Using Fault Tree Analysis to Evaluate Protection Scheme Redundancy

Ramón Sandoval and César A. Ventura Santana, *Comisión Federal de Electricidad, Mexico*
Héctor J. Altuve Ferrer, Ronald A. Schwartz, David A. Costello, Demetrios A. Tziouvaras, and David Sánchez Escobedo, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—In this paper, we apply fault tree analysis to compare the dependability and security of transformer and generator protection schemes with different degrees of redundancy. We also compare the scheme costs. For each scheme, we use a single protection scheme as the reference. We then evaluate schemes with dual redundancy and two-out-of-three voting schemes. We also evaluate the effect of comprehensive commissioning testing, hidden failures, and common-mode failures, as well as using relays from the same or different manufacturers in redundant schemes.**

I. Introduction

In a redundant protection scheme, all of the components except the breaker are redundant. Breaker failure protection provides a functional duplication of the breaker. Redundant scheme design must consider both aspects of reliability: dependability and security. Dual-redundant schemes enhance dependability because two independent schemes operating in parallel are less likely to fail to clear a fault. However, dual-redundant schemes can also reduce security because there are two schemes that could operate for an out-of-zone fault. A fully redundant two-out-of-three voting scheme enhances security without impairing dependability. However, such a scheme would be very expensive, considering the cost of dc power systems, channels, and instrument transformers. Sharing these scheme components affects the voting scheme dependability and security. In addition, voting schemes are more complex than dual-redundant schemes and require redundant relays to have similar sensitivities to ensure the operation of at least two of the three relays.

In the past, protection schemes were composed of several discrete relays, with each relay performing a single function. These traditional multirelay schemes provided no redundancy. Today, microprocessor-based relays provide many protection functions. One relay can replace a whole scheme of discrete relays at a much lower cost. Adding a multifunction relay provides redundancy, without significantly increasing cost.

Fault tree analysis is a practical tool for system reliability evaluation. Engineers can use fault tree analysis to compare the relative reliability of proposed protection schemes. Analyzing protection scheme dependability and security requires different fault trees. When constructing each tree, the protection engineer identifies which component failure causes a failure to trip or an undesired trip. This analysis leads to different tree topologies and different unavailabilities or failure rates.

In this paper, we compare the dependability and security of transformer and generator protection schemes with different degrees of redundancy. We also compare the scheme costs. We start from a single protection scheme and add equipment to create dual- and triple-redundant (with two-out-of-three voting logic) schemes. We also evaluate how comprehensive commissioning testing, hidden failures, common-mode failures, and the use of relays from the same or different manufacturers influence scheme reliability.

II. Reliability Concepts

Reliability is the ability of an item to perform a required function under stated conditions for a stated period of time. Reliability and related variables are time-dependent probability quantities. In many applications, reliability analysis using time-independent quantities provides results that are approximate but still of practical value. Table I defines the measures often used to describe product reliability performance, assuming constant failure and repair rates [1].

TABLE I
COMMONLY USED RELIABILITY MEASURES

Measure	Definition
Failure	Termination of the ability of an item to perform its required or specified function.
Failure rate (λ)	Total number of failures divided by total unit operating time or uptime. Data are collected from field observations or tests.
Repair rate (μ)	Total number of repairs divided by total unit operating time or uptime.
Mean time to failure (MTTF)	Average time between start of operation or return after repair and failure. For a constant failure rate, MTTF = λ^{-1}.
Mean time to repair (MTTR)	Average time to correct a failure and restore a unit to operating condition. Includes preparation, active maintenance, and logistics time. For a constant repair rate, MTTR = μ^{-1}.
Mean time between failures (MTBF)	Average time between failures for units repaired and returned to use.

MTBF is the sum of MTTF and MTTR. Because MTTR is usually small compared to MTTF, we assume that MTBF is approximately equal to MTTF and that MTBF = λ^{-1}.

Protective relays and protection systems are designed to be repairable. Therefore, measures of reliability should include the possibility of failure and repair. Availability is a measure that considers repeated cycles of failure and repair.

Availability is the probability or fraction of time that a device or system is able to operate. Equation (1) defines availability A for constant failure and repair rates.

$$A = \frac{\mu}{\lambda + \mu} = \frac{MTTF}{MTTF + MTTR} \approx \frac{MTBF}{MTBF + MTTR} \quad (1)$$

Relay users are often concerned with the amount of annual downtime that may occur in a protection system. Unavailability is the probability or fraction of time a device or system is unable to perform its intended function. Equation (2) defines unavailability U for constant failure and repair rates.

$$U = 1 - A = \frac{\lambda}{\lambda + \mu} = \frac{MTTR}{MTBF} \approx \lambda \, MTTR \quad (2)$$

From (2), observe that we can lower unavailability by decreasing the MTTR (monitor the self-testing of microprocessor-based relays, and keep spares in stock). We can also lower unavailability by increasing the MTBF (use equipment with low failure rates and robust designs).

As probabilities, availability and unavailability are dimensionless numbers from 0 to 1. However, we can convert them to minutes or seconds per year by multiplying by the appropriate factors.

III. Protection Scheme Redundancy

Protection systems consist of devices that detect faults on the power system (protective relays) and apparatus that interrupt fault current (circuit breakers) [1] [2]. In some cases (fuses and automatic circuit reclosers), both functions are combined.

The protection system design philosophy for responding to the failure to detect faults and the failure to interrupt faults is generally in one of two categories [1]:

- Redundant systems.
- Overlapping relays tripping different interruption devices (remote backup protection).

Redundant protection systems use redundant components to eliminate single points of failure for detecting faults. Redundant systems are typical in transmission lines of networked systems, because relays are less able to detect faults in adjacent zones and because the result of delayed tripping is more severe Redundant protection system are increasingly used in large transformers and generators.

A redundant protection system may include the following:

- Redundant primary relays.
- Redundant communications channels.
- Redundant instrument transformers or separate voltage secondary circuits for each set of primary relays.
- Redundant dc control power systems.
- Breakers with redundant trip coils.

A breaker failure protection scheme covers failure of the breaker to interrupt the fault.

The application of redundant systems is now economical at all voltage levels because of the low cost of modern multifunction relays and the elimination of most other equipment by using the ancillary features of these relays. Redundant system architecture actually reduces the complexity of many tasks, such as coordination and designing to eliminate single points of failure. It also enables the design of continuous self-testing features that reduce the chance of hidden failures and eliminate most periodic maintenance and inspection [2].

Redundant protection systems may include dual or triple sets of relays. Dual-redundant schemes typically use OR tripping logic to ensure fault clearing. This bias toward dependability comes from the assumption that delayed fault clearing may be more dangerous to the power system than tripping healthy power system elements. However, modern power systems operate close to their security limits. For example, an undesired trip of a heavily loaded transmission line, or a large generating unit or transformer, may cause transient stability problems or trigger a cascading breaker-tripping event. Several large power system blackouts have been triggered or compounded by undesired line and/or generator tripping. In protection systems with three sets of relays, two-out-of-three voting logic is an alternative to improve security. Some wide-area protection schemes, where an undesired trip may have devastating consequences for the power system, use two-out-of-three voting schemes.

Redundant protection systems may use identical or different relays. Some engineers consider that using relays with different operation principles and hardware platforms reduces the risk of incorrect operations caused by common-mode and hidden failures [3]. As a consequence, some of them recommend using relays from different manufacturers. However, modern multifunction relays allow the application of different protection principles even with identical relays. In addition, the same manufacturer usually provides similar protection functions in different relays (different hardware platforms). Some utilities use two different relays from the same manufacturer in redundant systems. Furthermore, relay manufacturers use many common types of components from the same suppliers. Finally, the probability for the same component to fail at the same time in two identical (or different) relays is very low.

Many industries requiring high reliability use dual-redundant systems with identical components. The aviation industry is one example [4].

Increasingly, utilities and other electric power users are adopting the redundant system approach of the aviation industry. According to an independent survey, 55 percent of utilities in the United States and Canada use the same manufacturer in dual primary systems for high-reliability protection designs [5].

Historically, utilities provided dual-redundant primary protection by applying two electromechanical relays with different operating principles for protection either by zone or by phase. Today, each primary system can include different principles of operation: line differential and directional comparison primary protection, for example, complemented by breaker failure protection and distance and/or directional overcurrent backup protection.

Using identical relays in a dual primary protection system provides the following advantages [1]:

- Two identical systems allow engineers to design one system and use it twice—lower settings labor, higher settings reliability, and lower incidence of human error.
- Common designs, algorithms, and settings ensure optimum protection coordination.
- Common automation and integration simplify architecture and reduce cost.
- A common operator interface makes system operators more comfortable.
- Personnel can analyze data with the same skills and tools.
- Personnel can train in depth on one relay instead of having to learn how to use two relays for the same purpose.
- Troubleshooting is simpler because it is easier for users to compare the reports of two identical relays for the same fault.

IV. Fault Tree Analysis

Fault tree analysis is a practical tool for evaluating how a component failure contributes to a specific failure event [1] [6]. Fault tree analysis is useful for comparing the relative reliability of proposed protection schemes. It is appropriate for considering the top-down reliability performance of a system for specific failure events.

The failure event of interest is called the top event. A system may have more than one top event that merits investigation. The failure rate for the top event is a combination of the failure rates of the basic events (the tree roots) that contribute to the top event. Basic events are individual component failures with identified failure rates. We use AND, OR, and other gates to represent combinations of failure rates. OR gates express the idea that any of several failures can cause the protection system to fail. The OR gate output is the sum of the failure rates of the input events. AND gates express the idea that failures must occur simultaneously to cause the protection system to fail. The AND gate output is the product of the failure rates of the input events. We can also use availability, unavailability, or MTBF figures instead of failure rates in fault tree analysis.

The power system performance requirements (preserving transient stability, for example) determine the top event of the fault tree. If, for example, the power system requires high-speed fault clearing to preserve transient stability, the top event should only consider high-speed protection. However, if the power system remains stable after a breaker failure protection operation, the top event should also consider breaker failure protection.

Fault tree analysis helps in analyzing the security or dependability of a protection system. Security is the ability of a system to never trip for an out-of-zone fault or when no fault is present. Dependability is the ability of a system to never fail to clear an in-zone fault.

Analyzing the dependability and the security of a protection system requires different fault trees. For constructing each tree, we should identify which component failures may cause a failure to trip (a dependability problem) or an undesired trip (a security problem). This analysis leads to different tree topologies and different failure rate (or unavailability) values. For example, any relay failure could cause a failure to trip if a fault occurs during the relay downtime. However, not all relay failures cause an undesired trip. Hence the relay failure rate or unavailability value to use for dependability analysis is higher than the value to use for security analysis.

In this paper, we use unavailability for dependability fault trees because failures to clear faults depend on component downtime per failure. We use failure rate for security fault trees because undesired trips typically occur at the instant a component fails [7].

Fault trees allow comparing the relative unavailability of various protection schemes. By keeping the fault trees simple and making simplifying assumptions, engineers can analyze the fault trees easily with hand calculations. The advantages of fault tree analysis include the following [1]:

- While the failure rate or unavailability data of individual components are approximate, some are substantiated by field measurements, so fault trees give useful order-of-magnitude results.
- With different top events and fault trees, engineers can easily evaluate dependability-related failures versus security-related failures.
- Fault tree analysis is a critical step in ensuring the best application of limited engineering resources.

V. Transformer Protection Evaluation

A. Transformer Protection Schemes

In this paper, we compare the reliability of three schemes for protecting a delta-wye transformer with single breakers at both sides. All schemes use multifunction transformer relays with only current inputs.

