1 Introduction

This is a model of a relay supervisory system (RSS) that works passively in conjunction with the existing protective relaying system at a substation. During normal system operating conditions, the RSS supervises the relay system to prevent trips due to hidden failures. During wide area network disturbances, it adapts the relay system to increase security of the power system. The RSS works passively in the sense that it waits for events to occur in the existing relay system before taking any action.

This thesis performs an actual simulation of a RSS. The simulation includes a model of the RSS, simplified models of existing relays, and time synchronization between the two models, all performed in Matlab. A power system model in EMTP provides inputs to the RSS model. Multiple faults are applied to the EMTP model, and the RSS is tested under each fault condition, and with a variety of relay hidden failures. For all tests performed, the simulation of the RSS successfully prevents relay hidden failures from removing circuit elements inadvertently, while allowing correct relay operations to remove circuit elements.

1.1 Protection System Role in Power System Blackouts

The purpose behind this model is the prevention of unnecessary power system blackouts. Relaying has traditionally played a large role in major system disturbances as reported by NERC (North American Electric Reliability Council). NERC events include a major loss of system load for more than 15 minutes, or continuous interruption to a significant percentage of customers for more than 3 hours. Weather related disturbances, or any other disturbance beyond the utility's control, are not included.[4] Approximately ¾ of the NERC events from 1984-1989 directly involved relaying in some manner. As Table 1 shows, relaying involvement in NERC events is fairly consistent. The relaying system generally did not initiate the event, but mis-operated and contributed to the size of the disturbance.

Table 1: Protection System Role in Events Documented by NERC

Year	Cases with Relay System Involvement/Total Cases
1984	10/14 = 71%
1985	11/12 = 92%
1986	5/7 = 71%
1987	3/5 = 60%
1988	7/11 = 64%
Total	36/49 = 74%

Figure 1 shows the causes of relay mis-operation during NERC events by category. The important category to note is maintenance. The maintenance category includes physical defects in the relay system such as loss-of-carrier, defective relays, and other failed parts. The "Other" category includes cases where a specific cause for the disturbance could not be identified. Six of the seven cases in the Other category had unknown causes. It is quite probable that these were actually undetected or intermittent

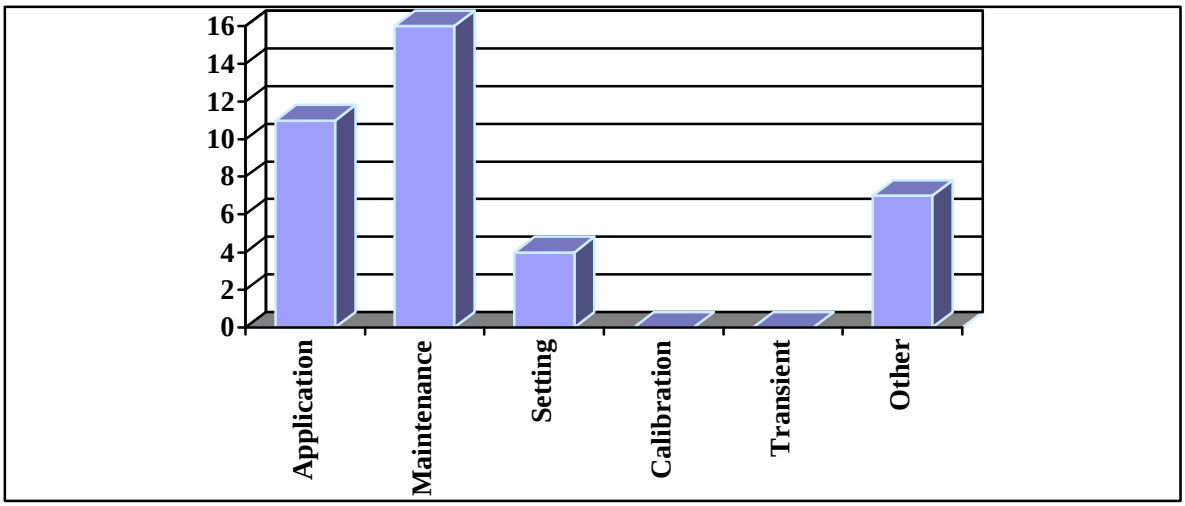

Figure 1: All Relay Mis-Operations by Category

Events Documented by NERC, 1984-1989

physical defects. This means maintenance, or essentially physical, defects account for about 45% of NERC disturbances during this period.[3]

