
**RELIABILITY ANALYSIS OF TRANSMISSION PROTECTION
USING FAULT TREE METHODS**

**E. O. SCHWEITZER, III,
BILL FLEMING, AND TONY J. LEE**

**SCHWEITZER ENGINEERING LABORATORIES, INC.
PULLMAN, WASHINGTON USA**

PAUL M. ANDERSON

**POWER MATH ASSOCIATES
SAN DIEGO, CALIFORNIA USA**

Presented before the

**24th ANNUAL
WESTERN PROTECTIVE RELAY CONFERENCE
SPOKANE, WASHINGTON
OCTOBER 21-23, 1997**

RELIABILITY ANALYSIS OF TRANSMISSION PROTECTION USING FAULT TREE METHODS

E. O. Schweitzer, III,
Bill Fleming, and Tony J. Lee
Schweitzer Engineering Laboratories, Inc.
Pullman, WA USA

Paul M. Anderson
Power Math Associates
San Diego, CA USA

ABSTRACT

Transmission line protective systems are sometimes very complex, incorporating many different equipment groups, often at widely separated places, and often requiring high-speed communications for proper operation. The inherent reliability of such complex systems is a concern of the protection engineer and presents a significant analytical problem. This paper describes the use of fault tree analysis as one method of analyzing the reliability of these complex systems.

INTRODUCTION

Protection engineers consider dependability as the tendency of the protection system to operate correctly for in-zone faults. They consider security as the tendency not to operate for out-of-zone faults. Dependability and security are reliability issues.

This paper introduces a tool with which a protection engineer can easily compare the relative reliability of proposed protection schemes.

Major motivations of quantifying reliability issues include driving the best decision-making on how to improve the system, how to manage dependability versus security tradeoffs, and how to get the best results for the least money. A quantitative understanding is essential in a competitive utility industry.

Since reliability is the reciprocal of failure, and failure is a random event, probabilistic measures are most appropriate, and we apply the laws of probability theory.

For example, suppose the reliability of a device is expressed with a mean-time-between-failure (MTBF) of 100 years. The failure rate is $1/100$ failures per year. And, if a system has 300 of these devices, then we would expect $300 \cdot (1/100) = 3$ device failures per year.

We use the method of combining component failure rates 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 ensuing years [1], is attractive because it does not require extensive theoretical work and is a practical tool that any engineer can learn to use. While computer programs are available to assist in developing and analyzing complex fault trees, this paper shows that small fault trees, which are easily analyzed manually, are also very useful.

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 which has a failure rate of $1/100$ failures per year. It might consist of two components, each with a failure rate of $1/200$

failures 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 satisfactory performance to the device. 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 a device failure.

Fault tree analysis is not the only tool used for reliability studies. Among other techniques, the authors of this paper also have experience using Markov models to compare relative performance of communications-based protection schemes, and to predict optimum routine test intervals for protective relays. (References 2, 3, 4, and 5)

As explained in Reference 4, Markov models cover the entire system of interest. All failure and success modes and transitions are incorporated. The outputs of a Markov model are the probabilities that the system resides in any one of the modeled states. Both normal and abnormal states are modeled. Since the entire system is modeled, model development requires considerable effort, and Markov model analysis typically requires a computer. Markov modeling also assumes that all state transitions are exponentially distributed [1], which is sometimes difficult to justify.

FAULT TREE CONSTRUCTION

A fault tree is tailored to a particular failure of interest and models only that part of the system which 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 which merits investigation. Figure 1 shows a protective system consisting of a circuit breaker, a ct, a relay, a battery, and associated control wiring. One might wonder what the chance is that the protective system will not clear a fault. The fault tree in the figure helps us analyze this chance.

