Test the Right Stuff: Using Data to Improve Relay Availability, Reduce Failures, and Optimize Test Intervals

Adrian Genz, Derrick Haas, and Karl Zimmerman,
Schweitzer Engineering Laboratories, Inc.

Revised edition released March 2022

Originally presented at the
75th Annual Conference for Protective Relay Engineers
College Station, TX
March 28–31, 2022

Test the Right Stuff: Using Data to Improve Relay Availability, Reduce Failures, and Optimize Test Intervals

Adrian Genz, Derrick Haas, and Karl Zimmerman, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—In the mid-1990s, Kumm, Schweitzer, and Hou proposed an approach to assess and evaluate the effectiveness of self-testing in microprocessor-based relays [1]. In that paper, the authors used actual field data and statistical modeling to help relay users establish guidelines for determining testing intervals, and they introduced a system-based approach to testing. This system-based approach, which includes performing comprehensive commissioning, detecting alarms, monitoring communications and analogs, evaluating event data, and carrying out periodic maintenance is described in [2]. System-based testing has become an industry standard [3] for protective relay systems and for establishing periodic maintenance intervals.**

In this paper, we revisit and update the original paper [1], using field data and expanding the system model to consider improved mean time between failures (MTBF), variances in hardware designs, and the impact of firmware updates in assessing the effectiveness of relay self-testing.

Finally, we describe and evaluate four practical levels of detecting the health of a protective relay. These are real-time monitoring of relay self-test alarms, continuous monitoring of communications and analog inputs, performing visual inspections, and lastly, identifying failures that are not detectable without a manual test. By using data and targeted approaches, protective relay users can know and improve relay availability, reduce failures, and optimize protection system testing intervals.

I. Introduction

Microprocessor-based relays include self-testing functions to verify that the critical components of the relay are operating properly [1]. The effectiveness of relay self-testing, along with other monitoring and testing, has been used to develop industry practices for system-based testing and establishing test intervals [1] [2] [3] [4].

Protection system testing should consider all protection subsystems. For example, for the transmission line shown in Fig. 1, this includes validating all individual subsystems: protective relays (R1, R2), circuit breakers (52), CTs, VTs, direct current (dc) power systems, communications, and corresponding interconnections; when practical, the protection system as a whole should be tested [5] [6].

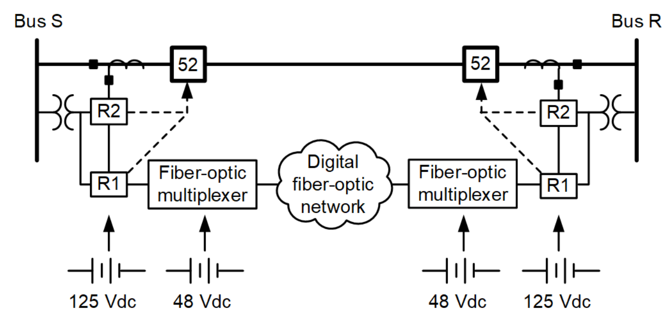

Fig. 1. One-line transmission line example

Each relay serves as the "brains" of the protection system. From a testing standpoint, that means the relay not only monitors its own functions, but also can monitor the health of many other protection subsystems including alternating current (ac) voltages and currents, communications channels, dc battery voltages, and breaker trip coil continuity.

In the sections that follow, we define four practical levels of testing, review current microprocessor-based relay testing practices, show recent field return data to evaluate the effectiveness of self-tests and other levels of testing, and, provide an updated model for evaluating and optimizing test practices. Finally, we will discuss how incorporating the practical levels into test practices will increase total effective test coverage and maximize routine test interval.

II. Four Practical Levels of Testing Defined

Microprocessor-based relays have traditionally consisted of four functional sections: 1) analog inputs and a data acquisition system, 2) contact inputs and outputs, 3) the processor and associated memory components, and 4) the power supply. As technology has advanced, we consider two additional functions that have increased in use: communications and displays/human-machine interfaces (HMIs).

Fig. 2 shows a practical block diagram of modern microprocessor-based relays.

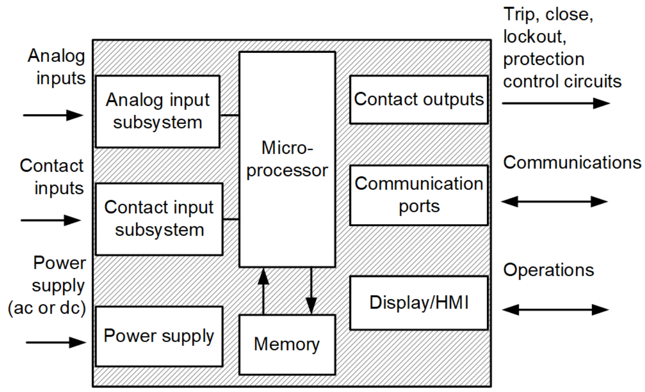

Fig. 2. Block diagram of microprocessor-based relays

After relays have been deployed in service, we define four practical levels of ongoing testing of these functional sections. The order of effectiveness/impact is as follows: 1) relay diagnostic self-tests, 2) continuous monitoring of analog inputs and communications channels, 3) maintenance testing, including periodic input/output (I/O) checks, and 4) those failures that can only be found by visual or physical inspection.

A. Relay Self-Tests

Relay diagnostic self-tests verify the functionality of the relay microprocessor and memory components. Relays also monitor and produce a self-test alarm for internal power supply failures. If the relay detects a failure, it will activate an output contact or can also be configured to send a message to the user. The relay disables trip and control functions when it detects critical failures.

Self-tests only partially monitor the data acquisition system. End users can add automatic monitoring functions, review event data, and perform testing to validate many of the functions not covered by self-tests.

B. Monitoring Analog and Communications Inputs

Nearly all relays continuously measure and monitor analog signals. This allows users to deploy loss-of-potential (LOP) and loss-of-current (LOI) functions to detect failures in the data acquisition system not covered by self-tests.

For example, LOP logic can detect system level failures of the voltage transformer, fuses, or wiring. LOP logic can also detect certain analog input failures, internal to the relay that are not detected by self-test. Whether the failure occurs outside or within the relay, the end user can monitor the LOP logic bit to produce an alarm and then use metering, event report data, and field inspections to ascertain root cause of the failure. Failures in the current circuit (e.g., a failed or shorted CT), or any other LOI can be detected by meter checks or event reports during operation or testing. Continuous monitoring of voltages and currents can be achieved by comparing metering data in adjacent relays [7].

