

# 1 INTRODUCTION TO PRACTICAL POWER SYSTEM PROTECTION

---

## PURPOSE

The purpose of this text is to provide a comprehensive guide to power system protection using SEL-based products. The anticipated audience is both the experienced protection engineer and the engineer just learning the art and science of power system protection. The information is organized in a way that permits easy information location and retrieval. SEL's goal in producing this document is to equip power engineers with the best opportunity to make electric power as safe and economical as possible.

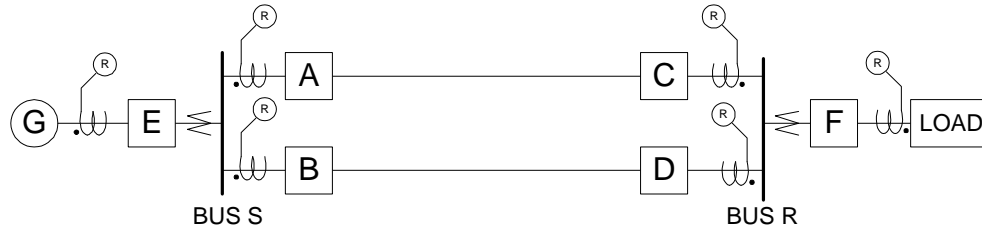
## REQUIREMENTS

The information in this text assumes that the reader has fundamental knowledge of electrical engineering, and introductory concepts of power system protection. A suitable level of knowledge would be a senior or graduate electrical engineering student. Electrical engineering fundamentals that pertain significantly to power system protection are necessary.

## WHAT IS POWER SYSTEM PROTECTION?

Power system protection is the process of making the production, transmission, and consumption of electrical energy as safe as possible from the effects of failures and events that place the power system at risk. It is cost prohibitive to make power systems 100 percent safe or 100 percent reliable. Risk assessments are necessary for determining acceptable levels of danger from injury or cost resulting from damage. Protective relays are electronic or electromechanical devices that are designed to protect equipment and limit injury caused by electrical failures. Unless otherwise noted, the generic term relay will be synonymous with the term protective relay throughout this text. Relays are only one part of power system protection, because protection practices must be designed into all aspects of power system facilities. Protective relays cannot prevent faults; they can only limit the damage caused by faults. A fault is any condition that causes abnormal operation for the power system or equipment serving the power system. Faults include but are not limited to: short- or low-impedance circuits, open circuits, power swings, overvoltages, elevated temperature, off-nominal frequency operation.

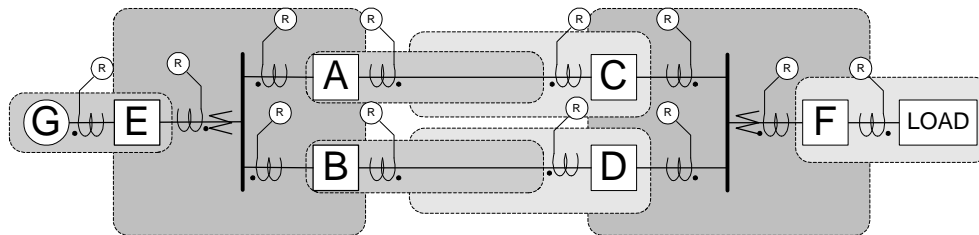
Power system protection must determine from measurements of currents and/or voltages whether the power system is operating correctly. Three elements are critical for protective relays to be effective: measurements, data processing, and control. Figure 1.1 shows a typical application of relays to a power system. This example system contains a single source that is connected to bus S through a step-up transformer, two transmission lines that connect bus S to bus R, and a load that is connected to bus R through a step-down transformer.



**Figure 1.1: Example of Power System Single-Line Diagram**

Breakers A through F provide the control to isolate faulted sections of the power system. Breaker F would not be required for this example except that customer-owned generation is becoming more common and a load can change to a source. The current transformers attached to the relays at strategic points in the power system provide the necessary instrumentation for relays to determine the presence of faults. Voltage instrumentation for protection systems may also be required, depending on the relaying scheme used. Any number of relay devices may use any single-voltage or current instrumentation device. It is important that the load or burden the relay devices create does not adversely affect the quality or accuracy of the measurements by these or other devices.

It is not clear from this diagram what is being protected or what function is being performed. Usually a designation number is put into the circles that Figure 1.1 shows as 'R'. The power system protection is divided into zones based on the type of equipment and location, as shown in Figure 1.2. Overlapping these zones increases protection reliability; if one protection system fails to perform, another is ready to provide the needed protection. Each protection zone consists of a sensing current transformer, a power control breaker that can deenergize the protected zone. The CTs shown in Figure 1.1 and Figure 1.2 have polarity marks to indicate that positive current flow is into the mark. CTs are necessarily outside the protection zone.



**Figure 1.2: Examples of Zones of Protection**

## GOALS OF PROTECTION

### Maintain the Ability to Deliver Electric Power

Power systems that have evolved in the 20<sup>th</sup> century consist of generation plants, transmission facilities, distribution lines, and customer loads, all connected through complex electrical networks. In the United States, electrical energy is generated and distributed by a combination of private and public utilities that operate in interconnected grids, commonly called power pools, for reliability and marketing. Elsewhere in the world, generation is tied to load through national or privatized grids. Either way, power flows according to electrical network theory.

Interconnection improves the reliability of each pool member utility because loss of generation is usually quickly made up from other utilities. However, interconnection also increases the complexity of power networks. Power pool reliability is a function of the reliability of the

transmission in the individual members. Protection security and dependability is significant in determining the reliability of electrical service for both individual utilities and the interconnected power system pool.

### Public Safety

Relays are designed to deenergize faulted sections as quickly as possible, based on the premise that the longer the power system operates in a faulted condition, the greater the chance that people will be harmed and / or equipment damaged. In some cases power system stability and government regulatory commissions set the speed requirements of extra high voltage (EHV) systems. Because of cost constraints, relays are not designed to prevent the deaths of people or animals who make direct contact with high voltage lines. Instead, designers use physical separation and insulation to prevent direct contact. Still, the faster a faulted system element can be detected, isolated, and deenergized, the lower the probability that anyone will encounter hazardous voltages.

### Equipment Protection

The primary function of power system protection is to limit damage to power system apparatus. Whether the fault or abnormal condition exposes the equipment to excessive voltages or excessive currents, shorter fault times will limit the amount of stress or damage that occurs. The challenge for protective relays is to extract information from the voltage and current instrumentation that indicates that equipment is operating incorrectly. Although different faults require different fault detection algorithms, the instrumentation remains the same, namely voltages and currents. (Refer to Table 4.1 for a more complete list of instrumentation requirements.)

### Power System Integrity

Properly operating relay systems isolate only the portions on the network directly involved with the fault. If relays operate too quickly or fail to operate, the fault-affected area expands and some circuits can be deenergized. Parts of the power system can become isolated or islanded from the rest of the network. A large mismatch between generation and load can put an islanded network in jeopardy of losing the generation control that holds frequency and voltage within acceptable limits. Without generation control, the isolated systems will eventually be tripped off by other relays. Widespread outages caused by cascading relay operations due to voltage or frequency excursions require many work hours to restore power, which is costly from both a labor and a lost revenue perspective.

### Power Quality

The factors measured to determine the quality of power are voltage amplitude, frequency, and waveform purity. Voltage amplitude quality takes into account persistent RMS value, flicker, and intermittent dips and peaks, as well as momentary and long-term outages. Frequency changes at most a few hundredths of a hertz, unless the power system has lost generation control. Induction motors have the most sensitivity to power system frequency. Waveform purity is largely a function of harmonic content and is predominantly influenced by load.

The quality of electrical power is an issue for loads that are sensitive to momentary outages and harmonics. In the past, when loads were primarily resistive and inductive, harmonics were either inconsequential or nonexistent. Also, momentary outages had little effect on residential

customers. Commercial and industrial customers compensated for momentary outages either with multiple feeds from the utility power sources or with local generation.

Today, every residential customer knows that there was an outage whether she or he was home to experience it. Outages affect home computers and the digital clocks on VCRs, microwave ovens, and other numerous appliances. Although the inconvenience may seem trivial to the relay engineer and perhaps the actual number of outages is even less than in years past, the customer may perceive that the power system is not as reliable today. Good relay selectivity is key to reducing the number of outages and faster relaying minimizes the duration of power dips. Hence a substantial component of power quality is not tripping unnecessarily.

