

Cybersecurity for Distance Relay Protection

Cybersecurity of Energy Delivery Systems
(CEDs) Research and Development

February 2020

TE McDermott
JD Doty
JG O'Brien
CR Eppinger
T Becejac

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights.** Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <<http://www.ntis.gov/about/form.aspx>>

Online ordering: <http://www.ntis.gov>

ACKNOWLEDGMENTS

This work was funded by the Department of Energy's Cybersecurity for Energy Delivery Systems program. We would like to thank Dr. Carol Hawk, Mr. Ryan Egidi and our partners at Western Area Power Administration for their support and feedback. We also thank Mr. Steven Kunsman and other members of the IEEE PES Power System Communication and Cybersecurity Committee for arranging and participating in a public feedback session for this project, at their September 2019 regular meeting.

Revision History

Revision	Date	Deliverable (Reason for Change)	Release #
1	1/14/2019	Initial draft for peer review	1
2	1/28/2020	Final draft for peer review	2
3	2/6/2020	Peer-reviewed final version	3
4	2/10/2020	Cleared PNNL internal review	4
5	2/19/2020	Cleared by sponsor, public release disclaimer	5

Summary

This project is a DOE follow-up effort on the CREDC workshop held on September 13, 2018 in Cambridge, MA to discuss cybersecurity of distance relays, which considered the benefits, vulnerabilities and risk mitigations for the use of communication systems in power system protection. The objectives of this project are to define the taxonomy of relay protection and associated communications; define use cases describing approaches to reduce the cyber-attack surface on those protective relays; and evaluate the loss of operational functional capability from changes to communication coverage. Mitigating controls will also be evaluated to understand if there are other approaches to reduce attack surfaces while maintaining communications or partial communications.

Distance relays are used to protect transmission lines of approximately 10 to 300 miles in length, by detecting short circuits (e.g., faults) on the lines and then tripping (i.e., opening) circuit breakers in the substation at one or both ends of the line. Such protection systems are a subset of the power system and they incorporate sensing, logic and communication functions. Protection system exposure to cyberattack could be drastically limited by disconnecting relays from all vulnerable communication systems, but this may adversely impact overall power system performance in the absence of cyberattack. This project began with a use case analysis of protection systems with communications, as summarized in this report. It continued with modeling, testing and evaluation in a miniature power system (MPS), located in the Western Area Power Administration (WAPA) Electric Power Training Center (EPTC). The project also incorporated feedback from two industry meetings held in February and September 2019.

Distance relays without communication systems rely on time delays to coordinate the tripping of only the components necessary to clear the fault. Fault locations are classified into Zones according to their estimated distance from the relay. For transmission line faults, total fault clearing times may be around 5 cycles for Zone 1, around 25 cycles for Zone 2 and 60-90 cycles for Zone 3. The longer Zone 2 and Zone 3 clearing times pose increased risk of:

- Temporary faults, which need no repair, evolving into permanent faults, which need repair.
- System instability due to the loss of power transfer capacity for longer periods of time.
- Damage to large power transformers, which have limited availability of spares.
- Wildfire starting and sustaining, due to faults from vegetation.

To mitigate these risks, the industry has developed over many years faster circuit breakers and relays to reduce Zone 1 times, and to achieve Zone 1 times for all fault locations. This latter objective has entailed the use of communication channels within “pilot protection” schemes, in order to eliminate the Zone 2 and Zone 3 fault clearing times. There could be other mitigations for the risks of longer fault clearing times, i.e., constructing more lines and substations to strengthen the system and make it more stable. Some of these alternatives are more expensive, and in any case, the protection system serves as the last line of defense.

This report summarizes several pilot protection schemes, of which permissive underreaching transfer trip (PUTT), permissive overreaching transfer trip (POTT) and line current differential (LCD) are widely used on extra high voltage (EHV) transmission lines, i.e., lines operating at 345 kV or greater, in the United States. For these EHV line pilot schemes, a number of communication channels are suitable, such as power line carrier (PLC), microwave, and fiber.

Each has its own set of vulnerabilities, although it seems possible to avoid exposing any pilot protection channel to the internet or to the cloud.

This is not true of communication channels that enable engineering access to relays. These are much more likely to use internet protocols or cloud-based servers. The engineering access functions are important for various purposes: settings changes, setting group definitions, testing, diagnostics, waveform and log retrieval for event analysis, firmware updates, etc. It would be useful to evaluate the communications for engineering access and pilot protection separately for vulnerability and risk mitigation.

Table 1 summarizes the use of communications for the relay functions of interest. These are relay technical functions, denoted by the IEEE device number (IEEE 2008) or the IEC logical node (IEC 2010). Given the complexity of modern relays, it proved helpful to organize the technical analysis by device number. There is still a gap if one tries to analyze the impact of communications according to a relay's business function. For example, 50BF can be important in preventing a cascading outage with great societal impact, and also in preventing damage to a transformer that will be difficult and expensive for the utility to repair. Available samples of electric utility business function analysis tend to focus on the value of energy, grid services, capital investment, maintenance and other normal operations. For the protection system, including relays, there should be an accepted way to value safety and reliability before attempting to use business function analysis, otherwise the answer will have to be all-or-none.

Table 1: Taxonomy of relay functions using peer-to-peer communication.

IEEE Device Number	IEC Logical Node	Function Description	Communications-based Protection Scheme
21	PDIS, PSCH	Distance relay	Various pilot schemes
30	--	Annunciator	Monitoring and control, not protection
32	PDOP	Directional power	Pilot scheme with directional comparison
50BF	PTOC	Breaker failure	Transfer trip
67/67G	PTOC	Directional overcurrent	Pilot scheme with directional comparison
68	RPSB	Power swing detection	PMU protection schemes
87B, 87T	PDIF	Differential	Bus and transformer differential
87L, 87PC	PDIF	Differential	Line current differential or phase comparison

The suggested next steps account for and complement the work already underway with DOE funding:

1. Study the performance of LCD and phase comparison (PC) vs. PUTT, which is less reliant on communication system performance and GPS timing references. The PUTT scheme could prove to be more resilient to cyberattack or communications-related disruption. It could also be more tolerant of message re-routing with software defined networking (SDN) communication systems (Meine 2019). On the other hand, it will be more vulnerable to false tripping during dynamic events or to loss of the voltage signal. The optimum choice of scheme may depend on the specific power system and risk assessment. This study could provide a new template for evaluation based on business functions.

2. Research and develop new methods to detect and monitor distributed physical attacks, possibly using drones, video sensors, thermal sensors, vibration sensors, machine learning and other advanced techniques. This will help mitigate the impact of cyberattack on the protection system and will also help mitigate the impact of wildfires.
3. Implement a scalable public key infrastructure (PKI) for use in electric utility protection systems. This will encourage widespread adoption of secure authentication methods that are already available, but not widely used at present. This will help secure engineering access to the relays.
4. Investigate the use of SDN in combination with software defined radio (SDR) to achieve better cybersecurity and electromagnetic security of the network, incorporating path variability (Usman, Gebremariam et al. 2015, Krishna and Lorenz 2019). This could help secure both engineering access and peer-to-peer IEC 61850 GOOSE messaging. However, SDR has vulnerability to congestion, jamming, and spectrum sensing attacks that would have to be addressed (Fragkiadakis, Tragos et al. 2013).
5. Perform additional testing, with operator evaluation of “panic button” scenarios, PUTT vs. LCD, relay mis-operations, and other cyberattacks in the electric power training center (EPTC). This is an important advantage of testing in the EPTC rather than by computer simulation or even hardware-in-the-loop simulation; the EPTC is already dedicated to managing the situational awareness, operator response times and other human impacts.

One of the project objectives was to settle on a common nomenclature for this problem space. We have concluded that the OSI layer model, supplemented by IEEE device numbers and other IEEE standards, is already well-accepted by the industry. The IEEE Power System Relay and Control Committee (PSRCC) knowledge base provides a great deal of public information about this topic, including tutorials, and it would facilitate dissemination of project results if DOE makes use of it.

Acronyms and Abbreviations

3ZD	three-zone distance protection
AEP	American Electric Power
AMI	automated metering infrastructure
ANSI	American National Standards Institute
ATP	Alternative Transients Program
BF	breaker failure
BPA	Bonneville Power Administration
CCT	critical clearing time
CCVT	coupling capacitor voltage transformer
CIP	critical infrastructure protection
COMTRADE	common format for transient data exchange
CREDC	Cyber Resilient Energy Delivery Consortium
CT	current transformer
DC	direct current
DCB	directional comparison blocking
DCUB	directional comparison unblocking
DER	distributed energy resource
DNP3	distributed network protocol 3
DTT	direct transfer trip
DUTT	direct underreaching transfer trip
EHV	extra high voltage, i.e., ≥ 345 kV
EPTC	Electric Power Training Center
ERCOT	Electric Reliability Council of Texas
FD	fault detection function
Fdr	feeder
FSK	frequency-shift key
Gen	generator
GOOSE	generic object-oriented substation events
GPS	global positioning system
GSU	generator step-up unit (i.e., a transformer)
HIL	hardware-in-the-loop
ICS	industrial control system
IEC	International Electrotechnical Commission
IED	intelligent electronic device
IEEE	Institute of Electrical and Electronic Engineers
INL	Idaho National Laboratory

ISO	International Standard for Organization
kHz	kilohertz
kV	kilovolts
LCD	line current differential
LED	light emitting diode display
LPT	large power transformer
MPS	miniature power system
MVA	mega-volt-ampere
NERC	North American Electric Reliability Corporation
NREL	National Renewable Energy Laboratory
ORNL	Oak Ridge National Laboratory
OP	relay operating coil
OSI	Open Systems Interconnection
PC	phase comparison
PES	(IEEE) Power and Energy Society
PKI	public key infrastructure
PLC	power line carrier
PMU	phasor measurement unit
POTT	permissive overreaching transfer trip
PSCCC	(IEEE PES) Power System Communication and Cybersecurity Committee
PSRCC	(IEEE PES) Power System Relaying and Control Committee
PUTT	permissive underreaching transfer trip
SCADA	supervisory control and data acquisition
SDN	software-defined networking
SDR	software-defined radio
SLGF	single line-to-ground fault
SONET	synchronous optical network
SSH	secure shell
SSR	subsynchronous resonance
VT	voltage transformer
W	watt
WAPA	Western Area Power Administration
Xfmr	transformer

Contents

Revision History	ii
Summary.....	iii
Acronyms and Abbreviations	vi
Contents.....	viii
1.0 Introduction	1
2.0 Pilot Protection Schemes	6
3.0 Communication Schemes	8
3.1 Communication Architectures	9
3.2 Communication Media.....	11
3.3 Communication Protocols	15
4.0 Testing	16
4.1 Test Plan	16
4.2 Test Results	17
4.3 Test Conclusions.....	19
5.0 Industry Review.....	20
5.1 Engagements in February and March 2019	20
5.2 IEEE Meeting of September 2019.....	21
6.0 Next Steps.....	23
7.0 References.....	24
Appendix A – Summary of Protection Schemes	A.1
Appendix B – Device Function Number Analysis.....	B.1

Figures

Figure 1: Non-pilot distance protection uses only local data, but faults outside of Zone 1 take at least 5x longer to clear.	2
Figure 2: During a fault, local and remote generators begin to separate because they can't transfer as much power.	3
Figure 3: In this example from a 2000-bus synthetic model of ERCOT, the system is barely stable with Zone 2 clearing.	3
Figure 4: High-speed reclosing relies on fast clearing; without it, more temporary faults will become permanent faults.	5
Figure 5: Dedicated point-to-point communication between relays.	9
Figure 6: String or drop-and-insert communication.	9
Figure 7: Star or tree communication.	10
Figure 8: Ring communication, including the SONET ring.	10
Figure 9: Mesh communication architecture with more redundant paths.	11

Figure 10: Power-line carrier (PLC) uses the transmission line as a communications medium. This is not the same PLC system that's been used in some smart meter projects..... 11

Figure 11: Twisted-pair copper pilot wires now have to be utility installed and owned..... 12

Figure 12: Electric-utility-owned microwave communication systems were installed from the 1960s through 1980s, when fiber optics began to take over..... 13

Figure 13: Fiber-optic communications are embedded in ground wires or phase conductors, buried under the line, or strung on separate poles. 13

Figure 14: Spread spectrum radio is an evolution of microwave systems, and also commonly used in advanced metering infrastructure (AMI) projects..... 14

Figure 15: Utility engineers and technicians access relay configuration and data using various networks and standards (e.g. IEC 61850, IEEE 1815 and C37.111)..... 14

Figure 16: 230-kV lines and protection schemes in a Miniature Power System at WAPA's Electric Power Training Center..... 16

Figure 17: Comparison of PowerWorld and Fluke Results for Three-Phase Fault at Midpoint of Biglow-Champa Line..... 18

Figure 18: Directional comparison blocking (DCB) dates from the 1930s. Interrupting a signal enables false trip.A.2

Figure 19: Directional comparison unblocking (DCUB) resists noise. Broken communication disables the scheme but can be detected. Injecting a signal can enable false trip.A.4

Figure 20: Underreaching transfer trip is susceptible to false trips due to signal injection.A.5

Figure 21: Permissive underreaching transfer trip (PUTT) mitigates noise or signal injection with local Zone 2 supervision. Loss of signal reverts to local distance protection.A.5

Figure 22: Permissive overreaching transfer trip (POTT) is like DCUB. Loss of signal reverts to local distance protection.A.6

Figure 23: Phase comparison relaying is independent of voltage measurement but requires communication to work.....A.7

Figure 24: Pilot wire relaying implements current differential or phase comparison over twisted pair, private or leased.....A.8

Figure 25: Zone 1 extension improves clearing speed for radial or looped systems without communications.A.9

Figure 26: Transformer Differential Protection needs Communication only within the Substation, if the Transformer has Interrupting Switchgear on All Sides.A.10

Figure 27: Direct Transfer Trip for Transformers without High-side BreakersA.11

Figure 28: Bus differential schemes may overlap line and transformer protection zones, but they don't require external communication channels.....A.11

Figure 29: Breaker failure schemes may use local or remote backup protection/tripping.....A.12

Figure 30: EHV substations with breaker-and-a-half bus must include remote backup.....A.12

Tables

Table 1:	Taxonomy of relay functions using peer-to-peer communication.....	iv
Table 2:	Use of communication methods in relaying.....	8
Table 3:	IEEE device number communications impact summary.	B.1

1.0 Introduction

This project is a DOE follow-up effort on the CREDC workshop held on September 13, 2018 in Cambridge, MA to discuss cybersecurity of distance relays (U. S. DOE 2018), which considered the benefits, vulnerabilities and risk mitigations for the use of communication systems in power system protection. The objectives of this project are to define the taxonomy of relay protection and associated communications; define use cases describing approaches to reduce the cyber-attack surface on those protective relays; and evaluate the loss of operational functional capability from changes to communication coverage. Mitigating controls will also be evaluated to understand if there are other approaches to reduce attack surfaces while maintaining communications or partial communications.

Distance relays are used to protect transmission lines of approximately 10 to 300 miles in length, by detecting short circuits (e.g., faults) on the lines and then tripping, (i.e., opening) circuit breakers in the substation at one or both ends of the line. Such protection systems are a subset of the power system and they incorporate sensing, logic and communication functions. Protection system exposure to cyberattack could be drastically limited by disconnecting relays from all vulnerable communication systems, but this may adversely impact overall power system performance in the absence of cyberattack. This project began with a use case analysis of protection systems with communications, as summarized in this report. It continued with modeling, testing and evaluation in a miniature power system (MPS), located in the Western Area Power Administration (WAPA) Electric Power Training Center (EPTC). The project also incorporated feedback from two industry meetings held in February and September 2019.

Figure 1 shows the operation of distance relays to protect a transmission line, without any communication systems. This narrative will focus on breaker A, but the same principles apply to breakers B, C and D. The distance relays for breaker A measure its current through a current transformer (CT) and voltage through a coupling capacitor voltage transformer (CCVT). The ratio of voltage to current defines an impedance seen by the relay, and if measured accurately enough, the impedance provides a good estimate of distance to the fault. For a Zone 1 fault located up to 80% of the line length from breaker A, shown in red, the measured impedance should be within the Zone 1 setting. If the breaker and relays are fast enough, the total fault clearing time could be as short as 5 cycles. Total fault clearing relies on breaker B also opening, which should also happen within 5 cycles because the red location would be in Zone 1 for breaker B. Some types of relay and circuit breaker could reduce this time to about 3 cycles.

If the fault is on the protected line but near one end, shown in left-most blue, then only breaker B can open within the Zone 1 time of 5 cycles. Breaker A will open in the Zone 2 time of 25 cycles because the measured fault impedance exceeds the Zone 1 setting. Zone 2's time delay always exceeds that for Zone 1. During the extra 20 cycles, high fault current continues to flow in breaker A and the line conductors, as well as the left-most transformer and source (i.e., generator) in Figure 1. The possible impacts of this extra fault-on time will be discussed later. For now, consider the right-most blue fault location as justification for the longer Zone 2 time delay for A. Breaker C should open first for this fault location, which would be inside C's Zone 1. The Zone 2 time delay for A must be longer than Zone 1 for C, so that C has enough time to reliably open first. If A opens instead of, or in addition to, C, then two lines are out of service instead of one line. This would violate the principle of selectivity in relaying; only the minimum set of components should be removed from service. (Note that Figure 1 has been simplified for clarity of the zones, to the point where selectivity may not seem to matter. A real power system would have parallel paths and networks, for which the loss of selectivity matters very much.)

If distance relays at breaker A have to provide backup protection for line C-D, then even longer Zone 3 clearing times will apply for faults near the remote end, shown in magenta. The Zone 3 time has to be longer at A, so that breaker C's Zone 2 has time to clear first. The zone time delays must increase in step-wise fashion for proper coordination. The Zone 3 clearing time is plotted at 60 cycles in Figure 1, but 90 cycles is probably more typical for Zone 3. This stepped zone distance scheme is state-of-the-art for line protection using no communication channels.