Communications channels can also be monitored in real time. Channel monitoring for protection schemes have been deployed for line current differential (87L) schemes [8], digital relay-to-relay communications [9], and IEC 61850 GOOSE [10]. Data communications used for metering and system operator controls can also be monitored. Monitoring communications channels has the advantage of detecting channel or communication equipment problems, and also detecting hardware failures of communications ports. A lack of response from a continuously polling device may indicate a communications port problem.

C. Maintenance Testing, Including Periodic I/O Checks

Commissioning tests should be performed at installation to prove that the entire protection system is set, interconnected, and operating as intended [5] [6]. Routine maintenance testing should verify relay functions that cannot be fully verified by relay self-tests or other monitoring. Many maintenance procedures can be performed remotely, such as exercising an output contact, to reduce routine maintenance.

Event reports can be used to validate the performance of the protection system, including inputs and outputs. Automatic retrieval of event report data allows engineers to gain quick access to determine the root cause of problems and to enhance management of data for regulatory purposes. Those relays that encounter faults less frequently may require more maintenance checks.

D. Visual and Physical Inspection

Finally, some relay functions require a periodic physical or visual inspection. In most cases, failures associated with these relay functions are not critical to the protection system (e.g., a failure of the HMI or display), and inspections can take place during other routine maintenance.

III. Microprocessor-Based Relay Maintenance Practices

While each asset owner's maintenance practices vary depending on many factors, we review several common approaches and standards.

For utility companies that own transmission or bulk electric system assets in the United States and Canada, the North American Electric Reliability Corporation (NERC) has created a standard that defines the minimum frequency and type of maintenance testing that is required [3]. The NERC standard specifies a 12-year maximum maintenance interval under the following assumptions for a microprocessor-based relay:

- Monitoring features include internal self-diagnostics and alarming, and voltage and current sampling of three or more times per power system cycle.
- Alarms include power supply failures.

The above criteria do not apply to underfrequency and undervoltage load-shedding relays. Reference [3] also specifies what functionality the maintenance testing needs to verify. For the remainder of this paper, we will refer to the NERC standard, assuming a basic level of monitoring and a 12-year maximum routine test interval.

Each bulk electric asset owner is expected to evaluate their system against the most up-to-date NERC standards and any other applicable standards. As a result, most transmission utilities in the United States and Canada base their routine testing on the NERC standard.

For entities that do not fall under NERC requirements, such as relays installed on a utility distribution system or any industrial facility that does not have any assets on the bulk electric system, there are other normative guides and publications. The InterNational Electrical Testing Association (NETA) has written a standard covering maintenance of protective relays [4]. The NETA standard addresses the testing of protection elements but outlines testing as three categories: visual inspection, mechanical inspection, and electrical testing. Visual inspection involves actions including verifying the display and target LEDs, and recording basic information on the relay, such as the part number, serial number, and firmware version. Mechanical inspection involves actions such as verifying the tightness of connections and inspecting, operating, and cleaning any shorting devices. Electrical testing involves application of voltage and current, and testing of the specific protection elements.

Reference [4] provides general guidelines for time-based maintenance intervals on protective relays. The recommended time intervals are weighted by equipment condition and reliability requirements. As an example, for a microprocessor-based relay in average working condition with a medium reliability requirement, the recommended maintenance is a visual inspection every month with electrical and mechanical testing every 12 months. Relays with higher reliability requirements or low working conditions will need to be visually inspected and tested more frequently. While the inspection and test intervals from NETA are much shorter than what NERC requires, the required activities are more focused on visual and mechanical inspection. For example, NETA lists the testing of protection elements as optional.

IV. Self-Testing Effectiveness From Field Data

One of the key components of determining maintenance intervals is the self-test effectiveness of microprocessor-based relays. While the features of modern-day relays have changed over the last 25 years to include liquid crystal or touch displays, and expanded use of communications methods (e.g., RS232, EIA-485, copper, and fiber Ethernet), self-test effectiveness is still comparable to [1], as shown in Fig. 3. However, categories for the HMI and communications are not included in Fig. 3 as the digital protective relays produced in the 1980s and early 1990s did not use these features for protection.

To properly evaluate the self-test effectiveness, field return data for more than 3,300 protective relays over several product models were evaluated to assess the percentage of those devices where the failure was detected by self-test diagnostics. Of those devices, 75.1 percent had failures detected by self-tests, consistent with [1]. Of the remaining 24.9 percent of failures not detected by self-test, respective categories are reflected in Table I.

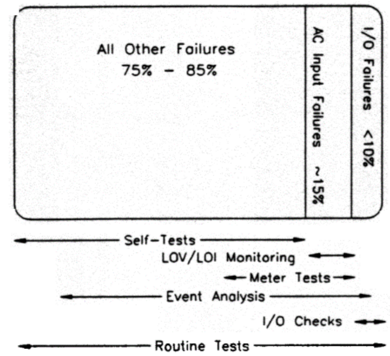

Fig. 3. A representation of digital relay self-testing covered by self-test diagnostics, as depicted in [1]; loss of voltage (LOV) is now more commonly referred to as LOP

TABLE I
DISTRIBUTION OF FAILURES NOT DETECTED BY SELF-TEST DIAGNOSTICS

Failure category	Percentage not detected by self-test diagnostics
HMI	8.9%
I/O	5.9%
Analog inputs	4.6%
Communications	4.1%
Other	1.4%

As presented in Table I, the highest undetected failure categories were HMI and I/O failures, followed by analog inputs, communications, and lastly other failures which include physical defects, such as broken cables, connectors, and hardware.

Fig. 4 includes an updated representation of relay self-test monitoring, test levels, and associated test coverage percentage. Fig. 4 further shows that by starting with a base test coverage of 75 percent from relay self-tests, the coverage can be improved to 100 percent with additional levels of testing implemented, as mentioned in Section II. With monitoring the relay self-test alarm, monitoring for analog inputs and communication failures, and conducting visual inspections of the HMI, the effective test coverage becomes greater than 90 percent.