## PROTECTION SYSTEM MANAGEMENT

### Protection Quality

There are four primary causes of protection system failures: instrumentation distortion, control failures, relay equipment failures, and incorrect relay settings. Instrumentation distortion is usually caused by saturation from excessive inputs or remnant flux. Breaker failures or faults in the dc controls can cause control failures. Relay equipment reliability depends on design and manufacturing processes. In addition to overlapping zones of protection, both redundant and backup protection increase reliability for critical applications. Improper settings render relay systems useless. Hence protection systems designers must know which relay is best suited for a particular application and how to set the relay parameters to obtain the proper selectivity and sensitivity. Proper relay application is the single most important factor in the quality of power system protection.

### Continuous Improvement

Power systems are not static networks. Transmission lines and generators are continuously put into or taken out of service. Each change in the network potentially affects the operations of protective relays. Protection engineers must decide how to alter the relay settings to compensate for a change in the power network configuration. Many modern computer based relays allow multiple setting which can be automatically selected depending on system conditions.

### Analysis of Data

Each fault tests the power system relays in the vicinity of the fault and presents an opportunity to analyze the behavior of the entire protection system. The fault location, type of fault, fault impedance, and relay sensitivity determine which relays respond to the fault. Relays either operate correctly (including in a timely manner) or incorrectly (including too slowly or too quickly). Microprocessor-based relays can now report information that provides the data to determine just how correct the operations were. Prior to microprocessor-based relays, oscillographs and sequential events recorders were used to determine the correctness of operations. Chapter 6 provides examples of this type of analysis.

### Economics of Protection

Plant equipment represents a significant investment to electric utilities. Figures from a representative utility that has a significant amount of hydro-based generation show that 50 percent of the plant investment is allocated to production, 14 percent to transmission, and

27 percent to distribution. In actual year-2000 dollars for a moderately sized utility, the investment in transmission and distribution alone is over one billion dollars. The cost of protection equipment is but a very small part of this investment.

### Capital Expense

A rule of thumb is an installed cost of \$30,000 per terminal end regardless of relay type. If the relaying scheme includes pilot protection, the cost of the communications is an additional expense.

### Operating Costs

Operating costs for relays are not the same as operating costs for protection systems. The former includes the costs of servicing and maintenance. Electromechanical and solid-state relays (also called static relays) require regular testing to determine their functionality. This means personnel must go to the substation and take the relay out of service during testing and calibration. If power system network changes require new relay settings, then personnel must again go to the substation to make appropriate modifications and tests. The expense of this manpower adds to the operating costs of relays.

Microprocessor-based relays are able to perform self-diagnostics and automated reporting with little or no additional investment, other than the original cost of the relays. They can be reconfigured remotely or automatically for new power system needs. Some relays have multiple group settings that automatically reconfigure the relays based on the open or closed position of one or more breakers. Communication with the relays eliminates service visits to the substation. The self-checking ability of microprocessor-based relays allows immediate detection of failed relays without waiting for the next scheduled maintenance visit or a misoperation to reveal the defective unit. Data logging also provides performance information that is not economically possible with static and electromechanical relays. Maintenance issues are discussed in more detail later in this chapter.

The cost of maintaining a protection system includes both the cost of maintaining the relays and the cost of assessing system performance. Every relay operation tests the protection system by verifying correct operations or exposing incorrect operations. Each fault has an area of effect where some relays are expected to operate and others to inhibit operation. If they do not all react correctly to the fault, the protection system has failed. Various instruments monitor the performance of the protection system, with varying degrees of expense associated with the cost of data collection and analysis. In the past, relay operations have been rather binary in that they either trip or don't trip. Today, microprocessor-based relays can also provide information on the certainty of a decision by recording the type of fault, fault location, and relative strength of the restraint and operate signals. Such information is invaluable for revealing potential problems and avoiding future misoperations. This analysis takes time, but the microprocessor-based relay is reducing the required time to achieve improved performance.

### Lifetime Costs

Lifetime costs include the purchase price, the cost of installation, and the operation of the protection system. The cost of protection must be justified by the value of potential losses from decreased revenue or damaged equipment. As greater demand is placed upon power systems, the cost of over tripping (tripping when not needed) is becoming as important as undertripping (slow

tripping or not tripping when needed). Proper protection requires a balance between speed and security, based on the needs of the system.

#### PERFORMANCE MEASURES

Protection engineers define dependability as the tendency of the protection system to operate correctly for in-zone faults. They define security as the tendency not to operate for out-of-zone faults. Both dependability and security are reliability issues. Fault tree analysis is one tool with which a protection engineer can easily compare the relative reliability of proposed protection schemes. Quantifying protection reliability is important for making the best decisions on improving a protection system, managing dependability versus security tradeoffs, and getting the best results for the least money. A quantitative understanding is essential in the competitive utility industry.

#### Resolution, Precision, and Accuracy

All too often, these terms are used interchangeably. However, they describe signals from totally different perspectives. These three attributes of measurement are completely independent; they are easiest to illustrate with examples from analog metrology.

Resolution is the difference between calibrated markings. For example, an outside thermometer might have markings every two degrees Fahrenheit, a two-degree Fahrenheit resolution. A higher resolution is possible by interpolating between markings, but doing so influences precision.

Precision is the ability to achieve repeatability. For analog measurements, precision is actually based upon both the instrument and the observer. For the instrument, precision is the ability to produce the same output every time the same input is applied. Many environmental factors influence the precision of analog instruments, but friction and temperature tend to dominate. Observers can also influence precision by their position when making the observation, ability to interpolate correctly, and judgment skills. Using the thermometer example once again, if 10 different observers are asked to read the temperature when the outside temperature is exactly 77.20 degrees Fahrenheit and they all read the same temperature every time, the instrument has high precision. This is true even if they always read 75 degrees.

Accuracy is the ability to measure exactly. The thermometer in our example has an inaccuracy of 2.2 degrees, even though it has two degrees of resolution and a high degree of precision. Accuracy can only be determined by calibration using a standard that has a higher degree of accuracy than the instrument being calibrated. The Air Force calibration laboratories require standards to be at least ten times more accurate than the instruments being calibrated. All standards used in those Air Force laboratories are directly traceable to the National Institute for Standards and Technology (NIST) in Boulder, Colorado. Analog instruments get out of calibration because of changes caused by temperature, mechanical and electrical stress, and wear from friction.

Measurements using digital systems are subject to the same inaccuracies and errors as analog systems except for friction and mechanical stress. The observer, whether human or machine, depends strictly on the resolution, precision, and accuracy of the primary instrumentation. The measurement is only affected by data truncation or errors introduced by communications noise. It would be a mistake to attribute any higher degree of accuracy to a system than is actually verified through calibration.

## Reliability

Above all else, relays must be reliable, both dependable and secure. This definition of reliability contains conflicting goals or goals that cannot be mutually maximized. Dependability includes timely operation, which denotes speedy detection and decision. The Heisenburg uncertainty principal (the speed of a particle and its position cannot be determined with the same degree of certainty) can be loosely applied to relaying. The longer one has to make a measurement, the more accurate the measurement can be (within the limitations of the measuring equipment) and the more certain the decision that is based upon this measurement.

Relays operate continuously by making correct decisions that discriminate between loads and faults and discriminate between faults that are in the zone of protection and all other faults. Protection reliability is affected by equipment failures and by appropriate application and installation.

Determining device reliability is more important for relays that cannot perform self-diagnostics and alarming. Failure rate (the inverse of device reliability) is usually expressed in mean time between failures (MTBF). For example, suppose the reliability of a device is expressed with a mean-time-between-failure (MTBF) of 100 years. The failure rate is 1/100 failure per year. Therefore, if a system has 300 of these devices, the expected failure rate is  $300 \cdot (1/100) = 3$  devices per year.

Failure rates are used to determine maintenance intervals to test for failed relays. The optimal maintenance interval is determined by computing the probability of a failure over an interval, multiplied by the expected cost of an incorrect operation caused by a relay failure and the cost of maintaining the relay. The interval that makes the two costs equal is the optimal maintenance interval. The difficulty with this approach is determining the expected cost of an incorrect operation.

