How Disruptions in DC Power and Communications Circuits Can Affect Protection

Karl Zimmerman and David Costello
Schweitzer Engineering Laboratories, Inc.

This paper was presented at the 68th Annual Conference for Protective Relay Engineers and can be accessed at: http://dx.doi.org/10.1109/CPRE.2015.7102189.

For the complete history of this paper, refer to the next page.

Presented at the
43rd Annual Western Protective Relay Conference
Spokane, Washington
October 18–20, 2016

Previously presented at the
70th Annual Georgia Tech Protective Relaying Conference, April 2016,
PowerTest Conference, March 2016,
and 2nd Annual PAC World Americas Conference, September 2015

Originally presented at the
68th Annual Conference for Protective Relay Engineers, March 2015

How Disruptions in DC Power and Communications Circuits Can Affect Protection

Karl Zimmerman and David Costello, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—Modern microprocessor-based relays are designed to provide robust and reliable protection even with disruptions in the dc supply, dc control circuits, or interconnected communications system. Noisy battery voltage supplies, interruptions in the dc supply, and communications interference are just a few of the challenges that relays encounter.**

This paper provides field cases that investigate protection system performance when systems are subjected to unexpected switching or interruptions in dc or communications links. The discussion emphasizes the importance of environmental and design type testing, proper dc control circuit design and application, reliable and safe operating and maintenance practices with respect to dc control circuits and power supplies, and considerations for reliable communications design, installation, and testing. Some practical recommendations are made with regard to engineering design and operations interface with equipment to improve protection reliability and reduce the possibility of undesired operations.

I. The Role of DC and Communications in Protection Systems

Fig. 1 shows a one-line diagram of a typical two-terminal line protection system using distance relays in a communications-assisted pilot scheme.

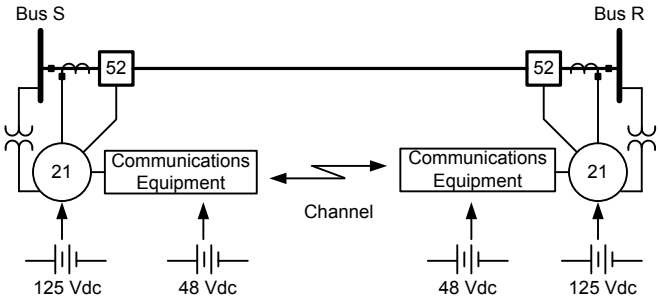

Fig. 1. Two-Terminal Digital Line Pilot Protection Scheme.

To successfully clear all faults on the line within a prescribed time (e.g., less than 5 cycles), all of the elements in Fig. 1—breaker, relay, dc supplies, communications, current transformers (CTs), voltage transformers (VTs), and wiring—need to perform correctly. It is not unusual for lines to have redundant and backup protection schemes, often using different operating principles, with multiple channels and/or dc supplies.

Human factors (such as design, settings, procedures, and testing) are not shown in Fig. 1 but must also perform correctly. Additionally, security is as important a consideration as dependability. All of the elements and human factors must perform correctly to ensure that the protection scheme correctly restrains for out-of-section faults or when no fault is present.

II. The Effect of DC and Communications Disruptions on Overall Reliability

Protection systems must be robust even with transients, harsh environmental conditions, and disruptions in dc supply, dc circuits, or interconnected communications. These disruptions include loss of dc power due to failure or human action, noise on the battery voltage, dc grounds, interruptions in dc supply, and subsequent restart or reboot sequences. In the case of communications, these disruptions include channel noise, channel delays, interruptions due to equipment problems or human action, unexpected channel switching, and restart or resynchronization sequences.

Fault tree analysis has been beneficial in analyzing protection system reliability, comparing designs, and quantifying the effects of independent factors. For example, the rate of total observed undesired operations in numerical relays is 0.0333 percent per year (a failure rate of $333 \cdot 10^{-6}$). By comparison, the rate of undesired operations in line current differential (87L) schemes where disturbance detection is enabled is even lower at 0.009 percent per year (a failure rate of $90 \cdot 10^{-6}$). However, undesired operations caused by relay application and settings errors (human factors) are 0.1 percent per year (a failure rate of $1{,}000 \cdot 10^{-6}$) [1].

Unavailability, which is the failure rate multiplied by the mean time to repair, is another measure used to compare reliability. The unavailability of dc power systems is low at $30 \cdot 10^{-6}$, compared with $137 \cdot 10^{-6}$ for protective relays and $1{,}000 \cdot 10^{-6}$ for human factors. These data assume a faster mean time to repair a dc power system problem (one day) compared to relays and human factors (five days). Communications component unavailability indices are similar to those of protective relays [2].

The North American Electric Reliability Corporation (NERC) *State of Reliability 2014* report found that from the second quarter of 2011 to the third quarter of 2013, 5 percent of misoperations involved the dc system as the cause, compared with 15 percent for communications failures, 21 percent for relay failures, and 37 percent for human factors [3].

From these data, we can see that dc and communications failures are a small but significant factor in reliability.

