CIGRE-193 **2019 CIGRE Canada Conference**
Montréal, Québec, September 16-19, 2019

New Methodologies for Accurate Modelling and Simulation of Advanced Telecommunication-Based Protection Schemes in a Software Environment

Hadi Khani, Daniyal Qureshi, Saman Alaeddini, and Ishwarjot Anand
Protection and Control Department, Quanta Technology, Canada

SUMMARY

The growing complexity of modern protective devices with hundreds of functionalities and the evolving nature of power grids have posed several challenges to transmission system operators. Numerous utilities around the globe have decided to employ advanced telecommunication-based protection schemes to enhance the reliability and resiliency of their grids. To determine the appropriate tele-protection schemes on a case-by-case basis, however, power system protection engineers need to simulate and analyze the behavior of such schemes using computer software. In addition, hidden and complicated coordination issues stemming from deficiencies in the existing tele-protection schemes cannot be discovered unless the true behavior of these schemes is modeled and simulated with sufficient detail. Simulation of the complicated logic of tele-protection schemes, however, introduces many challenges to the protection engineers.

Moreover, with very low fault current values generated by power electronics-based converters, robust and reliable protection schemes for microgrids are yet to be developed. Utilization of adaptive protection schemes and setting up communication channels between relays within a microgrid have been proposed as effective solutions to the problem. However, the logic diagrams of the relays protecting the microgrids can become very complicated in certain applications. This paper argues that in order to come up with a reliable design, such logic diagrams need to be accurately modeled in a software environment and analyzed thoroughly before issued to the field.

As such, development of tools for accurate modelling of complex tele-protection systems for both the transmission systems and microgrids are vital for the design and analysis purposes. To that end, this paper presents new methodologies and algorithms to tackle the aforementioned challenges. New tools are designed that can handle complicated tele-protection schemes in an advanced software environment and allow the user to replicate the behaviour of the real-world protection system.

In addition, manual modelling of a complex protection system that includes tele-protection schemes can be very laborious and prone to errors. This aspect has been a barrier in the past for transmission system operators to build a detailed protection model and take advantage of modern protection system analysis tools. To remove such barriers, the proposed tools have been developed in such a way that they are fully automation friendly and can be used for bulk modelling and analysis using automated approaches.

The presented approaches and the new telecommunication tools are utilized for protection modelling, simulation, and analysis in a real-world large-scale system. The efficacy and feasibility of the proposed methods and tools are tested on hundreds of lines and transformers. The designed tele-protection tools are robust and reliable and allow the user to create a very accurate protection model. The model can be

hkhani@Quanta-Technology.com

utilized for designing more robust tele-protection schemes for transmission systems and microgrids and uncovering hidden coordination issues that could have not been discovered otherwise.

KEYWORDS

Tele-protection schemes, pilot relay, transmission system protection, adaptive protection, microgrids, protective relays, modelling and simulation, design, performance analysis, automation.

INTRODUCTION

Development of automation-based approaches for accurate modelling of complex tele-protection systems for both the transmission systems and microgrids are vital for the design and analysis of protection systems. Some studies in the literature discuss about the application of automated approaches for protection modelling and coordination analysis in a computer program. In [1], a guide for development of a systematic method for performing a wide-area protection analysis is presented. The authors discuss the challenges that a protection engineer could be faced with and demonstrate examples where coordination cannot be acquired. The study also discusses the utilization of engineering software for automated studies and presents methods for resolving protection issues in power systems. The study in [2] argues that automated wide-area analysis allows power system utilities to capture protection issues in a short period of time as compared to traditional methods. Authors present discussions about the risks associated with protection coordination issues in a complex power grid. In all these studies, modelling and analysis of tele-protection schemes can result in capturing hidden coordination issues that would have not been found otherwise.

Additionally, adaptive protection schemes and setting up communication schemes between relays within a microgrid have been utilized for microgrid protection [3]-[5]. The logic diagram of the microgrid relays can become very complex in some cases. To design a robust protection scheme, such logic diagrams must be modeled, simulated, and analyzed accurately.

Prior studies, however, have not presented automation-based tools and approaches for accurate modelling of telecommunication-based protection schemes. To fill the gap between the existing studies and a more practical solution, this paper proposes new methodologies and tools that can handle complicated tele-protection schemes in an advanced software environment and allow the user to accurately replicate the behaviour of the real-world protection system. The presented approaches and tools are utilized for protection modelling, simulation, and analysis in a real-world large-scale system. The feasibility and practicality of the proposed solution are tested on hundreds of cases.

PROBLEM STATEMENT

The importance of accurate protection modelling in software has grown significantly. With poor or incomplete software models, protection engineers are unable to reliably assess telecommunication-based logic in their systems. However, existing tools in the software environment to model advanced telecommunication-based schemes are limited in their scope as well as their ease of implementation. Alternatives to software evaluation often require costly equipment and may not be easily available. Thus, it is common to avoid the modelling of advanced protection and telecommunication-based logic altogether. This will translate into mis operations in the real world, caused by hidden issues stemming from deficiencies in telecommunication schemes. The long-term value of an accurate software model comes from being able to find such hidden issues.