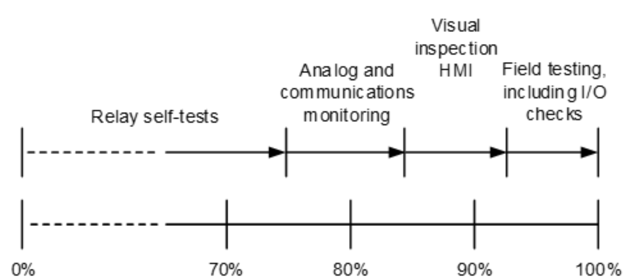

Fig. 4. An updated representation of digital relay test coverage, including self-test diagnostics and the benefit additional testing can provide

V. Updated Model and Optimized Test Practices

Markov models have been proposed in [1] and [11] to show the impact of self-testing on protection unavailability and routine test interval. The Markov models have been expanded to include the entire protection system in [12] using 32 states in the Markov model. For comparison of different schemes and evaluation of protection system components other than protective relays, fault tree analyses have also been used to evaluate the overall unavailability of a protection system [13].

To better quantify the benefits of self-testing in protective relays and how to modify the models to incorporate improvements in self-testing, overall relay capabilities made over the past several decades, and the four test levels, we outlined the following goals of our modeling effort:

- Keep the model as simple as possible.
- Focus on relay unavailability.
- Update the model to incorporate added features that were not commonplace in protective relays built prior to 1993.
- Consider test levels.
- Make use of other tools, such as fault trees for overall protection system unavailability and for situations when multiple relays and other components are factors.

The proposed updated model uses ten states. Since our focus is on protective relay unavailability, we removed the status of the primary electrical equipment from the model in [1]. Relay protection unavailability calculated from the Markov model can be included in other analysis tools (e.g., a fault tree) where the primary equipment and other components of the protective system can be modeled and accounted for. More details regarding the model and parameters used are included in the Appendix.

Fig. 5 shows the relay unavailability for two example cases. The first case is the 1993 model and assumptions used in [11], with a mean time between failures (MTBF) of 100 years and a self-test effectiveness of 85 percent. The second case is the base model described in the Appendix with an MTBF of 500 years, self-test effectiveness of 75 percent, with no metering and communications monitoring, and a high frequency of power system faults. In the context of this paper, we assume the MTBF metric includes field collected data that measures hardware failures associated with the product design, manufacturing process, or defective components, from a population of devices shipped from the relay manufacturer no more than 20 years before. This MTBF metric does not include any permanent or temporary failures (including those causing automatic diagnostic restarts) not reported to the relay manufacturer, or any failures detected and reported within six months of shipment from the manufacturer (i.e., out-of-box failures or failures discovered during commissioning).

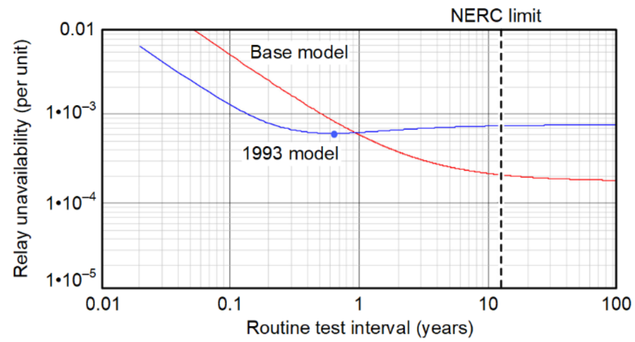

Fig. 5. Comparison of 1993 model vs. new base model

The practice of testing relays every 12 years based on the NERC PRC requirements is represented as a vertical dotted line in Fig. 5. There are notable differences between the model from 1993 (blue trace), and the new base model (red trace). But there are also some similarities as well. In the 1993 model, there is a minimum value of relay unavailability (blue dot at $600 \cdot 10^{-6}$ in Fig. 5) that occurs at a routine test interval of roughly every six months. Whereas, with the new base model, the curve flattens after ten years. After the curves flatten, the unavailability is constant, and increasing the testing interval yields no further improvement in unavailability. With respect to the 12-year NERC interval, the updated model shows that the curve does not flatten until well over 20 years, which is consistent with the intended design life of a microprocessor-based relay. It is important to note that the model does not account for the device being removed from service after exceeding its intended design life. Further discussion on this topic is in [14].

For the beginning portion of the curves, we can see that the slopes of the two models are identical. Given that we updated the time it takes to perform a relay test in the new base model from 0.5 hours to 4 hours (see the Appendix), the new base model starts at a higher unavailability. It now takes longer for a relay technician to test modern microprocessor-based relays based on the additional functionality, testing processes, and required documentation. The increase in testing time results in a higher unavailability for testing too often. But based on common experience, very few entities completely test their fleet of protective devices at an interval of less than once every several years.

Lastly, we notice that the unavailability is higher for the 1993 model than the updated base model. This is due to the increase in MTBF of microprocessor-based relays from 100 years to 500 years since 1993.

A. Improving MTBF

Relay manufacturers are constantly working on improvements to product quality and reliability. Fig. 6 shows the base model outlined from the Appendix, with a self-test effectiveness of 75 percent, and no meter and communications monitoring, with a frequent fault rate and MTBF values ranging from 100 years to 2,000 years.

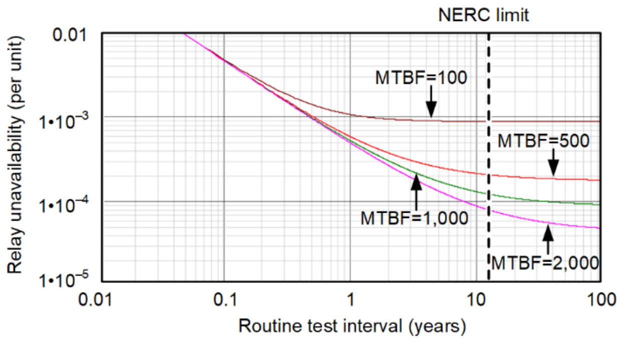

Fig. 6. Routine test interval vs. relay unavailability with varying MTBF of new base model

The relay unavailability decreases as the product reliability, represented by MTBF, increases. We can also see in Fig. 6 that the curves more gradually flatten out as MTBF increases. To better visualize how an increase in MTBF can decrease the relay unavailability, Fig. 7 includes the plot of minimum relay unavailability for each case of MTBF. For example, with an MTBF of 500 years, the minimum relay unavailability from Fig. 6 is $1.772 \cdot 10^{-4}$.