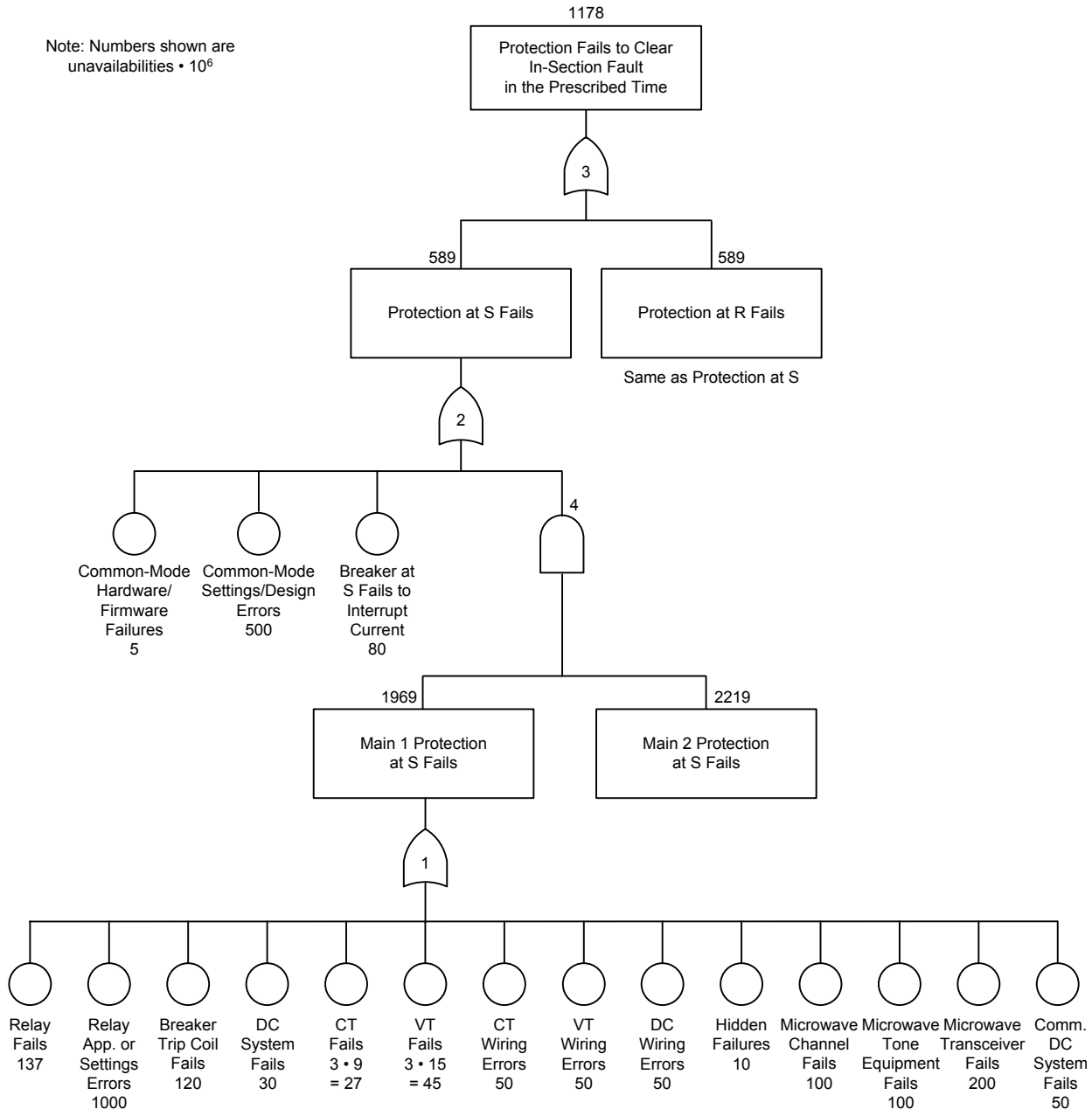

Fig. 2. Dependability Fault Tree for Dual-Redundant Permissive Overreaching Transfer Trip (POTT) Scheme [2].

Fault trees allow us to see how the failure rate of one device impacts the entire system (see Fig. 2). Fault trees also allow us to evaluate how hidden failures, common-mode failures, improved commissioning tests, and peer reviews impact reliability.

However, fault trees do not easily identify how a failure or activity in one subsystem affects another subsystem. Inspired by Christopher Hart, acting chairman of the National Transportation Safety Board, we wanted to investigate the interaction of components, subsystems, and human factors on the reliability of the entire protection system. At the 2014 Modern Solutions Power Systems Conference, Mr. Hart spoke of the aviation industry as a complex system of coupled and interdependent subsystems that must work together successfully so that the overall system works. In aviation, a change in one subsystem likely has an effect throughout other subsystems (see Fig. 3) [4].

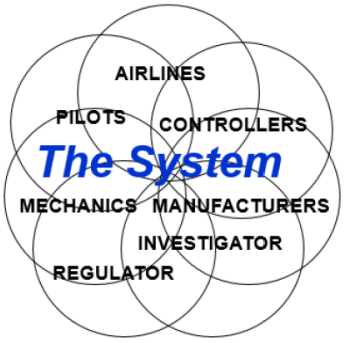

Fig. 3. Aviation Safety Involves Complex Interactions Between Subsystems.

The protection system, and the entire power system, is very similar to the aviation industry. Fault trees and high-level apparent cause codes do not necessarily make these subsystem interdependencies apparent.

For example, in December 2007, while performing maintenance testing, a technician bumped a panel and a microprocessor-based, high-impedance bus differential relay closed its trip output contact (87-Z OUT1 in Fig. 4), tripping the bus differential lockout relay (86B in Fig. 4). Fortunately, due to testing that was being performed that day, the lockout relay output contacts were isolated by open test switches that kept it from tripping any of the 230 kV circuit breakers.

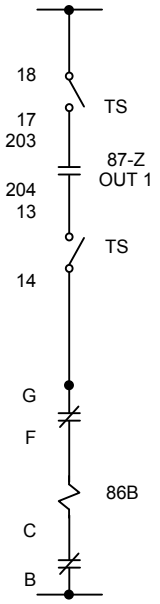

Fig. 4. DC Control Circuit Showing Bus Differential Trip Output.

The bus differential relay contact closure was easily repeated by bumping the relay chassis. The simple apparent cause could have been classified as human error, product defect (failure to meet industry shock, bump, and vibration standards), or relay hardware failure. However, subsequent analysis by the relay manufacturer showed momentary low resistance across the normally open contact when the chassis was bumped. Additionally, visual inspection noted evidence of overheating in the contact area (the outside of the plastic case was slightly dimpled). The contact part was x-rayed while it was still mounted on the main printed circuit board. The adjacent, presumed-healthy contact was x-rayed for comparison. The x-ray images are shown in Fig. 5, with the adjacent, healthy Form-C contact on the left and the damaged Form-C contact on the right. In each contact, there is a stationary normally open contact surface (top), a moving contact surface (center), and a stationary normally closed contact surface (bottom). Note the difference in contact surfaces and spacing. The relay manufacturer estimated that the output contact was likely not defective but rather had been damaged due to interrupting current in excess of the contact's interruption rating.

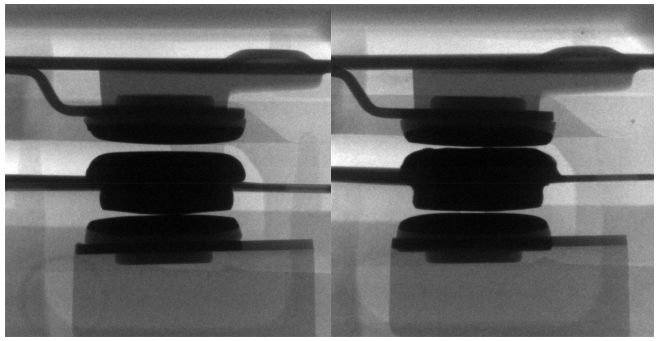

Fig. 5. X-Ray Images of the Healthy, Adjacent Contact (Left) and Damaged Contact (Right).

The output contact manufacturer further inspected the output contact part. The output relay cover was removed and the inside of the part was observed and photographed (see Fig. 6). The plastic components were melted, the spring of the contact point was discolored and deformed by heat, and the contact surfaces were deformed, rough, and discolored. The root cause of the contact damage was confirmed: at some point prior to the misoperation, the interrupting current was in excess of the contact's interruption rating.