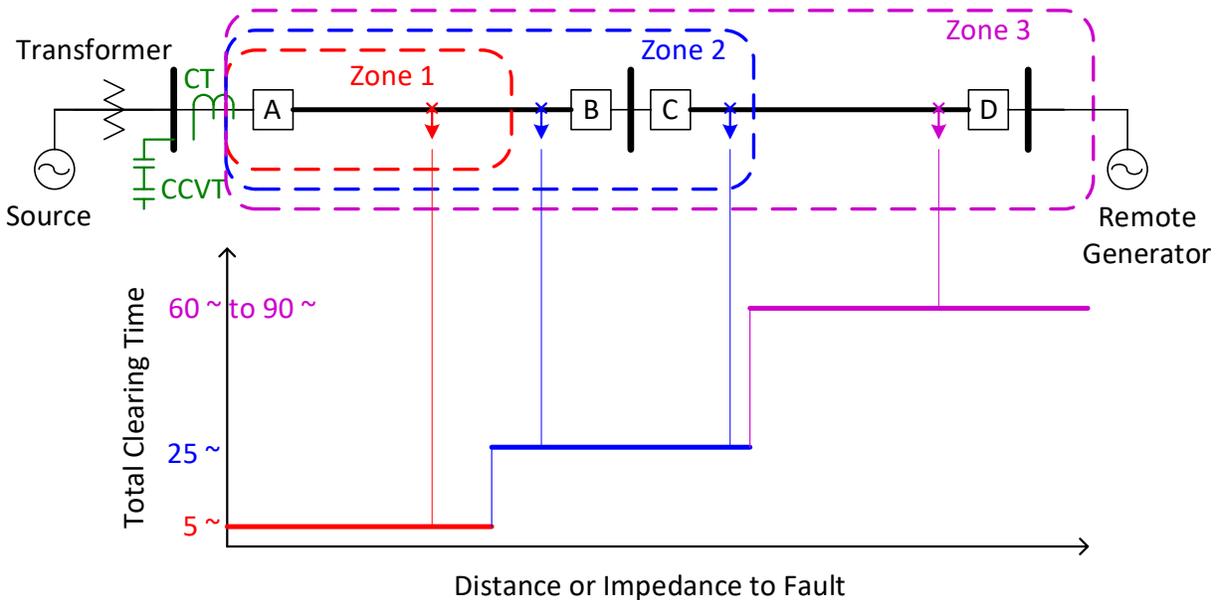


Figure 1: Non-pilot distance protection uses only local data, but faults outside of Zone 1 take at least 5x longer to clear.

When a line is faulted, electric power may not be transferred across it. One symptom is that generators accelerate because their mechanical input power can't be reduced in time to match the loss in electrical load. As time goes on, the generator rotor angle increases to the point where it may lose synchronism with other generators, i.e., a loss of "first swing" stability. After the fault is cleared, some of the electrical load returns and after the line is returned to service, even more electrical load returns, both events helping to preserve stability. There is a maximum critical clearing time (CCT) for faults that will preserve stability. The CCT value depends on the system configuration, including pre-fault contingencies and loading, but shorter fault clearing times are always better for system stability.

Figure 2 shows the transient stability simulation for one generator in a 2000-bus synthetic model of the Electric Reliability Council of Texas (ERCOT) system, for two different clearing times, Zone 1 (red) and Zone 2 (blue). In both cases, the CCT criterion is met and the generator is stable. However, the Zone 2 clearing time does produce a greater first-swing magnitude of -27.2 degrees compared to -12.5 degrees. The subsequent angle swings are more severe than for Zone 1 clearing times. Figure 3 shows the generator output power dynamics for Zone 1 and Zone 2 clearing times. With Zone 1 clearing, the first-swing power peaks at 195 MW, compared to the pre-fault power of 183 MW. With Zone 2 clearing, the first swing power peaks at 218 MW. The Zone 2 clearing time case is barely stable in this example, illustrating the importance of CCT. In fact, CCT has been a major driver in the utility industry's push to achieve faster relay and circuit breaker times.

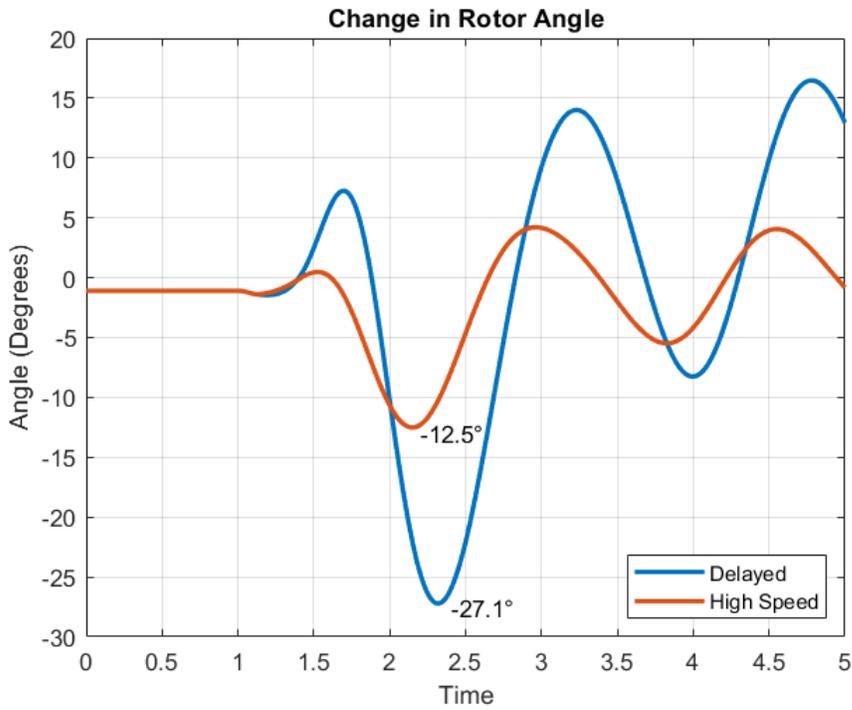


Figure 2: During a fault, local and remote generators begin to separate because they can't transfer as much power.

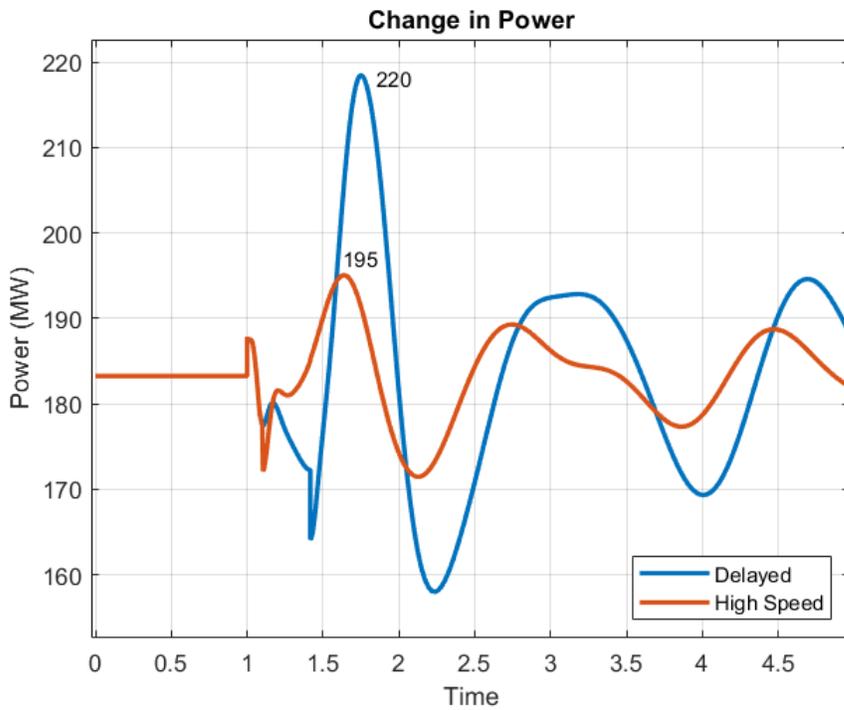


Figure 3: In this example from a 2000-bus synthetic model of ERCOT, the system is barely stable with Zone 2 clearing.

Another major driver for faster clearing time is to limit or prevent damage. If the fault was originally caused by vegetation contacting a conductor, then a longer clearing time would mean a wild fire is more likely to start and sustain itself (Russell, Benner et al. 2012, Watson 2014, Cigre Study Committee B2 2019). Faults have a wide variety of root causes. However, the protection system is the last line of defense in mitigating faults, and a faster fault clearing time is always better than a slower one.

Large power transformers (LPT) are especially vulnerable to damage from sustained faults, and the repair or replacement of LPT can be lengthy and costly (U. S. DOE 2014). The average age of LPT in the United States is about 40 years, and 70% of the LPTs are more than 25 years old. Transformers age thermally as they experience high loading conditions, but if they are not overloaded or damaged, transformers often last for many decades. In a thermally aged transformer the insulation is weakened and less able to withstand the heat and mechanical forces of external faults, i.e., through-faults. Internal faults, within the transformer itself, have to be cleared immediately and always require a repair or replacement. But even external faults, e.g., on a line or feeder outside the substation, produce high fault currents through the transformer until the external fault is cleared. Twenty-eight percent (28%) of transformer failures are already attributed to these external electrical disturbances. There are relatively few LPT spares available. Depending on the size and voltage rating, there may no longer be any domestic manufacturers of LPT. To a lesser extent, extra high voltage (EHV) switchgear, i.e., circuit breakers and disconnect switches operating at 345 kV or greater, also has limited availability of spares if a fault-caused failure occurs.

For example, in 2005, a 1000-MVA Generator Step-Up (GSU) Transformer suffered a catastrophic fault at a generating station. Exposure to external faults caused the low-voltage bus bar of two phases to migrate towards each other due to mechanical forces, resulting in a phase to phase fault. GSUs are specifically designed to the generator's electrical characteristics. In this case, the generator could not operate for 17 days until a temporary, de-rated transformer was installed allowing the generator to operate with limited output. A full-rated replacement transformer was not installed until 2008, at which time the generator was able to produce full output (Widmann and Rapp 2005, Yule, Brock et al. 2015).

High-speed automatic reclosing goes along with high-speed fault clearing, both to maintain and restore power transfer capacity for transient stability, and to prevent temporary faults from evolving into permanent faults. Reclosing involves tripping the line for a short period and automatically re-closing the breaker to determine if the fault was temporary and cleared itself. If the fault remains after a configurable number of clearing attempts, the line trips permanently until the fault is cleared and the line reenergized. Up to 90% of power system faults are temporary, meaning they will clear themselves once the circuit is deenergized, with no need for a lengthy and costly repair process. Typical causes of temporary faults include lightning, incidental tree branch contact, incidental conductor contact in windy conditions, etc. However, if the temporary fault remains energized, then continued melting or arcing will eventually cause the fault to become permanent, necessitating repairs before restoring service. Figure 4 illustrates the interaction between fault clearing time and reclosing time. The blue fault is cleared in 5 cycles from breaker B, but not until 25 cycles from breaker A because the location is outside Zone 1A. If this is a temporary fault, it has 5 times as long to evolve into a permanent fault, compared to a case where breaker A could have also tripped in 5 cycles. The reclosing time at breaker B could be as short as 12 cycles, but that must be set longer in order to give Zone 2A time to operate, whether or not the fault is actually in Zone 2A or Zone 1A. The shortest possible reclosing time is beneficial in maintaining system stability.

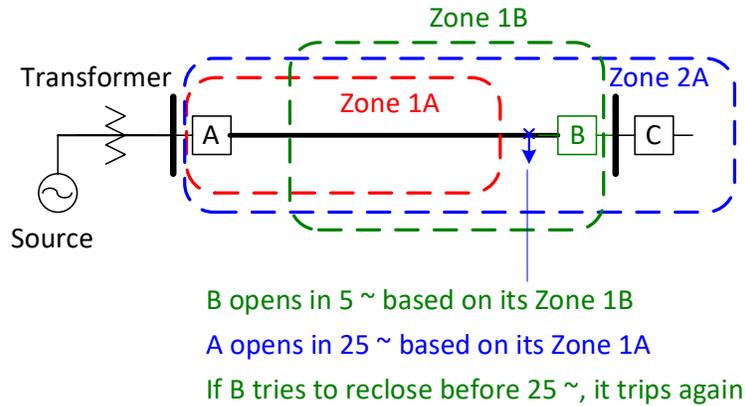


Figure 4: High-speed reclosing relies on fast clearing; without it, more temporary faults will become permanent faults.

This introduction has described how distance relays can work without communications, but also pointed out the benefits of high-speed fault clearing. To date, faster relays and circuit breakers have been more economical for improving stability than constructing new transmission lines and substations.

2.0 Pilot Protection Schemes

Pilot line protection schemes achieve faster fault clearing times by using communication channels, which were originally designated as “pilot wires”. They can use two kinds of fault detector (FD) functions:

- Device 21 – distance relays measure impedance to the fault as, $Z = V/I$. These relays need both CTs to supply current (I) and CCVT¹s to supply voltage (V).
- Device 67 – directional overcurrent relays detect the sign or polarity of current, and whether the current magnitude exceeds a set threshold. These relays do need a sufficient voltage input as an angle reference for the current, but the voltage magnitude is not critical.

Pilot line protection may also use the current differential principle, which is embodied in device 87. A modern protective relay is a complicated intelligent electronic device (IED), and it may implement dozens of the traditional relay device functions² (IEEE 2008). For any specific application, the user may enable and set only a few of the device functions available in the relay. When evaluating the impact of communications, device functions described by their IEEE device numbers offer a more focused taxonomy than general terms like “line protection”, “distance relay”, “pilot protection”, etc. In this report, we mainly focus on device functions numbered 21, 67, 87L and 87PC rather than relay types. It’s also necessary to consider how device functions are used in various protective schemes, and how the device functions and schemes depend on communication channels.

There are many algorithms or schemes for communications-enabled pilot protection; see Appendix A for details. In practice, permissive overreaching transfer trip (POTT), permissive underreaching transfer trip (PUTT) and line current differential (LCD) are widely used on EHV lines in the United States. There are many communication channel options that are suitable for each method, as summarized in Section 3. There are also some important common design principles applicable to any scheme:

- Dependability means the relay will trip for any fault condition in the protected zone. This is the first determinant of a FD setting, such as minimum current or maximum impedance to trip for a specific zone.
- Security means the relay will not trip, unless there is a fault. This is often achieved with margins in both the time to trip and the FD threshold.
- Selectivity means the relay will not trip for a fault that is outside its zone, and the zones are designed so the minimum number of relays trip for a given fault. Without communications, it’s often necessary to use time delays for selectivity, leading to longer fault clearing times.
- Sensitivity means the relay will trip for low values of fault current, but not for high values of load current, which would violate the principle of security.
- Speed is better, but only if the other principles are still met. Section 1 described the main reasons to value speed.

¹ Simpler magnetic voltage transformers (VT) can be used at voltage levels 138 kV and below, but EHV lines and substations generally use CCVTs.

² The full name in the standard is “device function number”, but this is often shortened to “device number” or “function number” or “device function”. The IEEE standard is also an ANSI standard, so sometimes these numbers are referred to as “ANSI numbers”.

- Reliability generally means redundancy and backup to compensate for protection system failures, as discussed in more detail below.

Any relay scheme requires backup protection. On a distribution feeder, the backup for a recloser may only be the next upstream recloser or circuit breaker, which is set for a longer time to trip. On a typical EHV line, the concept of backup is much more comprehensive, ideally including:

- Redundant sensors, i.e., CTs and CCVTs
- Redundant relays, from different vendors
- Redundant communication channels, e.g., leased line and power-line carrier
- Redundant relay algorithms, e.g., PUTT and local stepped distance
- Breaker failure (BF) schemes to back up the circuit breaker
- Redundant relay secondary wiring

This level of redundancy is not always achieved for transmission at 138 kV and below, and it's generally not achieved for distribution systems. However, EHV transmission lines and bulk system generators usually have full redundancy. Because modern relays incorporate many device functions, it could be tempting to use the same product in both primary and backup protection schemes. This is undesirable, as it exposes the protection scheme to common-mode vulnerabilities related to hardware, location, vendor, firmware, physical access, etc.

The cost of relays, with sensors and communications, is no more than a few percent of a transmission system's total cost. (Note: this doesn't include the cost of circuit breakers in the substation, which can be a little more significant.) Protection system design, commissioning and testing comprise a higher portion of the utility's engineering labor, due to the complexity and possible interactions of modern digital relays. Errors in relay setting and operation still occur, but seem to be decreasing as the industry focuses on reducing misoperation events (NERC 2018).

Adaptive relaying, which includes relay setting groups for different operating or environmental conditions, offers one method of coping with system complexity and system configuration changes. The setting group may change by the season, during thunderstorms, during system contingencies, etc. One setting group may suffice, but there are many exceptions that require either field or remote-access reconfiguration. Remote configuration entails the use of communication systems for engineering access, but this is different from the use of peer-to-peer communications within the protection scheme.

3.0 Communication Schemes

Table 2 summarizes the communication channels available and used for both transmission and distributed energy resource (DER) systems. It's not known how much leased wired systems are still used today. Telephone companies no longer provide new copper-wire service for leased lines. Low-cost spread spectrum radio is increasingly common on distribution systems, but probably less so on transmission. Conversely, fiber optics are used on just a few distribution systems, but are increasingly prevalent on EHV transmission systems.

Table 2: Use of communication methods in relaying.