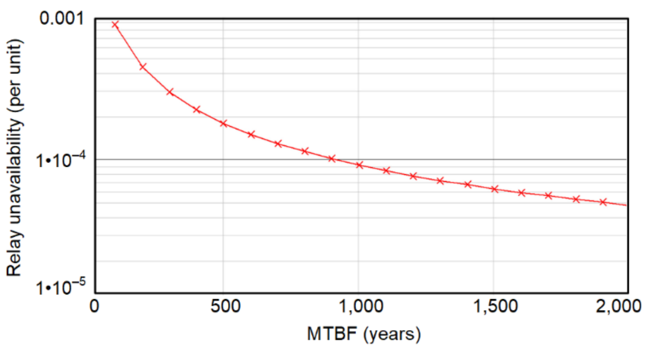

Fig. 7. MTBF vs. relay unavailability

There is a factor of 9.5 improvement in relay unavailability in Fig. 7 when we increase the MTBF from 100 to 1,000 years, from $8.615 \cdot 10^{-4}$ to $9.097 \cdot 10^{-5}$. However, when we increase MTBF from 1,000 years to 2,000 years, the decrease in relay unavailability is only a factor of 1.9, from $9.097 \cdot 10^{-5}$ to $4.780 \cdot 10^{-5}$.

Based on interpreting Fig. 7, after about 1,500 years, further increases in MTBF do not yield as dramatic of a reduction but still lowers relay unavailability.

B. *Improving Self-Testing Effectiveness*

There are ways that manufacturers can improve the effectiveness of device self-testing. In this section, we will group all automatic or self-test capabilities together, using our base model, with an MTBF of 500 years, assuming a frequent fault rate, and varying the self-test effectiveness from 0 percent to 95 percent. The results are shown in Fig. 8.

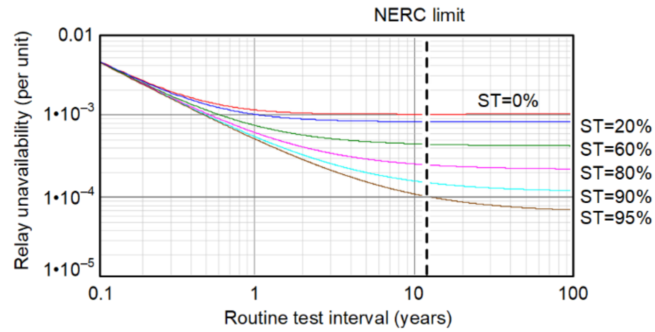

Fig. 8. Routing test interval vs. relay unavailability with varying self-test effectiveness, as denoted by ST

To better visualize how an increase in self-test effectiveness can decrease the relay unavailability, Fig. 9 includes the plot of minimum relay unavailability for each case of self-testing effectiveness.

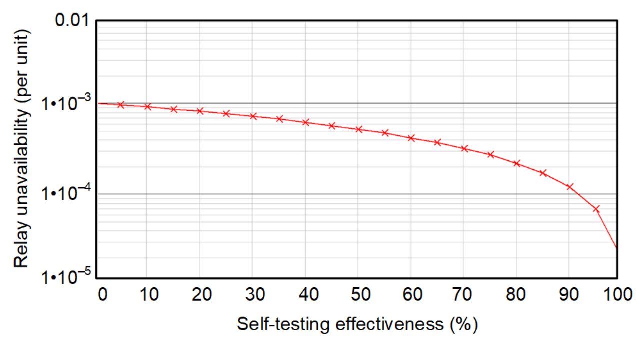

Fig. 9. Self-test effectiveness vs. relay unavailability

In Fig. 9 we see a modest improvement in relay unavailability as self-test effectiveness increases from 0 percent to 60 percent. As the self-test effectiveness gets closer to 100 percent, we see a greater incremental reduction in relay unavailability. Contrasting Fig. 9 (self-test variation) with Fig. 7 (MTBF variation), we do not see the same diminishing return on self-test improvement as we did with MTBF. Rather, as we get closer to 100 percent self-test effectiveness in Fig. 8 we benefit with larger improvements in relay unavailability.

While any improvement to self-tests seems to be desirable, there are practical limitations to self-test effectiveness. A relay manufacturer designs self-tests to detect failures of the internal hardware that affect protection. If one makes a self-test algorithm too sensitive to disable relay protection for unrelated functions (i.e., displays), it could be prone to unnecessary alarms. In addition, some self-test methods require hardware adjustments and added complexity. Relay manufacturers must carefully balance the value added in self-test improvements against added complexity. Complexity leads to reductions in overall quality.

C. *Impact of Faults per Year and Industrial Systems*

In [1], the number of faults per year on the primary equipment and power system are considered. However, the scenarios modeled looked at frequent fault rates that are found in utility overhead systems where temporary faults caused by lightning or other natural causes are common. In this paper, we include a lower fault rate to consider the case of a typical industrial power system where installation factors, such as insulated cable and indoor metal-clad switchgear, change the number of faults per year that those power systems would experience. Additionally, in [1], the authors selected to model abnormal unavailability. Abnormal unavailability is impacted by switching practices on the primary power system, whether or not there is a primary or backup relaying system, and it is impacted by the reliability of other components of the protection system, such as current transformers. As highlighted in a Section V, we only focus on the relay. As a result, we only consider the unavailability of the relay.

In Fig. 10, we plot the relay unavailability for the base model with a high rate for power system faults (two faults per year) and the base model considering the low-fault rate (one fault every two years).

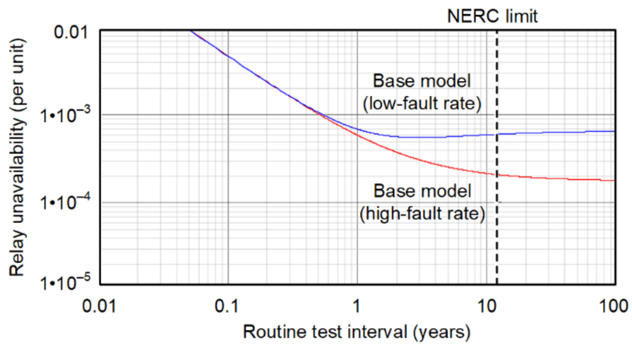

Fig. 10. Comparison of high-fault and low-fault rates for base model

We can see in Fig. 10 that the lower number of faults per year, plotted in blue, increases relay unavailability. If there are fewer faults on the system, an undetected relay failure is not noticed as quickly as a system with more faults, and the unavailability increases. When a power system fault occurs and the relay is not functioning, this often results in an undesired operation of the protection system (false trip or failure to trip). A careful analysis of relay event reports can detect failures of a protective relay without experiencing an undesired operation.