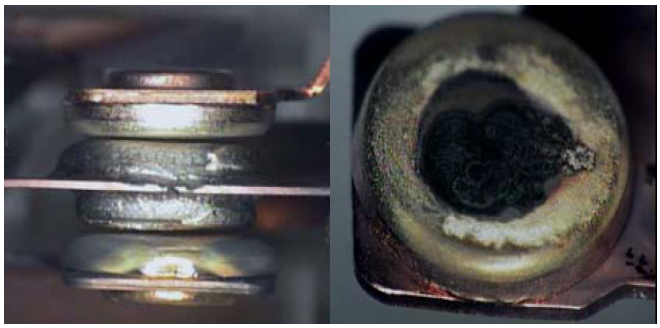

Fig. 6. Pictures From Contact Manufacturer Confirming Heat Damage From Exceeding Current Interruption Rating.

It is important at this point to persist in analysis and examine testing mandates, procedures, and work steps to find root cause. In this case, commissioning testing, represented as one human factor subsystem in the fault tree (relay application), performed to improve reliability was flawed in such a way that the protective relay hardware was damaged and induced a failure in that subsystem. In addition, maintenance testing, mandated by NERC and intended to improve reliability, was flawed in such a way that the relay was damaged and could have potentially caused a misoperation.

In this example, the failure mode was a relay contact closing when the relay chassis was bumped. According to NERC data, 60 percent of root-cause analyses stop at determining the mode [5]. True root-cause analysis requires us to dig deeper to understand the failure mechanism or process that led to the failure. Then, we can educate others and ensure that improvements prevent the problem from reoccurring. In NERC contributing and root-cause vernacular, this incident would be due to a *defective relay* (A2B6C01) caused by an *incorrect test procedure* (A5B2C07) caused by a *failure to ensure a quality test procedure* (A4B2C06). An important

theme in the case studies that follow is how an action or failure in one subsystem affects other subsystems and overall reliability.

III. Traditional DC Problems

The dc control circuits used in protection systems have always been complex. Problems that need to be mitigated include circuit transients, sneak or unintended paths, stored capacitance, let-through and leakage currents, and more [6]. For example, electromechanical auxiliary relays were once commonly used for local annunciation, targeting, or contact multiplication. Some of these relays were high speed and quite sensitive. Care was taken to ensure that let-through currents from connected output contacts did not inadvertently cause these auxiliary relays to pick up.

Especially when used with transformer sudden pressure relays with poor dielectric withstand capability, extra security measures were taken to prevent auxiliary relays from operating in case a voltage surge caused a flashover in the normally open contacts of the pressure relay. In Fig. 7, the normally closed contact from the sudden pressure relay (63) shunts the auxiliary relay operating coil (94) so that if the normally open contact flashes during a voltage transient, the auxiliary relay will not operate [7].

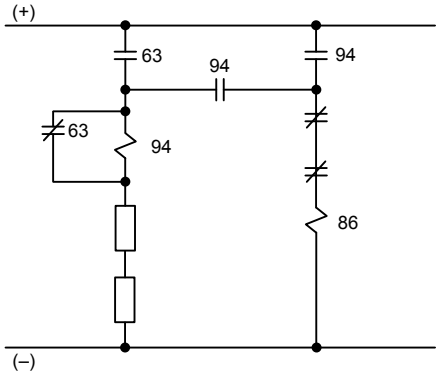

Fig. 7. Typical Security Precaution for Dielectric Strength Failure of a Sudden Pressure Relay Contact.

Precautions must be taken to avoid these same dc circuit anomalies as we transition to new technology platforms and design standards. As auxiliary relays are replaced by microprocessor-based relays, pick-up time delays are required on relay inputs that are used to directly monitor these same sudden pressure relay normally open contacts to maintain security [8].

IV. Traditional Communications Problems

Communications that are used for protection systems perform well but are not perfect. One well-known communications component problem involves the application of power line carrier for transmission line protection schemes. In directional comparison blocking (DCB) schemes, high-frequency transients can produce an undesired momentary block signal during an internal fault. Fig. 8 shows one such incident. Engineers must adjust frequency bandwidths, add contact recognition delay, or tolerate the possibility of a slight delay in tripping for internal faults.

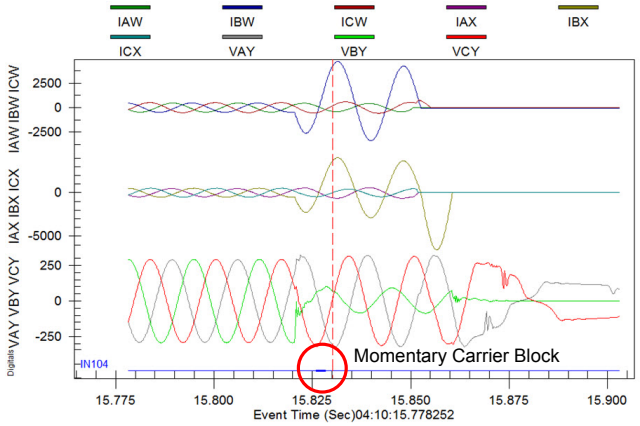

Fig. 8. Momentary Carrier Block Input Produced by Fault-Induced Transient.

Conversely, if an external fault occurs, the momentary dropout of the carrier blocking signal, referred to as a "carrier hole," can produce an undesired trip, as shown in Fig. 9. These dropouts are often attributed to a flashover of the carrier tuner spark gap and can be avoided by improved maintenance of the carrier equipment or can be dealt with by adding a dropout delay on the received block input.

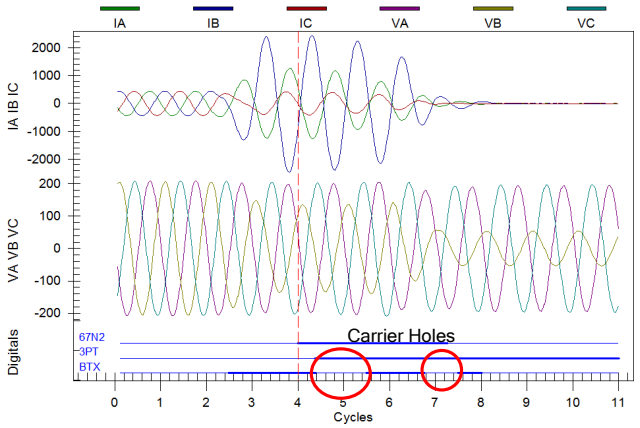

Fig. 9. Carrier Holes in a DCB Scheme.