One contributing factor to relay mis-operation is the design philosophy of relay systems. Relay systems are traditionally weighted in favor of dependability. A dependable relay system *always* operates for faults within its zone of protection. It is preferable to incorrectly trip occasionally, than to not trip at all for a fault. This penalizes the security of a relay system, or the ability to only trip for faults within its zone of protection. The RSS proposed in this thesis attempts to increase the security of the protective relay system without adversely affecting its dependability.

1.2 Computer Relaying Techniques

Some background of concepts used in computer relays is necessary to help understand the RSS.

1.2.1 Phasors

A phasor is a representation of a single frequency sinusoid, described by the expression $y(t) = \sqrt{2}Y_m \cos(w_0 t + j)$. Y_m is the rms value of the sinusoid, and φ is the angle between the t=0 reference and the peak of the sinusoid. Since it only represents one frequency, a phasor representation is not directly applicable under transient conditions, where many frequencies are present. Computer relays use the phasor representing the fundamental frequency of a waveform sampled over a finite window. A Fourier transform is the most common method to calculate the fundamental frequency phasor.

1.2.2 Fourier Transform

Computer relays commonly use a Discrete Fourier Transform to convert sampled data into a representation of the fundamental frequency phasor. The Discrete Fourier Transform for the p^{th} harmonic phasor at a sampling rate of N times a cycle is

$$F_p = \frac{2}{\sqrt{2}N} \sum_{n=0}^{n=N-1} f_n e^{\frac{-j2\pi np}{N}}$$

In the frequency domain, the Fourier transform of sampled signals can be thought of as an ideal low-pass filter with a cutoff frequency of ω_c. The Nyquist sampling frequency is $\omega_f = 2\omega_c$, or twice the highest frequency in the bandlimited signal. If $\omega_f < 2\omega_c$, the lobes of the spectra of the sampled signal would overlap, producing an output signal different from the original signal. This effect is known as aliasing. To avoid aliasing, it is necessary to filter the signal to a bandwidth of a frequency equal to half the sampling rate. One advantage of the Discrete Fourier Transform is that a one cycle algorithm removes the DC offset from the fault current waveform, so there is no need to use a mimic circuit or a digital mimic representation in the relay.[6]

1.2.3 Anti-Aliasing Filter

The anti-aliasing filter of a computer relay removes the unwanted frequencies from a sampled waveform. If the Nyquist frequency corresponds to a sampling rate of N times per cycle, it also determines the highest order harmonic frequency in the waveform which can be estimated. All harmonics of a waveform above half the Nyquist frequency are mirrors of the lower frequencies. These harmonics will corrupt the phasors for the lower harmonics. Of particular concern is the fundamental phasor, which is used in relay applications. The anti-aliasing filter removes harmonics above $\omega_0 N/2$ to prevent corruption of the desired phasor.

There are two issues to consider in selecting the anti-aliasing filter. One issue is the frequency response of the filter, and the other is the time domain response of the filter. A sharp frequency response is desirable to completely remove the unwanted harmonics. However, as the frequency response of a filter becomes sharper, the time domain response becomes worse. So a balance must be achieved between the two.

An anti-aliasing filter may be either a passive or active filter. Active filters, which use operational amplifiers, provide a sharper cutoff at the expense of transient response. For this reason, passive filters, such as a two stage RC filter, are used.