Fig. 1a shows the single protection scheme, which includes one relay, one set of current transformers (CTs) on the transformer high-voltage (HV) and low-voltage (LV) sides, one dc power system, and breakers with single trip coils. Fig. 1b shows the dual-redundant protection scheme, which includes two relays, two sets of CTs on each side of the transformer, two dc power systems, and breakers with redundant trip coils. The scheme has only one CT on the transformer neutral grounding conductor, but we also evaluate the effect of adding another CT to the neutral circuit. To create a two-out-of-three voting scheme, we add a third relay to the Fig. 1b scheme, connected to the same CTs and the same dc power system as one of the other two relays. In redundant schemes, we assume all the redundant components are of similar quality. We assume relays have the same reliability indices, sensitivities, and speeds of operation.

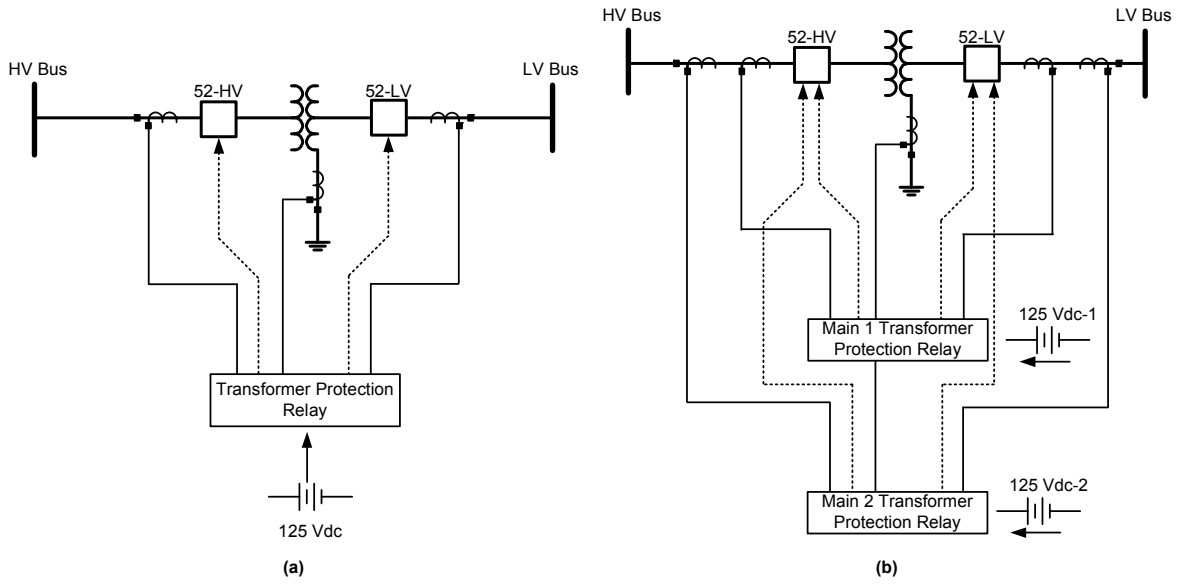

Fig. 1. Single and dual-redundant transformer protection schemes using multifunction relays.

B. Fault Tree Analysis

We created 24 fault trees (12 for dependability analysis and 12 for security analysis) for the following combination of transformer protection schemes and other factors:

- Single scheme.
- Dual-redundant scheme with two neutral CTs.
- Dual-redundant scheme with one neutral CT.
- Dual-redundant scheme with relays from different manufacturers.
- Dual-redundant scheme that experiences common-mode failures.
- Redundant two-out-of-three voting scheme.

For each of these schemes, we created a fault tree that considers the normal process of commissioning testing of the protection scheme and another fault tree that reflects the effect of comprehensive commissioning testing. Reference [8] describes a process with a checklist for consistent and thorough commissioning tests. Reference [9] reviews best practices and provides a list of lessons learned from commissioning protective relay systems.

Table VI in the appendix shows the reliability indices that we used in the fault trees and includes an explanation of the method we followed to determine each value.

We describe several fault trees in this section and then summarize the results obtained from all the fault trees in Table II in the next section.

1) Single Schemes

Fig. 2 shows the dependability fault tree for the single scheme (see Fig. 1a). The top event is "protection fails to clear an in-zone fault," which means that this fault tree considers only protection for faults inside the differential zone defined by the CT location. We assume the relay provides differential and restricted earth fault (REF) protection functions [1]. The basic events considered in this fault tree are: relay failures, relay application or settings errors, breaker failures, dc power system failures, CT failures, dc system and CT wiring errors, and hidden failures. We assign to these events the unavailability values shown in Table VI in the appendix. In this fault tree, the OR gate reflects the fact that, in a single protection scheme, the failure of any component causes a scheme failure to clear a fault. We can modify the fault tree as required to consider other scheme configurations, to include other events of interest, or to use other unavailability values.

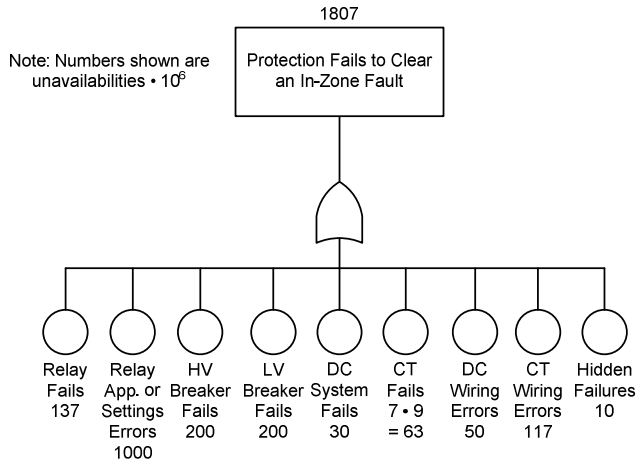

Fig. 2. Dependability fault tree for the single transformer protection scheme.

According to [9], we include in a separate fault tree the effect of comprehensive commissioning testing by modifying, as explained in the appendix, the unavailabilities corresponding to the following:

- Relay application or settings errors.
- DC power system failures.
- DC wiring errors.
- CT wiring errors.
- Hidden failures.

Fig. 3 shows that comprehensive commissioning testing reduces the single scheme unavailability from 1,807 • 10^{-6} to 821 • 10^{-6}, a significant improvement.

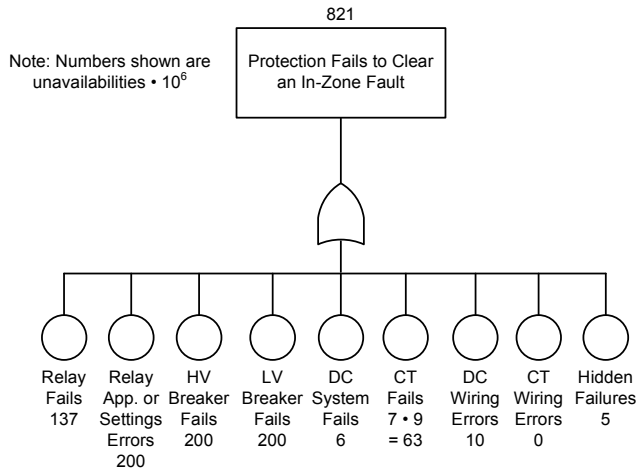

Fig. 3. Effect of comprehensive commissioning testing on the dependability fault tree for the single transformer protection scheme.

Fig. 4 shows the security fault tree for the single scheme. The top event is "protection produces an undesired trip." This security fault tree considers the same events as the corresponding dependability fault tree shown in Fig. 2 but uses the security failure rates shown in Table VI in the appendix.

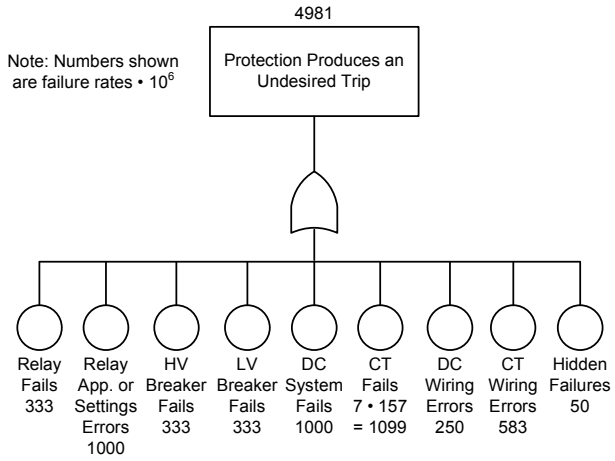

Fig. 4. Security fault tree for the single transformer protection scheme.

2) Redundant Schemes

Fig. 5 depicts the fault tree for the dual-redundant transformer protection scheme, which results from adding a second neutral CT to the scheme shown in Fig. 1b. The AND gate reflects the fact that the failure of any redundant component does not cause a failure to clear a fault. The inputs to this gate have slightly different values because, in a scheme with relays from the same manufacturer, we assign slightly different unavailabilities to relay application and settings errors, as explained in the appendix. The multiplication of unavailabilities reduces the output of the AND gate to a value close to zero. We can modify this fault tree as required to represent systems with lower redundancy (single neutral CT or dc power system or breaker trip coil, for example).

In the fault tree shown in Fig. 5, we assume the breakers to have redundant trip coils, so we split the breakers into two parts. We represent breaker trip coil failures or dc circuit fuse operations at the basic level (under OR Gate 1). Their contribution to a failure to clear the fault is practically eliminated by the AND gate. If the trip coils operate correctly, a breaker failure to interrupt current (a stuck contact mechanism or a failure of the contacts to extinguish the arc) will cause a failure to clear the fault, no matter the redundancy of the scheme. Hence we represent breaker failures to interrupt current above the AND gate in Fig. 5 as inputs to OR Gate 2. Because the other input to this OR gate has a very low unavailability value (because of redundancy), the breaker failures to interrupt current become the dominant factor in the scheme dependability. This fact emphasizes the importance of good breaker maintenance and monitoring and the need for breaker failure protection. A more expensive solution would be to install two breakers in series in a critical system.

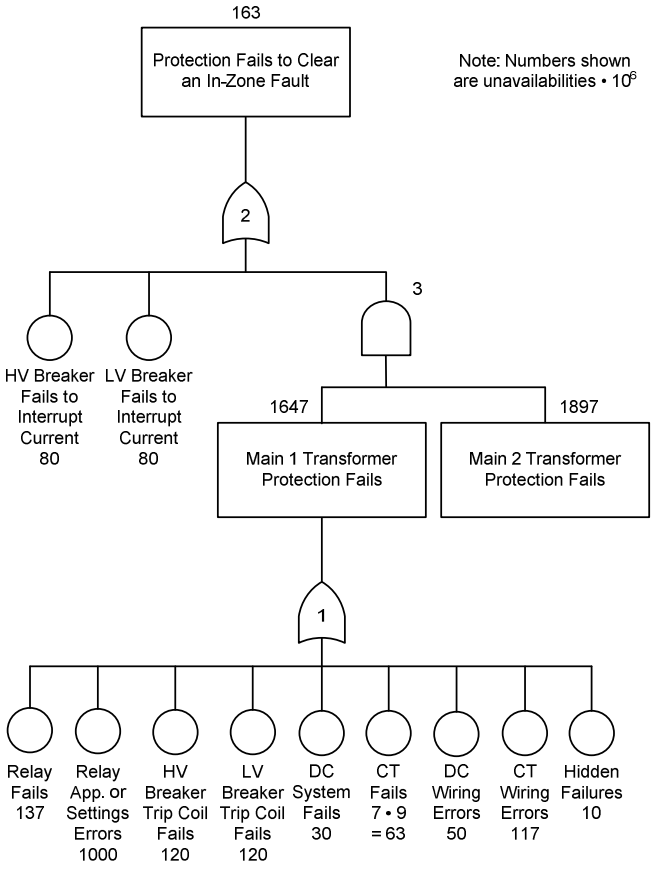

Fig. 5. Dependability fault tree for the dual-redundant transformer protection scheme, using relays from the same manufacturer.