The reliability of other equipment besides the protective relay must be considered when computing the reliability of a protection system. This equipment includes instrumentation, control power (station batteries), auxiliary control devices, and the primary controls such as circuit breakers. Techniques for making reliability assessments are described in a later section of this chapter.

Three ways of improving reliability for protective relay systems are: redundant systems, backup systems, and overlapping zones of protection. Critical applications may use all three methods as well as redundant instrumentation and control circuits. Redundant protection uses multiple installations of identical equipment, whereas a backup protection scheme uses multiple relays that are based on different concepts of detecting and identifying faults.

## Redundancy

In protection systems, recent use of the term redundant refers to ensuring reliability by duplicating effort. Systems that are 100 percent reliable do not require redundancy, but few systems are 100 percent reliable. As the cost of protection equipment declines, the feasibility of ensuring reliability by duplication increases. Two different approaches to improving reliability by redundancy are discussed below.

## Backup Protection

The two most common types of redundancy are dual and parallel redundancy. Dual redundancy is where two identical units are operated with identical inputs. The outputs are placed in parallel for added reliability or in series for added security. Parallel redundancy uses two units of different design but the two units are functionally equivalent. They may or may not use the same inputs but the outputs are connected as they are in dual redundancy.

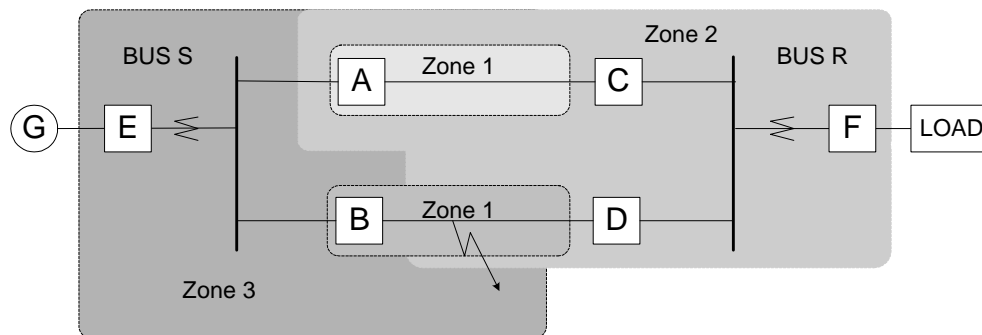
## Diversity Overlapping Zones of Protection

Protection systems improve reliability by organizing the protection function with overlapping zones in such a way that each relay has a primary zone and provides backup protection for one or more other expanded zones. Relays frequently have multiple operational zones, as illustrated in Figure 1.3. The speed of trips for faults in zone two is generally slower to allow opportunities for other relays that see the fault in zone 1 to clear the fault. Zone 2 therefore provides backup protection by overlapping other zones that are normally protected by other relays. Zone 3 can be used to send signals to block other relays from operating or for reverse direction protection.

The relay is designed to determine which zone of protection a fault is in and provide the proper operation for any fault within the assigned zone or zones. As Figure 1.2 shows, the zones overlap, so more than one relay may operate for a specific fault. Figure 1.3 shows how different zones can be assigned for a relay whose primary function is to protect the transmission line between breakers A and B. The different zones usually have different operating times worked out in relay coordination plans.

In the example in Figure 1.3, zone-one trips for faults from breaker A to 80 percent of the line length toward breaker C. Zone two operates for faults beyond bus R including some percentage of the transmission line between breakers D and B and the transformer supplying the load at bus R. Zone three looks backward toward the source and covers the step-up transformer, plus a percentage of the transmission line between breaker B and D. After the initial fault, as time passes and the fault persists, the relay expands its reach by activating more zones of protection.

The backup protection provided by this scheme can be illustrated using the following example. Consider a fault on the transmission line between breakers B and D. Assume that breaker B operates correctly but breaker D does not. The relay at breaker A waits until the Zone 2 delayed output activates, and then trips because it sees the fault on the increased sensitivity as the reach expands. The fault is now cleared because breakers at A and B are open. If the fault is closer to breaker B, then the relay at A would not have sufficient sensitivity until the timers allow Zone 3 operations.



**Figure 1.3: Zone Assignments for a Three-Zone Relay**

Older relays with limited functionality implemented the various zones of protection using independent devices. Newer microprocessor-based relays are able to implement the functions of numerous protection, control, and monitoring devices.

### Analysis of Reliability Using Fault Tree Methods [6060]<sup>i</sup> [6073]<sup>ii</sup>

The method of combining component failure rates is called “fault tree analysis,” a concept first proposed by H. A. Watson of Bell Telephone Laboratories to analyze the Minuteman Launch Control System. This method, used and refined over the years, is attractive because it does not require extensive theoretical work and is a practical tool any engineer can learn to use. While computer programs are available to assist in developing and analyzing complex fault trees, this text shows that small fault trees, which are easily analyzed manually, are also very useful. The goal of fault tree analysis is to quantify system reliability and justify or analyze proposed changes to a system.

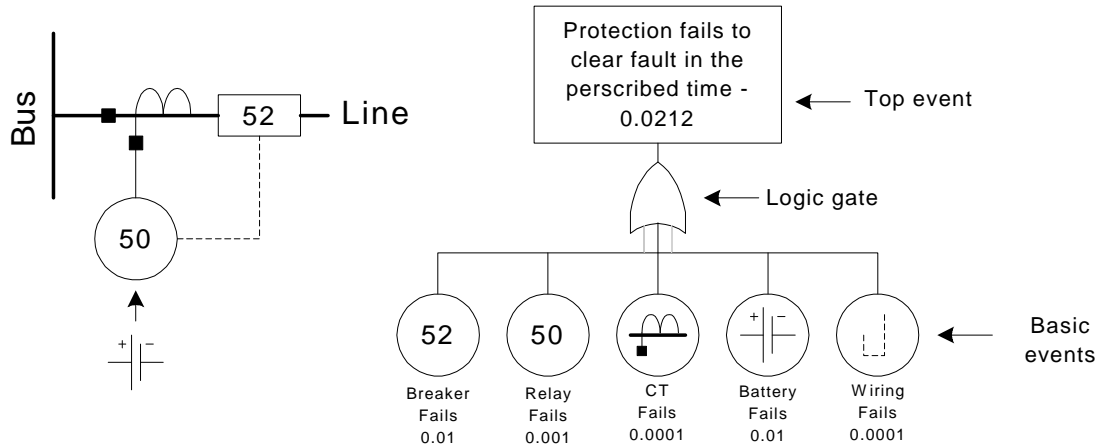
If a device consists of several components, then a fault tree helps us combine component failure rates to calculate the device failure rate. Refer again to our device that has a failure rate of 1/100 failure per year. It might consist of two components, each with a failure rate of 1/200 failure per year. Both components must operate properly for the device to be sound. The individual failure rates of the two components add up to the total failure rate of 1/100. We add the component failure rates to obtain the device failure rate if either component can cause the device to fail.

On the other hand, our device with the 1/100 failure rate might consist of two redundant components each with a failure rate of 1/10 failures per year. Either component can give the device satisfactory performance. The product of the individual component failure rates is the device failure rate. We multiply component failure rates to obtain the device failure rate if both components must fail to cause the device to fail.

Fault tree analysis is not the only tool used for reliability studies. Among other techniques, the Markov models compare relative performance of communications-based protection schemes, and predict optimum routine test intervals for protective relays.<sup>iii,iv</sup> Markov models cover the entire system of interest and incorporate all failure and success modes and transitions. The outputs of a Markov model are the probabilities that the system resides in any one of the modeled states. This technique models both normal and abnormal states. Since the Markov technique models the entire system, model development requires considerable effort, and Markov model analysis typically requires a computer. Markov modeling also assumes that all state transitions are exponentially distributed, which is sometimes difficult to justify.

### Fault Tree Construction

A fault tree, tailored to a particular failure of interest, models only the part of the system that influences the probability of that particular failure. The failure of interest is called the Top Event. A given system may have more than one top event that merits investigation. Figure 1.4 shows a protective system consisting of a circuit breaker, a CT, a relay, a battery, and associated control wiring. The fault tree in this figure helps us analyze the chance that the protective system will not clear a fault.