Method	Transmission	DER
Power-line Carrier (PLC)	Yes	Yes
Wired – Utility Owned	Yes	
Wired – Leased	No	No
Microwave	Yes	
Fiber Optic	Yes	Yes
Spread Spectrum Radio	No	Yes
Configuration – Internet	Yes	
Configuration – Private Network	Yes	

Some of the newer pilot protection schemes have only been possible with high-speed and reliable communication systems, such as dedicated fiber optics or digital microwave. Line current differential (LCD) and phase comparison (PC) schemes work by high-speed comparison of either the whole waveform (LCD) or just the phase angle (PC) of current entering the protected zone at each point. If these do not balance properly, a fault within the protected zone may be inferred. The advantage of both LCD and PC is that they do not use voltage measurements.¹ In turn, this means the schemes are not vulnerable to loss of the voltage measurement, e.g., due to a fuse blowing on a voltage transformer. Equally important, they are not vulnerable to mis-operation during dynamic power swings, during which the measured impedance may temporarily swing through the trip zone. To achieve these advantages, both LCD and PC require better communication systems than their older alternatives. Only some of the media in Table 2 will suffice. As noted above, fiber optics or digital microwave most readily support the LCD and PC schemes.

Delays in communication channels need to be compensated for in LCD and PC schemes. An extra delay of just 1 ms translates to a 21.6-degree phase angle error in the PC scheme. The same 1-ms extra delay translates to a 37.48% magnitude error in the difference between balanced currents, which should be zero, in the LCD scheme. Therefore, LCD and PC schemes could be more vulnerable to degradation or uncertainty in the communication system.

The rest of this section summarizes the characteristics and vulnerabilities of the various communication architectures and media. See (IEEE Power System Relaying Committee

¹ The backup scheme, e.g., stepped distance protection as in Figure 1, may very well use the local voltage measurements. In that case, the cost of the CCVT is not saved, but the other described advantages of LCD or PC still obtain.

Working Group H9 2002) and the full knowledge base (IEEE Power System Relay and Control Committee 2020) for more details.

3.1 Communication Architectures

Figure 5 shows a point-to-point communication system architecture between two relays, one at each end of the transmission line. Device number 21 refers to a distance or impedance relay function, while device number 87 refers to a differential relay function, either LCD or PC. The communication link is dedicated and could be implemented using any of the media listed in Table 2. Examples of this might include PLC, utility-owned fiber and utility-owned microwave. This architecture could be more secure or dependable than others, but it's less amenable to sharing the cost and functionality with other uses, and it lacks redundancy.

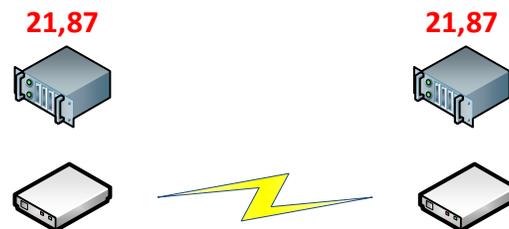


Figure 5: Dedicated point-to-point communication between relays.

Figure 6 shows a string or drop-in communication architecture, in which the protection system paths are shared with other uses. In this case, the relay signals must pass through an intermediate node. During this signal transmission, the path “inserts” both intermediate links. When the signal transmission is complete, the link capacity is “dropped” for other uses.

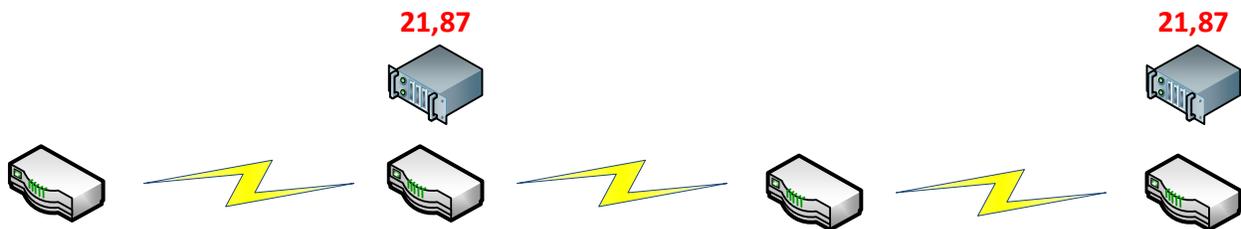


Figure 6: String or drop-and-insert communication.

Figure 7 shows another legacy architecture, called the star or tree, in which signal transmissions pass through a hub. Neither of these include backup, so in practice, parallel redundant systems are usually installed.

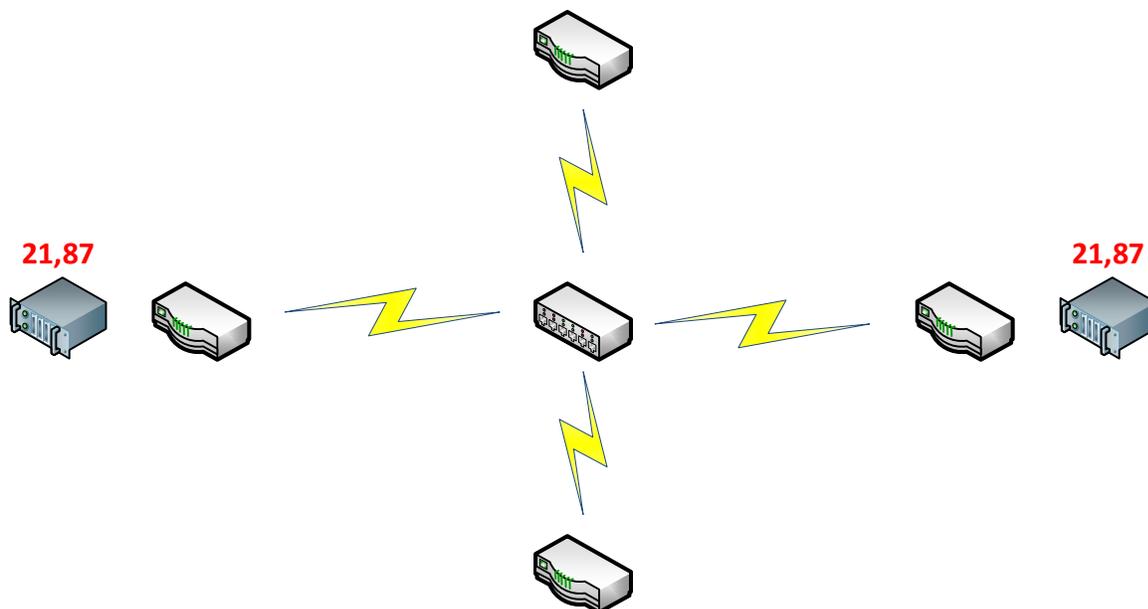


Figure 7: Star or tree communication.

Figure 8 shows the more commonly used ring architecture, particularly for the synchronous optical network (SONET) ring. It offers better reliability, in that signals can be re-routed if one link becomes unavailable, but more than one link failure may not provide reliable communications in all cases, i.e., N-1 reliability. The normal signal transmission path could be clockwise or counterclockwise, so in the example shown, the communication delays between the two relays may not be equal in both directions. This difference has to be accounted for in the relay setting. If a link does go down, the speed and type of response, i.e., “line switching” vs. “path switching”, may produce different channel delays in addition to any “reconfiguration” delays that occur while the network heals itself. In the normal course of events, the relays already have to respond to these changes dynamically, but the response takes time.

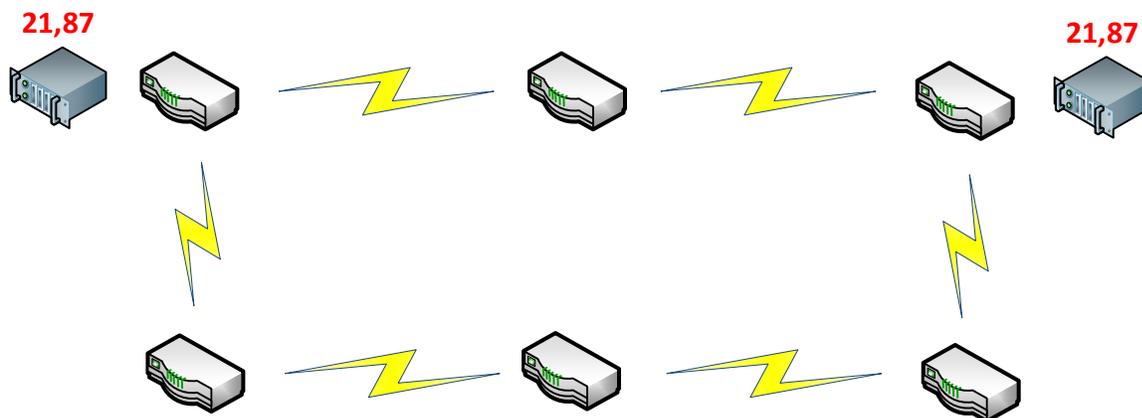


Figure 8: Ring communication, including the SONET ring.

Figure 9 shows a meshed architecture, which is derived from Figure 8 by adding a few redundant links, shown in blue. The additional links help resolve the multiple link failure scenario of the ring architecture. This architecture doesn't necessarily operate as a ring, although there are variants that initially operate as a ring, using the alternative links only during contingencies. In either case, the relays must adapt to different channel delays, and to changes

in channel delays that may occur during contingencies, or during re-routing due to network traffic. Modern relays may do this now by continuously monitoring channel delays (IEEE Power System Relaying Committee Working Group H9 2002), but path switching complicates the problem (Bächli, Häusler et al. 2017). As a benefit, the multiple path options in a ring or mesh architecture make it more difficult for an attacker to identify or inject a trip signal.

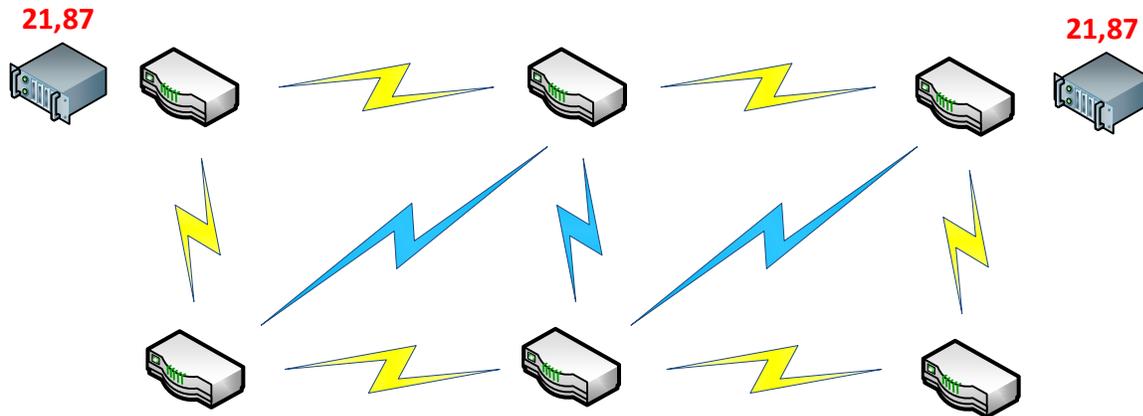


Figure 9: Mesh communication architecture with more redundant paths.

Any of the architectures in Figure 6 through Figure 9 could be implemented with fiber, ethernet, radio or any other type of media, including mixtures, although using different media complicates the calculation of communication delay. These architectures can also be implemented with SDN or SDR. The next section discusses the impact of media type.

3.2 Communication Media

Figure 10 illustrates power line carrier (PLC) channel on the transmission line conductors. A carrier signal is injected onto the line conductors through transceiver equipment connected to low-side CCVT terminals, where the CCVTs are already present. The tuned wave traps (Figure 10 right, https://en.wikipedia.org/wiki/High_frequency_line_trap, CC BY-SA 3.0) confine the carrier signal to the protected line section. The carrier signal may be on/off, an audio tone, or a frequency shift key scheme using two or more frequencies. The range of frequencies is typically 30-500 kHz, and the transceiver power level is typically 1-10 W. The PLC system may include one or two channels. Noise and attenuation have to be evaluated through modal analysis, which has been a niche subtopic in protection system design.

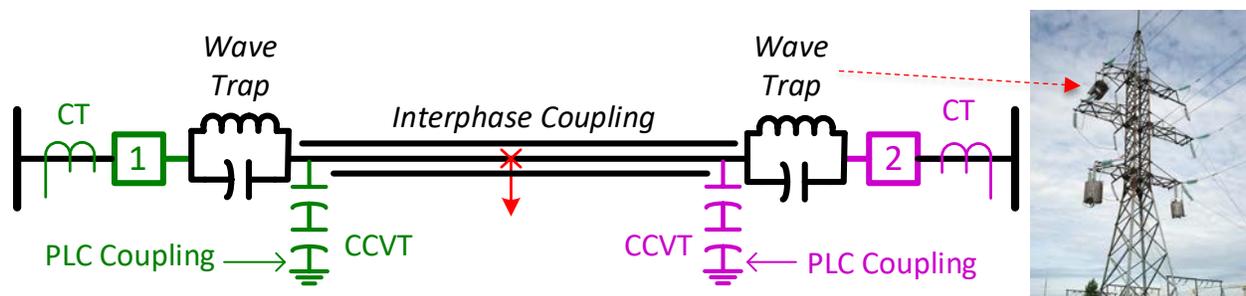


Figure 10: Power-line carrier (PLC) uses the transmission line as a communications medium. This is not the same PLC system that's been used in some smart meter projects.

The PLC transmission path will be interrupted by some (not all) short-circuit and open-conductor faults in the protected line. Figure 10 shows a single-line-to-ground fault (SLGF) in the middle

phase, which is the only one carrying the PLC signal in this example. Due to high-frequency interphase coupling, the PLC signal can actually pass between both line ends on either or both of the unfaulted conductors. Of course, a three-phase-to-ground fault (much less common than the SLGF) would interrupt the PLC transmission. Ham radio frequencies may also interfere with PLC.

Figure 11 shows examples of twisted-pair copper pilot wires, either in utility-installed cable [left (BBC Cables 2019)] or, in the past, leased from the phone company (right). They are suited for short distances and DC, 60 Hz, or audio tone signals. The vulnerabilities include:

- Phone company technicians may accidentally interfere with leased line protection schemes, for example, by connecting test equipment to the line.
- Physical access or physical damage to the wire is possible, although leased lines for protection are likely obfuscated in the phone company network.

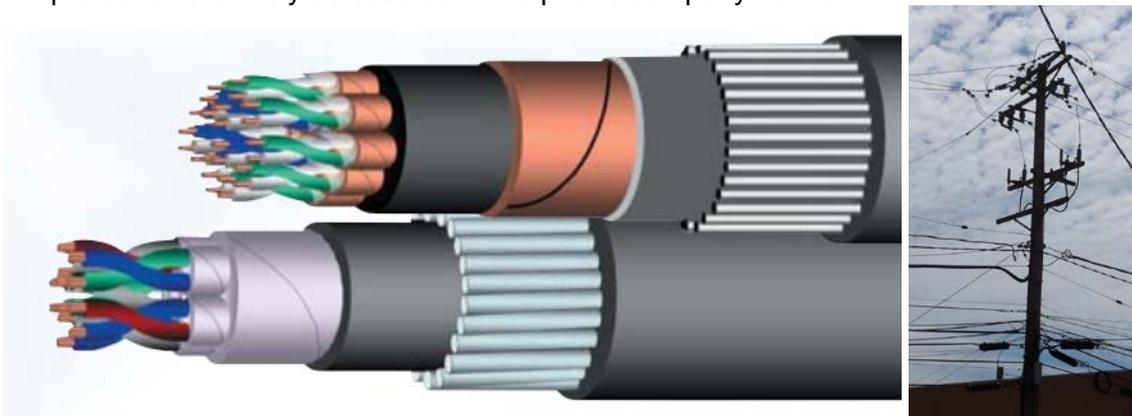


Figure 11: Twisted-pair copper pilot wires now have to be utility installed and owned.

Figure 12 [left (GeorgeLewis 2008)] shows an example microwave radio installation, of the type installed by many electric utilities several decades ago. In 2002, AEP had a microwave network with 258 repeaters installed in 11 states, valued at \$100M (Urgent Communications 2002). Fiber optic systems have probably superseded microwave for new installations, but microwave systems are still in operation. Like fiber, the microwave systems are higher cost than PLC or alternatives, but they support multiple uses like data transmission and industrial control systems (ICS) for utility operations¹. Microwave antennas need line-of-sight, so that repeater stations are necessary, approximately 30-40 miles apart. They are vulnerable to line-of-sight interception or interference, and also to physical access or physical damage. Non-standard protocols may be used, but if the protocol were known to an attacker, Figure 12 [right (Decora 2011)] shows a possible vulnerability to spoofing from a satellite microwave transmitter. Directional antennas might also be used to locally spoof a microwave receiver.

¹ Supervisory control and data acquisition systems (SCADA) are a subset of ICS. Electric utilities have used SCADA for decades, and some are now exploring other ICS concepts like distributed control.

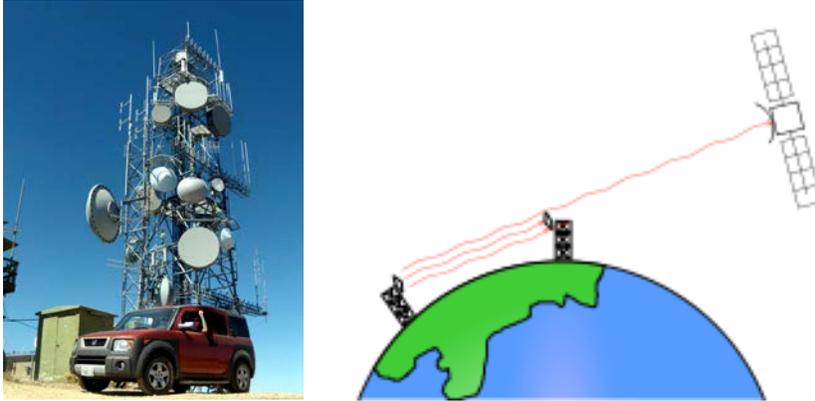


Figure 12: Electric-utility-owned microwave communication systems were installed from the 1960s through 1980s, when fiber optics began to take over.