In order to effectively model and evaluate telecommunication-based protection schemes in a software environment, a relay must be designed which can accurately represent the diverse logic of a conventional relay. This relay should furthermore be flexible enough to have applications in the modelling of adaptive and complex logic-based protection schemes. There should also exist automation-based tools to efficiently transfer the data within power system utility databases to a software model with pilots. With the use of this relay and accompanying modelling tools, protection engineers should be able to complete studies that reveal hidden issues they would be unable to detect otherwise.

The creation of this relay must be accomplished using resources native to the software environment, such that it does not necessitate the use of additional software in its functions. The design should also be automation friendly and well integrated with the automatic approaches for protection modelling and analysis.

PROPOSED SOLUTION

Figure 1 shows the proposed pilot relay integrated with the existing protection system.

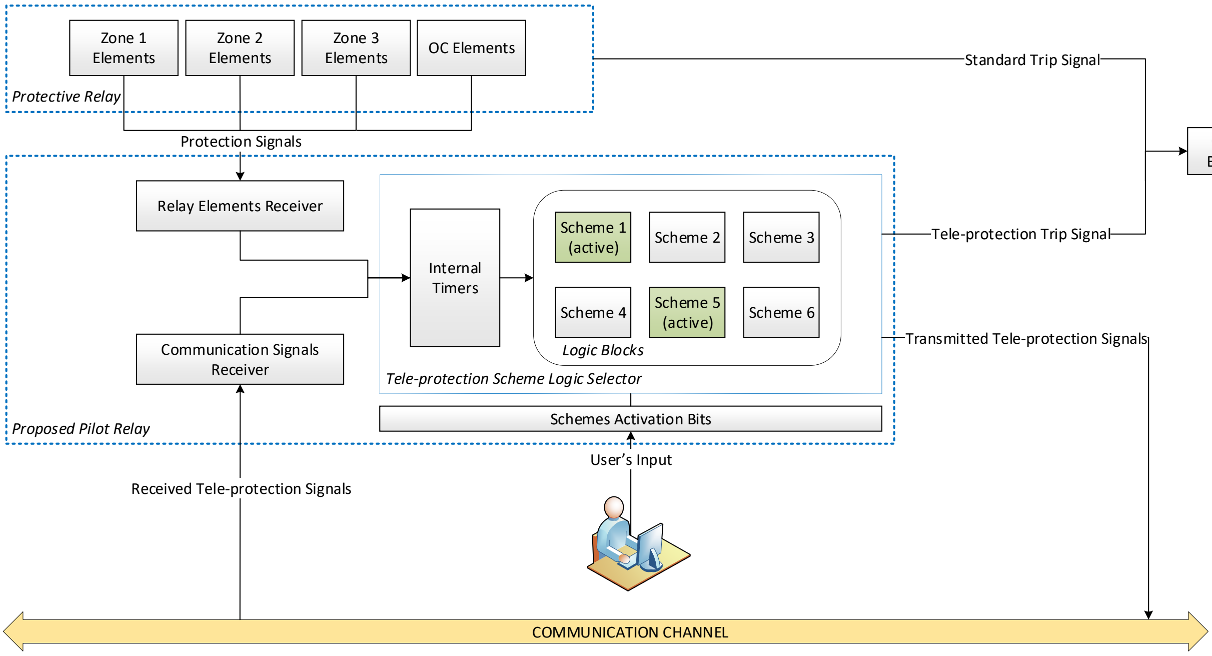

Figure 1. Proposed pilot relay integrated with the existing protection system.

As shown in Figure 1, the proposed solution is to utilize a separate relay (to be named the *pilot relay* in this paper) in the software environment which connects to the output signals of the modelled protective devices. The user utilizes one pilot relay connected to an existing protective device at the local terminal. It also has connections to one or more pilot relay(s) at the remote terminal(s) on the protected equipment. The pilot relay includes two types of elements:

- *Local elements*: Elements connected to the local protective relay.
- *Communication-based elements*: Elements connected to the remote pilot relay.

These elements interact with each other in accordance to sets of Boolean logic that are equivalent to the logic implemented in the real-world relay. This logic contains items like AND, OR and NOT gates as well as timers. The pilot relay, in addition to elements, has taps that control features in the logic such as scheme activation and timers.

Upon using a pilot relay and connecting the necessary local and communication elements for a protective scheme, the user would set the taps in the pilot relay to enable the desired protection scheme and populate its timers.

CONVENTIONAL APPLICATION

The most apparent application of the pilot relay is in the modelling, analysis, and design of standard telecommunications-based protection schemes. The pilot relay will house several elements used as the components of protection schemes, including permissive over-reaching transfer trip (POTT), permissive under-reaching transfer trip (PUTT), directional comparison blocking (DCB), etc. Within the pilot relay, there is internal logic between these components that is activated based on the scheme that the user selects to use.