The same trends apply with a lower fault rate, such as the impact of increased MTBF and self-test effectiveness on protection unavailability. Additional plots for the lower fault rate are not included in the paper for brevity's sake.

D. Practical Improvements and Model Impact

After reviewing the updated base model, we hope to answer two questions. First, what are some practical ways to improve the total effective test coverage? Second, how do we relate the model to protection levels discussed in Section II?

We can start by considering the impact of including the monitoring of analog inputs and communications. In Fig. 11, we plot the base model with an MTBF of 500 years and self-test effectiveness of 75 percent, with no analog inputs or communications monitoring. We have also included in Fig. 11 the curve when communications monitoring is added, as well as the curve when both communications monitoring and monitoring of analog inputs are added. The overall relay unavailability at the NERC routine test interval of 12 years decreases from $2.0514 \cdot 10^{-4}$ when neither additional monitoring method is applied to $1.2175 \cdot 10^{-4}$ (1.68 times better) when both communications monitoring and analog inputs monitoring are applied.

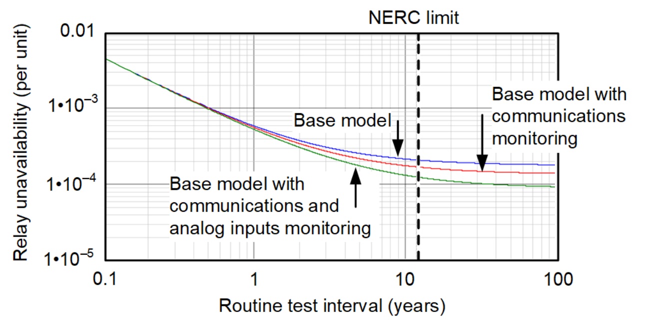

Fig. 11. Routine test interval vs. relay unavailability and impact of communications and analog inputs monitoring for a high-fault rate

In Fig. 12 we plot the base model with an MTBF of 500 years and self-test effectiveness of 75 percent with no analog inputs and communications monitoring, with the low-fault rate. In addition to Fig. 12 we add the curve when communications monitoring is added, as well as the curve when both communications monitoring and monitoring of analog quantities are added. The overall relay unavailability decreases from $5.9381 \cdot 10^{-4}$ at the 12-year routine test interval, when neither additional monitoring method is applied, to $2.9625 \cdot 10^{-4}$ (2.0 times better), when both communications monitoring and analog inputs monitoring are applied.

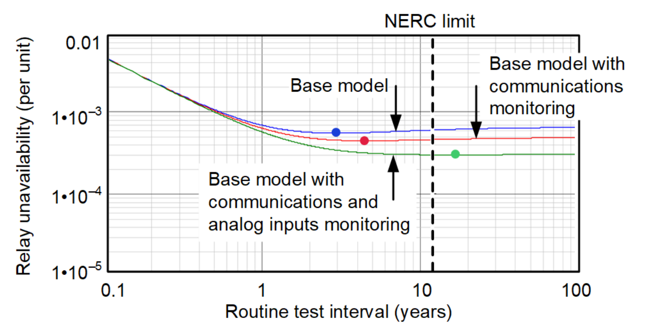

Fig. 12. Routine test interval vs. relay unavailability and impact of communications and analog inputs monitoring for low-fault rate

For both the high and lower fault rates, adding analog inputs and communications monitoring resulted in a reduction of relay unavailability by a factor of 1.68 to 2. That is a substantial improvement in unavailability that can be gained by simply using monitoring features that are already available in the protective relays. Furthermore, the optimal location on the graph for Fig. 12 where minimal unavailability and maximum routine test interval coincide shifted from approximately 3 years for the base model, to greater than 12 years when adding communications and analog inputs monitoring.

Visual and physical inspection were the last portion of the four levels of testing. The biggest impact of visual and physical inspection is the detection of failures (e.g., a failed display) that are not caught by other means, as previously discussed. Since we assumed a failed display did not result in the protection being unavailable in the model, visual inspection has little impact on protection unavailability in the Markov model.

However, there are failure modes in wiring and other categories that can be caught with a thorough visual inspection that are not addressed in this model.

VI. Conclusion

According to field data from over 3,300 protective relays, relay self-tests detect 75.1 percent of failures. From Table I, we know that HMI failures (8.9 percent), analog input failures (4.6 percent), and communications failures (4.1 percent) attributed to a total of 17.6 percent of total failures.

After monitoring the relay self-test alarm, monitoring for analog input and communications failures, and conducting visual inspections of the HMI, the effective test coverage becomes greater than 90 percent. Maintenance testing accounts for the remaining effective test coverage percentage (e.g., tests for I/O and other failures).

The NERC recommended 12-year routine test interval is sufficient and could be extended according to the base model in Section V. Based on the findings outlined in this paper, the authors conclude that performing maintenance testing on a microprocessor-based relay at least once during its more than 20-year design life is sufficient, particularly where power system faults are less frequent.

VII. Appendix

The state diagram for the updated Markov base model is shown in Fig. 13.

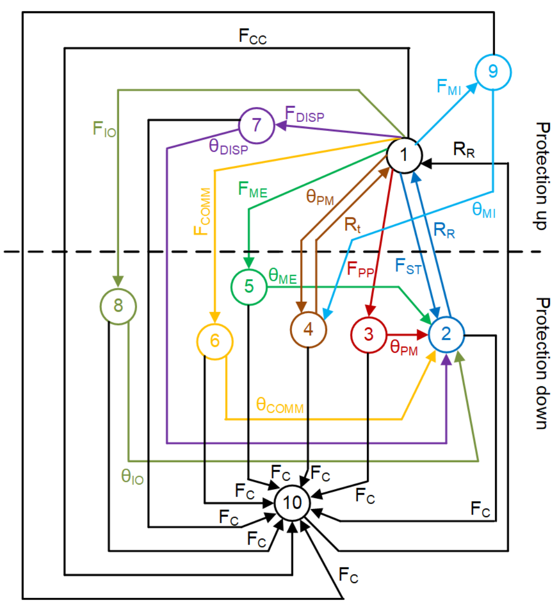

Fig. 13. State diagram of updated Markov base model

The states are described in Table II. Many of the parameters are taken from [15] and updated as applicable to reflect changes in reliability or typical operation practice.

Table III provides the parameters that are Markov model inputs. To keep the units consistent, we calculate all event transition rates in terms of occurrences per hour.

