEEE Power Engineering Review*, vol. 18, no. 10, pp.60 -61, 1998.

J. McDonald, D. Cáceres, S. Borlase, M. Janssen, "Standardized design of transmission substation automation systems," *Congreso del Centro de Argentino de Ingenieros 1998*, Buenos Aires, Argentina, 1998.

NERC, 'Review of selected electric system disturbances in North America," *Disturbance Analysis Working Group*, Princeton, New Jersey 08540-5731, 1979-1995.

NERC, "Terms and Their Definitions as Used in the NERC Planning Standards," 2002. ftp://www.nerc.com/pub/sys/all_updl/pc/pss/DefandTerms_BOTapprvd02-20-02.pdf, last accessed 08/24/2003.

NERC, "DAWG Database," *NERC Disturbance Analysis Working Group*, 2003. http://www.nerc.com/~dawg/database.html, last accessed 06/03/2003.

E.K. Nielsen, M.E. Coultes, D.L. Gold, J.R. Taylor, P.J. Traynor, "An operations view of special protection systems," *IEEE Trans. on Power Systems*, vol. 3, no. 3 , pp. 1078 –1083, 1988.

A.G. Phadke, J.S. Thorp, *Computer Relaying for Power Systems*, Taunton, Somerset, England: Research Studies Press LTD, 1993.

A.G. Phadke, S.H. Horowitz, and J.S. Thorp, "Anatomy of power system blackouts and preventive strategies by rational supervision and control of protection systems," *ORNL Report*, ORNL/Sub/89-SD630C/1, Jan. 1995.

A. G. Phadke, S. H. Horowitz, and J. S. Thorp, "Aspects of power system protection in the post-restructuring era," *Proc. of the 32nd Hawaii International Conference on System Sciences*, Hawaii, 7 pages, 1999.

A. G. Phadke, "Hidden failures in protection systems," *Proc. of CRIS Conference on Power Systems and Communications Infrastructures for the Future*, Beijing, 2002.

Z.M. Radojevic, V.V. Terzija, N.B. Djuric, "Numerical algorithm for overhead lines arcing faults detection and distance and directional protection,", *IEEE Trans. on Power Delivery*, vol. 15, no. 1, pp. 31 –37, 2000.

R. Ramaswami, M.J. Damborg, and S.S. Venkata, "Coordination of directional overcurrent relays in transmission systems - a subsystem approach," *IEEE Trans. on Power Delivery*, vol. 5, no. 1, 1990.

Y. Ronen, *Uncertainty analysis* / editor, Yigal Ronen. Boca Raton, Florida: CRC Press, 1988

S.M. Rovnyak, C.W. Taylor, and J.S. Thorp, "Performance index and classifier approaches to real-time, discrete-event control," *Control Engineering Practice*, vol. 5, no. 1, 1997.

A. Sang-Pil, K. Chul-Hwan, R.K. Aggarwal, A.T. Johns, "An alternative approach to adaptive single pole auto-reclosing in high voltage transmission systems based on variable dead time control," *IEEE Trans. on Power Delivery*, vol. 16, no. 4, pp. 676-686, 2001.

T. Seegers et al., "Transmission line protective systems loadability," *WG-D6 report to the Power System Relay Committee of the IEEE Power Engineering Society*, 2001.

T. S. Sidhu, et al., "Bibliography of relay literature, 2000 IEEE committee report," *IEEE Trans. on Power Delivery*, vol.17, no.1, pp. 75-84, 2002.

W. Stallings, *Data & Computer Communications*, 6th Ed. Prentice Hall, 2000.

J.C. Tan, P.A. Crossley, D. Kirschen, J. Goody, J.A. Downes, "An expert system for the back-up protection of a transmission network," *IEEE Trans. on Power Delivery*, vol. 15, pp. 508–514, 2000.

C.W. Taylor, D.C. Erickson, "Recording and analyzing the July 2 cascading outage," *IEEE Computer Applications in Power*, vol. 10, no. 1, pp. 26-30, 1997.

C.W. Taylor, "Improving grid behavior," *IEEE Spectrum*, vol. 36, no. 6, pp. 40-45, 1999.

C.W. Taylor, "The future in on-line security assessment and wide-area stability control," *Proc. of the 2000 IEEE PES Winter Meeting*, 2000.

The MathWorks Inc., *Fuzzy Logic Toolbox User's Guide*, ver.2, 1995.

H. R. Tizhoosh, "Fuzzy logic & probability theory: Clarification towards building a bridge," *Fuzzy Image Processing*, University of Waterloo, 1997. http://watfor.uwaterloo.ca/tizhoosh/probability.htm, last accessed 08/27/2003.

Tuan Tran-Quoc, N. Hadj-Said, J.C. Sabonnadiere, R. Feuillet, "Reducing dead time for single-phase auto-reclosing on a series-capacitor compensated transmission line," *IEEE Trans. on Power Delivery*, vol. 15, no.1, pp. 51 -56, 2000.

U.S./Canada Power Outage Task Force, "August 14, 2003 Outage, Sequence of Events," September 12, 2003. ftp://www.nerc.com/pub/sys/all_updl/docs/pressrel/BlackoutSummary-Draft-6b.pdf, last accessed 10/21/2003.

M. Walker et al. (editors), *Aluminum Electrical Conductor Handbook*, 2nd ed. Washington, DC: The Aluminum Association, 1982.

H. Wan, J. D. McCalley, and V. Vittal, "Increasing thermal rating by risk analysis," *IEEE Trans. Power Systems*, vol. 14, no. 3, pp. 815–828, 1999.

F. Wang, M.H.J. Bollen, "Quantifying the potential impacts of disturbances on power system protection," *IEE Proc. of the Seventh International Conference on Developments in Power System Protection*, pp. 262 –265, 2001.

S.P. Websper, A.T. Johns, R.K. Aggarwal, R.W. Dunn, "An investigation into breaker reclosure strategy for adaptive single pole autoreclosing," *IEE Proc. of Generation, Transmission and Distribution*, vol. 142, pp. 601 -607, 1995.

L. A. Zadeh, "Fuzzy sets," *Information and Control*, vol. 8, no.3, pp. 338-353, 1965.