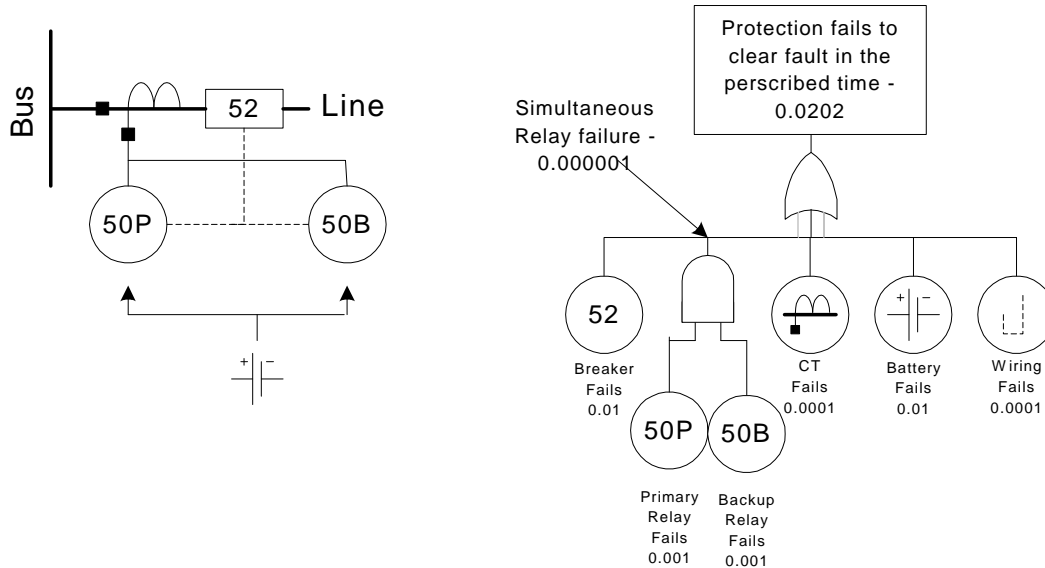


**Figure 1.4: Fault Tree for Radial Line Protection**

The Top Event is a box containing a description of the failure event of interest. This description usually includes the event that occurred and the maximum tolerable delay for successful operation. For example, our top event here is “Protection Fails to Clear Fault in the Prescribed Time.” We assume the power system is faulted and we assume the protection system is intended to detect and isolate the fault in question in a very short time, usually a few cycles. We wish to know the probability that the protection system will fail to clear the fault in the prescribed time limitation.

The fault tree breaks down the Top Event into lower-level events. Logic gates show the relationship between lower-level events and the Top Event. The OR gate in Figure 1.4 shows that any of several failures can cause the protection system to fail. If the dc system, the current transformer, the protective relay, the circuit breaker, or the control wiring fail, then the Top Event, “Protection Fails to Clear Fault in the Prescribed Time,” occurs. Assume the following chances of failure of the individual devices: 0.01 for the breaker, 0.0001 for the CT, 0.001 for the relay, 0.01 for the battery, and 0.0001 for the control wiring. (These component reliability estimates are for purposes of this example only. We will develop more substantiated estimates later.) The chance the system will fail to clear a fault is the sum: 0.0212 failures to clear a fault per year. We can improve the system by finding better components, which lowers the individual failure rates, by designing simpler systems, or by adding redundancy.

Let us improve the system by adding a redundant relay. The fault tree of Figure 1.5 contains an AND gate. This AND gate shows that both protective relays must fail for the event “Relays Fail to Trip” to occur. Our failure rate for the relays taken together is  $0.001 \cdot 0.001 = 0.000001$ . The sum implied by the OR gate is 0.0202. The reliability improvement in this case is small, because failures other than those of the relay dominate the system.



**Figure 1.5: Fault Tree for Radial Line Protection With Redundant Relays**

There are other gates besides the AND and OR gates [1,6]. However, many fault trees require only those gates, and we restrict our discussion to these basic items in this introductory text.

The roots of our fault tree are failures of devices such as the breaker and the relay. Are these basic enough? Should we, for instance, break the relay down into a coil, contacts, disk, bearings, tap block, etc.? If we are comfortable with the failure rates for the devices, then we need not break the devices into their components. The roots are referred to as basic events.

### Device Failure Rates and Unavailability

A device failure rate gives us the number of failures we can expect per unit time. During the useful lifetime of a device, we frequently assume a constant failure rate. Failure rates can come from theoretical calculations, such as MIL-HDBK-217F [7] parts-count procedures, or from field experience. For example, suppose there is an in-service population of 10,000 devices, and we observe 10 failures of devices in one year. An estimate of the failure rate from these field data is  $10/10,000 = 0.001$  failures per year. The reciprocal gives an estimated MTBF of 1000 years. This does not imply that a device is likely to last 1000 years. Instead it is a reliability figure valid during the useful lifetime of the device.

Our experience with relays shows that the MIL-HDBK-217F parts-count procedure gives very pessimistic figures. For example, a parts-count analysis might predict an MTBF of 20 years, yet field failure rates might convert to a field MTBF of 100 years or more. Also, the “217F” parts-count procedure does not consider manufacturing or design quality.

The strict definition of MTBF is the sum of Mean Time To Fail (MTTF) and the Mean Time To Repair (MTTR). MTTF is the reciprocal of failure rate. However, MTTR is usually small and, in this text, we assume MTBF is approximately equal to MTTF.

Failure rates are very useful in predicting maintenance costs, but do not tell the whole story about whether a device will be available when called upon to perform. Thus we need to consider unavailability, the fraction of time a device cannot perform. It is without units.

Roberts, et al. describe calculating unavailability from a failure rate and the time it takes to detect and repair a failure.<sup>v</sup>

$$q \cong \lambda T = \frac{T}{\text{MTBF}} \quad \text{Equation 1.1}$$

where:  $q$  is unavailability  
 $\lambda$  is some constant failure rate  
 $T$  is the average down-time per failure  
 $\text{MTBF} = \frac{1}{\lambda}$  is Mean Time Between Failures.

Each failure causes downtime  $T$ . Therefore, the system is unavailable for time  $T$  out of total time  $\text{MTBF}$ . The fraction of time the system is not available is therefore  $T/\text{MTBF}$ .

As an example, consider a protective relay with self-tests that detect all relay failures. If the relay has an  $\text{MTBF}$  of 100 years, then it has a failure rate of 0.01 failures/year.

First, assume self-tests detect problems within seconds, but it takes two days to repair the failure once it is detected. If the alarm contact of the relay is monitored, then the relay can be back in service in two days, and the unavailability is 0.01 failures/year  $\cdot$  2 days = 0.02 days/year.

On the other hand, if the alarm contact is NOT monitored, we must consider how we discover relay failures. Suppose we test the relay every two years, and repair it the same day we test it. If a test detects a failure, then on the average the relay was down for a year. The unavailability is 1 year  $\cdot$  0.01 failures per year = 3.65 days/year. This is 183 times worse -- so monitoring the alarm contact really pays off!

Protection using relays with self-tests, and with monitored alarm contacts, has better availability if periodic testing is not performed. This is because one day of service lost to testing every two years is much greater than the expected loss of service from automatically-detected failures which are promptly (2 days) repaired.

For the purpose of this text, we have estimated some failure rates, downtimes, and unavailability. We have confidence in our relay failure rates, which we have tracked for years. However, we have less confidence in other figures, and would appreciate field information that will refine our estimates of the failure rates of other components.

### Reliability Protective Relay Equipment

Based on our field experience, an  $\text{MTBF}$  of 100 years is conservative for modern computer-based relays of quality design and construction. These products demonstrate a self-test effectiveness of 80 percent or better. When loss-of-voltage and loss-of-current monitoring is enabled and monitored in the relay, the coverage of the relays and their instrument transformers increases to 98 percent effectiveness. These figures and some other assumptions lead to an unavailability of  $100 \cdot 10^{-6}$ . See Reference 4 for a detailed analysis.

Relays can fail to perform because they are applied improperly. Human factors are very difficult to represent in statistical models; however, based on field experience, we believe that human factors are of the same order of magnitude as relay failures themselves. Therefore we will assume the unavailability contribution caused by human error in installing and setting a relay is also  $100 \cdot 10^{-6}$ .