Fig. 6 depicts the fault tree for the dual-redundant transformer protection scheme with only one neutral CT (see Fig. 1b), which is a typical scheme. All the scheme components are redundant, except the neutral CT, which constitutes a single point of failure for the scheme. Neutral CT failures affect REF protection, but not differential protection.

The right side of the Fig. 6 fault tree represents the differential protection. The output of OR Gate 2 is the unavailability value resulting from differential protection failing to operate. We multiply this value by 0.9 under the assumption that differential protection detects 90 percent of all internal faults (AND Gate 2). The output of AND Gate 2 is an input to AND Gate 5, which represents differential protection redundancy. AND Gate 5 practically eliminates the contribution of differential protection to the top event.

The left side of the Fig. 6 fault tree represents the REF protection. We represent neutral CT failures and neutral CT wiring errors as inputs to OR Gate 3. We multiply the value of the OR Gate 3 output by 0.1 (AND Gate 3) under the assumption that ground low-current faults (detected only by REF protection) represent 10 percent of all transformer internal faults. The output of OR Gate 1 represents all the other events that affect REF protection. This output does not include the contribution of the phase CTs connected on the transformer delta side because REF protection does not use currents from the delta side. We use the output of OR Gate 1 (represented by the triangle symbol) multiplied by 0.1 in AND Gate 1 as an input to AND Gate 4. This AND gate, which represents protection redundancy, practically eliminates the contribution of this part of REF protection to the top event. The single neutral CT represents the greatest contribution of REF protection to the top event. Adding a second neutral CT moves the failure events related to this CT to the lowest level in the fault tree, as shown in Fig. 5.

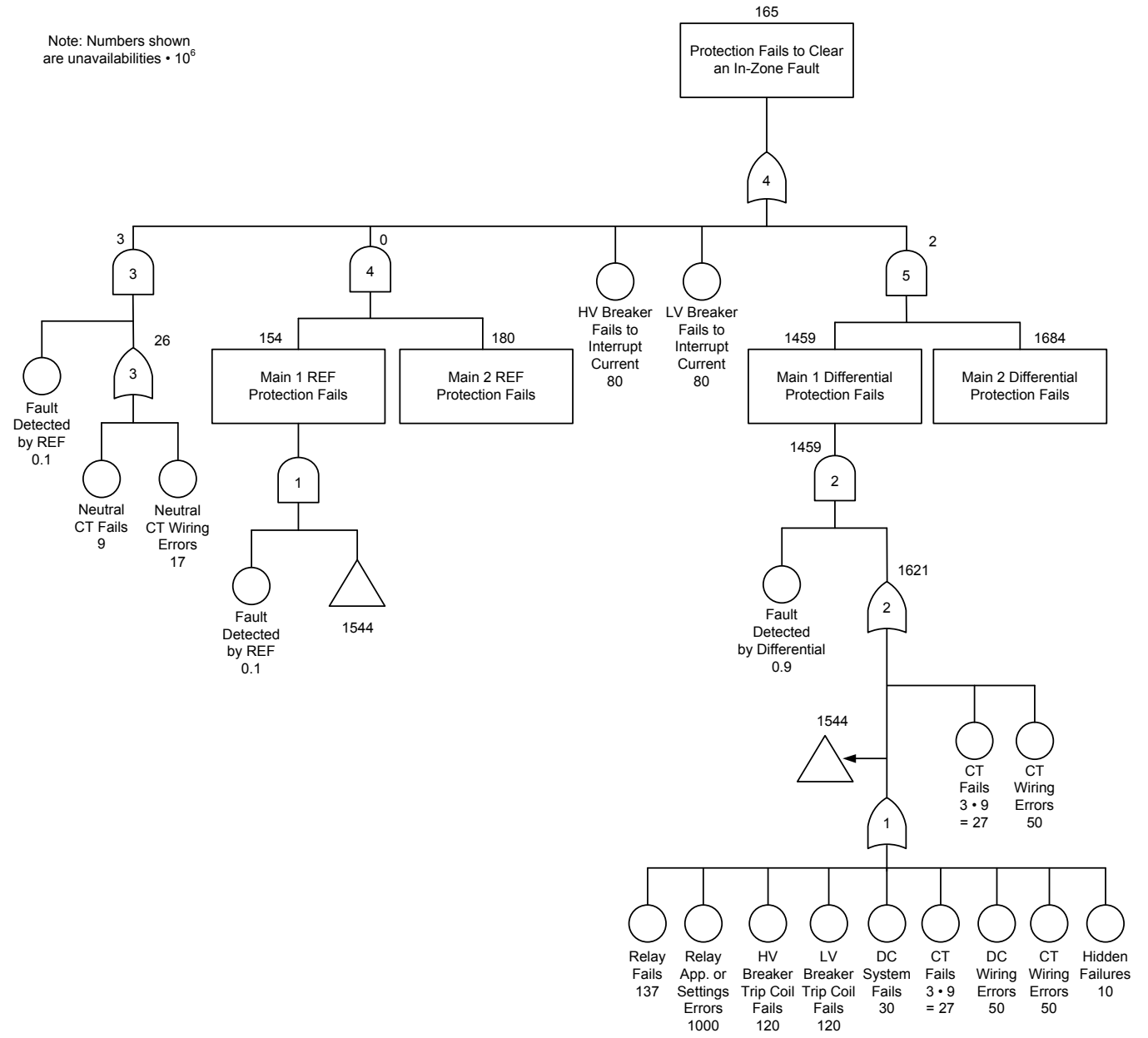

Fig. 6. Dependability fault tree for the dual-redundant transformer protection scheme with one neutral CT.

The topology of the fault tree for the dual-redundant scheme using relays from different manufacturers is identical to that of Fig. 5. In this fault tree, we use a higher unavailability value for relay application and settings errors than for the case of relays from the same manufacturer, as explained in the appendix.

Fig. 7 represents the effect of common-mode failures on the dependability of the dual-redundant transformer protection scheme. To create this fault tree, we started from the Fig. 5 fault tree and added the common-mode failures at the same level as breaker failures to interrupt current. We split common-mode failures into two types: failures that result from the hardware or firmware of two devices failing simultaneously and those that result from common errors in device settings or in system design.

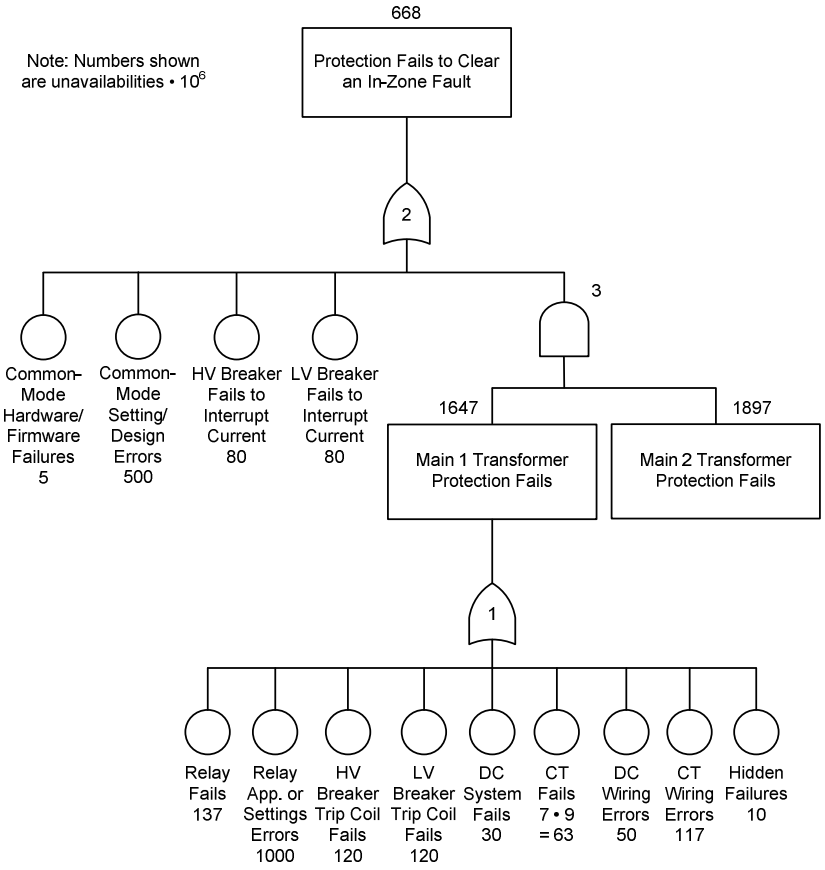

Fig. 7. Dependability fault tree for the dual-redundant transformer protection scheme, considering common-mode failures.

Fig. 8 shows the security fault tree for the dual-redundant transformer protection scheme. OR Gate 2 reflects the effect of redundancy: any of the two schemes may cause an undesired trip. The result is lower security (a higher failure rate) than that of the single scheme (see Fig. 4).

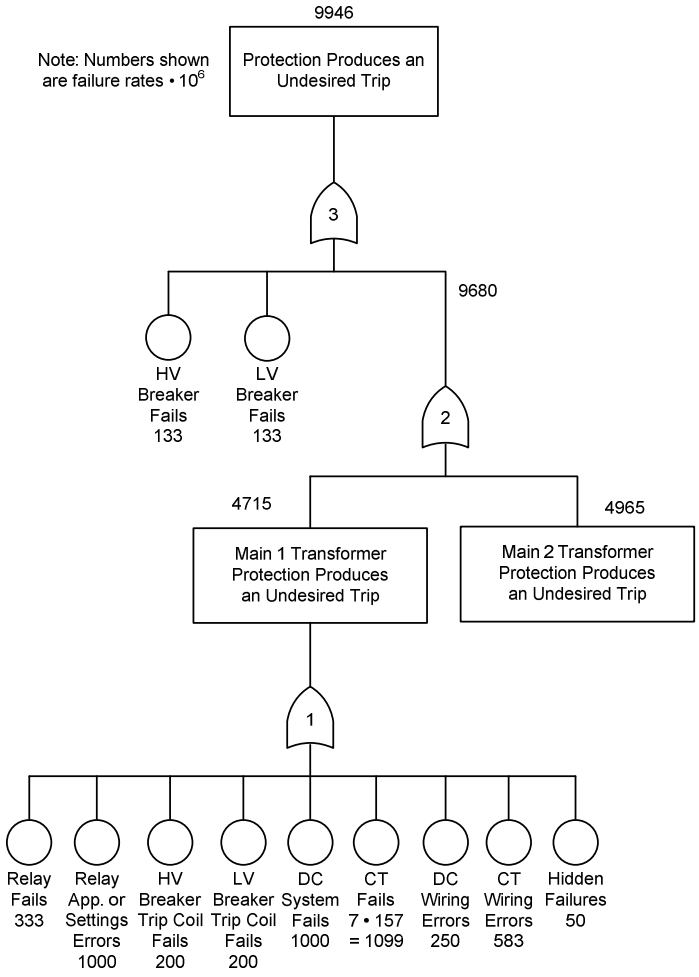

Fig. 8. Security fault tree for the dual-redundant transformer protection scheme.