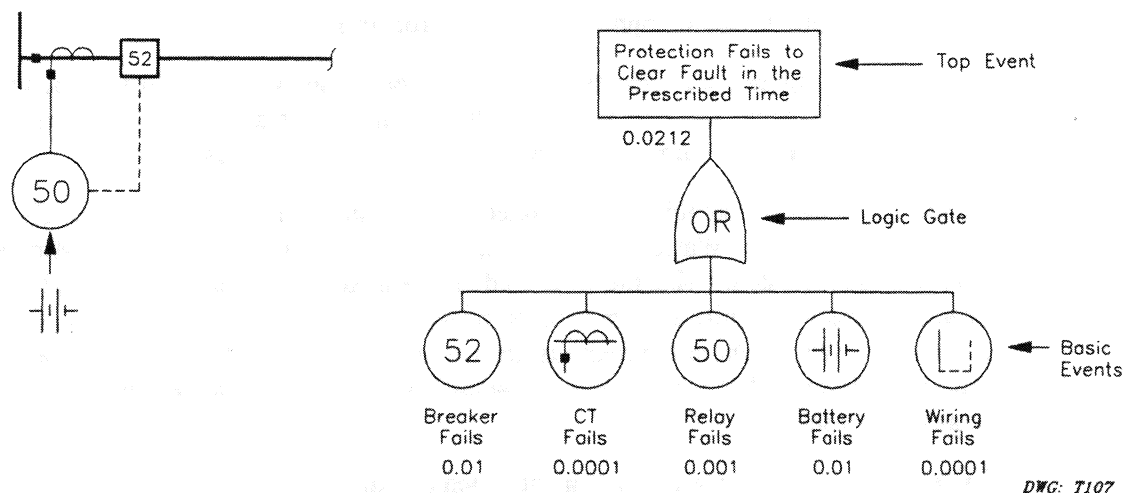
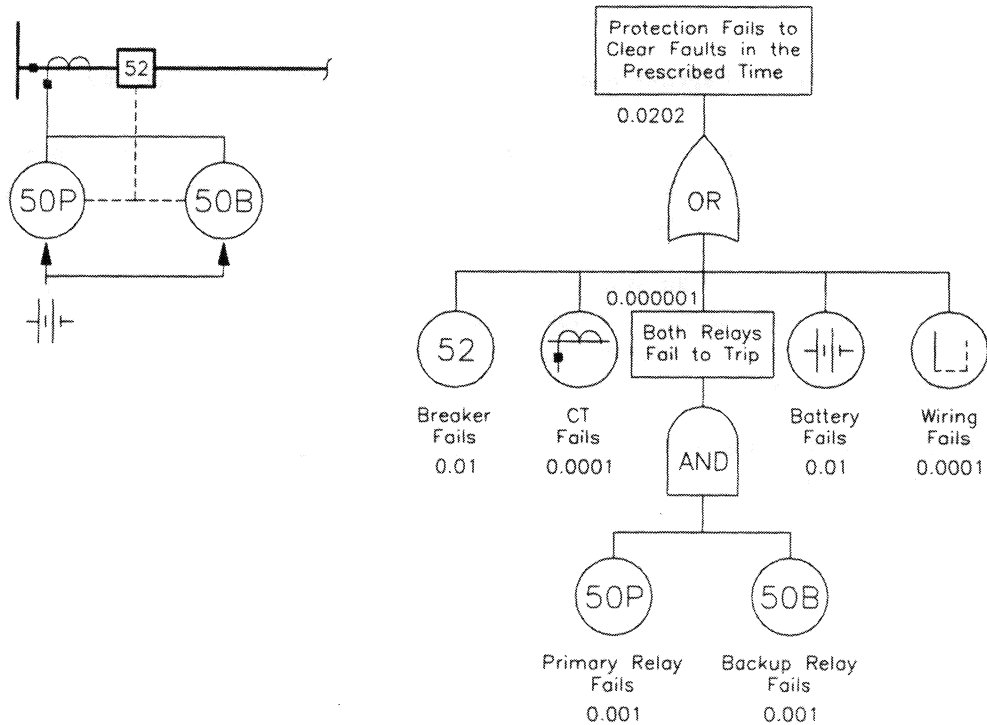


Figure 1: Fault Tree for Radial Line Protection

The Top Event is a box containing a description of the failure event of interest. The selected top event is usually described in terms of what event 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 expresses the idea that any of several failures can cause the protection system to fail. If either 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. Later we will develop more substantiated estimates.) The chance the system will fail to clear a fault is the sum: 0.0212 failures to clear per fault. 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 2 contains an AND gate. This AND gate expresses the idea 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 that of the relay dominate the system.