Protection system communications options today include many media in addition to power line carrier, such as microwave, spread-spectrum radio, direct fiber, multiplexed fiber networks, Ethernet networks, and more. Each medium has its own set of potential problems, such as channel noise, fault-induced transients, channel delays, dropouts, asymmetry, security, buffers and retry, interruptions due to equipment problems or human action, unexpected channel switching, and restart or resynchronization sequences. The trends in our industry include communicating more, exploring new and creative applications for communications, and replacing intrastation copper wiring with microprocessor-based devices and communications networks. As more and more communications and programmable logic are used, it is critical to analyze, design, and test for potential communications problems.

V. Traditional Procedure Problems

The sequence in which work tasks are performed is important. A familiar example will highlight this concept. A primary microprocessor-based line relay had been taken out of service for routine maintenance testing. Trip and breaker failure initiate output contacts, as well as voltage and current circuit inputs, had been isolated by opening test switches. After successful secondary-injection testing, the relay tripped the circuit breaker during the process of putting the protection system back into service [9].

Event data showed only one current (A-phase) at the time of trip. This indicated that the technician had reinstalled the trip circuit first by closing the trip output test switch. Next, a single current was reinstalled by closing its test switch. Because there was load flowing through the in-service breaker and CTs, the relay, at this step in the sequence of events, measured A-phase current and calculated 3I0 current and no voltages. It issued a trip.

This was a valuable lesson for this utility in the early adoption phase of these relays and led to a specific procedure and sequence that is used when returning a relay to service. The sequence of steps used to restore the system to service is the reverse of that used to remove the system from service and is as follows.

1. Place all three voltage circuits back into service (i.e., close the voltage test switches).
2. Place all three current circuits back into service.
3. Use meter commands or event data to verify the proper phase rotation, magnitude, and polarity of the analog measurements.
4. Reinstall the dc control inputs.
5. Use target commands or event data to verify the statuses of control inputs.
6. Reset relay targets and verify that trip and breaker failure outputs are reset.
7. Place the trip and breaker failure output circuits back into service.

Similarly, when disrupting communications circuits or dc power, we must thoughtfully consider what parts of the protection system should be isolated and the careful order of steps to take in the process of returning the system to service. Analysis, design, and testing should be devoted to this, considering our increased dependence on interdevice communications and programmable logic.

The following section highlights some interesting system events where disruptions in dc and/or communications directly affected protection.

VI. Protection System Events Caused by DC or Communications System Disruptions

A. Case Study 1: Breaker Flashover Trip After Relay Restart

Fig. 10 shows the simplified one-line diagram of a 161 kV substation for an event in which a breaker failure flashover logic scheme operated after a relay restart (i.e., dc power supply to the relay was cycled off and on), causing a substation bus lockout.

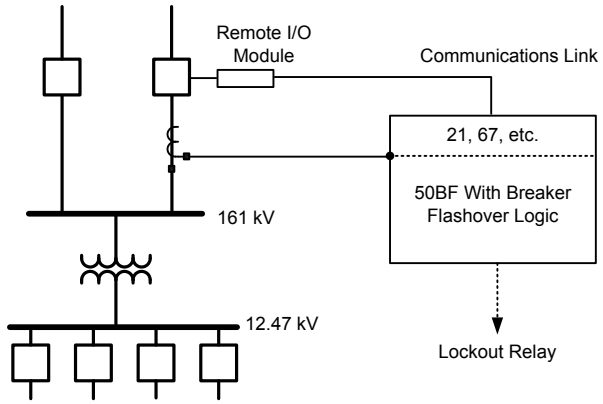

Fig. 10. Case Study 1 System One-Line Diagram Uses Remote I/O Module for Breaker Interface.

In this system, the breaker status auxiliary contacts (52a and 52b) and other monitored breaker elements are connected to a remote I/O module. The I/O module converts hard-wired inputs and outputs to a single fiber link from the module at the breaker to the relay located in a remote control house (see Fig. 11).

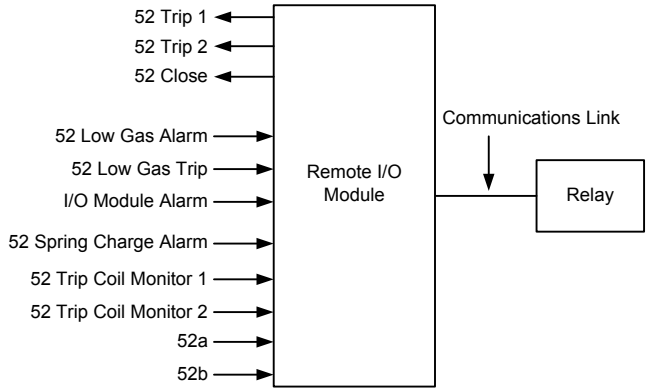

Fig. 11. Monitored Points From the 161 kV Circuit Breaker Using a Remote I/O Module and Fiber Interface to the Relay.

The user applied the I/O module to eliminate extra wiring and inherent noise and hazards associated with long (i.e., several hundred feet) runs of copper wire. Also, the fiber connection was continuously monitored.

The monitored communications link can be set to default to a safe state, as specified by the engineer. In this case, if communications were lost (e.g., fiber was disconnected or damaged or there was an I/O module failure), the breaker status would default to its last known state before the communications interruption.

The breaker failure flashover logic is shown in Fig. 12. It detects conditions where current (50FO) flows through an open breaker (NOT 52a). When a breaker trips or closes, the logic is blocked with a 6-cycle dropout delay. The user can define a time delay for breaker failure to be declared. In this case, it was 9 cycles.

The event data in Fig. 13 show the status of the relay elements immediately after the power cycle. Current is already present, but the breaker status (52AC1) is a logical 0 (not asserted). Thus, the breaker failure flashover element (FOBF1) asserts and produces the breaker failure output

(BFTRIP1), which subsequently operates the substation lockout relay.

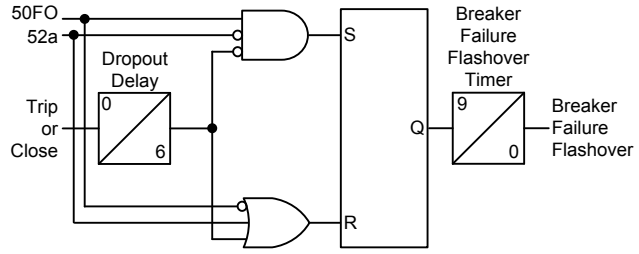

Fig. 12. Breaker Failure Flashover Logic.