Fig. 9 shows the dependability fault tree for the two-out-of-three voting transformer protection scheme. The scheme has three multifunction relays. Tripping occurs when at least two of the relays operate. The effect of the voting logic is that the output of AND Gate 3 is practically zero. A fully redundant voting scheme (having three sets of each scheme component) would have a very high dependability, only limited by the breaker failures to interrupt current [10]. However, in Fig. 9, we assume that two of the schemes (referred to as Main 2 and Main 3) share the dc power system and the CTs. The shared components become single points of failure for the Main 2 and Main 3 schemes. When one of these components fails, both schemes fail simultaneously and the voting scheme fails to clear the fault. For this reason, we represent dc power system failures, CT failures, and CT wiring errors at the same level as breaker failures to interrupt current, as inputs to OR Gate 3. The result is lower dependability (a higher failure rate) than in a fully redundant voting scheme. We keep dc system wiring errors at the lowest level in the fault tree because we assume that dc circuits for the Main 2 and Main 3 schemes are independent even with a common battery. We keep breaker trip coil failures at the lowest level in the fault tree because we assume that the voting scheme is arranged to energize both breaker trip coils [10]. In this analysis, we assume the three schemes have the same sensitivity. If the schemes had different sensitivities (because of different settings, principles of operation, or manufacturers) and if two of the schemes did not detect a high-resistance in-section fault, the two-out-of-three voting scheme would fail to clear the fault. For this reason, we recommend that voting schemes use relays with the same sensitivity.

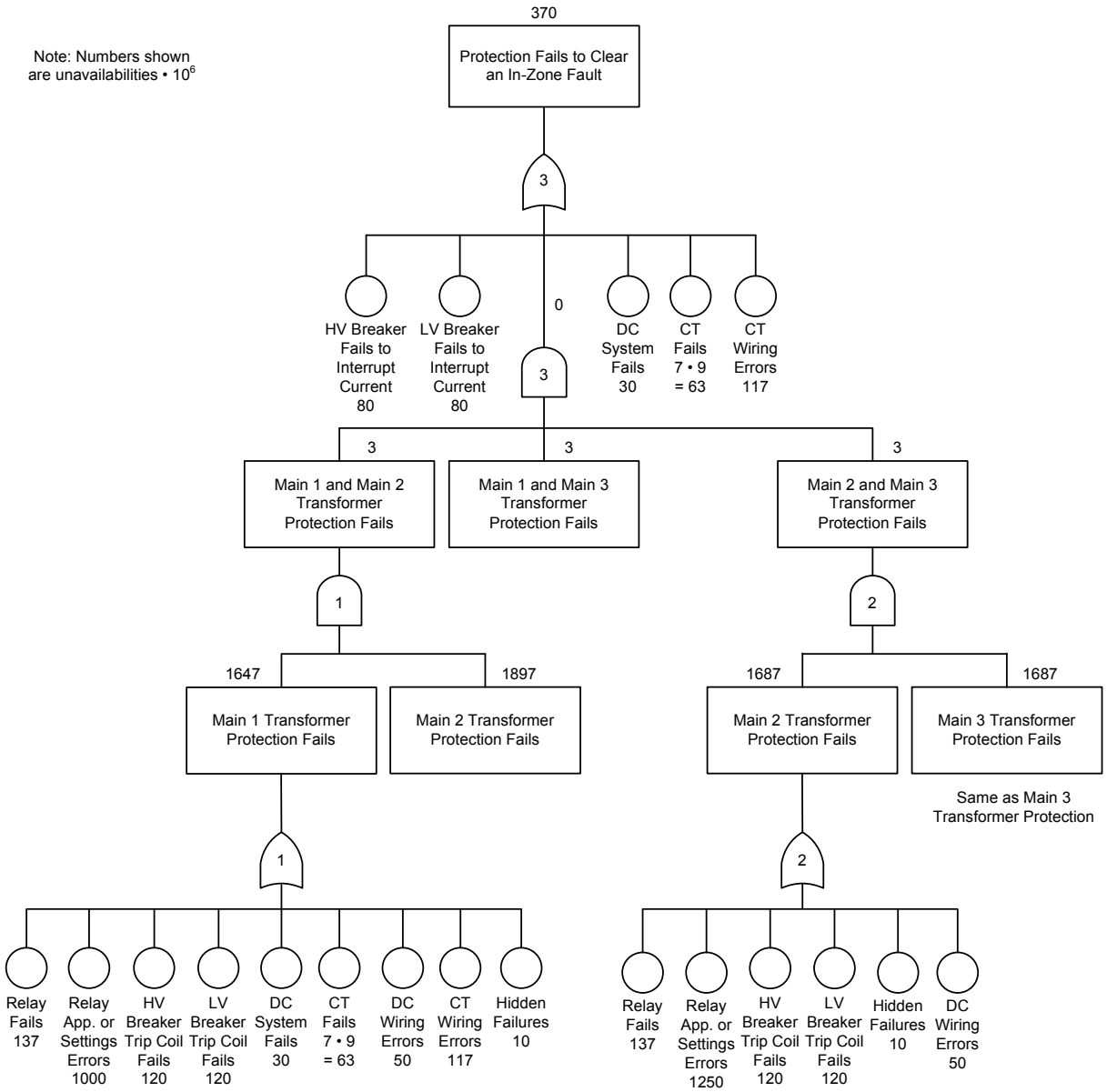

Fig. 9. Dependability fault tree for the two-out-of-three voting transformer protection scheme.

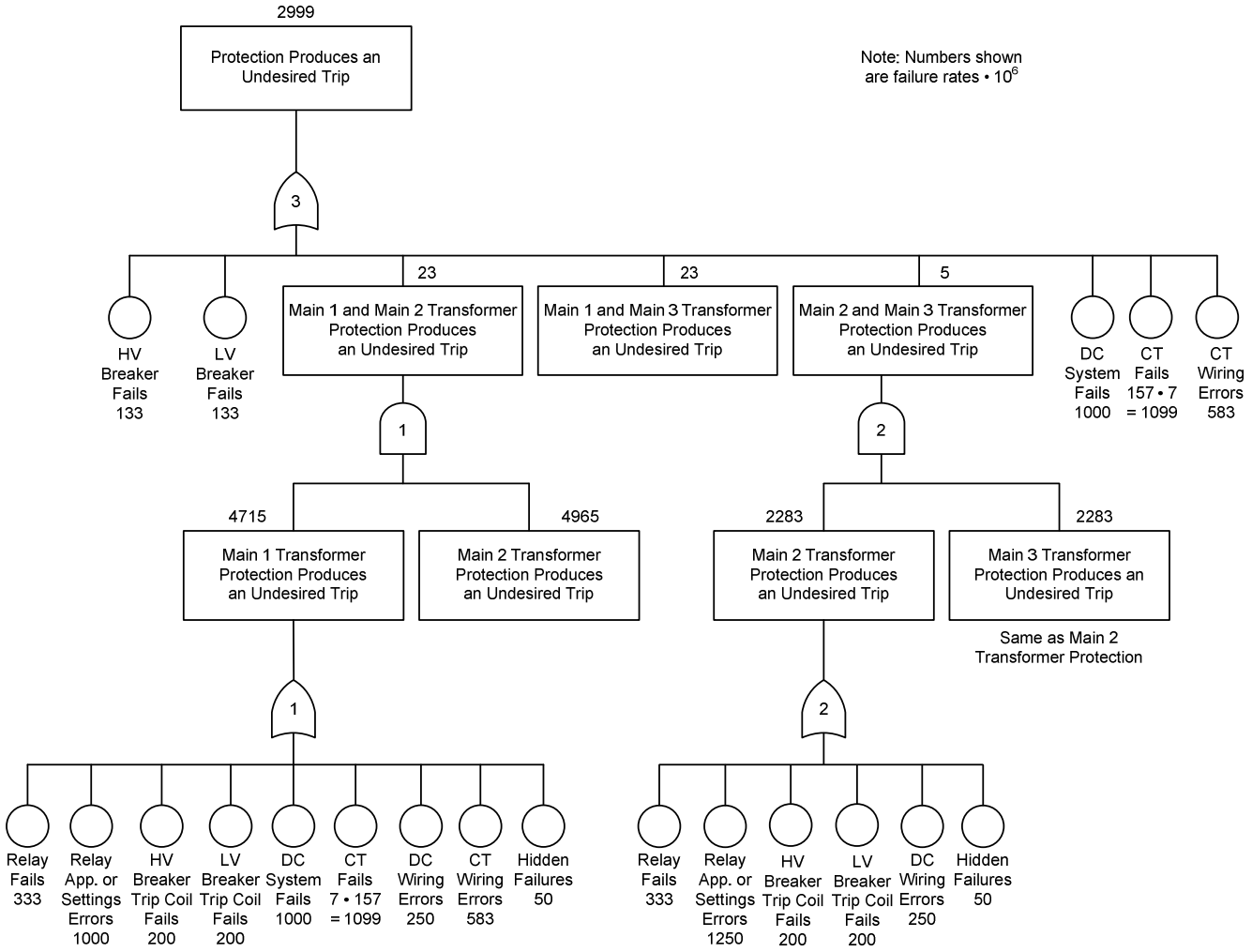

Fig. 10. Security fault tree for the two-out-of-three voting transformer protection scheme.

Fig. 10 shows the security fault tree for the two-out-of-three voting transformer protection scheme. AND Gates 1 and 2 reflect the fact that two schemes need to misoperate to cause an undesired trip. The result is high security (a low failure rate). However, the shared dc system and CTs, which we represent as inputs to OR Gate 3, impair the scheme security.

C. Protection Scheme Reliability Comparison

Table II summarizes the results obtained from the 24 transformer protection fault trees.

From Table II, we conclude the following:

- Comprehensive commissioning testing improves the single scheme dependability 2.2 times.
- In dual-redundant schemes, the effect of breaker failures to interrupt current significantly reduces the impact of comprehensive commissioning testing on dependability. When considering common-mode failures, comprehensive commissioning testing improves the dual-redundant scheme dependability 3.1 times. It also improves the voting scheme dependability 1.6 times.
- Comprehensive commissioning testing improves security between 1.9 and 2.2 times.
- The dependability of the dual-redundant scheme is 1,807/163 = 11.1 times that of the single scheme.
- In a dual-redundant scheme, adding a second neutral CT does not significantly improve dependability. If we assume that breaker failure protection meets the performance requirements of the power system, the second neutral CT improves the scheme dependability 5/3 = 1.7 times. We calculated these values by considering the unavailability value for breaker failures to interrupt current to be zero.
- If we assume that breaker failure protection meets the performance requirements of the power system, the dependability of the dual-redundant scheme is 6/3 = 2 times higher when using relays from the same manufacturer than when using relays from different manufacturers. We calculated these values by considering the unavailability value for breaker failures to interrupt current to be zero.
- The dependability of the voting scheme is 1,807/370 = 4.9 times that of the single scheme.

TABLE II
TRANSFORMER PROTECTION RELIABILITY COMPARISON

Protection Scheme	Dependability (Unavailability • 10^6)		Security (Failure Rate • 10^6)	
	Normal Commissioning Testing	Comprehensive Commissioning Testing	Normal Commissioning Testing	Comprehensive Commissioning Testing
Single	1,807	821 (2.2 times)	4,981	2,573 (1.9 times)
Dual redundant	163	160 (1.0 times)	9,946	4,930 (2.0 times)
Dual redundant with one neutral CT	165	163 (1.0 times)	10,020	5,087 (2.0 times)
Dual redundant with relays from different manufacturers	166	161 (1.0 times)	11,196	5,180 (2.2 times)
Dual redundant with common-mode failures	668	213 (3.1 times)	10,471	4,955 (1.9 times)
Redundant two-out-of-three voting	370	229 (1.6 times)	2,999	1,576 (1.9 times)

Note: The numbers in parentheses represent the effect of comprehensive commissioning testing. These numbers are the ratios of the unavailabilities or failure rates with normal testing to the unavailabilities or failure rates with comprehensive testing.