DWG: T108

Figure 2: Fault Tree for Radial Line Protection With Redundant Relays

There are other gates besides 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 paper.

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 failure rates for the devices, then we need not break the devices into their components. The roots are referred to as basic events.

Fault Tree for a Two-Terminal Line Protected by a POTT Scheme

Figure 3 shows a transmission line with a single circuit breaker and relay at each end. The two relays communicate through tone equipment and analog microwave gear to effect a POTT (Permissive Overreaching Transfer Trip) scheme. Assume that the protection operates from a 125 Vdc battery, and the communications operate from a 48 Vdc battery.

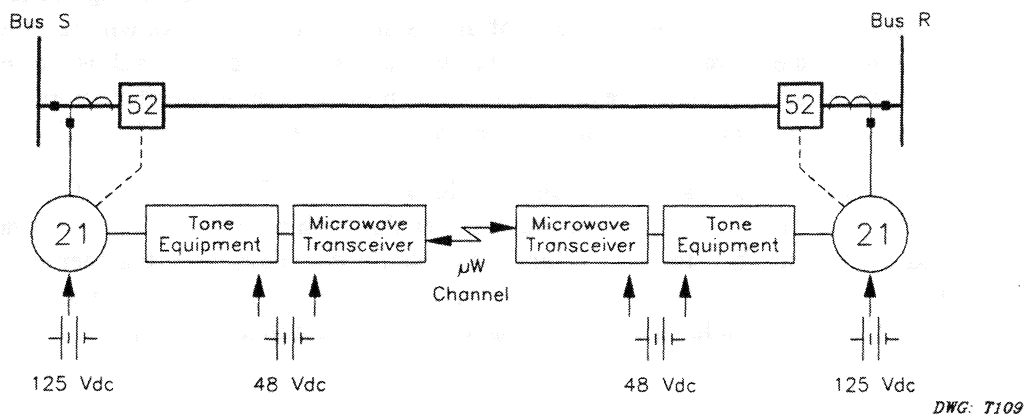


Figure 3: One-Line diagram of a Tone/Microwave Based POTT Scheme

To construct a fault tree for this simple system, we first choose a top event of interest. Let the Top Event be "Protection Fails to Clear In-Section Fault in the Prescribed Time." We are interested in how each component contributes to the Top Event.

Figure 4 is a fault tree for the system in Figure 3. The fault tree contains only OR-gates, so we immediately learn that all devices must function properly to clear in-section faults. Later we will add some redundancy to reduce the number of single point failures or devices which can singly cause the system to fail.

We can use the fault tree to predict a system failure rate once we have some estimates of the device failure rates.

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. Unavailability is the fraction of time a device cannot perform. It is unitless.

Reference 6 describes how to calculate unavailability from a failure rate and the time it takes to detect and repair a failure.

$$q \cong \lambda T = \frac{T}{MTBF}$$

where: q is unavailability
 λ is some constant failure rate
 T is the average down-time per failure

$$MTBF = \frac{1}{\lambda} \text{ is Mean Time Between Failures.}$$

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

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

1. 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 $0.01 \text{ failures/year} \cdot 2 \text{ days} = 0.02 \text{ days/year}$.
2. 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 $1 \text{ year} \cdot 0.01 \text{ failures per year} = 3.65 \text{ days/year}$. This is 183 times worse – so monitoring the alarm contact really pays off!

Reference 4 demonstrates that 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 lost service every two years due to testing is much greater than the expected loss of service due to automatically-detected failures which are promptly (2 days) repaired.

For the purpose of this paper, we have estimated some failure rates, downtimes, and unavailabilities. 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.