Satellite signals from the Global Positioning System (GPS) are also used in power systems to derive precise timing references in substations. These precise times are critical to the performance of 87L and 87PC schemes, and they need to be secured (U. S. DHS 2015). In other pilot protection schemes, precise time references are less important

Fiber optic cables may be embedded in a power line conductor, such as the overhead ground wire in Figure 13 (AFL 2019), or separate cable. They are higher cost compared to PLC and spread spectrum radio options. However, fiber offers higher capacity and multiple uses. Fiber is probably less vulnerable to interference and cyber-attack than the alternatives, except that it's still vulnerable to physical damage. Fiber does not run continuously from one end of the transmission line to the other; the channel will have repeaters and splice boxes every few miles. This could permit access to the channel at remote locations, with less chance of detection.



Figure 13: Fiber-optic communications are embedded in ground wires or phase conductors, buried under the line, or strung on separate poles.

Figure 14 shows a spread spectrum radio system on a distribution feeder. Like a lower-cost microwave system, spread spectrum radio requires line-of-sight (although not directional line-of-sight like microwave), which is relatively short. It may require a set of repeaters on multiple poles. Some automated metering infrastructure (AMI) projects have included meshed spread spectrum radio systems to collect meter data. However, such AMI systems may not have the reliability and bandwidth suitable for protection, unless that use case was included in the original system design. Vulnerabilities include physical access and line-of-sight interference, just as with microwave. In addition, there could be more competition for available frequency spectrum

because microwave tends to use licensed channels, while spread-spectrum may use either licensed or unlicensed channels.

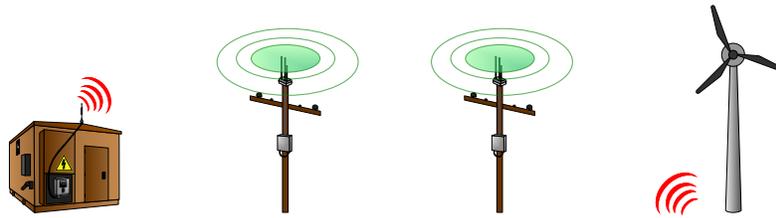


Figure 14: Spread spectrum radio is an evolution of microwave systems, and also commonly used in advanced metering infrastructure (AMI) projects.

Figure 15 illustrates the communication system options for remote engineering access to relays¹, to perform definition of setting groups, setting updates, firmware updates, testing and diagnostics, event log retrieval, etc. These functions are not used for fault detection and tripping. Compared to the methods described earlier for the implementation of pilot protection, a communication system for engineering access is much more likely to use the shared communications infrastructure such as the internet or shared corporate communications, servers in the cloud, and other components that have larger attack surfaces. Engineering access also includes connections to other shared networks, including corporate office and engineering environments, and third parties and are often accessible by large numbers of utility and contractor staff. Therefore, in assessing vulnerability and mitigation, it's probably useful to separate the pilot protection communications from the engineering access communications. Likewise, separate laptop computers are suggested for engineering access and corporate business functions, e.g., email and document preparation.

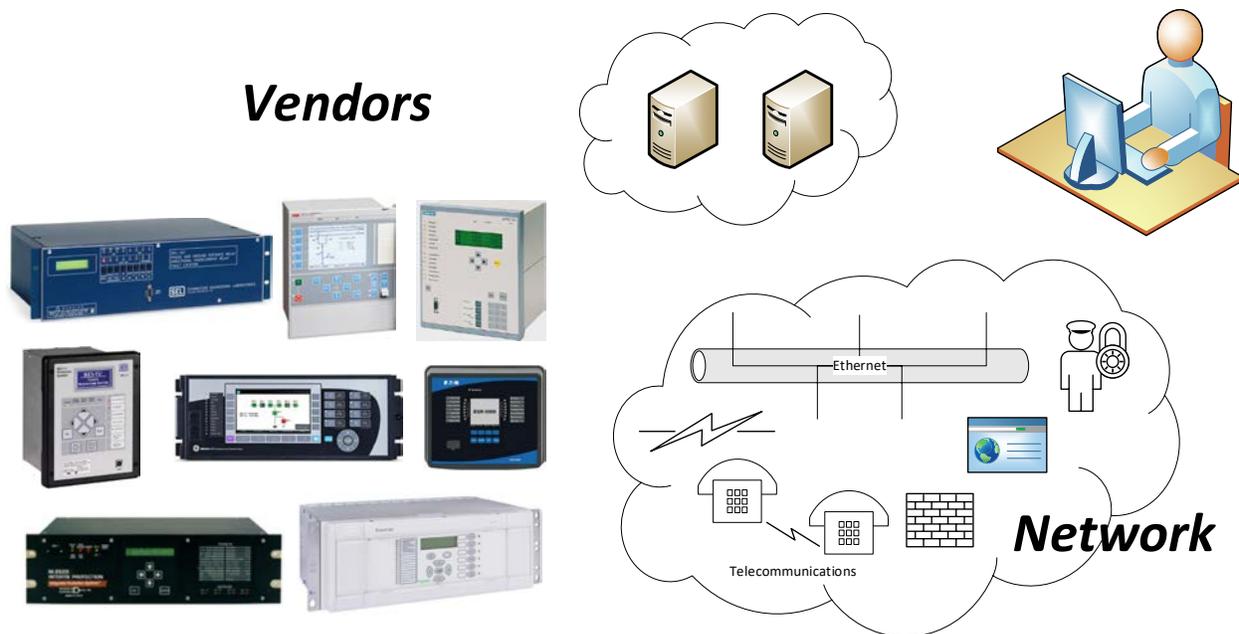


Figure 15: Utility engineers and technicians access relay configuration and data using various networks and standards (e.g. IEC 61850, IEEE 1815 and C37.111).

¹ There are 8 example products shown that implement device function 21: SEL321, ABB REL670, Siemens 7SA522, Beckwith BE1-11f, GE D60, Eaton EGR-5000, Basler M3520, Schneider P43x.

3.3 Communication Protocols

The kind of information transmitted is governed by a communication system protocol, and there is usually a choice of architectures and media that will support the protocols of interest. As some media evolved from analog to digital, they have come more capable. Microwave communication is an example of this. However, some protocols are easier to secure than others.

Pre-owned relays and their manuals can be purchased on-line, so it's possible to reverse engineer the user interface, available settings and behavior of practically any relay found on the power system. This is especially true with physical access to the power system relay, otherwise, an attacker wouldn't necessarily know what options were ordered with the relay. It's not as easy to reverse engineer the firmware that handles peer-to-peer communication, so compromising that probably also requires physical access.

However, securing the engineering access is another matter. When using IEEE Standard 1815 (also known as distributed network protocol 3 [DNP3]) for relay configuration, the Secure Authentication option (available in non-legacy versions of the protocol) should be used along with it. When logging in to a relay using a terminal access, the secure shell (SSH) protocol providing encryption and authentication should be used rather than the non-encrypted telnet protocol. When IEC 61850 is used, the security standard IEC 62351 should also be used. For example, GOOSE messages, including trip signals, are sent in clear text for performance and diagnostic reasons. They are not inherently secure. Additional network security measures need to be taken with GOOSE. IEC 62351 is still a work in progress, and it's not yet possible to secure all portions of IEC 61850.

4.0 Testing

The WAPA Electric Power Training Center (EPTC) includes a Miniature Power System (MPS) that comprises a good testbed for examining distance relay use cases in operational settings (Western Area Power Administration 2019). Instructors are able to set up system faults and other events on the MPS, including three-phase, phase-to-phase, phase-to-phase-to-ground and phase-to-ground faults at 37 different locations. The faults can be either temporary, so that automatic reclosing succeeds, or permanent, so that automatic reclosing will not succeed until the repairs are assumed to be completed. Whenever a fault occurs, actual power system relays are supposed to detect the fault and open the correct breakers to clear it. In the meantime, physical machines in the MPS will respond dynamically and create high fault currents, frequency deviations, voltage deviations and angle swings. Relay and breaker mis-operations may be simulated, too. The student operators react to these training scenarios based on the information they would normally have in real time in a control room.

4.1 Test Plan

Figure 16 shows a one-line diagram of the 230-kV MPS lines, highlighted in red. The existing line fault protection schemes are also indicated in red, but these can be modified in testing or with the acquisition of new relays. The MPS includes three hydro-based rotating machine generators, and a wind generator implemented for WAPA as a power electronic source by NREL. One of the longer 230-kV lines has an option for 0%, 25% or 50% series compensation. However, the implementation uses inductor bypass rather than capacitor insertion, so it's not suited for evaluating the impact of capacitors on fault current angles and apparent directionality. The MPS includes four substations, each with bus and transformer differential schemes that are not shown in detail here. The loads and 115-kV line connections are also not shown in detail, but their locations are indicated with triangles in Figure 16. The aforementioned 37 fault locations include each line, capacitor, transformer and generator terminal in Figure 16, plus more within the Champa switchyard.

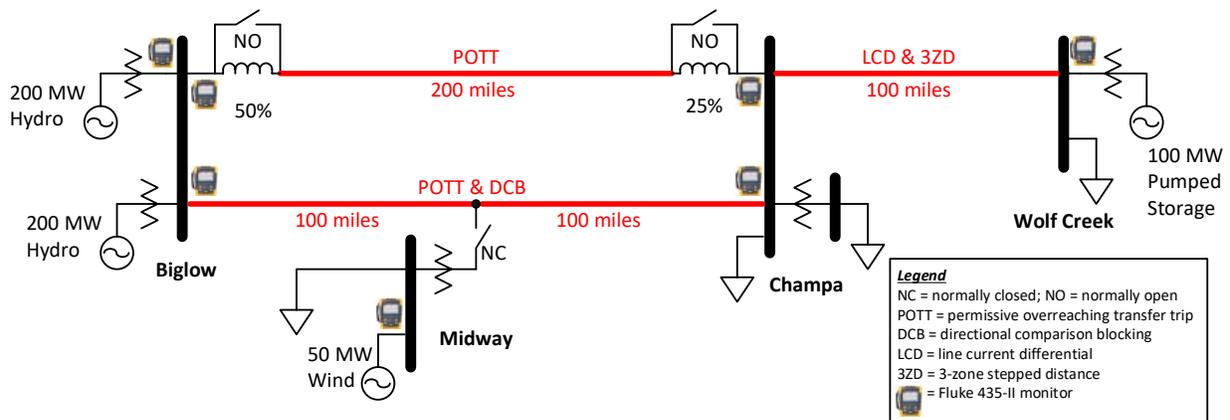


Figure 16: 230-kV lines and protection schemes in a Miniature Power System at WAPA's Electric Power Training Center.

The 230-kV line topology in the MPS enables the testing of faults on parallel lines, zone overreach and breaker failure scenarios at different source strengths and loading conditions. There are also transformers and generators exposed to “damage” if a fault is not cleared,

although the actual MPS components are sized to withstand training mishaps. With reference to Figure 16, PNNL considered the following use cases:

1. Execute the base case training scenarios that WAPA uses with all relay schemes operating as designed. Barring operator error, the system should remain stable, all faults should be cleared with minimum loss of load, and no equipment should be damaged.
2. Disable the POTT, directional comparison blocking (DCB) and LCD line protection schemes in Figure 16, relying on local three-zone distance (3ZD) protection for all 230-kV lines. There are communication channel outage switches in the EPTC that automate this contingency for one of the lines. This represents the loss of communications between the relays at pairs of line terminals, and the fault current clearing times will increase as a result. Repeat the training scenarios to evaluate any possible changes in system stability, loss of load and equipment damage.
3. Disable the remote trip coil at Midway, emulating the failure of DTT remote breaker failure scheme in the MPS, and repeated the training scenarios. This represents the loss of communication channel assistance to BF schemes, and again should result in longer fault clearing times.
4. Simulate spontaneous false trips of relays, as might occur during a cyber-attack. These may be similar to, or more severe than, training scenarios already used in the EPTC. Evaluate adverse impacts to system stability and loss of load.

PNNL has built and validated a transient model of the MPS in the Alternative Transients Program (ATP), with supplemental software models of the relay scheme algorithms (Dusang and Johnson 2008). A dynamic model of the MPS in PowerWorld (PowerWorld Corporation 2020) has also been built and validated. Model-based test planning saves time by identifying the situations most likely to generate interesting results, before using up the limited time in the EPTC. For example, different pre-contingencies and initial conditions can be explored more efficiently in the model than in the EPTC, which is not automated to the degree of a dedicated hardware in the loop (HIL) simulator. It's also possible to expand the system model and investigate new protection algorithms before acquiring new hardware.

For validation of the models, and for waveform data collection during the tests, PNNL and WAPA used Fluke 435-II power quality monitors connected at the locations shown in Figure 16. Although some relays collect waveform data, the older ones do not have such capability. The power quality monitors provided higher resolution, higher frequency response and consistent software interfaces for data download and analysis. They also remained connected in the same locations as the various relays were enabled or disabled for specific tests.

4.2 Test Results

This test was performed from February 19-22, 2019, according to the plan submitted to DOE on February 2. That plan was developed after a planning visit to EPTC from January 21-23. Some of the planned breaker failure testing was shifted from the Midway station to Wolf Creek, some additional testing was done with all communications disabled, and some additional exploratory tests were done on the last day.

The EPTC relays are of mixed vintage, from electromechanical through solid-state to first-generation digital. A few could record waveforms, but we were not able to download from these legacy devices during the testing period. We recorded the relay targets after each test, but in many cases those targets were inconsistent, and the relay LEDs often provided incorrect

distances to the fault. The Fluke power quality monitors served as the primary means of waveform data acquisition, and they worked well individually. However, we had to develop scripts that extract and combine all of the data in batch mode for analysis in MATLAB (Mathworks 2020). In a real setting, engineers or operators could face the same barriers in performing event analysis. This highlights the importance of the logging functions in modern relays, the use of timing references to synchronize event records from different locations, and the use of data exchange standards like COMTRADE (IEEE 2013).

With communications disabled, we were able to observe longer fault clearing times as expected, and some events where generators tripped offline. On the last day of testing, we were able to create some extreme conditions of voltage (e.g. 0.6 per-unit) and frequency (e.g., +/- 6 Hz), during which the miniature power system kept operating. Some of this was done for ATP and PowerWorld model validation. Through software simulation, we could explore other faults and sequences that were not tested. However, a simulation may fail to converge through some of those events. One reason for this is that non-linearities and frequency-dependent losses in real hardware can allow the system to reach a stable operating point, which is not always apparent in simplified computer models.

Figure 17 shows a sample PowerWorld simulation of a three-phase fault, compared to the recorded Fluke data for the same event. The general behaviors and frequencies agree, with noticeable differences in transient magnitudes. Further improvement in model fidelity may occur with a more detailed characterization, including hardware testing, of the Woodward governor models in the MPS. The ATP and PowerWorld models have been provided to WAPA, along with electronic copies of all the tabulated and plotted test data.

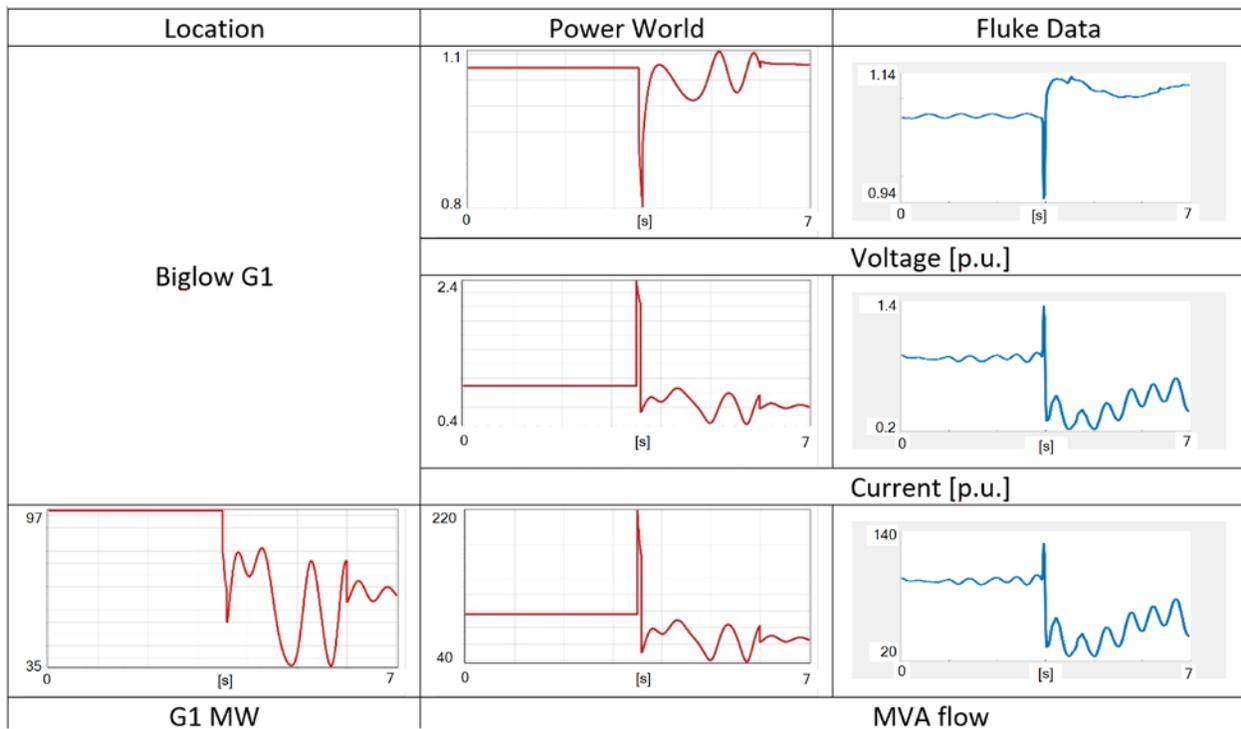


Figure 17: Comparison of PowerWorld and Fluke Results for Three-Phase Fault at Midpoint of Biglow-Champa Line

4.3 Test Conclusions

Failures of relay communication happen today, and utilities design backup schemes to mitigate those failures. We saw that working in the test program, and we did not observe any false trips or failures to trip, other than those we deliberately created.