Claiming relay unavailability caused by hardware failures is equal to the unavailability caused by human failures does not mean that hardware failures and human failures are equally likely. The time to detect and repair human errors is indefinite while hardware failures are quickly detected and repaired. Assume human failures take one year to detect and repair and are 100 times less likely than relay hardware failures. In this case, unavailability caused by human failures would be:

$$q = \frac{\lambda_{\text{relay}}}{100} \cdot 1\text{year} = \frac{1}{100\text{years}} \cdot \frac{1}{100} \cdot 1\text{year} = 100 \cdot 10^{-6} \quad \text{Equation 1.2}$$

Table 1.1: summarizes the unavailability of commonly-used equipment in power system protection in descending order of unavailability.

**Table 1.1: Unavailability of Several Protection Components**

| <i>Component</i>                            | <i>Unavailability x 10<sup>-6</sup></i> |
|---------------------------------------------|-----------------------------------------|
| <i>Leased telephone line</i>                | 1000                                    |
| <i>Circuit breaker</i>                      | 300                                     |
| <i>Analog microwave equipment</i>           | 200                                     |
| <i>Protective relay misapplications</i>     | 100                                     |
| <i>Protective relay hardware</i>            | 100                                     |
| <i>Tone equipment</i>                       | 100                                     |
| <i>Microwave transmission channel</i>       | 100                                     |
| <i>Fiber Optic Channel</i>                  | 100                                     |
| <i>Multiplexing Fiber Optic Transceiver</i> | 100                                     |
| <i>DC power system</i>                      | 50                                      |
| <i>Modem</i>                                | 30                                      |
| <i>Simple Fiber Optic Transceiver</i>       | 10                                      |
| <i>Current transformer (per phase)</i>      | 10                                      |
| <i>Voltage transformer (per phase)</i>      | 10                                      |

### Fault Tree Analysis

After entering basic event data, analysis of the fault tree shown in Figure 1.4 is very straightforward with a single simplifying assumption known as the rare event approximation. It ignores the possibility that two or more rare events can occur simultaneously. For two events, each of which occurs with probability less than 0.1, the rare event approximation produces less than 5 percent error. When the events in question are failures, the rare event approximation is always conservative; the approximated probability of failure is always greater than the actual probability of failure.

Employing the rare event approximation, we calculate the unavailability associated with each event expressed with an OR gate as the sum of the unavailability for each input to the OR gate. For example, the unavailability associated with event “Protection at S Fails to Clear Fault in the Prescribed Time” is the sum of the unavailability of the eight inputs to that OR gate. The fault tree of Figure 1.4 contains only basic events and OR gates. Therefore the unavailability associated with the Top Event is simply the sum of all of the basic events, or  $2120 \cdot 10^{-6}$ .

Suppose we add a redundant relay to the system depicted in Figure 1.3. Assume that the backup relay uses the same instrument transformers, communications gear, dc system, most of the same control wiring, and trips the same circuit breakers as the primary relay. The AND gate in Figure 1.5 shows that both relays must fail for event “Both Primary and Backup Relays Fail to Trip” to occur. The simultaneous unavailability of both relays is the product of the unavailability of each relay. This calculation assumes the failures are independent (a failure in one relay does not influence the other relay), and are not triggered by a common cause.

In fact, we explicitly separated many possible common-cause failures higher in the fault tree (common instrumentation transformers, common dc supply, common communications gear, some common control wiring, common circuit breakers, and common operating principles). If you determine that other common causes of failure are important (extreme temperature, radio frequency interference, relay misapplications, etc.), include those as separate inputs to OR gates 2 and 3 in Figure 1.6. The unavailability of this protection system to clear faults is  $1620 \cdot 10^{-6}$ .

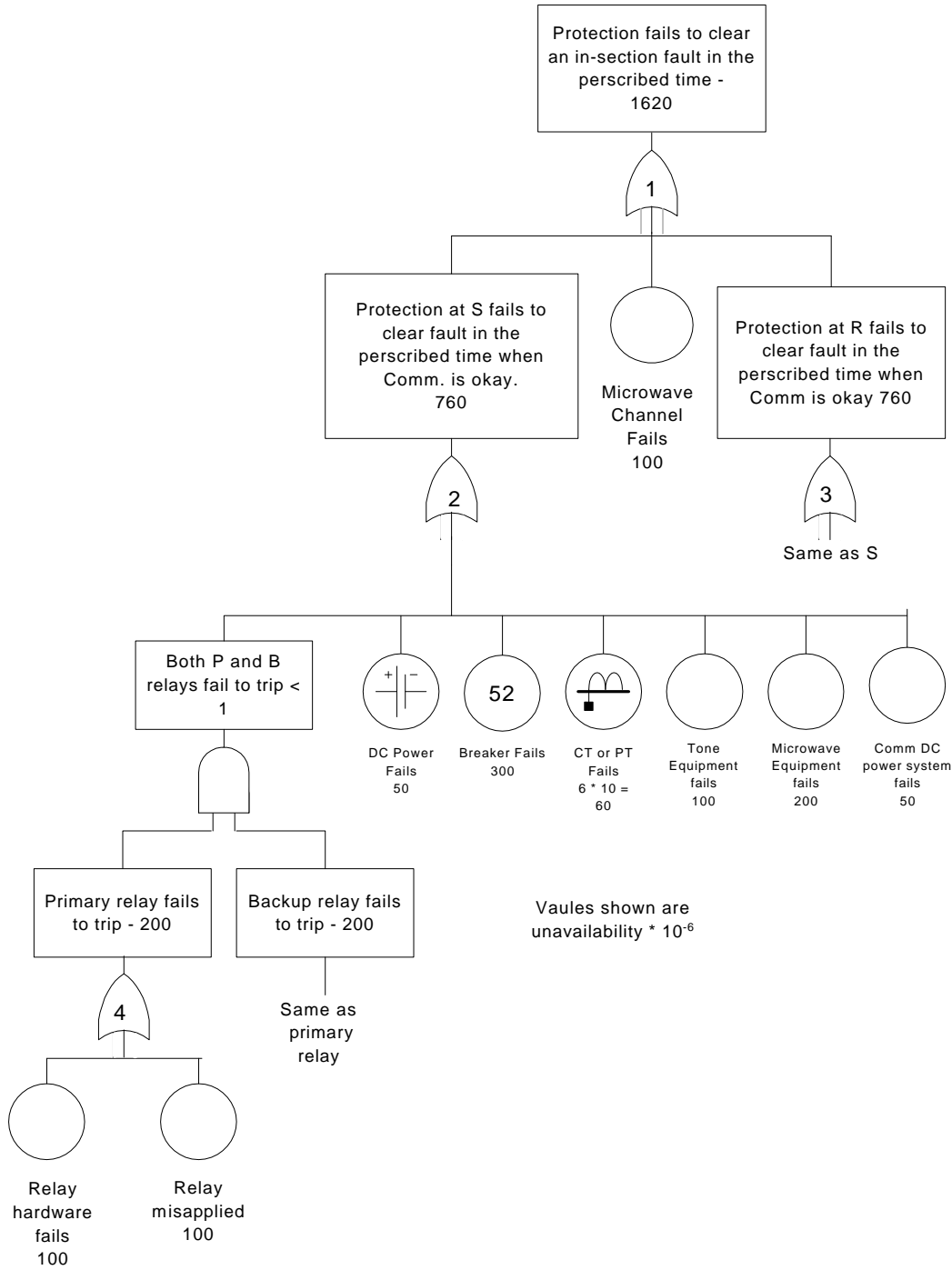
When constructing and analyzing fault trees, keep these simple rules in mind:

Use an OR gate to express a failure caused by any of several possible lower level failures. The unavailability of a subsystem represented by an OR gate is the sum of the device unavailability.

Use an AND gate to express a failure caused only when all (usually two) lower level simultaneous failures occur. The unavailability of a subsystem represented by an AND gate is the product of the device unavailability.

Use AND gates to express redundancy. Be careful to isolate common causes of failures above the AND gate that expresses redundancy.

Express basic event data in terms of unavailability when the Top Event is of the form “System Fails to Operate.” For top events of the form “System Operates Unexpectedly,” basic event data in the form of failure rates are more appropriate. This is because unexpected operations or false trips typically occur at the instant a component fails. Therefore the probability of a false trip is not as dependent on component downtime per failure.