- The dependability of the dual-redundant scheme is 370/163 = 2.3 times that of the voting scheme. Sharing the dc power system and the CTs affects the voting scheme dependability.
- Common-mode failures impair the dependability of the dual-redundant scheme 668/163 = 4.1 times. Comprehensive commissioning testing and detailed setting and design reviews reduce the dependability impairment to 229/160 = 1.4 times.
- The security of the single scheme is 9,946/4,981 = 2.0 times that of the dual-redundant scheme.
- The security of the voting scheme is 4,981/2,999 = 1.7 times that of the single scheme. Sharing the dc power system and the CTs affects the voting scheme security.
- The security of the voting scheme is 9,946/2,999 = 3.3 times that of the dual-redundant scheme.
- The security of the dual-redundant scheme is 11,196/9,946 = 1.1 times higher when using relays from the same manufacturer than when using relays from different manufacturers.

D. Cost Comparison

We evaluated the costs resulting from adding redundancy to the single transformer protection scheme. We used a computer program for protection system cost estimation to determine the cost of the basic, dual-redundant, and voting schemes. Our cost evaluation includes the following:

- Relays.
- Engineering (relay programming and panel wiring design).
- Panel wiring and testing.
- Field wiring, including cable and labor costs (assuming the distances from the instrument transformers and breakers to the relays to be 300 meters).

Table III summarizes the cost estimation results. It shows that, for this example, converting the single scheme into a dual-redundant scheme costs $13,480 and converting the single scheme into a two-out-of-three voting scheme costs $21,110. This is a low price to pay for the protection scheme reliability improvement provided by redundancy, given the high costs of transformer outages and repairs. However, if we require the addition of a dc power system or a set of CTs to achieve full redundancy, we must consider their cost in the comparison.

TABLE III
COST COMPARISON OF TRANSFORMER PROTECTION SCHEMES

Item	Protection Scheme		
	Basic	Dual Redundant	Voting
Relays	$5,860	$11,720	$17,580
Engineering	$4,000	$5,000	$6,000
Wiring and testing	$1,790	$2,510	$3,280
Field wiring	$9,300	$15,200	$15,200
Total cost	**$20,950**	**$34,430**	**$42,060**
Incremental cost	–	**$13,480**	**$21,110**

VI. GENERATOR PROTECTION EVALUATION

A. Generator Protection Schemes

We compare the reliability of three schemes for protecting a high-resistance-grounded generator connected in a unit arrangement with the step-up transformer. The unit has a single breaker on the transformer HV side and no generator breaker. All the schemes use multifunction relays that provide generator protection and include the step-up transformer in the unit differential zone. The relays do not provide dedicated transformer protection.

Fig. 11a shows the single protection scheme, which includes one relay, single sets of CTs and voltage transformers (VTs), one dc power system, and one breaker with a single

trip coil. Fig. 11b shows the dual-redundant protection scheme, which includes two relays, two sets of instrument transformers, two dc power systems, and a breaker with redundant trip coils. To create a two-out-of-three voting scheme, we add a third relay to the Fig. 11b scheme, connected to the same instrument transformers and the same dc power system as one of the other two relays. In redundant schemes, we assume all the redundant components are of similar quality. We also assume relays have the same reliability indices, sensitivities, and operation speeds.

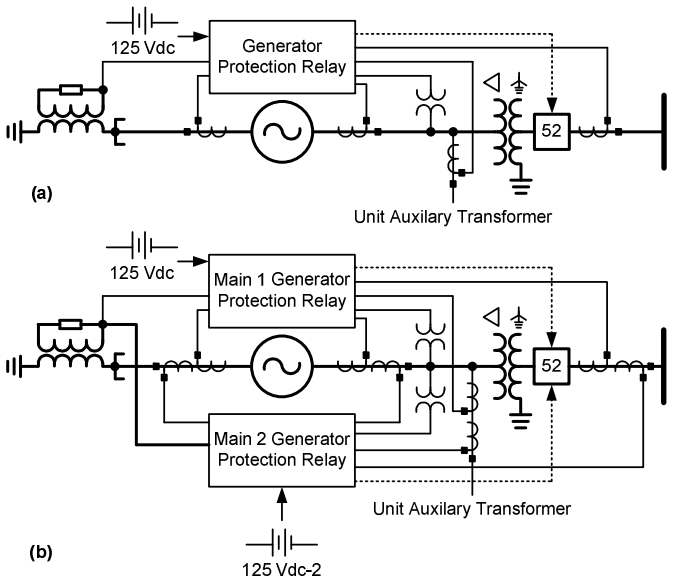

Fig. 11. Single and dual-redundant generator protection schemes using multifunction relays.

B. Fault Tree Analysis

We created 20 fault trees (10 for dependability analysis and 10 for security analysis) for the following combinations of protection schemes and other factors:

- Single scheme.
- Dual-redundant scheme.
- Dual-redundant scheme with relays from different manufacturers.
- Dual-redundant scheme that experiences common-mode failures.
- Redundant two-out-of-three voting scheme.

Table VI in the appendix shows the reliability indices that we used in the fault trees.

Fig. 12 shows the dependability fault tree for the single generator protection scheme (see Fig. 11a). The top event is "protection fails to trip unit for in-zone faults or abnormal conditions." The fault tree includes the basic events considered for transformer protection (see Fig. 2) and the failures of the generator grounding system because this system provides a voltage input signal to the relay. This fault tree considers all the generator protection functions that the multifunction relay can provide using the current and voltage inputs shown in Fig. 11a. The fault tree does not include other possible scheme modules, such as resistance temperature detector (RTD) modules for thermal protection, ground modules for field ground fault protection, or signal injection modules for stator ground fault protection. In this fault tree, we use the unavailability values shown in Table VI in the appendix. We can modify the fault tree as required to consider other scheme configurations, to include other events of interest, or to use other unavailability values. The other fault trees for the single generator protection scheme (dependability fault tree considering the effect of comprehensive commissioning testing and security fault trees) have the same topology as that of Fig. 12 but different reliability indices.

Fig. 13 depicts the dependability fault tree for the dual-redundant generator protection scheme shown in Fig. 11b. All the scheme components are redundant, except the generator grounding system, composed of a transformer with a resistor connected to its secondary. The transformer provides a voltage input signal to the relays. The relays use this signal and the zero-sequence voltage measured at the generator terminals to provide 100 percent stator ground fault protection. This protection combines a neutral overvoltage element with a third-harmonic voltage differential element [1]. The generator grounding system is a single point of failure for stator ground fault protection. As a result, the fault tree topology is similar to that of the dual-redundant transformer protection scheme with one neutral CT (Fig. 6).

The left side of the Fig. 13 fault tree represents the stator ground fault protection. We assume stator ground faults to be 30 percent of all generator internal faults and abnormal operating conditions, so we use a 0.3 multiplier as an input to AND Gates 1 and 3.

The right side of the Fig. 13 fault tree represents all the other generator protection functions. The output of OR Gate 2 is the unavailability value resulting from these other protection functions failing to operate. We use a 0.7 multiplier as an input to AND Gate 2 in this case. AND Gates 4 and 5 practically eliminate the contribution of the redundant protection scheme to the top event. Hence the breaker failures to interrupt current and the generator grounding system failures determine the protection scheme dependability.

We created the other fault trees for the dual-redundant generator protection scheme (security fault trees and dependability fault trees considering the effect of comprehensive commissioning testing and common-mode failures) using the same methodology as for dual-redundant transformer protection schemes.

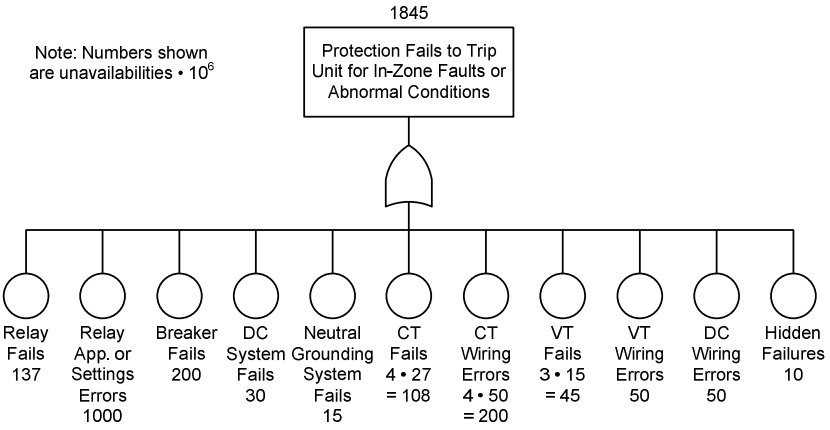

Fig. 12. Dependability fault tree for the single generator protection scheme.

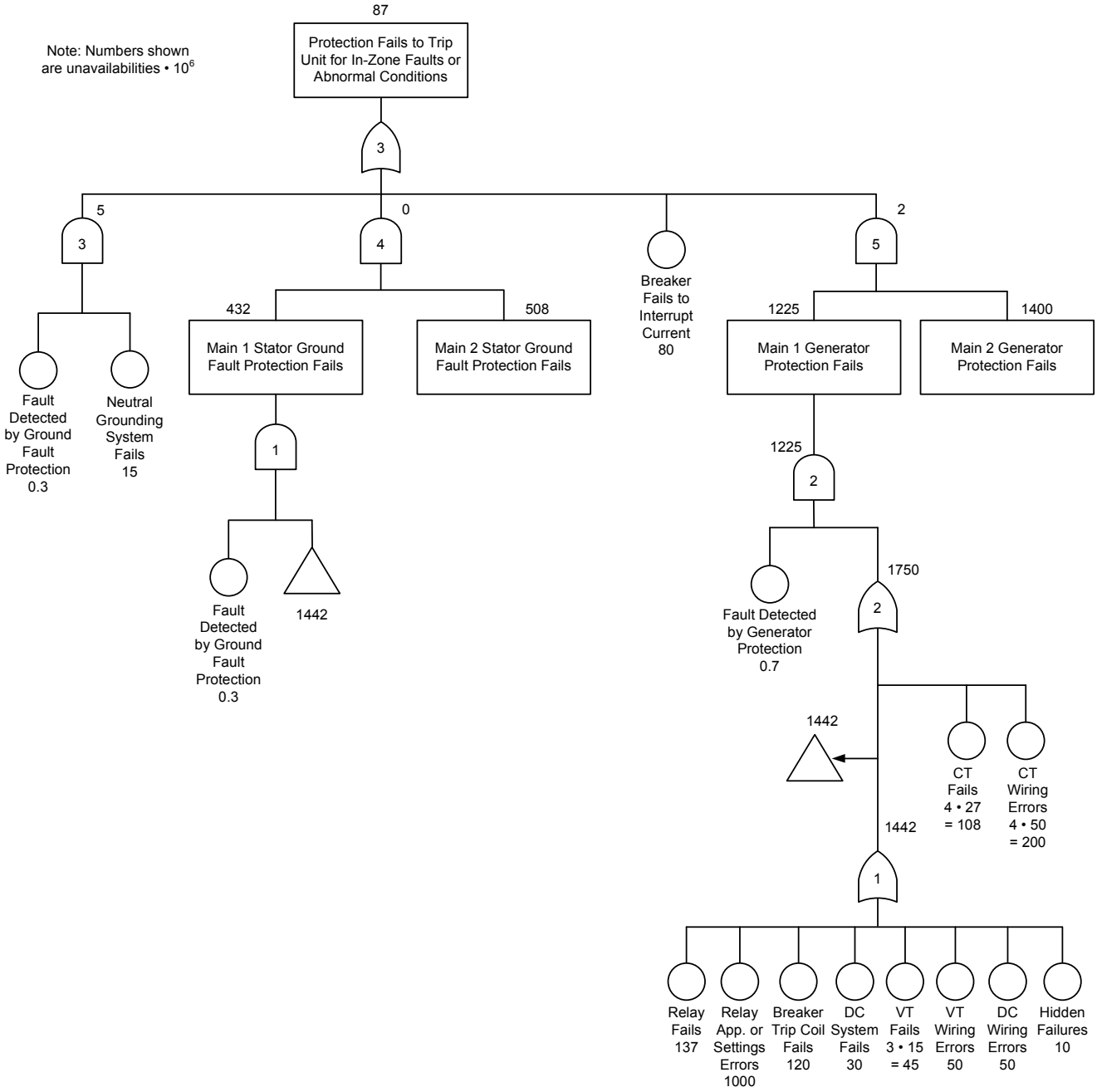

Fig. 13. Dependability fault tree for the dual-redundant generator protection scheme using relays from the same manufacturer.