The miniature power system in the EPTC is a good venue for this kind of testing. Suggestions for upgrades in possible future tests include:

1. Install physical series capacitors in the Biglow-Champa line #1. At present, series capacitance is emulated by reducing the inductive impedance. This doesn't have the same impact on distance relays and machine subsynchronous transients.
2. Install one or two new generations of digital relays, while retaining some of the mixed-vintage and mixed-vendor characteristics of what the EPTC already has.
3. Install modern GPS timing sources. These could be used in protection schemes and event record synchronization during realistic scenarios, including lost or compromised timing signals.
4. Update the data collection system to aggregate and display the event records, which come from relays of different make and model. The data collection system should show the impact of lost or compromised GPS timing sources.
5. Continue working to better characterize the behavior of the machines, governors and exciters in the MPS. With real series capacitors, the subsynchronous resonance (SSR) behavior of the shaft torsional systems will become relevant. The governor and exciter dynamics are already important, sometimes contributing to unexpected trips of the machines during events, load changes or system startup.
6. Include the response of real human operators in test scenarios. This time, the instructors set up the scenarios and they knew what was coming. The EPTC's main purpose is to train power system operators in a realistic setting, and a future cybersecurity project could take advantage of that.

One may ask whether a modernized EPTC should be a fully digital simulator, or an HIL simulator. Either would be acceptable for cybersecurity testing so long as real protective relays are interfaced (i.e., HIL) and the simulation is robust through extreme events (e.g., our last-day testing). It's also important that the user interface mimic a power system operation center, not a research lab's test facility. In either case, analog or digital, the suggested relay and series capacitor upgrades should still be made.

5.0 Industry Review

The September 2018 post-CREDC workshop on Cybersecurity of Digital Relays helped set the objectives of this project. It was clear from the workshop that engineering access to relays and peer-to-peer communication between relays needs to be addressed separately. Also, that it is important to use the IEEE device numbers, the IEC logical nodes, or some other standard terminology to help organize the analysis. The post-CREDC workshop attendees mainly included researchers, with a few utility representatives. During this project, the team sought more opportunities to engage with industry experts.

5.1 Engagements in February and March 2019

WAPA hosted a Cybersecurity for Protective Relays Workshop at their Golden office, co-located with EPTC, on February 7-8, 2019. The attendees represented some electric utilities, consultants, the DOE National Laboratories, and DOE staff. The project team attended, presented some use cases and test plans from this project, and took notes. Brainstorming by workshop attendees produced a list of 60 initial solutions for DOE to investigate, starting at INL with WAPA participation. Many of these could be categorized under the following:

1. Engineering access needs to be controlled but is too important to just give up in many cases. With unfettered engineering access, a person could change trip equations or initiate trips, effectively gaining control of the relay (i.e., the equivalent of administrative access). Data diodes might be used to enable the monitoring and logging functions, while denying write access to the relay. Newer field devices might allow for better control and monitoring of logins, firmware updates and settings changes.
2. Extensions of the state estimator concept can be used to help maintain the dependability and security of relays, even when compromised. For example, peer voting systems and operator alarms have been suggested. State estimators can be used at both the system and substation levels to detect faults or other abnormal conditions.
3. A “panic button” should be available for emergency disconnection of relay communications, for situations when advance warning of an attack is available. The distance relays would then operate autonomously as in Figure 1.

Later in February, the team collected material from a vendor seminar on grid cyber security, which suggested:

1. Substation-level gateways, data diodes and software defined networks (SDN) are well-accepted or promising mitigation techniques.
2. SDN is not necessarily randomized, and it also doesn't do deep packet inspection. An intrusion detection system (IDS) should be added to it.

The question remains whether SDN is vulnerable to electromagnetic or physical monitoring or spoofing. In exploring that question, the team concluded that:

1. There can be vulnerabilities in hybrid systems that mix SDN and non-SDN components or configurations.
2. Fiber has no electromagnetic exposure, but it remains vulnerable to physical access. The total communication system should provide some variability of paths to mitigate these risks. This will also introduce variable performance, which must be accounted for in the protection schemes.

3. SDR can provide path variability and resilience to physical disruption (Usman, Gebremariam et al. 2015, Krishna and Lorenz 2019). However, SDR has vulnerability to congestion, jamming, and spectrum sensing attacks that would have to be addressed (Fragkiadakis, Tragos et al. 2013).
4. The delivery time performance requirements are more stringent for the 87L and 87PC schemes than for other pilot protection schemes (IEEE 2005). We found many references that SDN can meet the more stringent delivery requirements within a substation, but not between substations as needed for the 87L and 87PC schemes. GPS timing sources can help resolve the problem, but those timing sources can be vulnerable. Aside from SDN, direct fiber connections between the relays can be used.

We then met with two vendors active in transmission line relaying at TechAdvantage in March 2019. Neither thought that peer-to-peer communication between relays would be readily vulnerable to cyberattack. Such communication is non-routable layer 2 traffic (ISO 1994) and often uses some type of encryption. This trade show contact led to a presentation at the next IEEE PSCCC/PSRCC meeting, described in the next section.

5.2 IEEE Meeting of September 2019

PNNL and WAPA moderated a public evening session at the IEEE PSCCC Meeting on September 18, in Denver. Preliminary results from this project were presented, along with findings of the February 2019 workshop at WAPA. This was the first public opportunity for feedback on the project and the first one with vendor participation. Thirty-three people representing seven vendors, seven utilities and seven consulting/research organizations attended. Earlier feedback opportunities in Cambridge and Golden were by invitation only and they did not include vendors. Participants offered new ideas about scalable public key infrastructure (PKI) for protection, along with some clarifications and additions to use case details. Many of these have been incorporated into the final report.

While reviewing February workshop results, there were concerns expressed that a “panic button” mitigation could expose another single point of failure. The presence of a “panic button” may also lead to decreased operator confidence in the power system. It was pointed out that data diodes are expensive and can be bypassed. Some of the brainstormed ideas have been tried, such as a relay voting system at 500 kV by Bonneville Power Administration (BPA), along with various adaptive or setting-less relay pilots, and pilots of voltage-supervised 87B schemes. Some of the participants were aware of other DOE projects in this space.

On the other hand, remote locations of towers and repeater stations provide opportunity for undetected and sustained physical access. Relays are widely available in the marketplace (including eBay and resellers), giving more opportunities for potential attackers to “practice”. Maintenance laptops used by relay technicians present another vulnerability, and these should not be able to connect with a relay that’s in service.

The most worrisome scenario (to this session’s attendees) was:

1. Disable or slow down the protection, followed by
2. Distributed physical attacks with cheap tools that create short-circuit faults (ICF International 2016).

The typical characteristics of remote locations (e.g., transmission towers, control shacks and substations) increases the likelihood of an attack. The combination can lead to widespread damage that is difficult to repair. However, the impacts would be regional in scale as a worst case, not spread over the whole interconnection¹.

The consensus among this group was that better and broader use of authentication would be more cost-effective than encryption, which does impose a computational burden on relay hardware. Other available security measures, listed in section 3.3, should be more widely used. A new relay functional test could simply examine a hash value to verify whether memory contents have changed; this could also be more cost-effective than encryption.

When asked a final question, “what should the government do?” about this issue, there were two consensus responses from the group:

1. Implement an electric utility internet. NERC CIP sharing limitations would have to be resolved. Oak Ridge National Laboratory (ORNL) may already be working on this method in its DarkNet project (ORNL 2018).
2. Build a scalable Public Key Infrastructure (PKI) that would facilitate the industry using authentication methods that are already available but not used. Again, it was a consensus opinion that authentication would be more cost-effective and less resource-intensive than encryption. Therefore, a PKI system for power system protection would be useful immediately.

¹ There are three interconnections in the continental United States, namely Eastern, Western and Texas (i.e., ERCOT).

6.0 Next Steps

The suggested next steps account for and complement the work already underway with DOE/CESER funding:

1. Study the performance of LCD and PC vs. PUTT, which is less reliant on communication system performance and GPS timing references. The PUTT scheme could prove to be more resilient to cyberattack or communications-related disruption. It could also be more tolerant of message re-routing with SDN communication systems. On the other hand, it will be more vulnerable to false tripping during dynamic events or to loss of the voltage signal. The optimum choice of scheme may depend on the specific power system and risk assessment. This study could provide a new template for evaluation based on business functions.
2. Research and develop new methods to detect and monitor distributed physical attacks, possibly using drones, video sensors, thermal sensors, vibration sensors, machine learning and other advanced techniques. This will help mitigate the impact of cyberattack on the protection system and will also help mitigate the impact of wildfires.
3. Implement a scalable PKI for use in electric utility protection systems. This will encourage widespread adoption of secure authentication methods that are already available, but not widely used at present. This will help secure engineering access to the relays.
4. Investigate the use of SDN in combination with SDR to achieve better cybersecurity and electromagnetic security of the network, incorporating path variability for resilience to physical disruption. This would help secure both engineering access and peer-to-peer IEC 61850 GOOSE messaging.
5. Perform additional testing, with operator evaluation of “panic button” scenarios, PUTT vs. LCD, relay mis-operations, and other cyberattacks in the EPTC. This is an important advantage of testing in the EPTC rather than by computer simulation or even hardware-in-the-loop simulation; the EPTC is already dedicated to managing the situational awareness, operator response times and other human impacts.

One of the project objectives was to settle on a common nomenclature for this problem space. We have concluded that the OSI layer model, supplemented by IEEE device numbers and other IEEE and IEC standards, is already well-accepted by the industry. The PSRCC knowledge base provides a great deal of public information about this topic, including tutorials, and it would facilitate dissemination of project results if DOE makes use of it.

7.0 References

- AFL. (2019). "Optical Ground Wire." Retrieved January 14, 2019, from <https://www.aflglobal.com/Products/Fiber-Optic-Cable/Aerial/OPGW.aspx>.
- Bächli, R., M. Häusler and M. Kranich (2017). Teleprotection solutions with guaranteed performance using packet switched wide area communication networks. 2017 70th Annual Conference for Protective Relay Engineers (CPRE).
- BBC Cables. (2019). "Pilot Cables." Retrieved January 14, 2019, from http://www.bbccable.com/uploads/prysmian/prysmian_5kv_and_15kv_pilot_cables.pdf.
- Blackburn, J. L. and T. J. Domin (2014). Protective relaying : principles and applications. Boca Raton, CRC Press, Taylor & Francis Group.
- Cigre Study Committee B2. (2019). "Proposal for Creation of a New Working Group: Guide for Prevention of Vegetation Fires Caused by Overhead Line Systems." Retrieved January 14, 2019, from https://cigre-usnc.org/wp-content/uploads/2019/02/TOR-WG-B2_73_Guide-for-Prevention-of-Vegetation-Fires-Caused-by-Overhead-Line-Systems.pdf.
- Decora. (2011). "Satellite Intercepting Microwaves." Retrieved January 14, 2019, from https://commons.wikimedia.org/wiki/File:Rhyolite_sat.svg.
- Dusang, L. V. and B. K. Johnson (2008). Evaluation of fault protection methods using ATP and MathCAD. 2008 IEEE Canada Electric Power Conference.
- Elmore, W. (1999). Pilot Protective Relaying, CRC Press.
- Fragkiadakis, A. G., E. Z. Tragos and I. G. Askoxylakis (2013). "A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks." IEEE Communications Surveys & Tutorials **15**(1): 428-445.
- GeorgeLewis. (2008). "Communications Tower on Frazier Mountain." Retrieved January 14, 2019, from https://en.wikipedia.org/wiki/Microwave_transmission#/media/File:Frazier_Peak_tower_and_Honda_Element.jpg.
- Horowitz, S. H. and A. G. Phadke (2014). Power System Relaying. Chichester, West Sussex, United Kingdom, Wiley.
- Ibrahim, M. A. (2016). Protection and Control for Power System, CreateSpace Independent Publishing Platform.

ICF International. (2016). "Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats." Retrieved February 10, 2020, from <https://www.energy.gov/sites/prod/files/2017/01/f34/Electric%20Grid%20Security%20and%20Resilience--Establishing%20a%20Baseline%20for%20Adversarial%20Threats.pdf>.

IEC (2010). IEC 61850-7-4:2010 Communication networks and systems for power utility automation - Part 7-4: Basic communication structure - Compatible logical node classes and data object classes.

IEEE (2005). "IEEE Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation." IEEE Std 1646-2004: 1-36.

IEEE (2008). IEEE Standard Electrical Power System Device Function Numbers, Acronyms, and Contact Designations. IEEE Std C37.2-2008 (Revision of IEEE Std C37.2-1996): 1-48.

IEEE (2013). IEEE/IEC Measuring relays and protection equipment Part 24: Common format for transient data exchange (COMTRADE) for power systems. IEEE Std C37.111-2013 (IEC 60255-24 Edition 2.0 2013-04): 1-73.

IEEE Power System Relay and Control Committee. (2020). "Knowledge Base." Retrieved January 24, 2020, from <https://www.pes-psrc.org/kb/published/reports.html>.

IEEE Power System Relaying Committee Working Group H9 (2002). Digital Communications for Relay Protection.

ISO. (1994). "ISO/IEC 7498-1:1994, Information technology—Open Systems Interconnection—Basic Reference Model: The Basic Model." Retrieved January 24, 2020, from <https://www.iso.org/standard/20269.html>.

Krishna, M. B. and P. Lorenz (2019). "Cognitive Radio Enabled Cache Map-and-Route Using Context Mapping and Decision Making Approach in Software Defined Networks." IEEE Transactions on Vehicular Technology **68**(6): 5849-5858.

Mathworks. (2020). "MATLAB." Retrieved January 24, 2020, from <http://www.mathworks.com/products/matlab/>.

Meine, R. (2019). A Practical Guide to Designing and Deploying OT SDN Networks. Power and Energy Automation Conference. Spokane.

NERC. (2018). "Protection System Misoperations." Retrieved January 14, 2019, from <https://www.nerc.com/pa/RAPA/Pages/Misoperations.aspx>.

ORNL. (2018). "DarkNet - Architecture." Retrieved January 24, 2020, from <https://www.energy.gov/sites/prod/files/2018/12/f58/ORNL%20-%20DarkNet.pdf>.

PowerWorld Corporation. (2020). "PowerWorld Simulator." Retrieved January 24, 2020, from <https://www.powerworld.com/>.

Russell, B. D., C. L. Benner and J. A. Wischkaemper (2012). Distribution feeder caused wildfires: Mechanisms and prevention. 2012 65th Annual Conference for Protective Relay Engineers.

U. S. DHS. (2015). "Best Practices for Improved Robustness of Time and Frequency Sources in Fixed Locations." Retrieved January 24, 2020, from <https://www.dhs.gov/sites/default/files/publications/GPS-PNT-Best-Practices-Time-Frequency-Sources-Fixed-Locations-508.pdf>.

U. S. DOE (2014). "Large Power Transformers and the U. S. Electric Grid."

U. S. DOE (2018). Post-CREDC Industry Meeting: Cybersecurity of Digital Relays: Meeting Summary. Cambridge, MA.

Urgent Communications. (2002). "In Defense of 800 MHz Private Radio." Retrieved February 4, 2020, from <https://urgentcomm.com/2002/04/01/in-defense-of-800mhz-private-radio/>.

Usman, M., A. A. Gebremariam, U. Raza and F. Granelli (2015). "A Software-Defined Device-to-Device Communication Architecture for Public Safety Applications in 5G Networks." IEEE Access **3**: 1649-1654.

Watson, B. A. (2014). A protection scheme using ultra-fast circuit breakers for wildfire mitigation and reliability improvement for rural distribution. 2014 IEEE PES T&D Conference and Exposition.

Western Area Power Administration. (2019). "Electric Power Training Center." Retrieved January 14, 2019, from <https://www.wapa.gov/EPTC/Pages/eptc.aspx>.

Widmann, M. and C. Rapp. (2005). "PNO-II-05-010: Edwin I. Hatch Nuclear Plant, Unit 1 - Hatch Unit 1 Main Transformer Fire." Retrieved January 14, 2019, from <https://www.nrc.gov/docs/ML0530/ML053060198.pdf>.

Young, J. and D. Haas (2008). The Importance of Relay and Programmable Logic Documentation. 2008 61st Annual Conference for Protective Relay Engineers.

Yule, K., D. Brock and J. Purdy (2015). Accountability and Evaluation of Aggregate Effects of Through Faults on Power Transformers. Electric Power Conference and Exposition. Rosemont, IL.