Protective Relay

Based on our field experience, an MTBF of 100 years is conservative for modern digital relays of quality design and construction. Our products demonstrate a self-test effectiveness of 80% 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% 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, from 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 due to human error in installing and setting a relay is also $100 \cdot 10^{-6}$.

Claiming relay unavailability due to hardware failures is equal to the unavailability due to 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 1 year to detect and repair and are 100 times less likely than relay hardware failures. In this case, unavailability due to human failures would be:

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

Tone Equipment

Given that tone equipment complexity is similar to that of a relay, we assume the unavailability of these devices is also $100 \cdot 10^{-6}$.

Analog Microwave Equipment

This equipment consists of a transceiver and multiplexing/demultiplexing equipment. Again, based on relative complexity, we estimate unavailability of $200 \cdot 10^{-6}$.

Microwave Channel

The medium between the microwave systems is subject to hard-to-estimate outside influences, including weather, radio-frequency interference, and vandalism. We offer a guess of an unavailability of $100 \cdot 10^{-6}$. (Fortunately, this particular factor has little effect in the overall calculation of scheme unavailability, and is therefore not very critical.)

DC Power System

The system consists of a battery and charger, and distribution circuits which are both inside and outside the control house. Assuming that loss-of-dc alarms are monitored and responded to in less than a day, and that the system is on the order of complexity of a relay, we estimated an unavailability of $50 \cdot 10^{-6}$.

Instrument Transformers

We assumed an MTBF of 500 years, an average protection down time of two days per ct or vt failure, and monitoring by the relays, to get an unavailability of $10 \cdot 10^{-6}$ per phase.

Circuit Breaker

Assume 90% of failures are detected by the usual monitors in the breaker, and in some relays (breaker monitoring, event reporting, trip and close circuit monitoring) and other devices. Another 5% are detected by visual inspections every two months. The remaining 5% are detected by maintenance every two years.

According to Reference 9, circuit breaker reliability increases with decreasing voltage. It cites an MTBF of 83 years for breakers used between 300 kV and 500 kV, increasing to 364 years for breakers used at voltages between 63 kV and 100 kV. We will use an MTBF of 200 years.

$$q = \frac{1}{200 \text{ years}} \cdot \left(\frac{0.90 \cdot 2 \text{ days}}{365 \text{ days/year}} + \frac{0.05 \cdot 1 \text{ month}}{12 \text{ months/year}} + 0.05 \cdot 1 \text{ year} \right) = 295 \cdot 10^{-6}$$
$$q \cong 300 \cdot 10^{-6}$$

Leased Telephone Line

We assumed a leased line is rather unreliable: $q = 1000 \cdot 10^{-6}$.

Minimal Delay Telephone Modem

A very simple audio modem is available, with sufficiently short delays to make it useful for pilot channels. We estimate the MTBF of this device to be in excess of 200 years, and again assume a two-day repair time. This gives an unavailability of $27 \cdot 10^{-6}$. We round to $30 \cdot 10^{-6}$.

Dedicated Fiber-Optic Transceivers

We must separate these into at least two classes.

One class multiplexes contact I/O onto a fiber channel. Its complexity is similar to that of a relay, so we assume an unavailability of $100 \cdot 10^{-6}$.

The other class is a simple transceiver that takes serial digital data directly from the relay, without a contact interface. It is extremely simple in comparison to the former device, so we assume an unavailability of $10 \cdot 10^{-6}$.

Fiber Channels

We will assume an unavailability of $100 \cdot 10^{-6}$, to cover mechanical damage, splices, and connectors.

Table 1 summarizes the unavailabilities noted above in descending order of unavailability.

Table 1: Unavailabilities of Several Protection Components

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

Tabulating component unavailability allows you to quickly see which components are most likely to cause problems. A column showing component price could be added, to shed early light on the economics of the quality problem.