Fig. 14 shows the dependability fault tree for the two-out-of-three voting generator protection scheme. The scheme has three multifunction relays. Tripping occurs when at least two of the relays operate. We assume that two of the schemes (referred to as Main 2 and Main 3 in Fig. 14) share the dc power system and instrument transformers, which become single points of failure for the voting scheme. We represent dc power system failures, instrument transformer failures, and wiring errors at the same level as breaker failures to interrupt current, as inputs to OR Gate 2. We represent the neutral grounding system, another single point of failure of the voting scheme, as another input to OR Gate 2. Because of the scheme redundancy, the outputs of AND Gates 2 and 5 are zero. Hence the shared component, the breaker failures to interrupt current, and the grounding system failures determine the scheme dependability. In this analysis, we assume that the three schemes detect the same faults and abnormal conditions. If the schemes had different fault or abnormal condition coverage (because of different settings, principles of operation, or manufacturers) and if two of the schemes did not detect an event, the two-out-of-three voting scheme would fail to trip the generator. For this reason, we recommend that voting schemes use relays with the same fault and abnormal condition coverage.

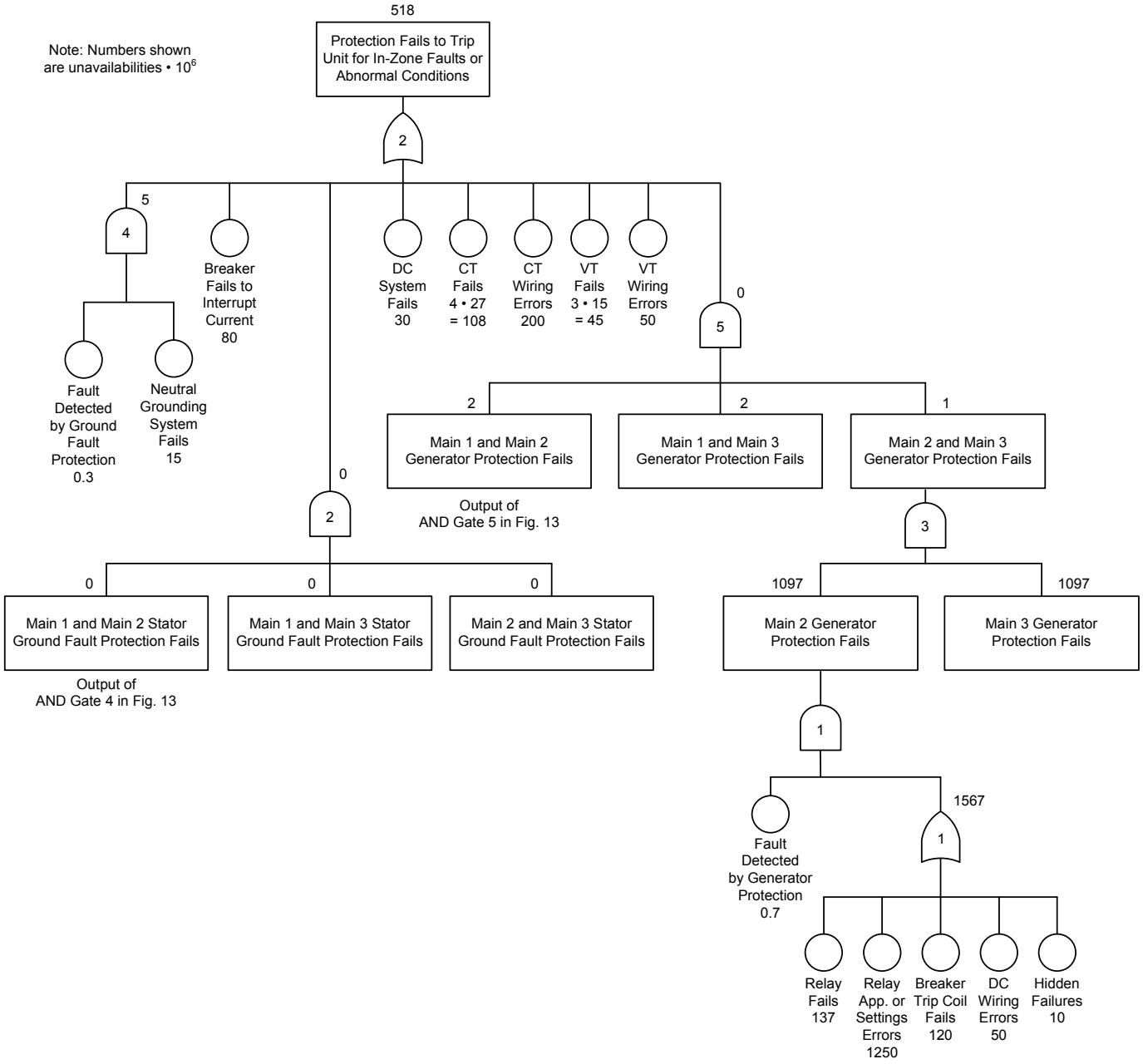

Fig. 14. Dependability fault tree for the two-out-of-three voting generator protection scheme.

TABLE IV
GENERATOR PROTECTION RELIABILITY COMPARISON

Protection Scheme	Dependability (Unavailability • 10^6)		Security (Failure Rate • 10^6)	
	Normal Commissioning Testing	Comprehensive Commissioning Testing	Normal Commissioning Testing	Comprehensive Commissioning Testing
Single	1,845	726 (2.5 times)	7,152	4,077 (1.8 times)
Dual redundant	87	85 (1.0 times)	14,143	7,793 (1.8 times)
Dual redundant with relays from different manufacturers	88	85 (1.0 times)	15,393	8,043 (1.9 times)
Dual redundant with common-mode failures	592	138 (4.3 times)	14,668	7,693 (1.9 times)
Redundant two-out-of-three voting	518	244 (2.1 times)	5,568	3,481 (1.6 times)

Note: The numbers in parentheses represent the effect of comprehensive commissioning testing. These numbers are the ratios of the unavailabilities or failure rates with normal testing to the unavailabilities or failure rates with comprehensive testing.

C. Protection Scheme Reliability Comparison

Table IV summarizes the results obtained from the 20 generator protection fault trees.

From Table IV, we conclude the following:

- Comprehensive commissioning testing improves the single scheme dependability 2.5 times.
- In dual-redundant schemes, the effect of breaker failures to interrupt current and the common use of the voltage signal from the grounding transformer significantly reduce the impact of comprehensive commissioning testing on dependability. When considering common-mode failures, comprehensive commissioning testing improves the dual-redundant scheme dependability 4.3 times. It also improves the voting scheme dependability 2.1 times.
- Comprehensive commissioning testing improves security between 1.6 and 1.9 times.
- The dependability of the dual-redundant scheme is 1,845/87 = 21.2 times that of the single scheme.
- The dependability of the voting scheme is 1,845/518 = 3.6 times that of the single scheme.
- The dependability of the dual-redundant scheme is 518/87 = 6.0 times that of the voting scheme. Sharing the dc power system and the instrument transformers affects the voting scheme dependability.
- The dual-redundant scheme has the same dependability when using relays from the same manufacturer as when using relays from different manufacturers.
- Common-mode failures impair dependability of the dual-redundant scheme 592/87 = 6.8 times. Comprehensive commissioning testing and detailed setting and design reviews reduce the dependability impairment to 138/85 = 1.6 times.
- The security of the single scheme is 14,143/7,152 = 2.0 times that of the dual-redundant scheme.
- The security of the voting scheme is 7,152/5,568 = 1.3 times that of the single scheme. Sharing the dc power system and the instrument transformers affects the voting scheme security.
- The security of the voting scheme is 14,143/5,568 = 2.5 times that of the dual-redundant scheme.
- The security of the dual-redundant scheme is 15,393/14,143 = 1.1 times higher when using relays from the same manufacturer than when using relays from different manufacturers.

D. Cost Comparison

We evaluated the costs resulting from adding redundancy to a generator protection scheme. Our cost evaluation includes:

- Relays.
- Engineering (relay programming and panel wiring design).
- Panel wiring and testing.
- Field wiring, including cable and labor costs (assuming the distances from the instrument transformers and breakers to the relays to be 150 meters).

Table V summarizes the cost estimation results.

TABLE V
COST COMPARISON OF GENERATOR PROTECTION SCHEMES

Item	Protection Scheme		
	Basic	Dual Redundant	Voting
Relays	$5,860	$11,720	$17,580
Engineering	$4,000	$5,000	$6,000
Wiring and testing	$1,790	$2,510	$3,240
Field wiring	$6,880	$12,540	$13,540
Total cost	**$18,530**	**$31,770**	**$40,360**
Incremental cost	–	**$13,240**	**$21,830**

Table V shows that, for this example, converting the single scheme into a dual-redundant scheme costs $13,240 and converting the single scheme into a two-out-of-three voting scheme costs $21,830. This is a low price to pay for the protection scheme reliability improvement provided by redundancy, given the high costs of generator outages and repairs. However, if we require the addition of a dc power system or a set of instrument transformers to achieve full redundancy, we must consider their cost in the comparison.

VII. Conclusions

From the transformer and generator protection schemes studied in this paper, we conclude the following:

- Fault tree analysis is an excellent tool to compare the relative reliability of protection schemes. The topologies and reliability indices of fault trees used for dependability analysis are different from those used for security analysis.
- This paper shows dependability and security fault trees for typical single, dual-redundant, and voting protection schemes for transformers and generators. We also show how to consider the effect of comprehensive commissioning testing, hidden failures, common-mode failures, and the use of relays from the same or different manufacturers in redundant schemes.
- The paper provides a table of reliability indices for use in fault trees. We calculated some indices from measured field data. However, other indices come from technical literature or were estimated based on experience. Utility engineers can refine these indices by using field data from their power systems.
- Comprehensive commissioning testing improves the dependability of single and voting protection schemes. When considering common-mode failures, this testing also improves the redundant scheme dependability.
- Comprehensive commissioning testing improves the security of all transformer and generator protection schemes.
- Dual-redundant transformer and generator protection schemes have higher dependability and lower security than single schemes.
- In transformer and generator protection schemes, the voting scheme has the highest security, and the dual-redundant scheme has the lowest security.
- Adding a second neutral CT improves the dependability of redundant transformer protection schemes when breaker failure protection meets the power system requirements.
- Breaker failures to interrupt current have a significant impact on the dependability of redundant schemes. A breaker failure to interrupt current causes a failure to trip the transformer or generator, no matter the redundancy of the rest of the scheme. To improve the redundant scheme dependability, we recommend providing good breaker maintenance and applying breaker failure protection.
- In generator protection schemes, the grounding system represents a single point of failure that limits the effect of redundancy on the scheme dependability.
- Using relays from the same manufacturer improves the dependability and security of redundant protection schemes.
- Hidden and common-mode failures do not significantly affect the reliability of redundant protection schemes.
- Common-mode failures affect the reliability of redundant protection schemes. Comprehensive commissioning testing and detailed setting and design reviews significantly reduce the dependability impairment.
- The costs of converting a single transformer or generator protection scheme into a dual-redundant scheme or a voting scheme are relatively low, unless this conversion requires adding a dc power system or instrument transformers.