Appendix A – Summary of Protection Schemes

This appendix describes power system protection schemes (Blackburn and Domin 2014, Horowitz and Phadke 2014, Ibrahim 2016), using a combination of logic and timing diagrams for each scheme (Young and Haas 2008). Device numbers of main interest include (IEEE 2008):

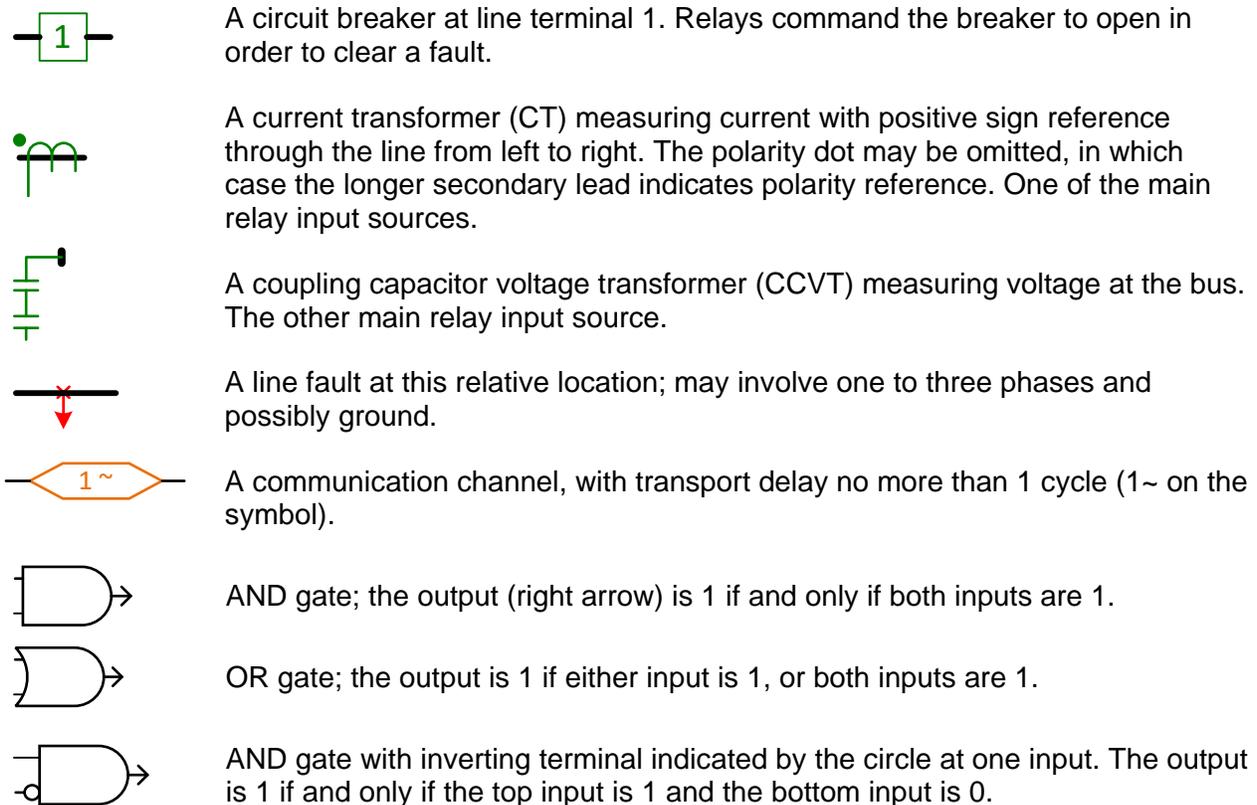
- 21 – distance relay
- 67 – directional overcurrent relay
- 87 – differential relay with bus (B), line (L), phase comparison (PC) or transformer (T) suffix

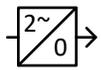
For transformer protection, we also consider:

- 50 – instantaneous overcurrent
- 51 – time overcurrent, including ground (G) time overcurrent
- 49 – temperature relay
- 63 – pressure relay, sensing the transformer oil pressure

See Appendix B for more details on the device numbers.

Figures in this appendix present one-line diagrams and logic diagrams for several protection schemes. The major diagram symbols are shown below, further described in a more detailed walk-through of the first scheme in Figure 18.





Delay block. The output will change from 0 to 1 at a delay of two cycles (2~) after the input turns from 0 to 1. If the input changes back to 0 before the two-cycle delay elapses, this block resets with 0 delay and the output stays at 0.



Logic signal connection, which is often called a junction. All connected lines carry the same signal value. If the lines cross with no dot, then they are not connected and may carry different signal values.

Recall that Figure 4 showed how stepped distance protection results in longer clearing times when a fault is located near either the end of a line. In that example, the fault was cleared in 25 cycles rather than 5 cycles. Figure 18 shows how communication systems result in lower fault clearing times in a directional comparison blocking (DCB) scheme, which was the first one developed for long-distance lines, for any fault location on the protected line. At each terminal, 1 and 2, a fault detection (FD) relay looks in the forward direction, while a blocking directional relay, denoted S, looks in the reverse direction.

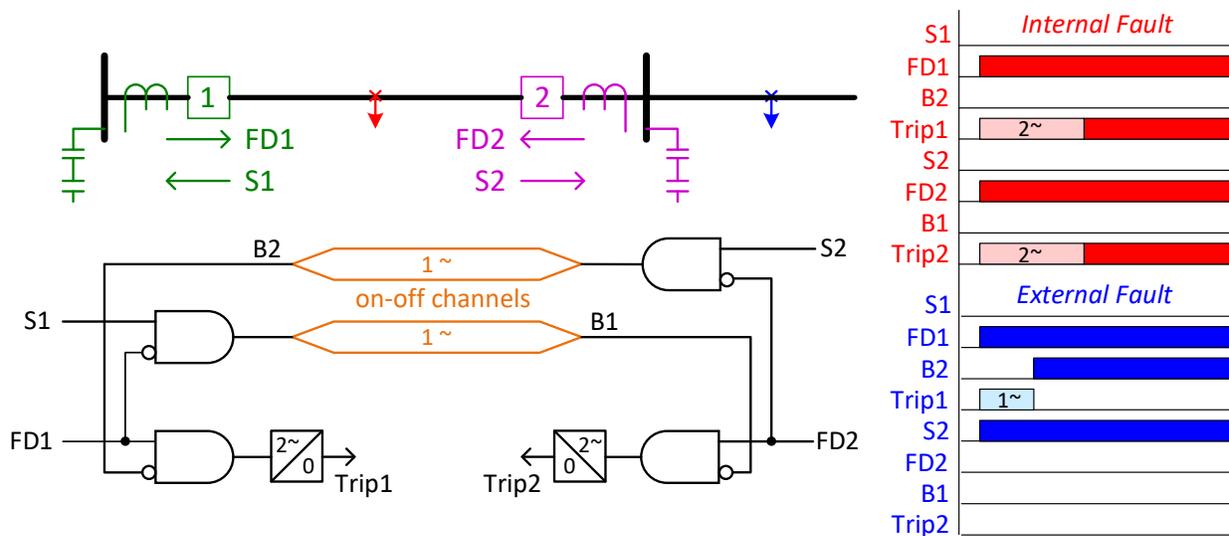


Figure 18: Directional comparison blocking (DCB) dates from the 1930s. Interrupting a signal enables false trip.

These relays don't necessarily measure impedance to the fault, but they require both current and voltage measurements in order to detect the phase angle between current and voltage. This phase angle is what distinguishes the forward and reverse directions. Under normal loading conditions, the direction can be forward or reverse, depending on the direction of power flow, so the FD relay also needs to distinguish between faults and heavy loading conditions. This combination of fault and direction detection can be done with directional overcurrent (67) or distance (21) relays. Each terminal requires a CT and CCVT for the protected line.

For the internal fault in Figure 18, shown in red, both FD1 and FD2 pick up within a half cycle. Some relays can pick up faster, within a quarter cycle, but a half cycle is definitely enough time to capture the first peak in fault current waveform and determine its forward or reverse direction with respect to the voltage waveform. Neither S1 nor S2 picks up because the fault location is in the wrong direction. Figure 18 shows this fault in the middle of the line, but in fact the same signal pattern would occur for any fault location between the two CTs. The signal plots in the upper right of Figure 18 show FD1 and FD2 turning on first, one half cycle into the Internal Fault

event. Considering the logic diagram to the bottom left, FD1 and FD2 have values of 1, while S1 and S2 have values of 0. The AND gate in the lower left corner will output a 1 when both inputs are 1. One of these inputs is FD1, which becomes 1 at the half-cycle time. The other is NOT B2, where the NOT is indicated with a small circle at the AND gate input, and B2 is the blocking signal from the other line end at terminal 2. B2 starts at 0 and actually stays there through the event. The And gate outputs a 1 into the time delay for Trip 1. The time delay is shown as 2 cycles to trip and 0 cycles to reset. If B2 never becomes 1, the delay will time out and the Trip1 signal turns to 1 at two and half cycles into the event. The Trip1 signal is plotted in the upper right corner of Figure 18, and this commands the breaker 1 to trip. If the breaker takes 2.5 cycles to trip, then the total fault clearing time is 5 cycles from terminal 1.

The exactly converse situation results in a 5-cycle clearing time from terminal 2, for the internal fault in Figure 18. The FD2 signal becomes 1 at 0.5 cycles into the event, while the B1 signal stays at 0. After a two-cycle delay, the Trip2 signal becomes 1 at 2.5 cycles, and the breaker at terminal 2 trips 2.5 cycles after that. Therefore, the fault has been cleared from both ends within 5 cycles, for any internal fault location between the two CTs.

Now consider the external fault in Figure 18, shown in blue, with signals plotted in the lower right corner. FD1 turns to 1 within 0.5 cycles, even if the fault current at terminal 1 is a little less for the external fault because it's further away than the internal fault was. The timing of FD1 is not sensitive to the magnitude of fault current, so long as that current is above a detection threshold. However, S2 picks up within 0.5 cycles, instead of FD2, because the external fault is "behind" terminal 2 from the viewpoint of the protected line. If FD2 stays at 0, then Trip2 also stays at 0. However, when FD1 becomes 0, that starts the 2-cycle delay timer for Trip1. We need to have B2 become 1 before that delay times out, otherwise the breaker at 1 will trip incorrectly. Once B2 becomes 1, the timer on Trip1 resets immediately. B2 is transmitted from the other line end, at terminal 2, through a communication channel (orange) assumed to have a delay of no more than 1 cycle. That channel's input comes from the upper-right AND gate in Figure 18, which is fed by S2 and NOT FD2. When S2 becomes 1 and FD2 stays at 0, the blocking signal transmits to the other line end at terminal 1 and is assumed to arrive no more than 1 cycle later. At 1.5 cycles into the event, B2's arrival suppresses a Trip1 output, as plotted in the lower right of Figure 18. Therefore, neither end of this line trips for the external fault.

One drawback of the scheme is the small overlap in detection zones between the FD and S functions. This is why the FD2 signal could have suppressed the transmission of B2 in Figure 18's logic diagram for the external fault, if FD2 had become 1 during the event. Otherwise, the breaker at terminal 1 might fail to trip for an internal fault very close to the other line end. A second potential weakness relates to communications; if the channel is broken then false trips will occur. For example, breaker 1 would have tripped during the external fault if B2 had never arrived. Conversely, injecting a false block signal into the communications channel would prevent a breaker from correctly tripping for internal faults; channel checking in the communication protocol or microprocessor-based relay would mitigate this. A third vulnerability is that the communication channel delay must be less than the timing block delays. If not, the breaker may trip incorrectly for external faults.

Figure 19 shows the directional comparison unblocking (DCUB) scheme in a similar format. Either device 21 or 67 relays can be used. From here on, rather than presenting a detailed walk-through of each scheme, only the key differentiators will be described.

The DCUB scheme has only the forward-looking FD function at each line terminal. For the internal fault, shown in red, both FD1 and FD2 pick up within a half cycle. However, the AND

gates at each end mean that a trip signal cannot be generated unless a UB signal arrives from the other end. When FD1 picks up, for example, it also sends a signal to the other end, where it arrives as UB1 no more than one cycle later. UB1 and FD2 then create an output of 1 from the right-most AND gate, with a Trip2 signal created 1 cycle later. Conversely, UB2 and FD1 create the Trip1 signal, and both breakers receive a trip signal for the internal fault with 2.5 cycles. This trip signal time is the same as resulted in Figure 18. For the external fault, shown in blue, the FD1 signal picks up and creates UB1 at the other end, but FD2 and UB2 are not produced. Therefore, neither breaker trips for the external fault. (NB: Directional comparison overreaching transfer trip is logically similar to this scheme.)

The communications channel is used differently in Figure 19, with frequency shift key (FSK) signaling. The channel is always “on”, with a change in signal value indicated by a change in frequency. In Figure 18, the channel turns on and off to change the signal value. With FSK, it’s less likely that noise will be interpreted falsely as turning the signal on because the frequencies have to match. Furthermore, if the channel breaks the scheme has to be disabled, but that should be detected immediately because FSK transmits continuously. The injection of a false signal with matching frequency would enable false trip, but not cause false trip by itself.

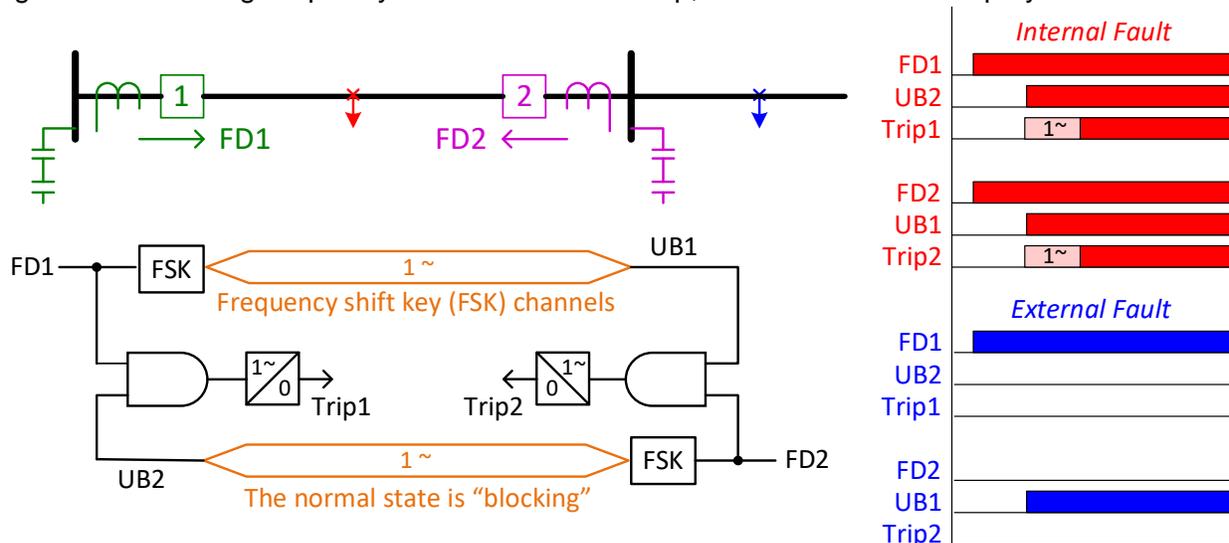


Figure 19: Directional comparison unblocking (DCUB) resists noise. Broken communication disables the scheme but can be detected. Injecting a signal can enable false trip.

Figure 20 shows a simple under-reaching transfer trip, mainly to illustrate historical development of the more widely used permissive under-reaching transfer trip scheme. Each line end has the FD function, which must be implemented using distance relays, device 21, that cover only about 80% of the line, i.e., Zone 1. The two OR gates mean that ultimately either FD signal can trip both breakers by itself. For a fault in the middle 60% of the line, shown in red, each FD signal picks up within one half cycle and trips its own breaker. For a fault near one end, shown in green, the FD2 signal picks up but FD1 does not, i.e., the green fault location is outside of Zone 1 for FD1. The FD2 signal creates Trip2 with no intentional delay, thereby tripping the #2 breaker. It also sends the FD2 signal to end 1 with a communication delay up to 1 cycle, causing the generation of Trip1. These relay operating times may be 1 cycle faster than in Figure 18 or Figure 19. For the external fault, shown in blue, neither FD signal picks up; the fault is too far away for FD1 to pick up, and in the wrong direction for FD2 to pick up. The use of FSK provides some resistance to random noise, but a false communication signal injection would, by itself, falsely trip a breaker. This scheme is not used very much.

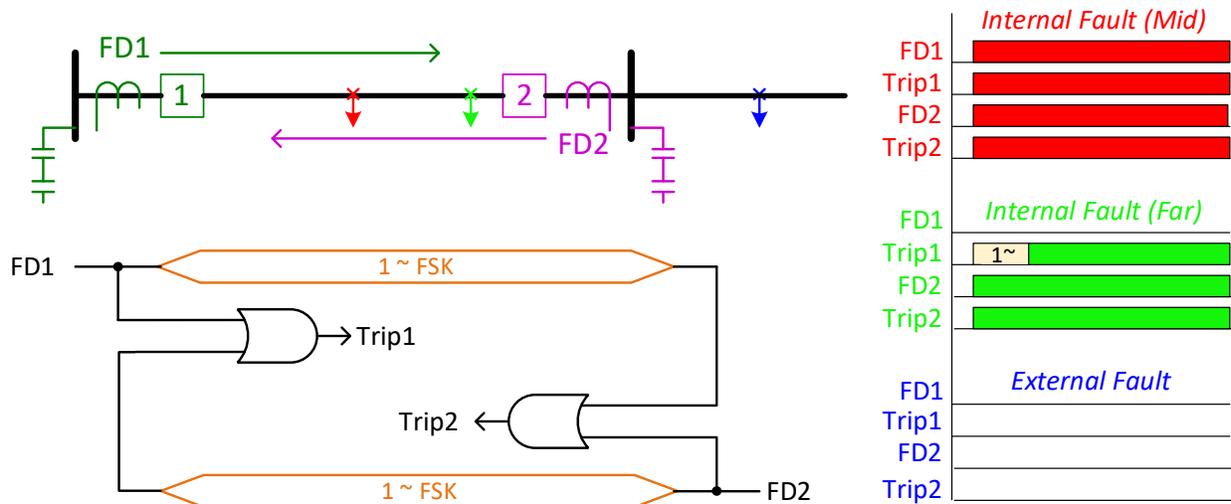


Figure 20: Underreaching transfer trip is susceptible to false trips due to signal injection.

Figure 21 illustrates a more widely used and practical permissive underreaching transfer trip (PUTT) scheme. It uses both Zone 1 and Zone 2 settings for distance relays, device 21, at each line end. For a fault in the middle 60% of the line, shown in red, both FD1 and FD2 pick up within one half cycle. Both signals have direct access to the OR gate at each end, resulting in Trip1 and Trip2 signals generated with no intentional delay. This result is the same as in Figure 20 for the red fault. For a fault near one end, shown in green, FD2 will trip breaker #2 with no intentional delay and transmit toward the other end, as before. However, at end 1 the new AND gate requires that the local Zone 2 function, FP1, also pick up before Trip1 can be generated. This does occur, and Trip1 is generated after a 1-cycle communication delay to receive FD2. The relay time is no more than 1.5 cycles for internal faults, faster than Figure 18 or Figure 19.