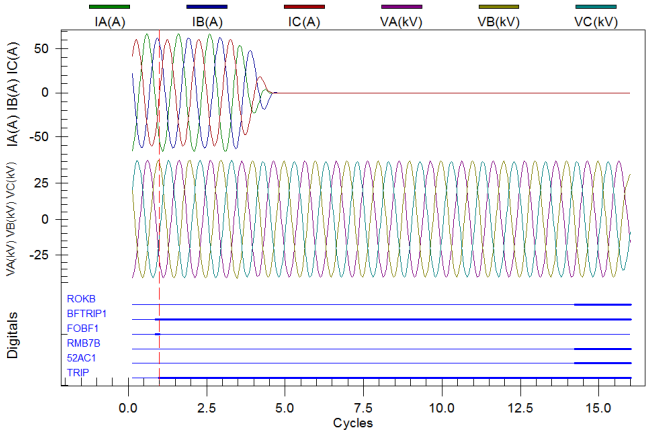

Fig. 13. Breaker Failure Flashover Logic Asserts Due to Current Measured While Breaker Is Sensed Open.

The undesired trip occurred because the breaker failure flashover logic began processing before the communications link between the I/O module and the relay was reestablished. We can see the communications link status between the relay and the I/O module (ROKB) asserted about 14 cycles later.

The event report does not show much about what happened before the trip during the relay restart process. However, from an internal sequential event record, we were able to assemble the timeline, as shown in Fig. 14.

The relay restart sets the latch (Q) and starts the 9-cycle breaker failure flashover timer. At 9 cycles, FOBF1 asserted. By the time the communications link was established (at 22 cycles), the trip had already occurred.

Important lessons were learned in this case study. Relays and I/O modules might reboot, operators may cycle power to relays when looking for dc grounds or performing other troubleshooting, relays may employ diagnostic self-test restarts, and so on. There is no default state for most logic during a relay restart. In a relay restart, all of the logic resets and begins processing from an initial de-energized state, as is the case when a relay is powered up and commissioned for the first time. In this case, designers considered a loss of communications but did not consider how a loss of dc supply or relay power cycle would affect the communications status and the logic processing order during a start-up sequence.

In the breaker failure flashover logic, the breaker status is used directly in a trip decision. We should supervise the breaker failure flashover logic with the monitored communications bit (i.e., FOBF1 AND ROKB) to prevent the flashover logic from being active until communication is established. To further avoid such undesired operations, commissioning tests should include power cycles to test for secure power-up sequences in logic processing.

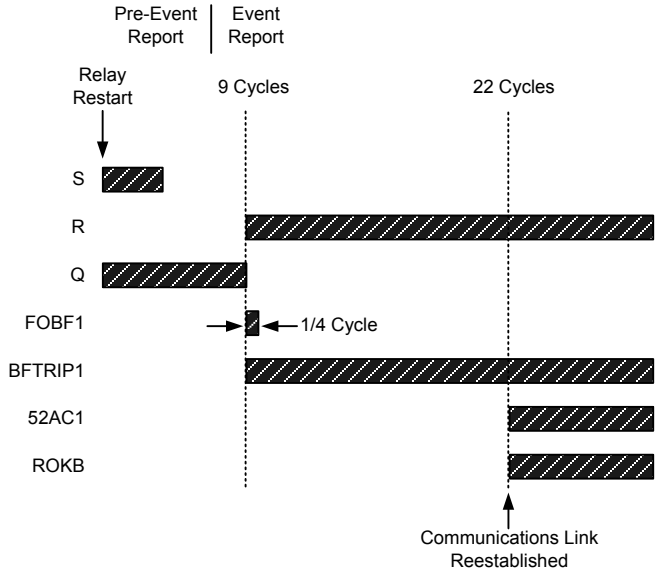

Fig. 14. Event Timeline Shows Relay Restart and Arming of Flashover Logic Before Breaker Status Is Recognized.

B. Case Study 2: Protective Relay Applied as a Lockout Relay Operates Due to a Power Cycle

In Case Study 2, a microprocessor-based transformer differential relay was applied as a lockout relay, as shown in Fig. 15. When dc power to the relay was switched off and on, the lockout logic output asserted, causing a substation trip and loss of supply to several customers.

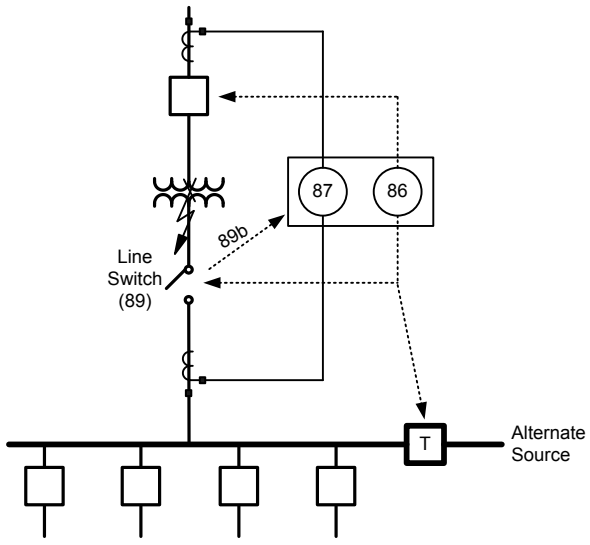

Fig. 15. One-Line Diagram of Relay Applied as a Transformer Differential Relay and Lockout Relay Together.

Discrete lockout and auxiliary relays are widely used in protection systems. Why not use a discrete lockout relay here instead of building these functions inside the microprocessor-based relay? The decision to do this was driven by several factors. One factor was reduced cost—fewer relays and less

panel space and wiring. In addition, periodic maintenance testing was reduced by having fewer devices and by extending the maintenance intervals due to the inherent self-monitoring capability of the microprocessor-based relay versus the electromechanical lockout relay. Additionally, some system events have also led engineers away from using discrete auxiliary and lockout relays. One infamous event that is often cited for this change in design was initiated by a failed auxiliary relay at Westwing substation [10].

The internal relay lockout logic for Case Study 2 is shown in Fig. 16.

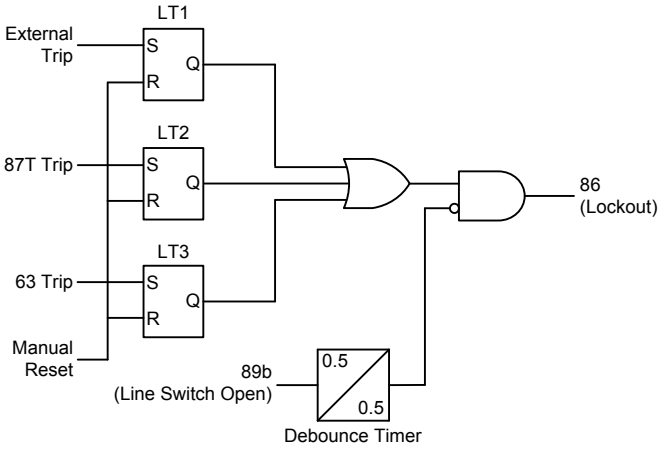

Fig. 16. Internal Lockout Logic.