VIII. Appendix

This appendix shows the reliability indices that we used in the dependability and security fault trees in this paper. We also explain how we calculated or estimated these indices. We have confidence in the relay failure rates because we have measured them for many years. We estimated other indices based on our experience and the information available in technical literature.

A. Reliability Indices Used in Fault Trees

Table VI shows the unavailability values that we used for dependability fault trees and the failure rate values that we used for security fault trees. We also show the MTBF values that we used to calculate the failure rates.

TABLE VI
RELIABILITY INDICES USED IN FAULT TREES

Event	Dependability	Security	
	Unavailability • 10^6	MTBF (Years)	Failure Rate • 10^6
Relay fails	137	3,000	333
Relay application or settings errors	1,000	1,000	1,000
Breaker fails	200	3,000	333
Breaker fails to interrupt current	80	–	–
DC power system fails	30	1,000	1,000
CT fails	9	6,370	157
VT fails	15	3,600	278
Generator grounding system fails	15	3,600	278
DC system wiring errors	50	4,000	250
CT or VT wiring errors	50	4,000	250
Hidden failures	10	20,000	50
Common-mode failures (hardware or firmware)	5	40,000	25
Common-mode failures (settings or design errors)	500	2,000	500

B. Comments on the Reliability Indices for Dependability Fault Trees (Unavailabilities)

1) Relay Fails

Our calculation using observed field failure data gives MTBF = 100 years ($\lambda = 10{,}000 \bullet 10^{-6}$) for dependability analysis. This MTBF value includes hardware and firmware failures and the effect of taking the relay out of service for corrective actions derived from service bulletins. Reference [11] gives an interval from 30 minutes to 2 weeks for MTTR. Assuming an average value of MTTR = 5 days, we have:

$$U = \lambda \bullet \text{MTTR} = (0.01 \text{ failures/year})\ (120 \text{ hours})\ (1/8{,}760 \text{ hours/year}) = 137 \bullet 10^{-6}$$

2) Relay Application or Settings Errors

Experience shows that relay application and settings errors cause more protection dependability problems than relay failures. For example, [12] analyzes incorrect protection operations in a utility during an 18-month period and concludes that settings errors and other human errors caused 45 percent of the incorrect operations, while relay failures caused only 4.5 percent of the incorrect operations. Using this information, we assume $U = 1{,}000 \bullet 10^{-6}$ for relay application or settings errors.

We assume this value falls 80 percent ($U = 200 \bullet 10^{-6}$) with comprehensive commissioning testing and by analyzing relay event reports to find application or settings errors.

For two identical relays, we use $U = 1{,}000 \bullet 10^{-6}$ for one relay and $U = 1{,}250 \bullet 10^{-6}$ for the other relay to account for possible additional errors when manually applying settings to this other relay. For two relays from different manufacturers, we assume the resulting unavailability to be close to the sum of the relay unavailabilities because of the differences in application considerations and settings rules. Hence we use $U = 1{,}750 \bullet 10^{-6}$ for each relay. We assume these values fall 80 percent ($U = 200 \bullet 10^{-6}$, $U = 250 \bullet 10^{-6}$, and $U = 350 \bullet 10^{-6}$, respectively) with comprehensive commissioning testing and by analyzing relay event reports to find application or settings errors.

3) Breaker Fails

References [13] and [14] provide utility breaker failure data collected in a CIGRÉ survey for the 1988 to 1991 period for breakers between 62.5 kV and greater than 700 kV. The reported failure rate for all the breakers is $\lambda = 6{,}720 \bullet 10^{-6}$, which gives MTBF = 149 years. Assuming that half of these failures are failures to open (a dependability problem), we can use MTBF = 300 years for dependability analysis.

Hence, for breakers with one tripping coil, we use MTBF = 300 years and calculate the unavailability assuming the following [7]:

- Ninety percent 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 percent of failures are detected by visual inspections every two months.
- The remaining 5 percent of failures are detected by maintenance every two years.

$$U = \frac{1}{300 \text{ years}} \bullet \left(\frac{0.90 \bullet 2 \text{ days}}{365 \text{ days/year}} + \frac{0.05 \bullet 1 \text{ month}}{12 \text{ months/year}} + 0.05 \bullet 1 \text{ year} \right) = 197 \bullet 10^{-6}$$

Hence, for breakers with one trip coil, we use $U = 200 \bullet 10^{-6}$. For breakers with redundant trip coils, we use $U = 80 \bullet 10^{-6}$ to account for the increased reliability resulting from trip coil redundancy and from the lower impact of blown fuses in the dc power circuits.

4) Breaker Fails to Interrupt Current

In redundant schemes, a breaker failure to interrupt current causes a failure to clear the fault, no matter the redundancy of the rest of the scheme. For this reason, in dependability fault trees, we represent breaker failures to interrupt current separately from trip coil failures and blown fuses in the dc tripping circuits. According to [14] and [15], which report

breaker failure data collected in a CIGRÉ survey for the 1974 to 1977 period, mechanical failures are around 70 percent of all breaker failures. Assuming that half the mechanical failures are caused by stuck trip coils, we can estimate that breaker failures to interrupt current after the trip coil operates represent around 40 percent of all breaker failures. Hence we use $U = 0.4 \bullet 200 \bullet 10^{-6} = 80 \bullet 10^{-6}$ for breaker failures to interrupt current and $U = (200 - 80) \bullet 10^{-6} = 120 \bullet 10^{-6}$ for all the other breaker failures.

5) DC Power System Fails

We use $U = 30 \bullet 10^{-6}$ according to [16]. We assume this value falls 80 percent ($U = 6 \bullet 10^{-6}$) when we provide proper battery maintenance, monitor the system voltage and the battery charger, and use efficient ground detection systems. We consider redundant dc power systems to have redundant batteries, battery chargers, and wiring.

6) CT Fails

Reference [14] provides instrument transformer failure data collected in a CIGRÉ survey for the 1985 to 1995 period. The reported failure rate for all CT failures that result in a CT outage is $\lambda = 1{,}570 \bullet 10^{-6}$, which gives MTBF = 637 years. For an MTTR = 2 days, we get $U = 8.6 \bullet 10^{-6}$ and will use $U = 9 \bullet 10^{-6}$ per CT.

7) VT Fails

According to [14], the failure rate for all VT failures that result in a VT outage is around $\lambda = 2{,}800 \bullet 10^{-6}$. Hence MTBF = 360 years. For an MTTR = 2 days, we get $U = 15.2 \bullet 10^{-6}$ and will use $U = 15 \bullet 10^{-6}$ per VT.

8) Generator Grounding System Fails

The generator grounding system consists of a transformer with its primary connected between the generator neutral and ground and with a resistor connected to its secondary. Generator stator ground fault protection receives voltage information from the secondary of the generator grounding transformer. A transformer or resistor failure could cause the stator ground fault protection to fail to operate. Assuming that the frequency of generator grounding transformer or resistor failures is comparable to that of VT failures, we use MTBF = 360 years, which gives $U = 15 \bullet 10^{-6}$ for MTTR = 2 days.

9) DC System Wiring Errors

Experience shows that dc system wiring errors cause more protection reliability problems than dc power system failures. We assume the unavailability caused by dc system wiring errors to be $U = 50 \bullet 10^{-6}$. We assume this value falls 80 percent ($U = 10 \bullet 10^{-6}$) with comprehensive commissioning testing and by analyzing relay event reports to find dc system wiring errors.

10) CT or VT Wiring Errors

We assume the unavailability caused by CT or VT wiring errors to be equal to that caused by dc system wiring errors. Hence we use $U = 50 \bullet 10^{-6}$ per CT or VT three-phase circuit. We assume this value falls to zero ($U = 0$) with comprehensive commissioning testing (using the advanced commissioning features available in modern relays) and by analyzing relay event reports to find CT or VT wiring errors.

11) Hidden Failures

Hidden failures are very infrequent events. We assume the unavailability caused by hidden failures is less than 10 percent of that caused by a relay failure. This is based on experience and the assumption that hidden failure unavailability must be less than known and measured data. Hence we use $U = 10 \bullet 10^{-6}$ for hidden failures. We assume this value falls to $U = 5 \bullet 10^{-6}$ with comprehensive commissioning testing and by analyzing relay event reports.

12) Common-Mode Failures

Common-mode failures may result from the hardware or firmware of two devices failing simultaneously or from common errors in device settings or in system design.

We assume the common-mode failures caused by hardware or firmware problems to be even less frequent than hidden failures. For example, the probability of a relay component failing at the same time in two redundant relays is very low, even if this component has an abnormally high failure rate. Hence we use $U = 5 \bullet 10^{-6}$ for these common-mode failures. We assume this value falls to $U = 3 \bullet 10^{-6}$ with comprehensive commissioning testing and by analyzing relay event reports.

We assume the common-mode failures caused by settings or design errors to be around half the failures caused by relay application and settings errors. Hence we use $U = 500 \bullet 10^{-6}$ for these common-mode failures. We assume this value falls 90 percent ($U = 50 \bullet 10^{-6}$) by carefully reviewing settings and designs and analyzing relay event reports.

C. Comments on the Reliability Indices for Security Fault Trees (Failure Rates)

1) Relay Fails

Relays are typically designed to fail in a safe mode, not to trip. Our calculation using observed field failure data gives MTBF = 3,000 years ($\lambda = 333 \bullet 10^{-6}$) for security analysis.

2) Relay Application or Settings Errors

Experience shows that relay application and settings errors cause more protection security problems than relay failures. Hence we assume MTBF = $1{,}000 \bullet 10^{-6}$ ($\lambda = 1{,}000 \bullet 10^{-6}$) for relay application or settings errors. We assume this value falls to $\lambda = 200 \bullet 10^{-6}$ with comprehensive commissioning testing and by analyzing relay event reports to find application or settings errors.

3) Breaker Fails

Assuming that the breaker failures that cause undesired closures are around ten times less likely than the breaker failures that cause failures to open, we define MTBF = 10 • 300 = 3,000 years ($\lambda = 333 \bullet 10^{-6}$) for breakers with one trip coil. For breakers with redundant trip coils, we define MTBF = 3,000 / 0.4 = 7,500 years ($\lambda = 133 \bullet 10^{-6}$).

4) DC Power System Fails

The $U = 30 \bullet 10^{-6}$ value that we adopted for dependability analysis represents MTBF = 100 years for an MTTR of one day, which is typical for battery systems. Assuming that

the dc power system failures that cause undesired trips are around ten times less likely than the dc power system failures that cause failures to trip (a conservative assumption), we define MTBF = 1,000 years ($\lambda = 1{,}000 \bullet 10^{-6}$) for security analysis. We assume this value falls 80 percent ($\lambda = 200 \bullet 10^{-6}$) when we provide proper battery maintenance, monitor the system voltage and battery charger, and use efficient ground detection systems.