Table II
Summary of Markov States

Markov state number	Description
1	Normal operating state
2	Failure detected and waiting for repair
3	Failure occurred and not covered by self-test
4	Device was out of service while being tested
5	Analog/metering failure occurred
6	Communications failure occurred
7	Display failure occurred
8	Input/output failure occurred
9	Firmware update or maintenance identified
10	Fault on power system occurred

Table III
Model Parameters

Parameter	Value	Description
F_P	$2.283 \bullet 10^{-7}$ failures/hour	Relay failure rate
θ_{PM}	Variable	Periodic testing interval
F_{ST}	$1.712 \bullet 10^{-7}$ failures/hour	Failures detected by relay self-tests
R_R	0.04167 repairs/hour	Relay repair rate
F_{ME}	$9.2462 \bullet 10^{-9}$ failures/hour	Analog input failures
θ_{ME}	120 tests/hour	Analog input test rate
F_{COMM}	$9.132 \bullet 10^{-9}$ failures/hour	Communications failures
θ_{COMM}	120 tests/hour	Communications failure tested every 30 seconds
F_{DISP}	$2.055 \bullet 10^{-8}$ failures/hour	Device display/HMI failures
θ_{DISP}	Variable, set to θ_{PM}	Display/HMI inspection rate
F_{IO}	$1.1370 \bullet 10^{-8}$ failures/hour	Digital I/O failures
θ_{IO}	Variable, set to θ_{PM}	Digital I/O testing
F_{PP}	$3.425 \bullet 10^{-9}$ failures/hour	Other failures not caught by any self-test
F_{MI}	$6.849 \bullet 10^{-7}$ repairs/hour	Manufacturer bulletin required maintenance
θ_{MI}	$2.283 \bullet 10^{-4}$ response/hour	Time to respond to manufacturer bulletin
R_t	0.25 tests/hour	4 hours to test a relay
F_{C_HIGH} F_{C_LOW}	$2.283 \bullet 10^{-4}$ faults/hour (high) $5.708 \bullet 10^{-5}$ faults/hour (low)	Occurrence of power system faults
F_{CC}	$4.566 \bullet 10^{-10}$ failures/hour	Common cause failures

A. Comments on Model Parameters

1) Relay Failure Rate

A baseline value of an MTBF of 500 years is assumed encompassing any relay failure regardless of the cause. The annual relay failure rate is simply the reciprocal of MTBF. And lastly, for consistency in units, we convert all failure rates to failures per hour, as calculated in (1).

$$F_p = (0.002 \text{ failures/year}) \bullet \left(\frac{1}{8,760 \text{ hours per year}} \right) = 2.283 \bullet 10^{-7} \text{ failures/hour} \quad (1)$$

2) Rate of Relay Failures Detected by Self-Tests

A baseline value for self-testing effectiveness of 75 percent is assumed based on data provided in Section IV. The self-testing effectiveness and relay failure rate can be used to calculate the rate of relay failures detected by self-tests in (2).

$$F_{ST} = ST \bullet F_P = (0.75) \bullet \left(2.283 \bullet 10^{-7} \text{ failures/hour} \right) = 1.712 \bullet 10^{-7} \text{ failures/hour} \quad (2)$$

3) Relay Repair Rate

Relay repair rates vary depending on various factors. Reference [15] cites several references and assumes an average five-day repair time. After reviewing and also making the assumption that a spare relay is available for replacements, we adjusted to an average one-day repair time and calculated in terms of repairs per hour in (3).

$$R_R = \left(\frac{1}{24 \text{ hours/repair}} \right) = 0.04167 \text{ repairs per hour} \quad (3)$$

4) Rate of Relay Failures Associated With the Analog Inputs

Based on the data in Table I, approximately 4.5 percent of relay failures are associated with failure of the analog inputs. Additional automatic testing methods, such as meter tests, are discussed in Section II. If we assume that such meter tests are 90 percent effective at detecting failures of the analog inputs, we can calculate the failure rate of the analog inputs in (4).

$$F_{ME} = (0.045) \bullet (0.9) \bullet \left(2.283 \bullet 10^{-7} \text{ failures/hour} \right) = 9.2462 \bullet 10^{-9} \text{ failures/hour} \quad (4)$$

5) Rate of Automated Testing of Analog Inputs

Several methods have been described to test the analog inputs. Depending on the specific logic, whether communications to another device like an automation controller, communications processor, or supervisory control and data acquisition (SCADA) master are required, the time can vary from cycles to minutes. We assume an average time of one test every 30 seconds, or 120 tests every hour.

6) Rate of Relay Failures Associated With a Failure of Communications

Based on the data in Table I, approximately four percent of relay failures are associated with some variety of failure in communications that can impact protection. Reference [8] cites a typical data integrity encoding method used in communications channels associated with line current differential protection, where the probability of a data error going undetected is below 1.2 • 10^{-10}. The likelihood of an undetected failure on other protection channel types is similarly very small. With such low probabilities of communications errors going undetected, we assume 100 percent of communications failures are detected without losing accuracy to the overall model. The failure rate due to failures in communications is calculated in (5).

$$F_{COMM} = (0.04) \bullet (1.0) \bullet \left(2.283 \bullet 10^{-7} \text{ failures/hour} \right) = 9.132 \bullet 10^{-9} \text{ failures/hour} \quad (5)$$

7) Rate of Automated Testing of Communications

Detection of communications failures can be between cycles and minutes depending on the type of channel and nature of the failure. We assume an average time of one test every 30 seconds or 120 tests every hour.

8) Rate of Relay Failures Associate With a Failed Display/HMI

Based on the data in Table I, approximately nine percent of relay failures are associated with the device display/HMI. We assume there is no self-test mechanism to catch display failures consistently and that display failures do not result in the loss of protection. The failure rate of display/HMI failures is calculated in (6).

$$F_{DISP} = (0.09) \bullet \left(2.283 \bullet 10^{-7} \text{ failures/hour} \right) = 2.055 \bullet 10^{-8} \text{ failures/hour} \quad (6)$$

9) Rate of Relay Visual Inspection of Relay Display/HMI

While it is possible to schedule a separate visual inspection, we assume as a baseline that visual inspection is performed when the rest of the periodic maintenance activities are performed.