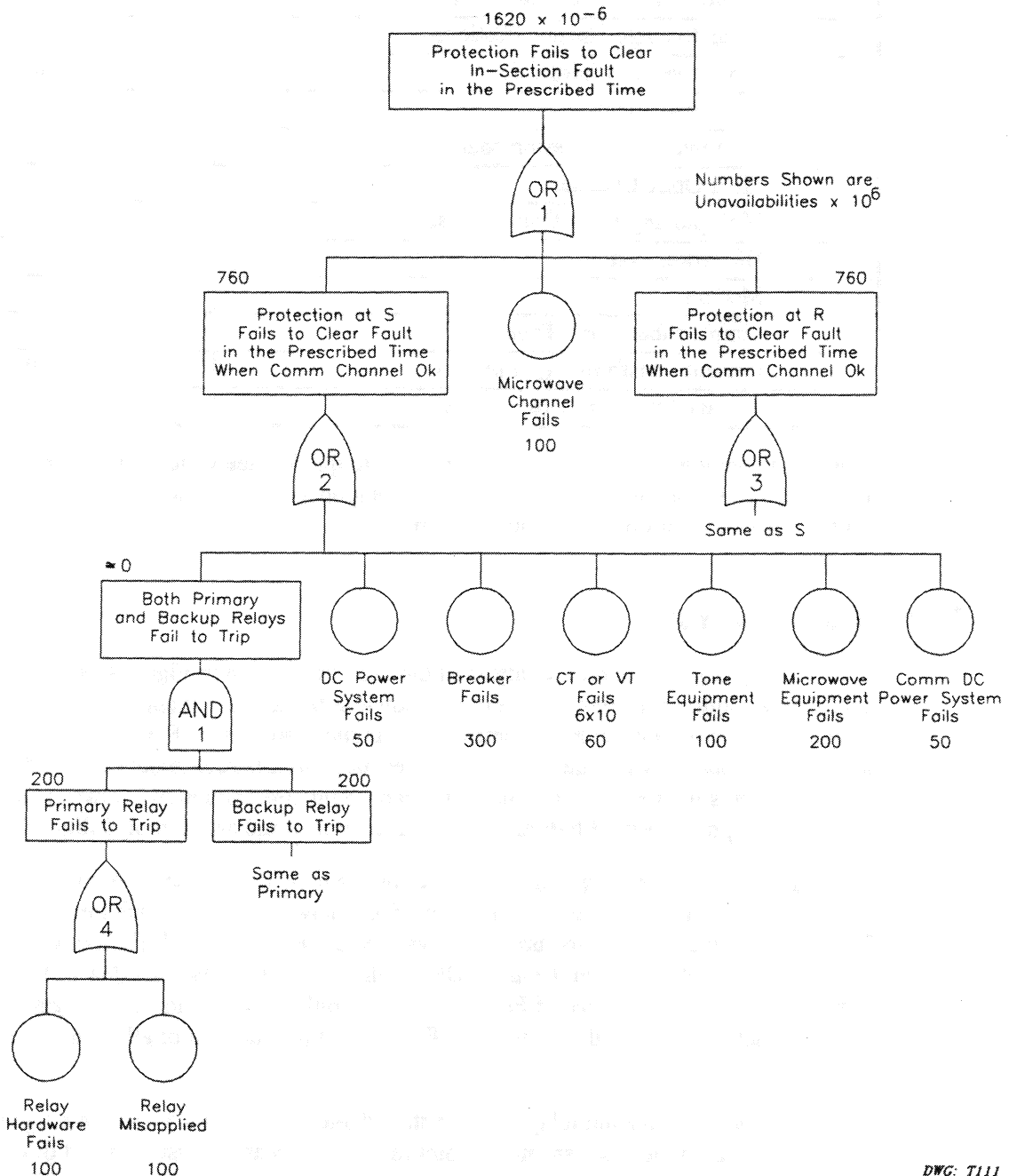
FAULT TREE ANALYSIS

After entering basic event data, analysis of the fault tree shown in Figure 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% 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 When Comm Channel OK" is the sum of the unavailability of the eight inputs to that OR gate. The fault tree of Figure 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 $2020 \cdot 10^{-6}$.