1.2.4 Sampling Rates

Computer relays generally sample waveforms between 4 and 64 times per cycle. Reliable relaying decisions need to be made based upon at least 6 to 10 samples. A high sampling rate appears likely to produce a more accurate result. However, there must be enough time between samples to perform relay calculations. A sampling rate of 12 times per cycle seems to be a good compromise, and is very commonly used. This rate is the slowest sampling rate that still permits calculation of the 5^{th} harmonic phasor, commonly used in transformer differential relaying algorithms.

1.3 Relay Hidden Failures

A relay hidden failure is a permanent defect that will cause a relay or relay system to incorrectly and inappropriately remove a circuit element or elements as a direct consequence of another switching event.[3] Failures that lead to an immediate mis-operation, and can be detected and corrected right away, are not hidden failures. One example of a hidden failure is the timer for a distance relay. If the timer fails so it is permanently picked up, nothing happens until a fault occurs within the relay zone, when the relay immediately trips for the fault. This results in loss of coordination. Electromechanical relays have a higher risk of a hidden failure than digital relays, since they have a larger number of mechanical parts, and don't have the self-checking capability of digital relays.

Hidden failures can be exposed by abnormal power system states. If a fault occurs near enough to the relay, the effects of the fault may be seen by that relay. This means hidden failures of a relay have a region of vulnerability associated with it. If an abnormal event occurs within the region of vulnerability, the hidden failure will cause the relay to incorrectly remove the circuit element. Figure 2 shows examples of the regions of vulnerability for relays. Reverse local bus vulnerability is due to a hidden failure in relays at the local bus that allows a trip of the local end. Every relay hidden failure has its own region of vulnerability based on the hidden failure and on the settings of the individual relay. For example, the region of vulnerability for an impedance relay may be the over-reach of the remote bus. The region of vulnerability for overcurrent relays is determined by the fault current provided by the fault. Some relays have greater vulnerability to hidden failures. Each region of vulnerability is assigned a vulnerability index, which is the relative importance or sensitivity of the power system to this region. Reference [3] describes the region of vulnerability for various types of protection schemes, the amount of exposure possible, and how to assign a vulnerability index.

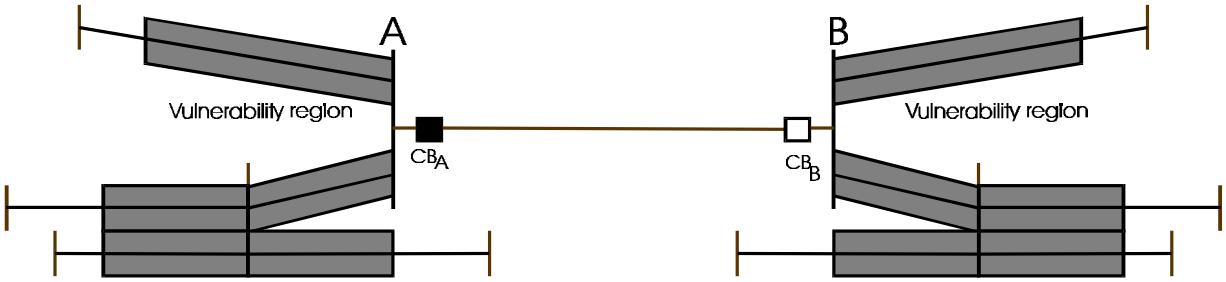

Figure 2: Region of Vulnerability

1.4 Adaptive Protection

Adaptive protection is a protection philosophy which permits and seeks to make adjustments in various protection functions automatically in order to make them more attuned to prevailing power system conditions.[7] To be practical, adaptive protection requires computer relays. Computer relay functions are determined through software, allowing easy changes to relay settings. Computer relays also have communications capabilities, which allows the relay to adapt settings based on the state of the power system. An example of adaptive protection is Security and Dependability Balance, where

conditions such as a wide area network disturbance may require changing the relay system from a more dependable system to a more secure system. Another example is transformer protection, where slope and pickup settings for a differential relay could be changed for system conditions or the setting of a tap changer. A final example is distance relays, which could adapt their settings based on the presence of infeed from a tap line. Further descriptions of adaptive protection applications may be found in Reference [7].