10) Rate of Relay Failures Associated With the Digital I/O

Based on the data in Table I, approximately six percent of relay failures are associated with the digital I/Os. While there are methods of checking the integrity of output contacts outside of routine relay maintenance, they are not applicable to all relay models and vintages, and as a baseline, we assume that problems with the digital I/Os must be detected via routine testing. The failure rate of the digital I/O failures is calculated in (7).

$$F_{IO} = (0.06) \bullet \left(2.283 \bullet 10^{-7} \text{ failures/hour} \right) = 1.1370 \bullet 10^{-8} \text{ failures/hour} \quad (7)$$

11) Rate of Testing of Digital I/Os

Testing of digital I/Os is typically done as part of periodic maintenance activities.

12) All Other Relay Failures Not Caught by Self-Testing

Based on the data in Table I, approximately 1.5 percent of relay failures are associated with some cause not detected by self-tests, and not included in the other categories already defined. The failure rate of relay failures due to the other causes is then calculated in (8).

$$F_{PP} = (0.015) \bullet (2.283 \bullet 10^{-7} \text{ failures/hour}) = 3.425 \bullet 10^{-9} \text{ failures/hour} \quad (8)$$

13) Manufacturer Bulletin Requiring Maintenance

Manufacturers will issue recommended maintenance bulletins. One example is if a firmware defect is identified, then the manufacturer sends out a notification to end users advising them of the firmware defect and recommended action, to proactively upgrade the firmware before the defect results in a failure. We assume that protection is not compromised, even though required maintenance has been identified. For simplicity, we estimate the required maintenance by multiplying the relay failure rate by a constant factor. After reviewing data on bulletins, we assume a factor (k) of 3, and the maintenance rate is calculated in (9).

$$F_{MI} = k \bullet F_P = (3) \bullet (2.283 \bullet 10^{-7} \text{ failures/hour}) = 6.849 \bullet 10^{-7} \text{ failures/hour} \quad (9)$$

14) Time to Respond to Manufacturer's Bulletins

Time to respond to a service bulletin can vary from days to no time at all. Factors such as availability of personnel and bulletin severity can impact the time to respond. We assume an average time to respond to a bulletin of six months. The rate of performing maintenance is calculated in (10).

$$\theta_{MI} = \left(\frac{1}{0.5 \text{ years}}\right) \bullet \left(\frac{1}{8,760 \text{ hours/year}}\right) = 2.283 \bullet 10^{-4} \text{ failures/hour} \quad (10)$$

15) Relay Out of Service Due to Routine/Periodic Test Rate

Reference [1] assumes an average time to test a relay of 0.5 hours. Relay testing tools have improved significantly since the publication of [1], in terms of the relay test set hardware, software, and processes in place. However, manufacturers have added more functions and features to digital relays that were not available since [1]. We considered two cases: testing simple feeder overcurrent relay and end-to-end testing of a line current differential system with backup protection involving multiple relays. The range of times, including isolation processes, etc., seemed to range between one hour and one working day. We assumed an average relay testing time of 4 hours, or 0.25 tests per hour.

16) Rate of Power System Faults

The likelihood of a fault on the equipment depends on a variety of factors, including location and physical construction. For example, for an overhead 345 kV transmission line in an area with a high-keraunic level (e.g., heavy lightning activity), the likelihood of a fault is much higher, simply due to the exposure to lightning when compared to a 15 kV industrial cable within a plant facility. Recognizing the variance in fault occurrence, we assumed two cases: a high-occurrence rate and a low-occurrence rate. This approach has been taken when evaluating the cumulative impact of through-faults on transformer damage [16]. Typical failure and fault rates are examined for equipment on an overhead utility line and for the case of a medium-voltage feeder in an industrial facility. Data from available standards are used to estimate the number of faults per year for the two cases, and an average value is assumed for each [17] [18]. For the high-occurrence case, we assume two faults per year. The occurrence rate for this high-occurrence case is calculated in (11).

$$F_{C\_HIGH} = (2 \text{ faults/year}) \bullet \left(\frac{1}{8,760 \text{ hours/year}}\right) = 2.283 \bullet 10^{-4} \text{ faults/hour} \quad (11)$$

For the low-occurrence case, we assume one fault every two years. The low-occurrence rate is calculated in (12).

$$F_{C\_LOW} = \left(\frac{1 \text{ fault}}{2 \text{ years}}\right) \bullet \left(\frac{1}{8,760 \text{ hours/year}}\right) = 5.708 \bullet 10^{-5} \text{ faults/hour} \quad (12)$$

17) Rate of Simultaneous Failures

In [1], a common cause failure rate of one failure in one million hours is assumed. Common cause failures occur when a failure causes both a fault on the power system and the failure of a protection device. After reviewing real-world data, we assume an average value of 250,000 years for a mean time between occurrences. The occurrence rate is then calculated in (13).

$$F_{CC} = \left(\frac{1 \text{ failure}}{250,000 \text{ years}}\right) \bullet \left(\frac{1}{8,760 \text{ hours/year}}\right) = 4.566 \bullet 10^{-10} \text{ failures/hour} \quad (13)$$

B. State Transition Matrix and Mathematical Model

The state transition matrix associated with the updated Markov model is given in (14).

$$T = \begin{bmatrix} a_{11} & F_{ST} & F_{PP} & \theta_{PM} & F_{ME} & F_{COMM} & F_{DISP} & F_{IO} & F_{MI} & F_{CC} \\ R_R & a_{22} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & F_C \\ 0 & \theta_{PM} & a_{33} & 0 & 0 & 0 & 0 & 0 & 0 & F_C \\ R_T & 0 & 0 & a_{44} & 0 & 0 & 0 & 0 & 0 & F_C \\ 0 & \theta_{ME} & 0 & 0 & a_{55} & 0 & 0 & 0 & 0 & F_C \\ 0 & \theta_{COMM} & 0 & 0 & 0 & a_{66} & 0 & 0 & 0 & F_C \\ 0 & \theta_{DISP} & 0 & 0 & 0 & 0 & a_{77} & 0 & 0 & F_C \\ 0 & \theta_{IO} & 0 & 0 & 0 & 0 & 0 & a_{88} & 0 & F_C \\ 0 & 0 & 0 & \theta_{MI} & 0 & 0 & 0 & 0 & a_{99} & F_C \\ R_R & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a_{1010} \end{bmatrix} \quad (14)$$

The diagonal terms in (14) are defined by (15) through (24).