The "latch" functions (LT1, LT2, and LT3) are all retained in nonvolatile memory. That is, even if the relay loses control power, it retains the status of the latch functions. In this case, an actual internal transformer fault occurred. The transformer protection (87T) and internal lockout function (86LO) operated to clear the fault. Dispatchers were able to switch load to an alternate source. All operations were correct up to this point.

The timeline in Fig. 17 shows the sequence.

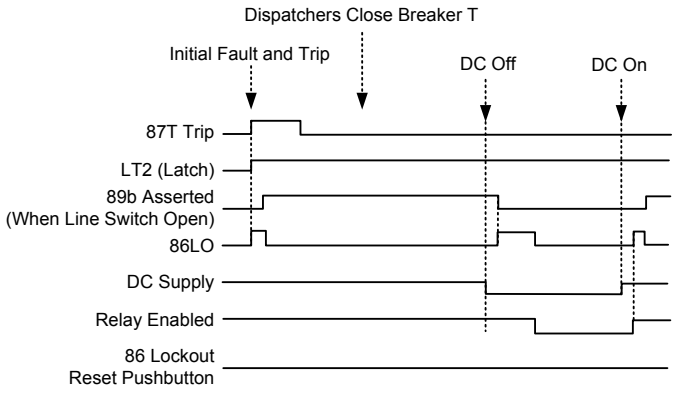

Fig. 17. Event Timeline Shows 86LO Trips for DC Off and On.

When the maintenance crew arrived at the station, the correct procedure was to reset the lockout using a pushbutton on the relay. Instead, as stated earlier, the dc supply was switched off and on. The 86LO function asserted incorrectly when dc was switched off and asserted incorrectly again when dc was switched on.

On power down, the relay stayed enabled for several cycles after the point at which logical inputs deasserted. Thus, the 89b input was sensed as deasserted (line switch closed) before the relay was disabled, producing the 86 lockout.

On power up, the relay enabled before the 89b input was sensed, thus producing the 86 lockout again.

The first and most obvious lesson learned in this case study is that, as technology changes, engineers and operators must strictly adhere to updated operating procedures for resetting lockout functions. Well-understood interfaces, such as physical lockout relays, are being mimicked or replaced, and it is important to document and train field personnel.

Another lesson learned is to test the impact of cycling dc power off and on. Protection systems should be robust, relays and I/O modules might reboot, and operators may cycle power to relays when looking for dc grounds or performing other troubleshooting. In this case, designers did not consider how a loss of dc supply or relay power cycle would affect the programmable logic processing order during a power-down or power-up sequence.

The user has since added logic so that the lockout function is supervised by a healthy relay (Relay Enabled). In addition, the line switch status is now supervised by a dropout delay that is longer than the relay power-down enable time (see Fig. 18).

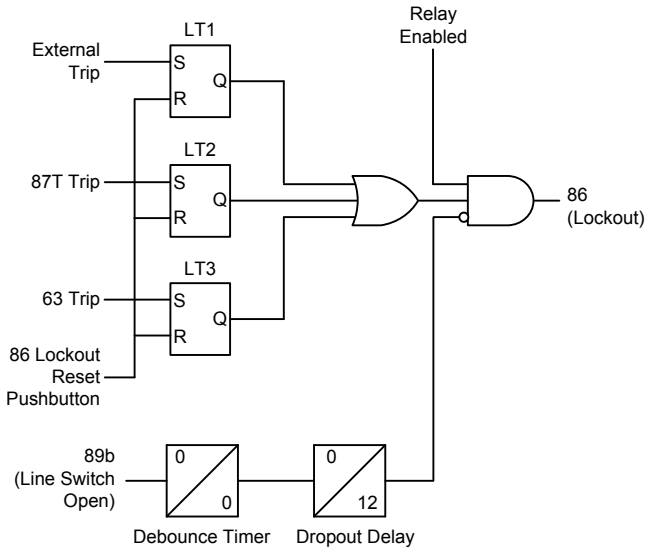

Fig. 18. Modified Lockout Function Logic.

C. Case Study 3: Direct Transfer Trip Due to a Noisy Channel

Fig. 19 shows the protection one-line diagram for a 138 kV system with two-ended transmission. The line is protected by distance and directional elements in a permissive overreaching transfer trip (POTT) scheme, along with a direct transfer trip (DTT) scheme if either end trips.

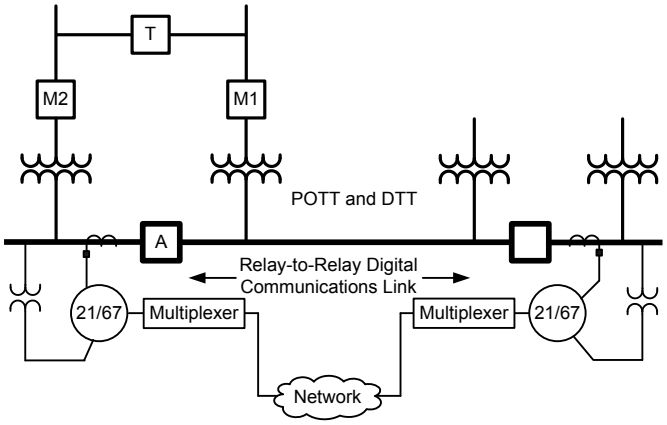

Fig. 19. One-Line Diagram of a 138 kV Transmission Line.

In this case, the communications channel is a multiplexed digital network. The channel was abnormally noisy, with about 10 channel dropouts per minute and an overall channel unavailability around 0.5 percent. One of the noise bursts and associated channel dropouts resulted in a momentary assertion of the DTT input (see Fig. 20). Note that the protection system also experienced an unrelated breaker failure.

Significant efforts are made to secure protective relays that use channels; these efforts include data integrity checks, debounce delays, disturbance detectors, watchdog counters, and more. In this case, even with a 50 percent bit error rate, the probability of a bad message getting through the relay data integrity checks was one in 49 million [11]. Although the probability was low, it was not zero, and if enough bad messages were sent, it was still possible for one to get through the integrity check, as in this case.

In this example, we see how monitoring a noisy channel may provide a leading indicator for detecting problems. Also, regardless of media and integrity checks, it is prudent to add security on schemes that use direct transfer tripping. In this case, requiring two consecutive messages (an 8-millisecond delay) instead of one (a 4-millisecond delay) improved security by an additional 10^4 factor.