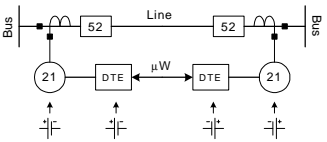
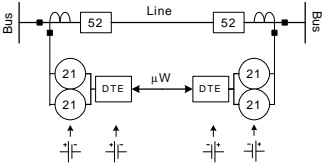
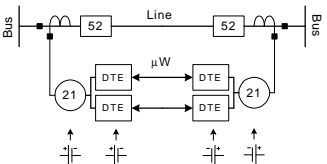
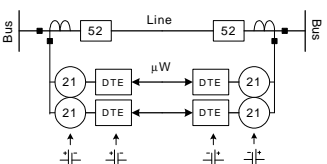
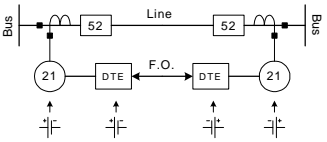
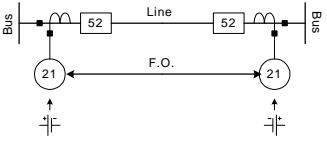
**Figure 1.6: Fault Tree for Tone/Microwave Based POTT Scheme With Redundant Relays**

Protection Unavailability Comparisons

We have already calculated unavailability for two possible protection schemes. The first was a basic POTT (permissive overreaching transfer trip) scheme with a single relay and a single communications medium. In the second we added redundant protective relays. The

unavailability of each of those systems, and several others to be described later, is shown in Table 1.2.

**Table 1.2: Unavailability Comparison of Several POTT Schemes**

| POTT Scheme                                                                         | Description                                                                                      | Unavailability x $10^{-6}$ Ignoring Zone 1 Coverage | Unavailability x $10^{-6}$ Considering Zone 1 Coverage |
|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|-----------------------------------------------------|--------------------------------------------------------|
|    | Single Relay<br>Single Channel<br>Microwave                                                      | 2020                                                | 1660                                                   |
|    | Redundant Relays<br>Single Channel<br>Microwave                                                  | 1620                                                | 1260                                                   |
|   | Single Relay<br>Redundant Channels<br>Microwave and<br>Relay-to-Relay on<br>Leased Line          | 1320                                                | 1275                                                   |
|  | Redundant Relays<br>Independent<br>Channels<br>Microwave and<br>Relay-to-Relay on<br>Leased Line | 920                                                 | 875                                                    |
|  | Single Relay<br>Single Channel<br>Multiplexed Fiber                                              | 1620                                                | 1440                                                   |
|  | Single Relay<br>Single Channel<br>Relay-to-Relay on<br>Dedicated Fiber                           | 1340                                                | 1286                                                   |

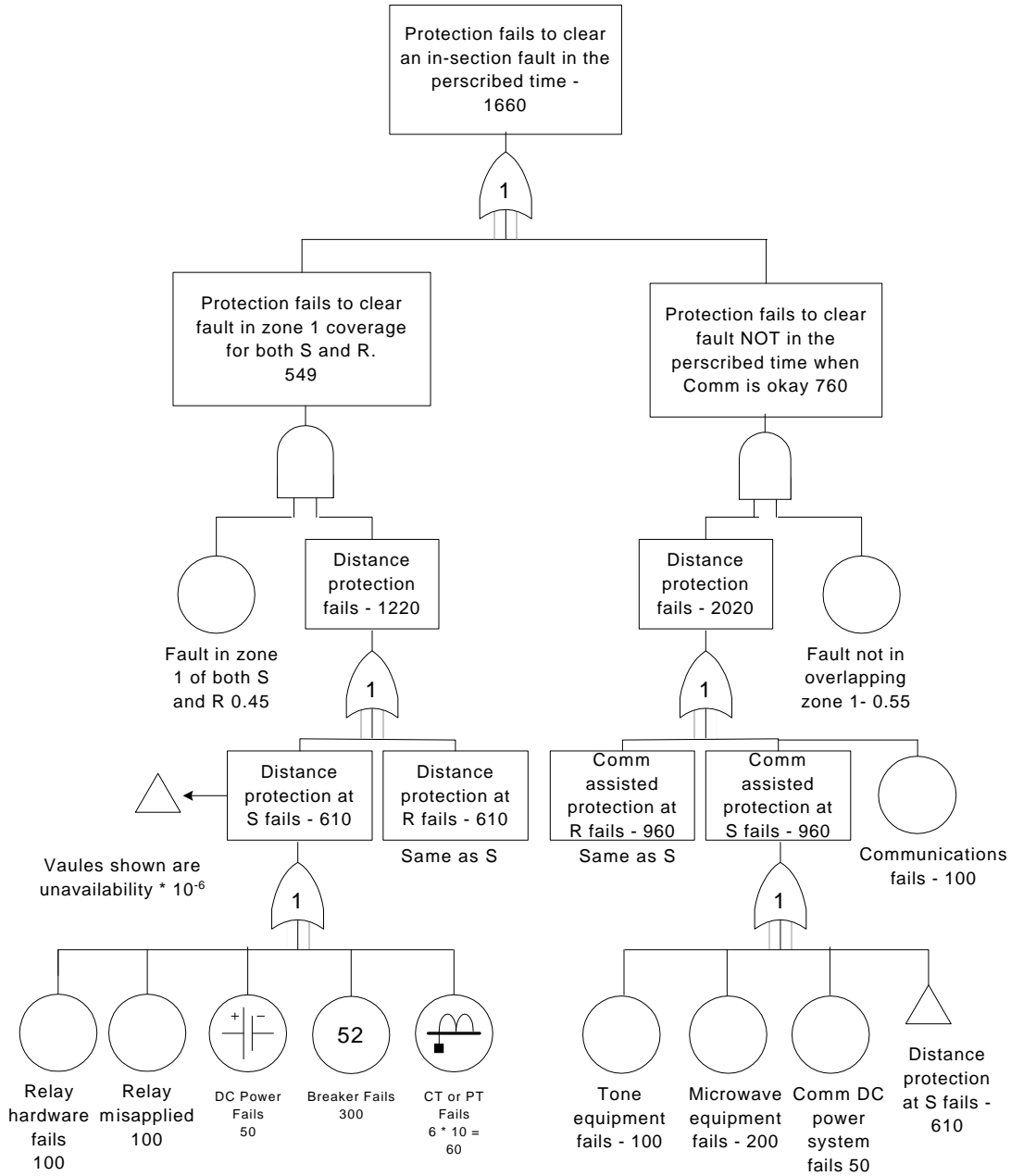
Each row of the table above describes a protection scheme. For instance, the first row describes a protection system consisting of a single relay and breaker with associated CTs and VTs at each line terminal, communicating via tone equipment and analog microwave gear. This is the system depicted in Figure 1.3.

While we limited our study to the POTT scheme, the same results would be obtained for any scheme where a communications failure results in a slow trip.

So far we have not considered the role of Zone 1 elements in the fault trees. Zone 1 elements set to 80 percent theoretically cover  $100 - 20 - 20 = 60$  percent of the line, independent of the channel. That does not imply the Zone 1 elements cover 60 percent of the faults. Fault resistance coverage of the Zone 1 distance elements may be no better than half that provided by the POTT scheme. If we assume one-half, and further assume 25 percent of the faults have enough resistance to (at least initially) not be detectable by Zone 1, then the apparent 60 percent coverage drops to  $75 \text{ percent} \cdot 60 \text{ percent} = 45 \text{ percent}$ . So, less than half the faults might be covered by the Zone 1 elements. To determine the unavailability across all faults that can be seen by either the POTT or the Zone 1 elements, we apply 55 percent of the faults to the unavailability of the POTT fault tree, and the remaining 45 percent of the faults to the unavailability given by the POTT fault tree, with the communications terms set to zero.

For example, assume the unavailability of the POTT scheme is  $2020 \cdot 10^{-6}$ , and that of the scheme, neglecting the communications, is  $2020 - 800 = 1220 \cdot 10^{-6}$ . The unavailability across all faults that can be seen by either scheme is:  $2020 \cdot 55\% + 1220 \cdot 45\% = 1660 \cdot 10^{-6}$ . Alternatively, we could have considered Zone 1 coverage while constructing the fault tree. Figure 1.6 shows how to include the effects of Zone 1 coverage in a fault tree.