Suppose we add a redundant relay to the system depicted in Figure 3. Assume that 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 5 conveys the idea 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 5. The unavailability of this protection system to clear faults is $1620 \cdot 10^{-6}$.



DWG: T111

Figure 5: Fault Tree for Tone/Microwave Based POTT Scheme With Redundant Relays

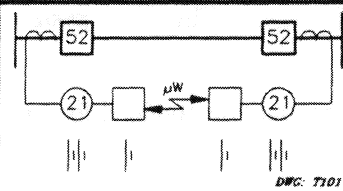
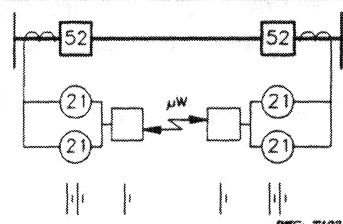
When constructing and analyzing fault trees, keep these simple rules in mind:

1. 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 unavailabilities.
2. Use an AND gate to express a failure caused only when all (usually two) lower level failures occur. The unavailability of a subsystem represented by an AND gate is the product of the device unavailabilities.
3. Use AND gates to express redundancy. Be careful to isolate common causes of failures above the AND gate which expresses redundancy.
4. 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 down-time per failure.

PROTECTION UNAVAILABILITY COMPARISONS

We have already calculated unavailability for two possible protection schemes. The first was a basic POTT 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 are shown in Table 2.

Table 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 Single Channel Microwave	2020	1660
	Redundant Relays Single Channel Microwave	1620	1260

POTT Scheme	Description	Unavailability x 10 ⁶ Ignoring Zone 1 Coverage	Unavailability x 10 ⁶ Considering Zone 1 Coverage
	Single Relay Redundant Channels Microwave and Relay-to-Relay on Leased Line	1320	1275
	Redundant Relays Independent Channels Microwave and Relay-to-Relay on Leased Line	920	875
	Single Relay Single Channel Multiplexed Fiber	1620	1440
	Single Relay Single Channel Relay-to-Relay on Dedicated Fiber	1340	1286