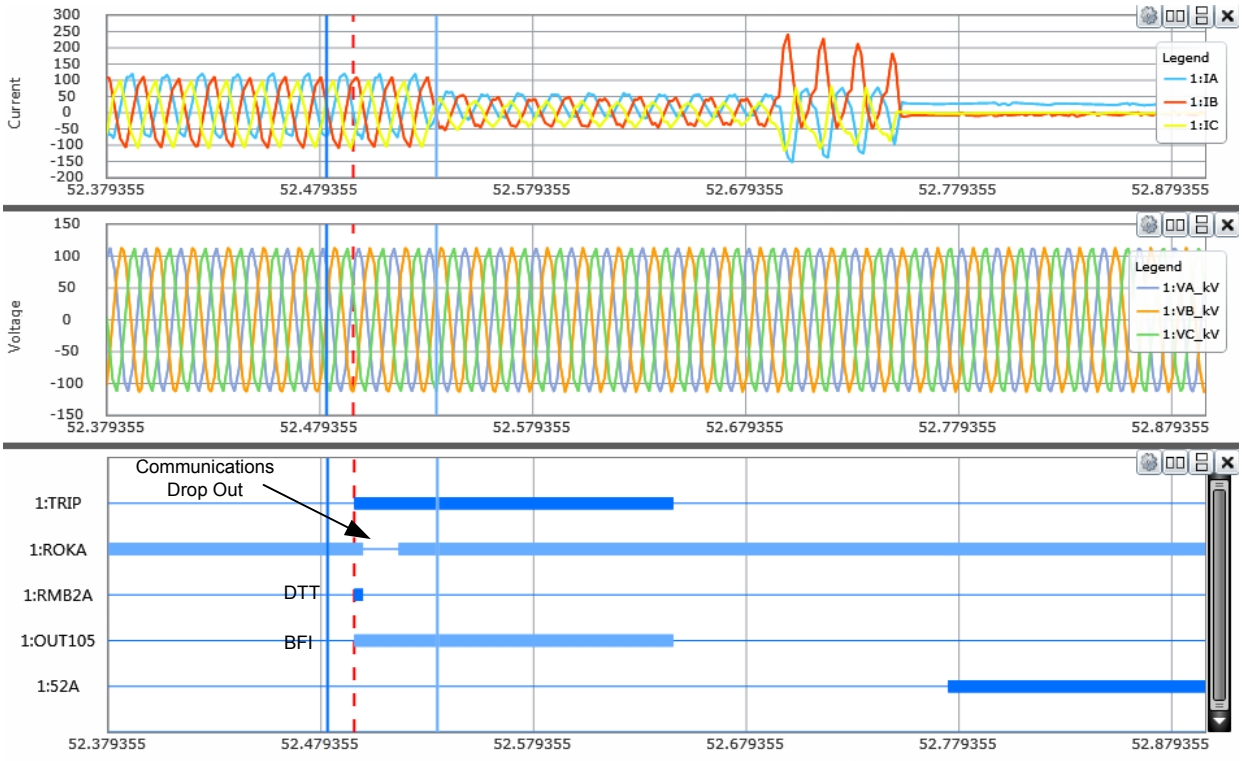

Fig. 20. Channel Noise Results in a Momentary DTT Assertion.

D. Case Study 4: Communications Channel Problem on 87L

Another two-terminal transmission line was protected by an 87L scheme. In the event data shown in Fig. 21, the system experienced a degradation of one of the optical fiber transmitters used in the 87L scheme. This failing component injected continuous noise into the channel and its connected equipment.

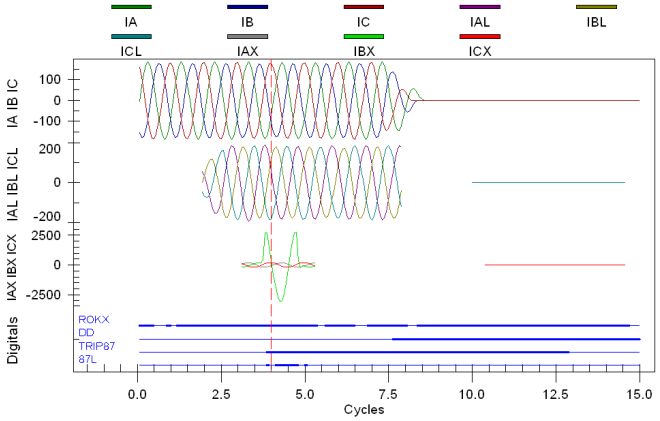

Fig. 21. 87L Produced Undesired Trip Due to Communications Failure With Disturbance Detection Not Enabled.

In Fig. 21, we can observe the channel status (ROKX) chattering—it should be solidly asserted. Eventually, bad data, in this case erroneous remote terminal current (IBX), made it through data integrity checks and caused an undesired 87L operation. Disturbance detection was not enabled.

Important lessons were learned in this case study. Channel performance must be monitored, and alarms, reports, and other notifications of noise and channel dropouts must be acted on with urgency. In modern 87L relays, regardless of data integrity checks, disturbance detection should be applied to supervise tripping. If disturbance detection had been enabled in this case, the 87L element would have been secure and the undesired operation would have been avoided.

E. Case Study 5: Relay Trips During Power Cycle While Performing Commissioning

An older microprocessor-based relay was being commissioned. During testing, the dc control power was cycled and the relay tripped by directional ground overcurrent. The problem was repeatable.

The relay power supply produces two low-voltage rails from its nominal input voltage for use by various hardware components. A 5 V rail, in this case, was used by the analog-to-digital (A2D) converter, and a 3.3 V rail was used by the microcontroller (µP) and digital signal processor (DSP). Protective circuits reset components when their respective supply voltages drop below acceptable operating limits.

Recall from a previous case study that, due to ride-through capacitance, the power supply stays active for several cycles after input power is removed. Fig. 22 provides a graphical representation of how the power supply rails decay at a certain ramp rate, rather than an instantaneous step change, after power is turned off at time T1.

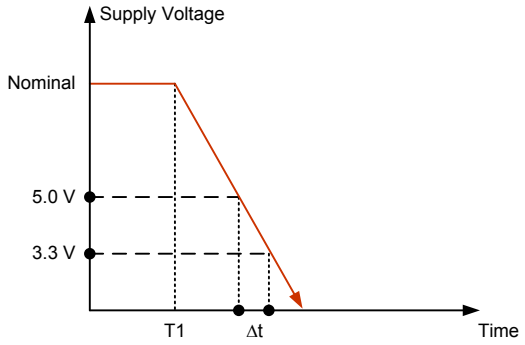

Fig. 22. DC Supply Voltage Ramp Down to 0 V After a Power Cycle at Time T1.