Figure 1.7 introduces a new symbol. The triangle is used as a connector that allows us to reuse “Distance Protection at S Fails” without replicating that portion of the fault tree.



**Figure 1.7: Expanded Fault Tree for Tone/Microwave-Based POTT Scheme Showing Effects of Zone 1 Coverage**

Unavailability, Frequency of Faults, and Cost

If we assume faults occur randomly and independently of protection system failures, then we can interpret unavailability as the likelihood that the system is not available when a fault happens.

Suppose the unavailability to clear faults in the prescribed time is  $2000 \cdot 10^{-6}$ . Suppose our power system has 100 lines and each line faults 10 times per year on the average. The system experiences  $100 \cdot 10 = 1000$  faults per year. The number of faults we expect to occur when the system is

not available is  $1000 \text{ faults per year} \cdot 2000 \cdot 10^{-6} = 2 \text{ faults per year}$  that are not promptly cleared. If actuaries can tell us the cost of one such uncleared fault, then we could find the cost of this level of unavailability and next evaluate the cost benefit of any proposed improvement.

### Analysis Results of Example POTT scheme

The following analysis refers to the results of the last column of Table 1.2: which considers the effects of Zone 1 coverage.

- Adding redundant relays improves unavailability by 24 percent.
- The improvement is limited because other component unavailability, especially the circuit breakers, dominate the fault tree.
- Adding a redundant channel improves unavailability by 23 percent.
- We use a computer-based relay-to-relay communications scheme on a leased telephone line. The fault tree shows that the unavailability of the redundant channel is relatively unimportant. We assume a channel unavailability of  $1000 \cdot 10^{-6}$ , or ten times the unavailability of the microwave channel, and still get a large increase. Improving the redundant channel to an unavailability of  $100 \cdot 10^{-6}$  would not be of any real benefit.
- Unavailability with a dedicated fiber using traditional multiplex/demultiplex units is 13 percent better than with tone gear and a microwave channel.
- Direct relay-to-relay digital communications over a dedicated fiber using relay-powered transceivers improved unavailability by 23 percent.
- Compared to adding a redundant channel, this method not only improves unavailability but also significantly reduces cost. Relay-powered transceivers cost about 1/10th as much as contact-sensing multiplex/demultiplex units.
- Just improving the communications channel using direct relay-to-relay communication improves unavailability about the same amount as redundant relays or a second channel when the first channel is microwave.
- Adding redundant relays with independent communications channels decreases unavailability by nearly half (47 percent). Adding a redundant channel to a scheme that already employs redundant relays improves unavailability by 31 percent.

### Dependability

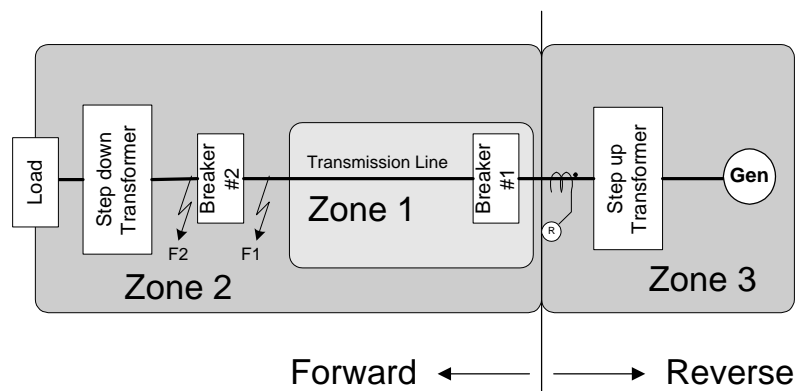
Dependability is the ability to detect and respond to a fault in a correct and timely manner. Dependable operation requires that the fault be detected (sensitivity), that detected faults in the protection zone be differentiated from those outside the protection zone (selectivity), and that the detection and discrimination effort be fast enough to be of value (speed). A completely dependable relay will always trip properly for a detected fault. This degree of dependability is obtained at the expense of an increased probability of operations when not required.

### Sensitivity

Sensitivity is critical to being able to detect high-impedance faults. There are three components to a measurement, accuracy, precision, and resolution. These components are independent qualities of a measurement.

## Selectivity

Selectivity is important for relays to be able to discriminate between load and faults and to distinguish one fault location and/or type from another. Sensitivity, or lack thereof, limits selectivity. Consider the two fault locations on either side of breaker 2, represented by F1 and F2 in the system shown in Figure 1.8. The relay to the right of breaker 1 will not be able to discriminate between the two faults by direct measurements of current and/or voltage alone. For these types of cases, fault discrimination is by time and/or communication. An example of discrimination by time is if faults detected in Zone 2 are delayed. Figure 1.8 also illustrates the concept of overreaching. If the sensitivity of Zone 2 is set too high, the relay at breaker 1 may operate for faults inside the customer's load if the customer's protection is slower than the Zone 2 delay. Figure 1.8 also illustrates discrimination by direction. Zone 3 detects faults to the right of the relay and may be used for backup protection of the transformer and generator or to inhibit other relays from operating.



**Figure 1.8: Sensitivity Limits Selectivity for Faults F1 and F2**

## Speed

Speed is important for limiting exposure and potential damage. The time to clear a fault is mainly determined by two elements, the speed of the circuit breaker and the time it takes for the relay to make the decision. Relay decision time is based on three functions inside the relay. Relay designers determine the time needed for two of these functions, filtering to isolate the 60 Hz information and processing the information to determine the appropriate output. The application engineer determines the third function, the time spent waiting for restraints to be removed from external inputs and which inputs will inhibit or delay outputs.

## Security

Security, in some respects, reflects the sureness of the relay decision. In the area of protective relaying, it refers to the quality of not operating for faults outside the zone of protection or not operating under heavy load conditions.

MAINTENANCE [6047], [6052], [6073], [6060]

Maintenance has two purposes: to repair relays known to be defective and to verify that relays are not defective. Before the advent of microprocessor-based relays, defective devices could only be found by testing or by incorrect operations. The goal of protective relay testing is to maximize the

availability of protection and minimize risk of relay misoperation. With this in mind, we must define adequate test intervals for the various types of protective relaying equipment.

Legacy relays (electrom-mechanical, semiconductor electronic and discrete logic digital relays or combinations thereof) do not provide self-tests or status monitoring, so they require routine testing to verify proper operation. If a problem exists in a legacy relay, the problem may go undetected until routine maintenance is performed or the relay fails to operate for a fault. The reliability of the legacy relay is, therefore, largely dependent on the frequency of routine maintenance.

Computer-based relay failures can also cause relay misoperation and prevent operation for faults. However, relay characteristics are typically not affected by failures. Failures tend to be significant enough to either generate a self-test failure indication or cause the user to recognize the problem during normal relay operation.

### Type Testing

When a utility engineer selects a new relay design, it is essential to test the selected relay to ensure proper operation for the intended application. These tests are referred to as type tests and are usually implemented on a single representative relay from the manufacturer. During type tests, the utility staff is introduced to new relay models and functions. If there are specific application questions, utility staff discusses these questions with the relay manufacturer until there is a clear understanding of all the protective functions. Type tests include detailed tests of the relay characteristics such as mho circle plots, time-overcurrent curve plots, relay element accuracy, etc. The main objective of type tests is verification of the relay algorithms and characteristics.

### Commissioning Testing

Utilities typically require commissioning or installation tests of each relay prior to placing the relay in service. Once the utility accepts the results of the computer-based relay type tests, the requirement for commissioning testing is reduced. The operating characteristics of microprocessor-based relays are consistent, which allows us to rely on the type tests for detailed characteristic tests and focus the commissioning tests on simple tests of the relay hardware.

Computer-based relay commissioning tests may include tests for calibration, input/output functionality, simple element accuracy tests, etc. Commissioning tests should also verify the effectiveness of calculated relay element and logic settings. Greater reliance on type tests for the detailed relay characteristic tests is well justified because those characteristics are fixed in the relay algorithms.