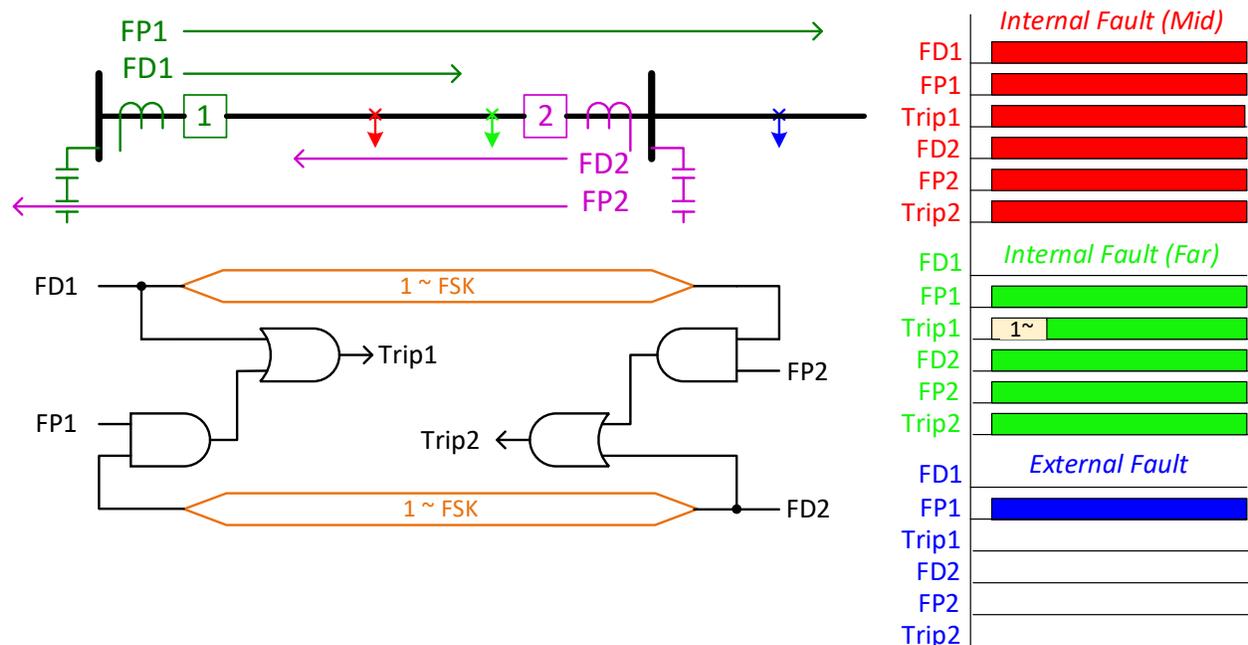


Figure 21: Permissive underreaching transfer trip (PUTT) mitigates noise or signal injection with local Zone 2 supervision. Loss of signal reverts to local distance protection.

For the external fault, shown in blue, neither FD1 nor FD2 pick up, for the same reasons as in Figure 21. However, FP1 may pick up when the fault location is within Zone 2, as shown. However, FP1 only feeds one of the AND gate inputs, so it can't generate Trip1 because FD2 never arrives from the other line end. PUTT offers some resilience to communication signal injection, because the required local Zone 2 pickup (FP1 or FP2) means that a communication signal can't produce a false trip by itself. Furthermore, the loss of communications can be detected with FSK, in which case the scheme reverts to local stepped zone distance protection. That would entail a loss of speed, but not of selectivity or sensitivity.

Figure 22 shows a commonly used permissive overreaching transfer trip (POTT). In many respects, POTT is like the DCUB scheme presented in Figure 19, but faster because there are no logical delay blocks. Each end uses a device 21 overreaching distance relay, i.e., Zone 2 in terms of reach, but Zone 1 in terms of speed. For internal faults, both FD1 and FD2 pick up within one half cycle, whether the fault is near the middle of the line (red) or near one end (green). Because of the two AND gates, neither FD1 nor FD2 can trip a breaker on their own; the corresponding signal must also be received from the other end, within a 1-cycle delay over the FSK communication channel. When this occurs, both Trip1 and Trip2 are generated in about 1.5 cycles of relay time. For the external fault, shown in blue, FD1 may pick up but FD2 will not because the external fault is in the wrong direction. Because of the AND gate, the Trip1 signal is never generated and neither breaker trips.

The use of FSK with POTT will provide some resilience to noise injection. A false signal injection will enable false trip but will not cause false trip by itself. The loss of communication capability can be detected, in which case the scheme should revert to local stepped zone distance protection. The performance and vulnerability of POTT and PUTT are similar, but PUTT is more widely used in practice (Horowitz and Phadke 2014). The "extra" relays in PUTT could make it more secure than POTT, and these relays are useful anyway for backup protection. However, POTT is also commonly used (Ibrahim 2016).

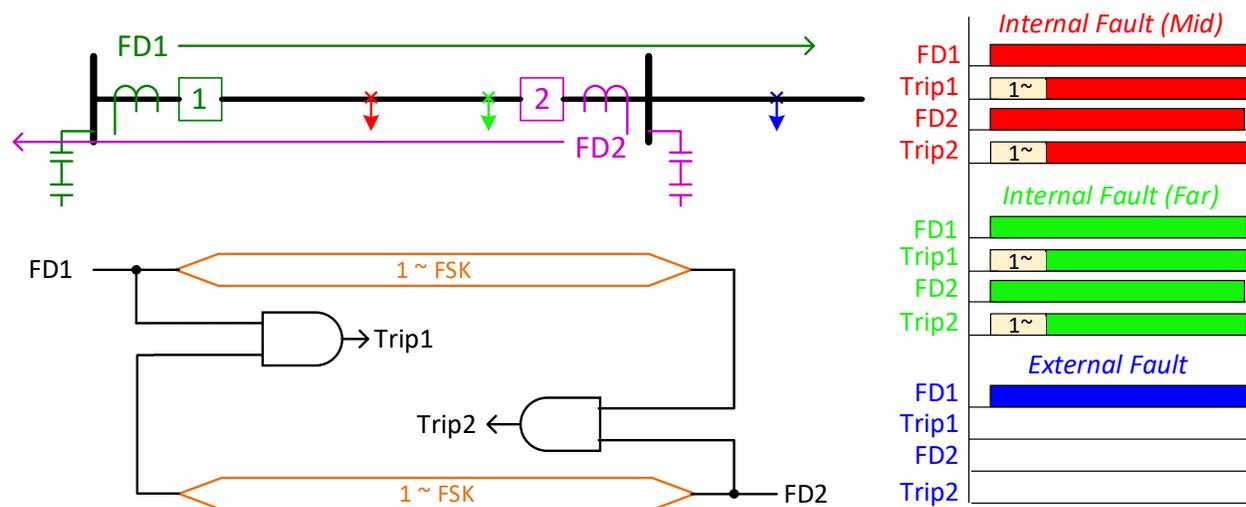


Figure 22: Permissive overreaching transfer trip (POTT) is like DCUB. Loss of signal reverts to local distance protection.

Figure 23 shows a phase comparison (PC) scheme based on current only. It does not require the CCVTs for voltage inputs but does require communication channels. Phase comparison is resilient to some of the voltage-dependent issues that occur with distance relays (e.g., zero-sequence mutual coupling, dynamic power swings). However, the CCVTs are probably needed

anyway for a backup scheme that uses distance relays, so the cost of CCVTs would actually not be saved. The communication channels may require higher bandwidth than in schemes previously discussed, because the phase comparison scheme works with waveform information at some level, even if simplified to half-cycle square waves.

Phase comparison begins with synthesizing one waveform signal that can effectively isolate the fault current from the measured phase currents (Blackburn and Domin 2014). In Figure 23, the function $V_F = k_1 I_1 + k_2 I_2 + k_0 I_0$ serves this purpose. The currents (I) and weighting factors (k) are based on symmetrical components, and in modern digital relays, the V_F waveform is calculated point-by-point in microprocessor code. The “sgn” block at each end converts V_F to a square wave, equal to 1 on the positive half cycles and 0 on the negative half cycles. Also, at each end, the FD function picks up whenever the local current exceeds a fault detection threshold, i.e., when $|I| \geq I_{FD}$. For the internal fault location, shown in red, the current magnitude is high enough that FD1 and FD2 both pick up, and the waveform synthesis begins to generate square-wave signals for S1 and S2. The key point is that S1 and S2 are out of phase with each other, because the fault current polarities are opposite at each end, i.e. left to right at end 1, and right to left at end 2. Through the upper left AND gate, S1 and FD1 combine to send an R2 signal to the other end, with some delay in the communication channel. The channel bandwidth must be sufficient to resolve the square-wave nature, so that R2 is a good representation of S1. Likewise for the upper right AND gate generating R1. For convenience, Figure 23 plots $\sim R1$ (i.e. “NOT R1”) and $\sim R2$, accounting for the inverting terminal inputs to the bottom-most AND gates. When we have $\sim R1$ in phase with S1, as occurs for the internal fault, this will generate a square wave output onto A1. After a delay of 4 ms, or one quarter cycle, the Trip1 signal is generated and latched to a value of 1, thereby tripping breaker #1. The same happens at the other end; when $\sim R2$ is in phase with S2, the A2 signal becomes 1 and latches Trip2 to 1 after a 4-ms delay.

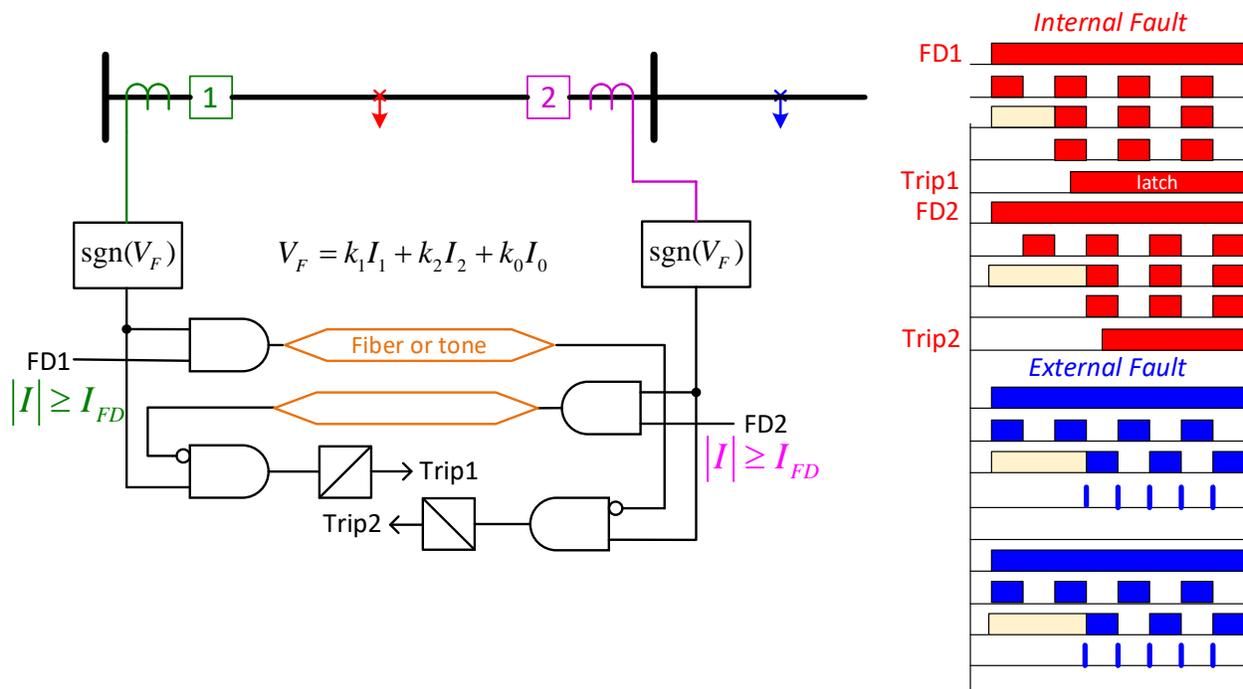


Figure 23: Phase comparison relaying is independent of voltage measurement but requires communication to work.

For the external fault location, shown in blue, the VF signals are synthesized as before at each end. However, in this case S1 and S2 are in phase because the fault current flows from left to right at each end of the line. At each end, ~R1 and ~R2 appear as before with some communication delay. They are nominally out of phase, but due to some measurement effects, there may be some short-lived positive A1 and/or A2 outputs from the two inverting AND gates. The 4-ms delays provide margin, so that brief A1 and/or A2 outputs don't produce false trips.

In PC schemes, the waveform information is transmitted instead of logic signals, but the scheme could still be vulnerable to noise and false signal injections. False tripping would not occur if the FD functions were used for local supervision, but a proper trip could be prevented or delayed.

PC is an example of the line current differential (LCD) principle, further illustrated in Figure 24. Device 87PC applies to phase comparison, while device 87L applies to the LCD scheme as described next. On the left side of Figure 24, copper wires are used to carry the CT secondary currents in the relay circuit; this is suitable for line distances up to 5-10 miles. For clarity, the left side of Figure 24 shows both leads of each CT secondary. For the internal fault, shown in red on the upper left diagram, the thick red arrows show the flow of transmission line fault currents, from each end toward the fault. These fault currents cause the green and magenta currents to flow in the CT secondary circuit, with directions established by the CT polarity dots. In each CT primary, i.e., the transmission line, the red fault current flows into the polarity dot. Therefore, in each CT secondary, the green or magenta current flows out of the polarity dot. The polarity dots enforce magnetic balance in the CT. The secondary circuit connections force both green and magenta currents to combine and flow through the relay operating coil, OP, so it will cause its breaker to trip. For the external fault, shown in blue at the lower left of Figure 24, the essential difference is that the thick blue fault current arrow now flows out of the polarity dot in the CT for breaker #2. This reverses the direction of the magenta arrows, which represent approximately the same magnitude of current as the green arrows. The secondary circuit connections cause these currents to now bypass the OP coil, so that relay will not trip its breaker for the external fault. In order for these currents to bypass the OP coil, the relay's impedance (sometimes called its "burden") must be significantly larger than the secondary circuit wire impedances. That is generally the case, but it must be checked and may impose a limit on the protected line length.

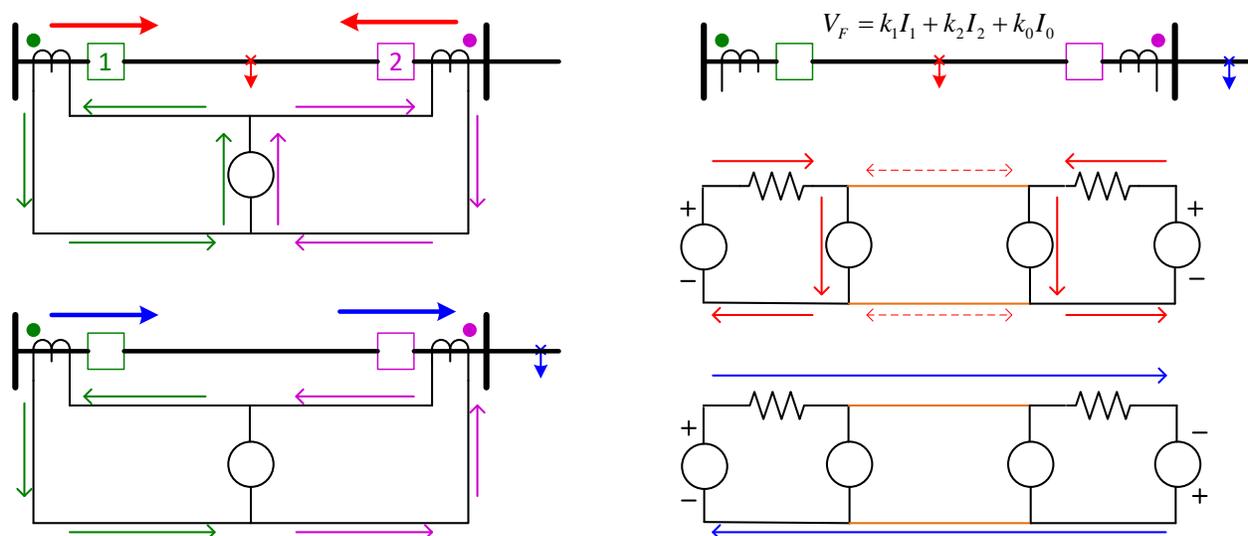


Figure 24: Pilot wire relaying implements current differential or phase comparison over twisted pair, private or leased.

The right-hand side of Figure 24 shows a modification of pilot wire relaying, using a synthesized fault function similar to that used for phase comparison relaying. That function can be used to drive voltage sources, V_{F1} and V_{F2} , at each end of the secondary circuit. Analog electronics may be used for both the synthesis and source. For the internal fault, shown in red, the CT polarity dots cause each voltage source to have the same polarity, so currents flow through both OP coils rather than through the pilot wires. Breakers at each end will then trip. For external fault, shown in blue, the CT polarity dots cause the polarity of V_{F2} to reverse, so that neither OP coil produces a trip. This version of the pilot wire scheme, with a relay at both ends, is most applicable to line protection.

Figure 25 shows a modification of local stepped zone distance protection that can produce faster fault clearing times in Zone 2, at the expense of some false trips for external faults that could be mitigated with high-speed reclosing. This may be called Zone 1 extension or Zone 2 contraction (Elmore 1999), implemented with device 21 relays. For a fault in the middle 60% of the line, shown in red, Zone 1 trips breaker A in about 5 cycles. Breaker B would trip on its own Zone 1 setting (not shown in Figure 25) so the total fault clearing time is 5 cycles.