The root cause for this case study was a hardware design that allowed the µP and the DSP to remain enabled for several milliseconds after A2D disabled. As A2D disabled, it sent erroneous data to the µP and the DSP, which appeared as a false 3I0 current pulse, which caused the trip.

Fortunately, this design issue was found during commissioning tests instead of much later when pulling relay dc power (with trips enabled) to find a dc ground.

Important lessons were learned in this case study. Cycling control power, while replicating as accurately as possible in service conditions, is invaluable and as important as industry standard environmental tests. In this case, the criticality of the power-down sequence of components common to one piece of hardware was revealed.

Consider that the North American Northeast Blackout of 2003 was aggravated by a lack of up-to-date information from the supervisory control and data acquisition (SCADA) system. A remote terminal unit (RTU) was disabled after both redundant power supplies failed due to not meeting industry dielectric strength specifications. Independent testing (simple high-potential isolation testing) had not detected this product weakness. Self-test monitoring did not alert the operators that the RTU was dead. Fail-safe design practices, such as reporting full-scale or zero values for all data fields during loss of communications or for watchdog timer failures, were not in place. Redundant power supplies, installed to improve the availability of the system, did not overcome these larger handicaps [2] [12]. These problems are not “hidden failures” just because we do not test or check for them.

As the industry moves toward more complicated and interdependent Ethernet IEC 61850-9-2 systems, power cycling tests become even more critical. Such systems may employ a data acquisition and merging unit built by one manufacturer, a subscribing protective relay built by a second manufacturer, and an Ethernet network built by a third manufacturer. What if the data acquisition shuts down at 5 V and outputs erroneous data to the rest of the components that remain active for a few cycles more?

VII. Conclusion

Protection systems and the power industry have much in common with the aviation industry. Both are complex systems of coupled and interdependent subsystems that must work

together successfully so that the overall system works. We must continue to understand root cause and that changes in one subsystem have an effect throughout other subsystems.

DC control circuits and communications channels have always had complexity and problems to overcome. Our work instructions and procedures have always had to be carefully considered. However, as we transition to new technology platforms and design standards, special precautions must be taken to avoid the types of pitfalls discussed in this paper.

When disrupting dc control circuits or communications channels, we must thoughtfully consider what parts of the protection system should be isolated from trip circuits. Isolate trip circuits before indiscriminately cycling power in relay panels when, for example, troubleshooting dc grounds.

Analysis, design, and testing should be devoted to understanding what happens when power is cycled on systems and subsystems, especially considering our increased dependence on interdevice communications and programmable logic. Critical communicated logic inputs should be supervised with device and communications link statuses. Logic should be forced to a secure state during communications interruptions. Status dropout delays should be included as a necessity for security margin. DTT signals should be supervised with debounce delays. Received analog values should be supervised with disturbance detectors.

Include the ability to isolate trip circuits and devices, whether by physical test links or virtual links for communicated signals. Especially when implementing new technology platforms, strive to make the operator interface familiar and ensure that operating procedures are clear, documented, and proven.

Test, test, test; avoid undesired operations by including power cycle and logic processing sequence checks in design and commissioning tests.

VIII. References

[1] K. Zimmerman and D. Costello, "A Practical Approach to Line Current Differential Testing," proceedings of the 66th Annual Conference for Protective Relay Engineers, College Station, TX, April 2013.

[2] 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.

[3] North American Electric Reliability Corporation, *State of Reliability 2014*, May 2014. Available: http://www.nerc.com/pa/rapa/pa/ performance analysis dl/2014_sor_final.pdf.

[4] D. Costello (ed.), "Reinventing the Relationship Between Operators and Regulators," proceedings of the 41st Annual Western Protective Relay Conference, Spokane, WA, October 2014.

[5] B. McMillan, J. Merlo, and R. Bauer, "Cause Analysis: Methods and Tools," North American Electric Reliability Corporation, January 2014.

[6] T. Lee and E. O. Schweitzer, III, "Measuring and Improving the Switching Capacity of Metallic Contacts," proceedings of the 53rd Annual Conference for Protective Relay Engineers, College Station, TX, April 2000.

[7] GE Multilin, HAA Auxiliary or Annunciator Instruction Leaflet. Available: https://www.GEindustrial.com/Multilin.

[8] D. Costello, "Using SELOGIC® Control Equations to Replace a Sudden Pressure Auxiliary Relay," SEL Application Guide (AG97-06), 1997. Available: https://www.selinc.com.

[9] D. Costello, "Lessons Learned by Analyzing Event Reports From Relays," proceedings of the 49th Annual Conference for Protective Relay Engineers, College Station, TX, April 1996.

[10] North American Electric Reliability Corporation, "Transmission System Phase Backup Protection," Reliability Guideline, June 2011. Available: http://www.nerc.com.

[11] IEC 60834-1, Teleprotection Equipment of Power Systems – Performance and Testing – Part 1: Command Systems, 1999.

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

IX. Biographies

Karl Zimmerman is a regional technical manager with Schweitzer Engineering Laboratories, Inc. in Fairview Heights, Illinois. His work includes providing application and product support and technical training for protective relay users. He is a senior member of IEEE, a member of the IEEE Power and Energy Society Power System Relaying Committee, and vice chairman of the Line Protection subcommittee. Karl received his B.S.E.E. degree at the University of Illinois at Urbana-Champaign and has over 20 years of experience in the area of system protection. He has authored over 35 papers and application guides on protective relaying and was honored to receive the 2008 Walter A. Elmore Best Paper Award from the Georgia Institute of Technology Protective Relaying Conference.

David Costello graduated from Texas A&M University in 1991 with a B.S. in electrical engineering. He worked as a system protection engineer at Central Power and Light and Central and Southwest Services in Texas and Oklahoma and served on the System Protection Task Force for ERCOT. In 1996, David joined Schweitzer Engineering Laboratories, Inc. as a field application engineer and later served as a regional service manager and senior application engineer. He presently holds the title of technical support director and works in Fair Oaks Ranch, Texas. David has authored more than 30 technical papers and 25 application guides. He was honored to receive the 2008 Walter A. Elmore Best Paper Award from the Georgia Institute of Technology Protective Relaying Conference and the 2013 Outstanding Engineer Award from the Central Texas section of the IEEE Power and Energy Society. He is a senior member of IEEE, a registered professional engineer in Texas, and a member of the planning committees for the Conference for Protective Relay Engineers at Texas A&M University.

Previously presented at the 2015 Texas A&M Conference for Protective Relay Engineers.

20150220 • TP6693-01