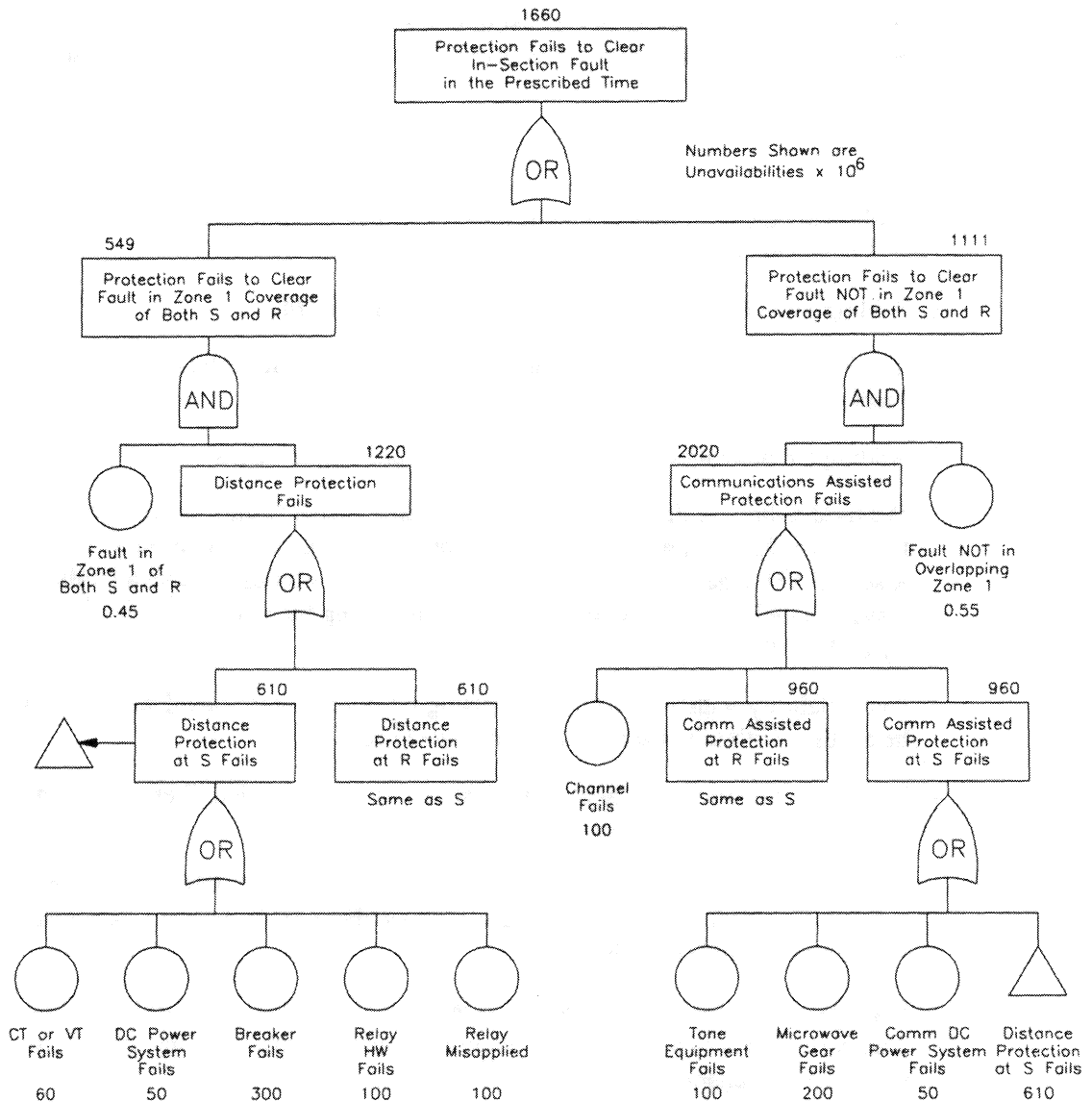
Each row of the table above describes a protection scheme. For instance, the first row describes a protection system consisting of a single relay and breaker with associated cts and vts at each line terminal, communicating via tone equipment and analog microwave gear. This is the system depicted in Figure 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% theoretically cover $100 - 20 - 20 = 60\%$ of the line, independent of the channel. That does not imply the Zone 1 elements cover 60% 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% of the faults have enough resistance to (at least initially) not be detectable by Zone 1, then the apparent 60% coverage drops to $75\% \cdot 60\% = 45\%$. 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% of the faults to the unavailability of the POTT fault tree, and the remaining 45% 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 6 shows how to include the effects of Zone 1 coverage in a fault tree.

Figure 6 introduces a new symbol. The triangle is used as a connector which allows us to reuse "Distance Protection at S Fails" without replicating that portion of the fault tree.



DWG: 7112

Figure 6: Expanded Fault Tree for Tone/Microwave Based POTT Scheme Showing Effects of Zone 1 Coverage

In Table 2, the column titled "Unavailability x 10⁶ Considering Zone 1 Coverage" summarizes the results of considering Zone 1 coverage.

UNAVAILABILITY, THE FREQUENCY OF FAULTS, AND COSTS

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 $1000 \text{ faults per year} \cdot 2000 \cdot 10^{-6} = 2$ faults per year which 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

The following analysis refers to the results of the last column of Table 2 where the effects of Zone 1 coverage are considered.

1. Adding redundant relays improved unavailability by 24%.

The improvement is limited because other component unavailabilities, especially the circuit breakers, dominate the fault tree.

2. Adding a redundant channel improved unavailability by 23%.

We used a digital 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 assumed a channel unavailability of $1000 \cdot 10^{-6}$, or ten times the unavailability of the microwave channel, and still got a big payoff. Improving the redundant channel to an unavailability of $100 \cdot 10^{-6}$ would buy essentially nothing.

3. Unavailability with a dedicated fiber using traditional multiplex/demultiplex units is 13% better than with tone gear and a microwave channel.
4. Direct relay-to-relay digital communications over a dedicated fiber using relay-powered transceivers improved unavailability by 23%.