### Routine Maintenance Testing

Routine testing of protective relays has been the primary method of detecting failures in legacy relays. The only other way of determining that a legacy relay has failed is to observe a misoperation. Routine testing is scheduled on the basis of utility experience with the devices in question. However, there is risk involved, both with performing the test and with leaving the relay untested. The goal of routine maintenance is to verify that the protective relay will not operate unnecessarily and will operate when required.

Typically, routine maintenance is performed at specified intervals. A common belief is that a shorter test interval increases overall system reliability. There are limitations to this statement,

however, such as the possibility that a system failure could be introduced while performing routine maintenance. Performing a routine test creates the risk that a functioning relay may be damaged by the tests or may be left in an unserviceable condition following the test.

The time between tests is typically measured in years. If a failed relay does not misoperate in that period, its failure goes unnoticed and not repaired for what may be a significant portion of the testing interval. So, the risk of leaving the relay untested is that it may not operate properly when necessary.

To schedule routine testing, the utility engineer must balance the risk of leaving a failed relay in service versus the smaller risk of damaging a sound relay. Examining the types of problems that can occur in both classes of relays is often helpful for finding problems that might be present. Then examine the types of tests being performed to see if they are exercising the relays in meaningful ways.

### Routine Testing of Traditional Relays

Legacy relays are often built with induction disks or cylinders that turn on jewel bearings. Heavy-duty resistor, inductor, and capacitor networks shape operating characteristics. Springs and levers define operating times. Tests of legacy relays necessarily check the operating characteristics that are affected by the individual components: pickup settings, operating times, and characteristics.

If routine testing detects a problem with a legacy relay, there is no way to know how long the problem has existed. The only date available for reference is the last time the relay was shown to operate properly in a fault record or a test report. The relay could have failed on the day following the last correct operation, on the day before this misoperation, or on any day in between.

### Routine Testing of Digital Relays

Computer-based relays are built using a microprocessor, an ac signal data acquisition system, memory components containing the relay algorithms, contact inputs to control the relay, and contact outputs to control other equipment. Computer-based relay operating characteristics are defined by the algorithms and settings contained in the relay memory.

Computer-based relays are often equipped with automatic self-test functions that verify correct operation of critical relay components. If a self-test detects an abnormal condition, it can close an output contact, send a message, or provide some other indication of the failure. When the alarm occurs, a technician can be dispatched to repair or replace the device quickly.

It is helpful to define the requirements of computer-based relay routine maintenance by dividing the hardware into three categories and specifying maintenance practices that adequately test each section. For the purposes of testing, it is convenient to divide the relay into the following three sections:

- Analog Input Section
- Contact Input/Output Circuitry
- Processing Section

The analog input section is typically monitored by automatic self-testing. This may be somewhat limited because a steady-state condition cannot be fully defined. With a protective relay, there

are often many steady-state conditions possible under each mode of operation. Since the analog input portion of the computer-based relay is only partially self-tested, routine maintenance assists in verification of the analog measuring components.

Many computer-based relays offer metering features that give the user a convenient means of verifying the accuracy of the relay analog input section. The user can verify metering quantities and be assured the relay is using valid data for its relay element computations. This practice is sound if the computer-based relay uses the same measuring circuitry for both metering and relaying. However, if the relay uses separate circuitry for its metering functions, the metering data checks only the components common to both the metering and relaying circuitry.

The contact input/output circuitry is another part of the computer-based relay that allows only partial automatic testing. For this reason, it may be appropriate to implement a routine trip check. Many computer-based relays provide a trip feature that allows the user to locally or remotely trip the relay. The trip check verifies the trip circuit wiring and the integrity of the trip coil. This trip command feature provides a convenient means of tripping the circuit breaker without injecting a simulated fault into the relay. If the relay is routinely operating for faults, the actual relay operations may be adequate verification of the relay input/output functions.

The digital processing section, typically a microprocessor, is the interface between the analog input section and the contact input/output section. Since the analog and contact input/output sections cannot function without the processing section, normal relay use and maintenance checks act as routine verification of the microprocessor. Additionally, manufacturers are able to offer very thorough self-tests to continually monitor the status of the computer.

Utility engineers should work closely with relay vendors to determine which relay functions are not checked by relay self-tests and how those functions should be checked in the field. There are typically no special tests required for the processing section.

Many of the maintenance features are executable by remote command and often could replace routine maintenance altogether. Also, the analysis of computer-based relay fault data is comparable to routine relay maintenance. Those relays that do not encounter faults may require more thorough routine maintenance checks.

Because the computer-based relay provides an indication when a problem occurs, the possibility that a failed computer-based relay could remain in service for a significant amount of time is reduced. If the utility monitors relay self-test alarm contacts, a failed relay can generally be repaired or replaced within hours or days of a failure.

### Digital Relay Data Analysis

As a minimum, computer-based relay self-tests include tests of memory chips, a/d converter, power supply, and storage of relay settings. These periodic self-tests monitor the status of the computer-based relay and close an alarm contact when a failure is detected. Additionally, the computer-based relay may disable trip and control functions upon detection of certain self-test failures. Since the relay self-tests are executed often, component failures are usually discovered when the failure occurs.

Computer-based relays provide event reporting and metering features that supplement routine maintenance. Event reports typically provide a record of each relay operation with the same resolution as the sample rate of the computer-based relay. If testing personnel devote a small percentage of their time to analyzing these fault records, they can find relay problems displayed in the event report data. Analysis of actual fault data is a true test of the instrument rather than a

simulated test. Careful analysis of relay event reports and meter information indicates problems that could otherwise go undetected by computer-based relay self-tests.

Event reports can also indicate problems external to the computer-based relay. Transformers, trip circuits, communications equipment, and auxiliary input/output devices are examples of external equipment that may be monitored indirectly using the event report.

### A Summary of Relay Maintenance Concepts

The features of computer-based relays reduce routine tests to a very short list: meter checks and input/output tests. Routine characteristic and timing checks are not necessary for computer-based relays. Probability analysis shows that relays with self-tests do not need to be routinely tested like relays without self-tests. If the relay is measuring properly, and no self-test has failed, there is no reason to test the relay further.

Use the computer-based relay reporting functions as maintenance tools. Event report analysis should supplement or replace routine maintenance checks of relays with self-tests. Event report analysis increases a tester's understanding of the computer-based relay and of the power system.

Because self-tests quickly indicate the vast majority of relay failures, the MTBF of a computer-based relay does not have a large impact on the power system unavailability. When a relay is equipped with self-tests, the benefit of a high MTBF is that fewer relays need replacement or repair. A high MTBF saves maintenance time and money. Relay self-testing saves routine testing time. When a relay is not equipped with self-tests, a high MTBF and a short test interval are both essential for minimizing system unavailability.

Reducing the complexity and frequency of routine computer-based relay tests saves labor. These labor resources can then be applied to more frequent and complete tests of legacy relays. The result will be higher overall reliability and availability from all relays, both digital and traditional.

---

<sup>i</sup> [6060] E. O. Schweitzer, B. Fleming, T. J. Lee, and P. M. Anderson, "Reliability Analysis of Transmission Protection Using Fault Tree Methods," 51<sup>st</sup> Annual Conference for Protective Relay Engineers, Texas A&M University, College Station, TX, April 6-8, 1998.

<sup>ii</sup> [6073] G.W. Scheer, "Answering Substation Automation Questions Through Fault Tree Analysis," 4<sup>th</sup> Annual Substation Automation Conference, Texas A&M University, University, College Station, TX, April 6-8, 1998.

<sup>iii</sup> [6047] E. O. Schweitzer, J. J. Kumm, M. S. Weber, and D. Hou, "Philosophies for Testing Protective Relays," 20<sup>th</sup> Annual Western Protective Relay Conference, Spokane, WA, Oct. 19-21, 1993.

<sup>iv</sup> J.J. Kumm, E.O. Schweitzer, and D. Hou, "Assessing the Effectiveness of Self-Tests and Other Monitoring Means in Protective Relays," 21<sup>st</sup> Annual Western Protective Relay Conference, Spokane, WA, Oct. 18-20, 1994.

<sup>v</sup> W. E. Vesely, F. F. Goldberg, N. H. Roberts, and D. F. Haasl, Fault Tree Handbook, NUREG-0492m, U.S. Nuclear Regulatory Commission, Washington D.C., 1981.