5) CT Fails

Assuming that the CT failures that cause undesired trips are around ten times less likely than the CT failures that cause failures to trip, we define MTBF = 6,370 years ($\lambda = 157 \bullet 10^{-6}$) for security analysis.

6) VT Fails

Assuming that the VT failures that cause undesired trips are around ten times less likely than the VT failures that cause failures to trip, we define MTBF = 3,600 years ($\lambda = 278 \bullet 10^{-6}$) for security analysis.

7) Generator Grounding System Fails

Assuming that the generator grounding transformer or resistor failures that cause undesired trips are around ten times less likely than those failures that cause failures to trip, we define MTBF = 10 • 360 = 3,600 years ($\lambda = 278 \bullet 10^{-6}$) for security analysis.

8) DC System Wiring Errors

Experience shows that relay application and settings errors cause more protection security problems than dc system wiring errors. Hence we assume MTBF = 4,000 years ($\lambda = 250 \bullet 10^{-6}$) for dc system wiring errors. We assume this value falls 80 percent ($\lambda = 50 \bullet 10^{-6}$) with comprehensive commissioning testing and by analyzing relay event reports to find dc system wiring errors.

9) CT or VT Wiring Errors

Experience shows that relay application and settings errors cause more protection security problems than CT or VT wiring errors, which are comparable with dc system wiring errors. Hence we assume MTBF = 4,000 years ($\lambda = 250 \bullet 10^{-6}$) for CT or VT wiring errors. We assume this value falls to zero ($\lambda = 0$) with comprehensive commissioning testing (using the advanced commissioning features available in modern relays) and by analyzing relay event reports to find CT or VT wiring errors.

10) Hidden Failures

Assuming it takes around six months to detect a hidden failure (MTTR = 0.5 years), the $U = 10 \bullet 10^{-6}$ value that we adopted for dependability analysis represents MTBF = 50,000 years. Assuming that hidden failures have the same likelihood of causing failures to trip as causing undesired trips, we assume a conservative value of MTBF = 20,000 years ($\lambda = 50 \bullet 10^{-6}$) for security analysis. We assume this value falls to $\lambda = 25 \bullet 10^{-6}$ with comprehensive commissioning testing and by analyzing relay event reports.

11) Common-Mode Failures

Assuming it takes around six months to detect a common-mode failure (MTTR = 0.5 years), the $U = 5 \bullet 10^{-6}$ and $U = 500 \bullet 10^{-6}$ values that we adopted for dependability analysis represents MTBF = 100,000 and MTBF = 1,000 years, respectively. We assume that common-mode failures have the same likelihood of causing failures to clear faults as causing undesired trips. Hence, for security analysis, we assume a conservative value of MTBF = 40,000 years ($\lambda = 25 \bullet 10^{-6}$) for failures caused by hardware or firmware problems and MTBF = 2,000 years ($\lambda = 500 \bullet 10^{-6}$) for failures caused by settings or design errors. We assume these values fall to $\lambda = 15 \bullet 10^{-6}$ and $\lambda = 50 \bullet 10^{-6}$, respectively, with comprehensive commissioning testing and by analyzing relay event reports.

IX. References

[1] H. J. Altuve Ferrer and E. O. Schweitzer, III (eds.), *Modern Solutions for Protection, Control, and Monitoring of Electric Power Systems.* Schweitzer Engineering Laboratories, Inc., Pullman, WA, 2010.

[2] M. J. Thompson, "The Power of Modern Relays Enables Fundamental Changes in Protection and Control System Design," proceedings of the 60th Annual Conference for Protective Relay Engineers, College Station, TX, March 2007.

[3] J. Sykes, V. Madani, J. Burger, M. Adamiak, and W. Premerlani, "Reliability of Protection Systems – What Are the Real Concerns?," proceedings of the 63rd Annual Conference for Protective Relay Engineers, College Station, TX, March 2010.

[4] D. Costello, "Fly Safe and Level: Customer Examples in Implementing Dual Primary Protection Systems." Available: http://www.selinc.com.

[5] Newton-Evans Research Company, *Worldwide Study of the Protective Relay Marketplace in Electric Utilities, 2006–2008, Volume 1, North American Market*, 2008.

[6] P. M. Anderson, *Power System Protection.* New York: IEEE Press/McGraw-Hill, 1999.

[7] E. O. Schweitzer, III, B. Fleming, T. J. Lee, and P. M. Anderson, "Reliability Analysis of Transmission Protection Using Fault-Tree Methods," proceedings of the 24th Annual Western Protective Relay Conference, Spokane, WA, October 1997.

[8] K. Zimmerman, "Commissioning of Protective Relay Systems," proceedings of the 34th Annual Western Protective Relay Conference, Spokane, WA, October 2007.

[9] K. Zimmerman and D. Costello, "Lessons Learned From Commissioning Protective Relay Systems," proceedings of the 62nd Annual Conference for Protective Relay Engineers, College Station, TX, March 2009.

[10] E. O. Schweitzer, III, D. Whitehead, H. J. Altuve Ferrer, D. A. Tziouvaras, D. A. Costello, and D. Sánchez Escobedo, "Line Protection: Redundancy, Reliability, and Affordability," proceedings of the 37th Annual Western Protective Relay Conference, Spokane, WA, October 2010.

[11] IEEE PSRC Working Group I-19, "Redundancy Considerations for Protective Relaying Systems," A Report to the IEEE Power System Relaying Committee, 2010. Available: http://www.pes-psrc.org/.

[12] R. Moxley, "Analyze Relay Fault Data to Improve Service Reliability," proceedings of the 30th Annual Western Protective Relay Conference, Spokane, WA, October 2003.

[13] Study Committee 13, Working Group 13.06, "Final Report of the Second International Enquiry on High Voltage Circuit-Breaker Failures and Defects in Service," CIGRÉ Technical Brochure No. 83, 1994.

[14] C. E. Sölver, "Past Cigré Surveys on Reliability of HV Equipment," CIGRÉ presentation, June 2006. Available: http://www.mtec2000.com/cigre_a3_06/Rio/past.pdf.

[15] G. Mazza and R. Michaca, "The First International Enquiry on Circuit-Breaker Failures and Defects in Service," Electra (CIGRÉ), No. 79, pp. 21–91, December 1981.

[16] R. Sandoval and J. Leon, "Evaluation of Methods for Breaker Flashover Protection," proceedings of the 31st Annual Western Protective Relay Conference, Spokane, WA, October 2004.

X. BIOGRAPHIES

Ramón Sandoval is a protection engineer for Comisión Federal de Electricidad (CFE) at the Topolobampo Thermal Power Station. He has worked for CFE since 1992 in the electrical maintenance of power and industrial equipment such as induction motors, synchronous generators, breakers, automatic voltage regulators (AVRs), and step-up transformers. For the last five years, Mr. Sandoval has been a power station protection engineer, installing, testing, and applying different types of protective equipment commonly used in industrial plants and power systems. This includes a variety of electromechanical, static, and digital multifunction relays. He received training in power system modeling and simulation from LAPEM using ATP and has worked on developing field procedures for protective relay testing using power system simulators and transient simulation software.

César A. Ventura Santana received a BSEE degree and an M.Sc. degree in Electrical Engineering from the Guadalajara Autonomous University in 1981 and 1997, respectively. He joined Comisión Federal de Electricidad (CFE) in 1983. Mr. Ventura served as a construction supervisor in the Nayarit Transmission Zone until 1984. From 1984 until 1997, he was a protection, control, and metering engineer at the Jalisco Transmission Zone of the CFE Western Transmission Region. From 1997 until 1998, Mr. Ventura was in the extra-high-voltage and high-voltage network studies department of the protection and metering division. Since 1998, he has been head of the metering department of the protection and metering division. Since 2006, Mr. Ventura has worked as head of the Western Metrology Laboratory of the CFE Western Transmission Region. He leads projects on power quality monitoring, measurement and instrumentation, and metering connectivity in the CFE Western Transmission Region.

Héctor J. Altuve Ferrer received his BSEE in 1969 from the Central University of Las Villas, Santa Clara, Cuba, and his Ph.D. in 1981 from Kiev Polytechnic Institute, Kiev, Ukraine. From 1969 until 1993, he served on the faculty of the Electrical Engineering School at the Central University of Las Villas. He served as a professor of the Graduate Doctoral Program in the Mechanical and Electrical Engineering School at the Autonomous University of Nuevo León, Monterrey, Mexico, from 1993 to 2000. From 1999 to 2000, he was the Schweitzer Visiting Professor at Washington State University's Department of Electrical Engineering. In January 2001, Dr. Altuve joined Schweitzer Engineering Laboratories, Inc., where he is currently a distinguished engineer and director of technology for Latin America. He has authored and coauthored several books and more than 100 technical papers and holds four patents. His main research interests are in power system protection, control, and monitoring. Dr. Altuve is an IEEE senior member.

Ronald A. Schwartz earned a BSEE from Ohio State University in 1968 and an M.Sc. in Electrical Engineering from the University of Maryland in 1970. He has served in the Oregon Quality Award Program as Senior Examiner. In addition, Mr. Schwartz joined Schweitzer Engineering Laboratories, Inc. in 1998 and has served on the board of directors since February 1994. He is currently a senior vice president for quality. Mr. Schwartz founded and served as principal for International Quality Associates, Inc. of Beaverton, Oregon, a consulting and training firm helping companies develop and implement effective management systems. Prior to founding International Quality Associates, he was employed for eight years by Sequent Computer Systems, also of Beaverton, as component engineering manager as well as a reliability engineer.

David A. Costello graduated from Texas A&M University in 1991 with a BSEE. He worked as a system protection engineer at Central Power and Light and Central and Southwest Services in Texas and Oklahoma. He has served on the System Protection Task Force for ERCOT. In 1996, Mr. Costello joined Schweitzer Engineering Laboratories, Inc., where he has served as a field application engineer and regional service manager. He presently holds the title of senior application engineer and works in Boerne, Texas. He is a senior member of IEEE and a member of the planning committee for the Conference for Protective Relay Engineers at Texas A&M University.

Demetrios A. Tziouvaras received his BSEE from the University of New Mexico and MSEE from Santa Clara University. He is an IEEE senior member and a member of the Power System Relaying Committee (PSRC) and CIGRÉ. Mr. Tziouvaras previously worked at Pacific Gas and Electric Company, where he held various protection engineering positions, including principal protection engineer for 18 years. In 1998, he joined Schweitzer Engineering Laboratories, Inc., where he currently holds the position of senior research engineer. Mr. Tziouvaras holds four patents and has authored and coauthored more than 50 technical papers. He served as the convener of CIGRÉ working group B5.15 on "Modern Distance Protection Functions and Applications" and is a member of several IEEE PSRC and CIGRÉ working groups.

David Sánchez Escobedo received his BSEE degree in 1994 from the University of Guanajuato, Mexico, and his M.Sc. degree in 2005 from the University of Guadalajara, Mexico. From 1994 until 1998, he was head of the Protection and Metering Office in the Western Transmission Area of Comisión Federal de Electricidad (CFE) in Guadalajara, Jalisco, Mexico. Mr. Sánchez served on the faculty of the Autonomous University of Guadalajara in 1998. From 1998 until 2000, he worked for INELAP-PQE in Guadalajara, Mexico, as a protection system design engineer. In 2000, Mr. Sánchez joined Schweitzer Engineering Laboratories, Inc., where he is currently the electrical engineering manager in San Luis Potosí, Mexico. He has authored and coauthored several technical papers.