Compared to 3 above, this method not only improves unavailability but also significantly reduces cost. Relay-powered transceivers cost about $1/10^{\text{th}}$ as much as contact-sensing multiplex/demultiplex units.

5. Just improving the communications channel using direct relay-to-relay communications (as in 4 above), improves unavailability about the same amount as redundant relays or a 2nd channel when the first channel is microwave.
6. Adding redundant relays with independent communications channels decreases unavailability by nearly half (47%). Adding a redundant channel to a scheme which already employs redundant relays improves unavailability by 31%.

7. Schemes using redundant channels have unavailabilities which are relatively unaffected by Zone 1 coverage.

This is because when communications are very reliable, the relays rarely rely on overlapping Zone 1 coverage to clear a fault quickly.

CONCLUSIONS

1. Fault trees allow a protection engineer to compare the relative unavailability of various protection schemes. By keeping the fault trees simple, and employing simplifying assumptions such as the rare event approximation, fault trees can easily be analyzed with hand calculations.
2. Even though the unavailabilities of individual components are approximate, fault tree analysis gives useful "order of magnitude" results.
3. In this paper we considered only POTT protection schemes. Fault tree methods are equally applicable to unblocking or hybrid schemes as described in Reference 5, or to schemes which do not rely on communications.
4. For existing installations which use tone equipment to key permissive trips, unavailability can be improved more than 20% by adding a simple relay-to-relay communications channel, even if that channel is relatively unavailable such as a leased telephone line. This conclusion holds whether the existing protection consists of a single relay, or redundant relays. Reference 5 describes other benefits of relay-to-relay communications.
5. New installations can achieve nearly the same unavailability improvement (over 20%) by either adding redundant relays, or by including relay-to-relay communications via an optical fiber.
6. Fault tree analysis is a critical step in ensuring limited resources are best applied.

REFERENCES

- [1] Hiromitsu Kumamoto and Ernest J. Henley, "Probabilistic Risk Assessment and Management for Engineers and Scientists," 2nd Ed.. IEEE Press, Piscataway, NJ, 1996.
- [2] P. M. Anderson, R. F. Ghajar, G. M. Chintaluri, and S. M. Magbuhat, "A New Reliability Model for Redundant Protective System - Markov Models," IEEE Paper 96 WM 324-4-PWRS, presented at the 1996 PES Winter Meeting, Baltimore, Jan 21-25, 1996.
- [3] E. O. Schweitzer, III, J. J. Kumm, M. S. Weber, and D. Hou, "Philosophies for Testing Protective Relays," Proceedings of the 20th Annual Western Protective Relay Conference, Spokane, WA., October 19 - 21, 1993.
- [4] John J. Kumm, Edmund O. Schweitzer, III, and Daqing Hou, "Assessing the Effectiveness of Self-Tests and Other Monitoring Means in Protective Relays," Proceedings of the 21st Annual Western Protective Relay Conference, Spokane, WA., October 18 - 20, 1994.

- [5] Edmund O. Schweitzer, III, and John J. Kumm, "Statistical Comparison and Evaluation of Pilot Protection Schemes," Proceedings of the 23rd Annual Western Protective Relay Conference, Spokane, WA., October 15 - 17, 1996.
- [6] N. H. Roberts, W. E. Vesely, D. F. Haas, and F. F. Goldberg, "Fault Tree Handbook" NUREG-0492m U.S. Nuclear Regulatory Commission, Washington, DC, 1981.
- [7] Military Handbook, "Reliability Prediction of Electronic Equipment," MIL-HDBK-217F, 2 December 1991.
- [8] J. B. Fussell, "Generic Techniques in Systems Reliability Assessment" E. J. Henley, and J. W. Lynn, eds., Noordhoff, Leyden, 1976.
- [9] Canadian Electricity Association, Report 485 T 1049, "On-Line Condition Monitoring of Substation Power Equipment Utility Needs," December 1996.