$$a_{11} = 1 - F_{ST} - F_{PP} - \theta_{PM} - F_{ME} - F_{COMM} - F_{DISP} - F_{IO} - F_{MI} - F_{CC} \quad (15)$$

$$a_{22} = 1 - R_R - F_C \quad (16)$$

$$a_{33} = 1 - \theta_{PM} - F_C \quad (17)$$

$$a_{44} = 1 - R_T - F_C \quad (18)$$

$$a_{55} = 1 - \theta_{ME} - F_C \quad (19)$$

$$a_{66} = 1 - \theta_{COMM} - F_C \quad (20)$$

$$a_{77} = 1 - \theta_{DISP} - F_C \quad (21)$$

$$a_{88} = 1 - \theta_{IO} - F_C \quad (22)$$

$$a_{99} = 1 - \theta_{MI} - F_C \quad (23)$$

$$a_{1010} = 1 - R_R \quad (24)$$

The probability vector that gives the probability that the system is in each state is defined by (25).

$$P^T = \begin{bmatrix} P_1 & P_2 & P_3 & P_4 & P_5 & P_6 & P_7 & P_8 & P_9 & P_{10} \end{bmatrix} \quad (25)$$

The state transition matrix and probability vector are combined in (26).

$$P^T \left[T - 1 \right] = 0 \quad (26)$$

where:

I is the identity matrix.

Solving (26) for the probability vector then gives the overall probabilities for each state of the system in the model. We are specifically interested in calculating the unavailability of the protection. To calculate the unavailability, we simply add together the system states where the protective relay is unavailable, as in (27).

$$\text{ProtUN} = P_2 + P_3 + P_4 + P_5 + P_6 + P_8 + P_{10} \quad (27)$$

VIII. Acknowledgment

We gratefully acknowledge the contributions of Daqing Hou and Ryan McDaniel for their guidance and questions. We also appreciate the data analysis and review performed by Alec Holtzapfel.

IX. References

[1] J. Kumm, E. O. Schweitzer, III, and D. Hou, “Assessing the Effectiveness of Self-Tests and Other Monitoring Means in Protective Relays,” proceedings of the 30th Annual Minnesota Power Systems Conference, Minneapolis, MN, October 1994.

[2] K. Zimmerman, “SEL Recommendations on Periodic Maintenance Testing of Protective Relays,” December 2010. Available: selinc.com.

[3] NERC Standard PRC-005-6, Protection System, Automatic Reclosing and Sudden Pressure Relaying Maintenance. Available: nerc.com.

[4] ANSI/NETA MTS-2019 Standard, Maintenance Testing Specifications for Electrical Power Equipment & Systems, NETA, 2019.

[5] K. Zimmerman, “Commissioning of Protective Relay Systems,” proceedings of the 34th Annual Western Protective Relay Conference, Spokane, WA, October 2007. Available: selinc.com.

[6] 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. Available: selinc.com.

[7] A. Hargrave, “Continuous Maintenance Testing With Automatic Meter Comparisons,” Application Guide, AG2011-03.

[8] B. Kasztenny, N. Fischer, K. Fodero, and A. Zvarych, “Communications and Data Synchronization for Line Current Differential Schemes,” proceedings of the 38th Annual Western Protective Relay Conference, Spokane, WA, October 2011.

[9] M. Diehl and A. Dulmage, “Understanding and Effectively Using the SEL MIRRORED BITS Protocol,” Application Guide, AG2018-24. Available: selinc.com.

[10] T. Tibbals and D. Dolezilek, “Case Study: New Testing and Verification Practices for Virtual Wiring Among IEDs Via Ethernet Communications,” proceedings of the Southern African Power System Protection Conference, Johannesburg, South Africa, November 2010. Available: selinc.com.

[11] J. Kumm, M. Weber, E. O. Schweitzer, III, and D. Hou, “Philosophies for Testing Protective Relays,” proceedings of the 20th Annual Western Protective Relay Conference, Spokane, WA, October 1993.

[12] P. Anderson, G. Chintaluri, S. Magbuhat, and R. Ghajar, “An Improved Reliability Model for Redundant Protective Systems – Markov Models,” IEEE PES Winter Meeting, Baltimore, MD, January 1996.

[13] E. O. Schweitzer, III, B. Fleming, and T. Lee, “Reliability Analysis of Transmission Protection Using Fault Tree Methods,” proceedings of the 24th Annual Western Protective Relay Conference, Spokane, WA, October 1997.

[14] D. Haas, M. Leoni, K. Zimmerman, A. Genz, and T. Mooney, “The Useful Life of Microprocessor-Based Relays: A Data-Driven Approach,” proceedings of the 72nd Annual Conference for Protective Relay Engineers, College Station, TX, March 2019.

[15] E. O. Schweitzer, III, D. Whitehead, H. Altuve Ferrer, D. Tziouvaras, D. Costello and D. Escobedo, “Line Protection: Redundancy, Reliability, and Affordability,” proceedings of the 64th Annual Conference for Protective Relay Engineers, College Station, TX, April 2011.

[16] IEEE Standard C57.109-2018, *IEEE Guide for Liquid-Immersed Transformers Through-Fault-Current Duration.*

[17] R. Brown, *Electric Power Distribution Reliability,* 2nd ed. CRC Press, Taylor and Francis Group, LLC, Boca Raton, FL, 2009, pp. 182–187.

[18] IEEE Standard 3000 Standards Collection for Industrial and Commercial Power Systems, Historical Reliability Data for IEEE 3006 Standards: Power Systems Reliability, 2012.

X. Biographies

Adrian Genz is a quality director with Schweitzer Engineering Laboratories, Inc. (SEL). He joined SEL in 2007 as a hardware engineer and has held engineering design and management positions. He received his BS in electrical engineering from Utah State University in 2004 and his MS in electrical engineering from Brigham Young University in 2006.

Derrick Haas graduated from Texas A&M University with a BSEE. He worked as a distribution engineer for CenterPoint Energy in Houston, Texas, until 2006 when he joined Schweitzer Engineering Laboratories, Inc. (SEL). Derrick has held several titles, including field application engineer, senior application engineer, team lead, and his current role of regional technical manager. He is a senior member of the IEEE and is involved in the IEEE Power System Relaying Committee.

Karl Zimmerman is a principal engineer with Schweitzer Engineering Laboratories, Inc. (SEL) in Saint Louis, Missouri. He is an active member of the IEEE Power System Relaying Committee and past chairman of the Line Protection Subcommittee. Karl received his BSEE degree from the University of Illinois at Urbana-Champaign. He has authored over 40 technical papers and application guides on protective relaying.

20220329 • TP7050-01