For a fault near the other end, shown in blue, the Zone 1x time will trip breaker A in about 10 cycles, compared to the normal Zone 2 time of 25 cycles. Breaker B still trips in 5 cycles on its own Zone 1 setting, so the total fault clearing time is 10 cycles, not 25 cycles.

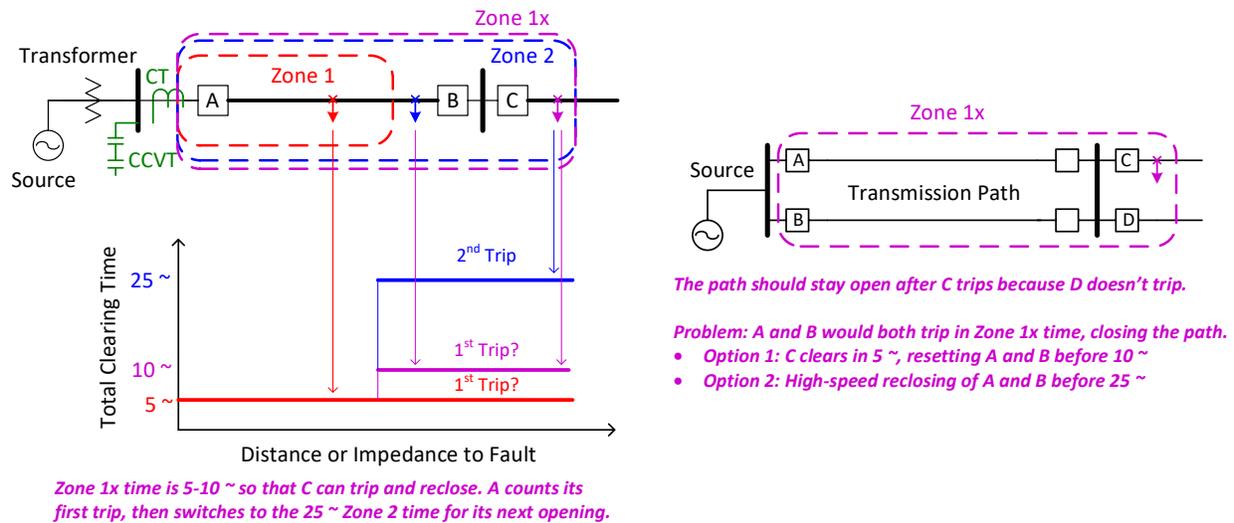


Figure 25: Zone 1 extension improves clearing speed for radial or looped systems without communications.

For an external fault, shown in magenta, the Zone 1x time would trip breaker A in about 10 cycles. However, breaker C may trip in 5 cycles on its own Zone 1 setting. There isn't enough time margin to guarantee that, but if breaker C does trip fast enough, then breaker A would not actually trip. In either case, breaker B does not trip because the external fault is in the wrong direction. Whichever breaker does trip, A or C, will attempt a high-speed reclose, after which breaker A needs to switch from Zone 1x to Zone 2 even if it didn't trip originally on the Zone 1x pickup. Breaker A can do this change based on local information, simply by counting fault current events, in the same way distribution line reclosers do for sequence coordination.

The benefit of Zone 1x is to reduce the worst-case clearing time for internal faults from 25 cycles to 10 cycles, even without communications. This may be significant in preventing

equipment damage, wildfires or loss of system stability. On the other hand, there will be some additional false trips and high-speed reclosing events. The tradeoff can only be evaluated through comprehensive system studies. This evaluation should include the optimization of Zone 1x time delay, either less than or more than the 10 cycles assumed here. Further, meshed systems and parallel transmission lines would produce even more false trips due to Zone 1x overreach, as illustrated on the right half of Figure 25. The idea may still prove useful in protection schemes that don't rely on communication systems.

Figure 26 shows an example of relatively complete EHV transformer protection, including a current differential scheme 87T. The 87T scheme adds up CT secondary currents on all sides of the protected transformer, similar to line pilot wire scheme shown on the left side of Figure 24. There is no voltage input required for 87T. There are some complicating details needed to adjust for measurement errors and the protected transformer's turns ratio, which are not important to show here. For this project, the main differentiator between 87T and the line protection (87L or 87PC) is that long-distance communication is not required. The distances are tens of yards for transformer protection, compared to tens of miles for lines. The communication links in 87T are implemented with metal wires or fiber optics, all within the substation fence. The other transformer relays include overcurrent (50, 51, 51G), pressure (63) and temperature (40), all of which use wiring or fibers inside the substation fence.

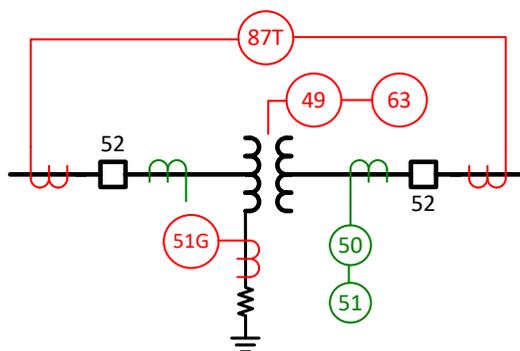


Figure 26: Transformer Differential Protection needs Communication only within the Substation, if the Transformer has Interrupting Switchgear on All Sides.

There are some use cases for transformer protection that do require long-distance communication, and Figure 27 shows one of them. In order to save money, a transmission or sub-transmission line has been installed to serve two or more load-serving substation taps, without a high-side interrupter on the load-serving transformers. Each transformer would need a load-breaking switch, but this may not be rated to interrupt faults. In that case, each transformer protection scheme needs to open its own load-side breaker for internal faults, but also send a direct transfer trip (DTT) signal to the nearest high-side breaker that can clear the fault. In Figure 27, a fault on either transformer will cause both line breakers to open just as they would for a line fault, interrupting service to both transformers. On EHV systems, this configuration would appear only in special cases, e.g., transformer-terminated lines in the early stages of system growth. Further, the advent of economical circuit switchers could mean that newer tapped transformer installations are more likely to have their own high-side interrupters. DTT is still used on existing systems. DTT is also widely used on distribution feeders with distributed energy resources (DER). A false DTT signal will produce a false breaker trip. Conversely, disabling DTT via cyber-attack would prevent clearing transformer faults in Figure 27.

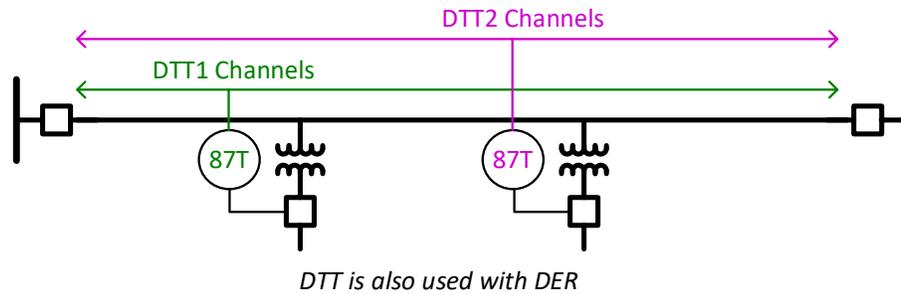


Figure 27: Direct Transfer Trip for Transformers without High-side Breakers

Figure 28 shows an EHV substation with breaker-and-a-half scheme, incorporating line distance (21), transformer differential (87T) and bus differential (87B) schemes. The protection zones overlap, and also must account for any breaker taken out of service for maintenance, by opening the switches on either side of the breaker. Each relay obtains operating current from the color-matched CTs bordering that zone. When disconnect switches open to isolate one of the breakers, there will be two CTs isolated along with the breaker and measuring zero current. However, the zone overlaps have been defined such that each color-coded zone should still measure the total current into the protected component. A fault located within the overlap between two zones will cause both relays to operate, which would remove additional equipment from service. A fault within a circuit breaker or CT is especially problematic, as the fault appears in two zones. However, the breaker-and-a-half scheme's advantage is in allowing for manual service restoration by isolating the affected breaker or CT.

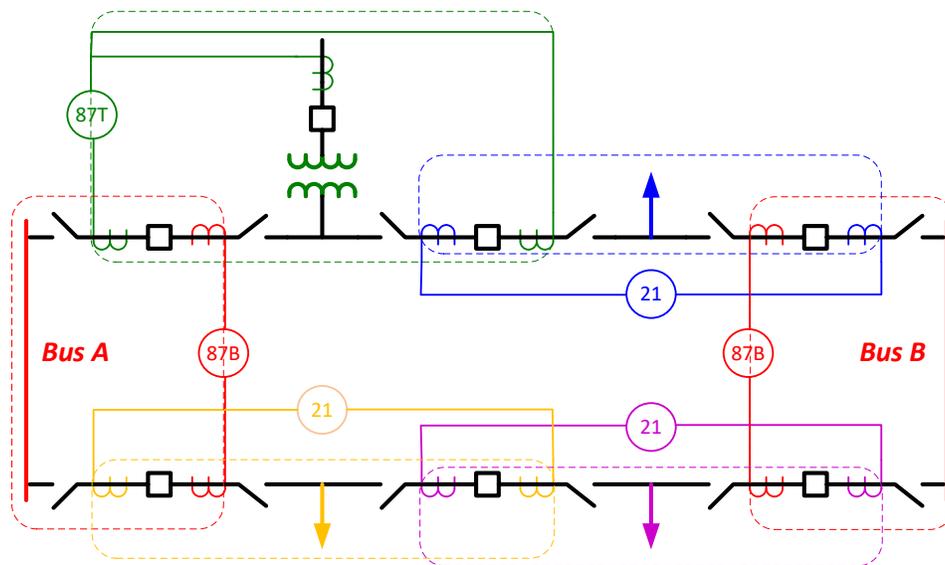


Figure 28: Bus differential schemes may overlap line and transformer protection zones, but they don't require external communication channels.

In addition to CTs, the device 21 relays need voltage inputs from CCVTs that aren't shown. The 87T and 87B schemes will use communications mainly within the substation fence, unless DTT is necessary. The 21 or 87L schemes will use remote communications to the other line ends, as discussed with Figure 18 through Figure 24.

Breaker failure (BF) schemes can use either local or remote tripping, as shown in Figure 29. Suppose there is a fault at the red location, and breaker G opens properly but breaker E does not. Note that either the local relays on E, the communication channel from G, or breaker E itself may have failed, but the system effects are the same. A local BF scheme would trip all of breakers C, D and F; this is necessary to clear the fault. Of course, that effectively removes the entire station from service. A breaker-and-a-half scheme as detailed in Figure 28 helps to mitigate this impact, albeit with some delay. If there is a problem affecting the entire middle substation, then a remote BF scheme would trip all of breakers A, B and H; this has become necessary to clear the fault. In this case, tripping either the local or remote backup would result in complete loss of the transmission capacity from left to right. However, if the fault persists without clearing, then power system equipment damage, wildfire, or other property damage is likely. Many BF schemes include some communication link, such as DTT, to the remote substations. Injecting false signals into BF communications would lead to false trips. Conversely, blocking BF communication channels would allow faults to persist on the system.

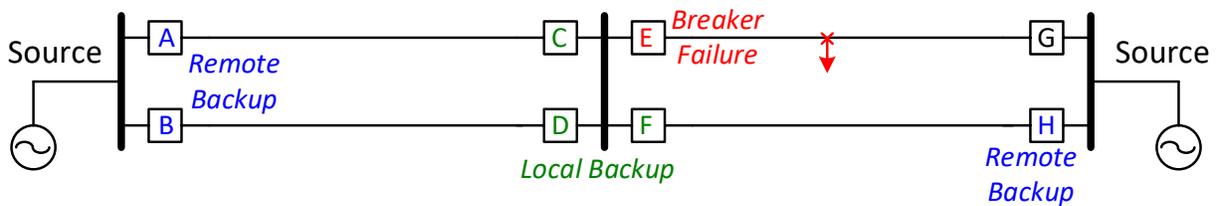


Figure 29: Breaker failure schemes may use local or remote backup protection/tripping.

It's not always possible to avoid communication channels in BF schemes. Figure 30 shows one breaker-and-a-half bay of an EHV substation with two lines connected. For the fault shown on the line to E, breakers C and E clear as expected, but breaker B fails for some reason. Breakers A and D must now open to clear the fault, but breaker D is located at a remote substation. Distance relays at D can't always be set to see the faulted location in Zone 2 or Zone 3. Even if the zone overreach settings can be coordinated at D, the tripping time will be relatively long. Instead, once it's known at the local substation that breaker B's relays have operated but the breaker did not actually open, a DTT signal would be sent to breaker D over a communication channel. A similar DTT requirement would apply to an EHV ring bus's BF protection.

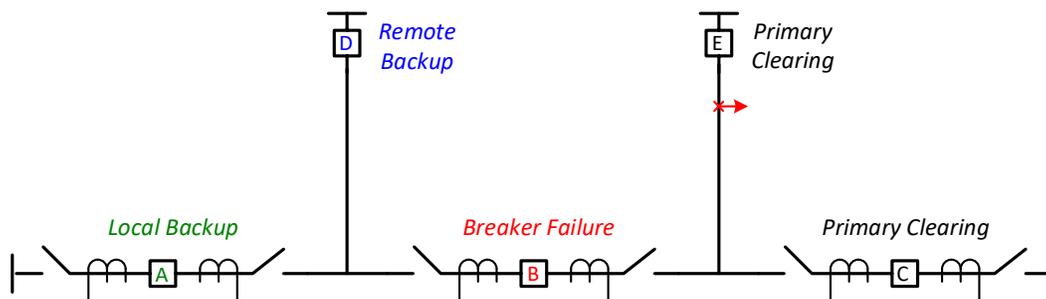


Figure 30: EHV substations with breaker-and-a-half bus must include remote backup.

Appendix B – Device Function Number Analysis

This appendix describes the standard device numbers (IEEE 2008) of most interest to protection of transmission lines, transformers, generators and substation buses. For each device number of interest, Table 3 shows the grid application area and the possible impact from communication systems. The corresponding IEC logical nodes are also shown because some modern relays support both IEEE and IEC nomenclature. For applications in the United States, the IEEE nomenclature is still more widely used.

Table 3: IEEE device number communications impact summary.

IEEE Device Number	Function Description	IEC 61850-7-4 Logical Node	Applies To							Impact of Communications	
			Bus	Xfmr	Line	BF	Gen	Fdr	DER		
21	Distance	PDIS PSCH			x					Communication is required for common pilot protection schemes (DUTT, PUTT, POTT, DCB, and DCUB). These schemes increase selectivity and reduce trip times. Lack of communication would reduce selectivity in over-reaching scenarios and increase trip times for end-of-line faults.	
24	Volts per Hz	PVPH		x					x	n/a	
25	Synchronism Check	RSYN						x		x	n/a
27	Under-voltage	PTUV								x	n/a
30	Annunciator Relay		x	x	x	x	x	x	x	x	Communication is required to collect data from other relays and present it through an annunciator. Annunciator enables better situational awareness for an operator. An annunciator is not required for protection; its primary role is for monitoring the overall system.
32	Directional power	PDOP		x	x						Communication is required for pilot protection schemes that use directional comparison. These include DUTT, PUTT, POTT, DCB, and DCUB schemes.

IEEE Device Number	Function Description	IEC 61850-7-4 Logical Node	Applies To							Impact of Communications
			Bus	Xfmr	Line	BF	Gen	Fdr	DER	
										Lack of communication would reduce selectivity in over-reaching scenarios and increase trip times for under-reaching scenarios.
40	Loss of field	PDUP						x		n/a
46	Reverse phase	PTOC						x		n/a
47	Phase Sequence	PTOV						x		n/a
49	Thermal	PTTR						x		n/a
50	Instantaneous Overcurrent	PIOC		x	x			x	x	n/a
50BF	Breaker Failure	PTOC	x	x	x	x	x	x	x	Communication is required for fast tripping of remote circuit breakers in the event local breakers fail. Remote terminal relays without breaker failure communication would wait for a pre-defined time delay (usually 0.3 – 0.6 seconds) before sending a trip command. Remote tripping may be even slower for high impedance faults that remote relays don't pick up.
51	Time Overcurrent	PTOC		x	x			x	x	n/a
59	Time overvoltage	PTOV							x	n/a
61	Density Switch							x		n/a
63	Pressure Switch Detector			x						n/a
67/67G	Directional Overcurrent	PTOC			x					Communication is required for pilot protection schemes that use directional comparison. These include DUTT, PUTT, POTT, DCB, and DCUB schemes. Lack of communication would reduce selectivity in over-reaching scenarios and increase trip times for end-of-line faults.
68	Power swing detection/blocking	RPSB			x			X		Communication is not required for traditional impedance-based, out-of-step detection. However, communications are used with PMU-based schemes.

IEEE Device Number	Function Description	IEC 61850-7-4 Logical Node	Applies To							Impact of Communications	
			Bus	Xfmr	Line	BF	Gen	Fdr	DER		
									Communication is required for Synchrophasor-based relaying schemes. These schemes are being evaluated for deployment.		
79	Reclosing	RREC			x				x		
81	Frequency							x	x	x	n/a
85	Receiver				x	x					This function receives the signals over PLC, fiber, pilot wire, or radio. It's used only with communication channels.
86	Lockout	-	x	x		x	x				Communication is required to remotely reset lockout relay.
87 87L 87GT 87PC TW87	Differential	PDIF	x	x	x		x			x	Communication is required for line differential (LCD). With no communication, line distance or directional elements would be used, which runs the risk of underreaching or overreaching their primary protection zone. Sensitivity is also lost for high fault resistance cases. Local differential schemes (e.g. transformer, bus, generator) don't require communication. For traveling wave or time domain protection, lack of communication causes some additional inaccuracy in fault location.

Pacific Northwest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99352
1-888-375-PNNL (7665)

www.pnnl.gov