The pilot relay itself, as discussed, does not include protective elements. These elements operate in the local protective relay and are mapped to elements within the pilot relay. The communication elements in the pilot relay are mapped to communication elements in other pilot relays at the remote terminal(s) to simulate telecommunication signals. Both types of elements are processed inside the pilot relay and a trip signal is issued to the local circuit breaker as per the internal logic expression.

Figure 2 shows an example communication matrix between the pilot relays at the line terminals and transformer station on a two-terminal line with one load tap.

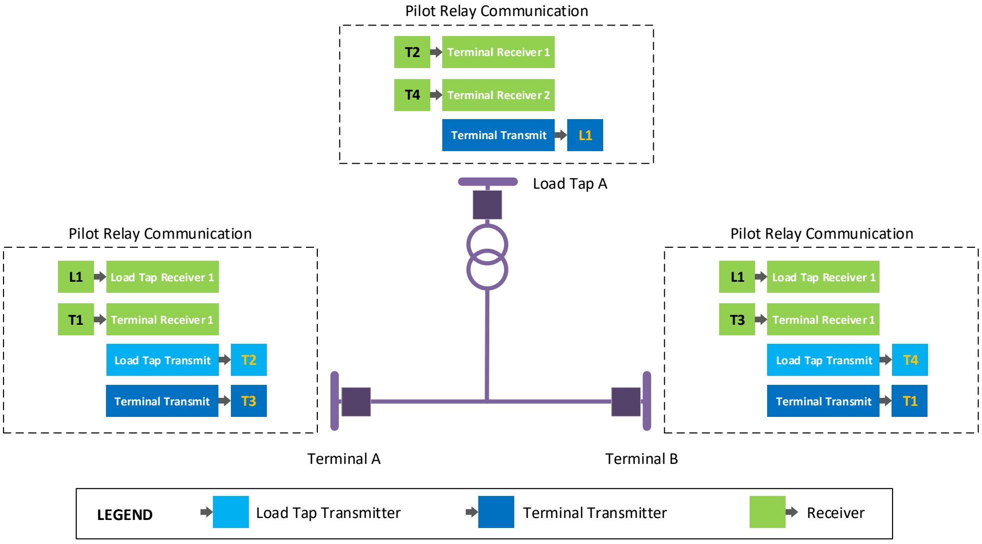

Figure 2. Communication matrix between pilot relays in short circuit software.

The illustration in Figure 2 could be a model for a transfer trip scheme, where the circuit breakers on the line as well as the low-side circuit breaker of the transformer must trip in order to clear a fault at a location anywhere on the line. The local elements in the pilot relays are mapped to protective relay elements.

All pilot relays have multiple transmitters and receivers, allowing for multi-terminal communication as well as different signals between different types of stations (e.g. load tap vs. line terminal). The receiver at each pilot relay is connected to the transmitter of the other pilot relay that has the same number as the receiver (e.g., L1, T1, etc.). The transmitted bit is produced through internal logic with the local elements, which in the case of transfer trip would correspond to the operation of any instantaneous local tripping element. The received bit at each pilot relay is connected to a transmitter of another pilot relay. There is tripping logic internal to the pilot relay, depending on the active scheme, which uses the received signals for evaluation. For transfer trip, simply receiving a transfer trip signal is enough to cause the pilot relay to issue a trip to the circuit breaker.

For a close-in fault on the line at Terminal A, the local Zone 1 distance relay will trip the circuit breaker. The pilot relay, which Zone 1 is connected to, will read the trip signal and transmitters T2 and T3 will issue a trip signal for load tap and terminal stations, respectively. At Load Tap A, the Terminal Receiver 1 in the pilot relay will read the transfer trip signal after a programmable delay meant to simulate the communication delay. Similarly, at Terminal B, Terminal Receiver 1 in the pilot relay will read the transfer trip following a time delay. Both pilot relays will trip their local circuit breakers.

ADVANCED APPLICATION

The use of the pilot relay surpasses conventional pilot protection modelling. The ability to model complex logic and telecommunication schemes allows the user to plan and simulate advanced protection schemes. For instance, the pilot relay can be used as a tool for modelling adaptive protection in a microgrid. Adaptive protection is defined as a category of protection where the active settings profile in a relay alternates based on logical expressions and signals, in response to changes in the system operating mode.

The future trend in microgrid design is towards purely renewable distributed generation with no rotating machines, utilizing only power electronics-based converters. The consequence of this is far lower fault current in the islanded operating mode than the fault contribution in the grid-connected mode. More sensitive overcurrent pickup settings are required in the islanded mode, causing possible load encroachment issues. In the grid-connected mode, however, higher pickup settings are needed due to higher fault current contribution from the grid. This is the chief challenge in designing protection for microgrids since a single set of protection must be secure and dependable for either operating mode. Adaptive protection and the use of custom logic in the relays seem to be reasonable solution to this challenge.

Figure 3 demonstrates an example of a microgrid with photovoltaic (PV) and wind generation, as well as an energy storage system (ESS).

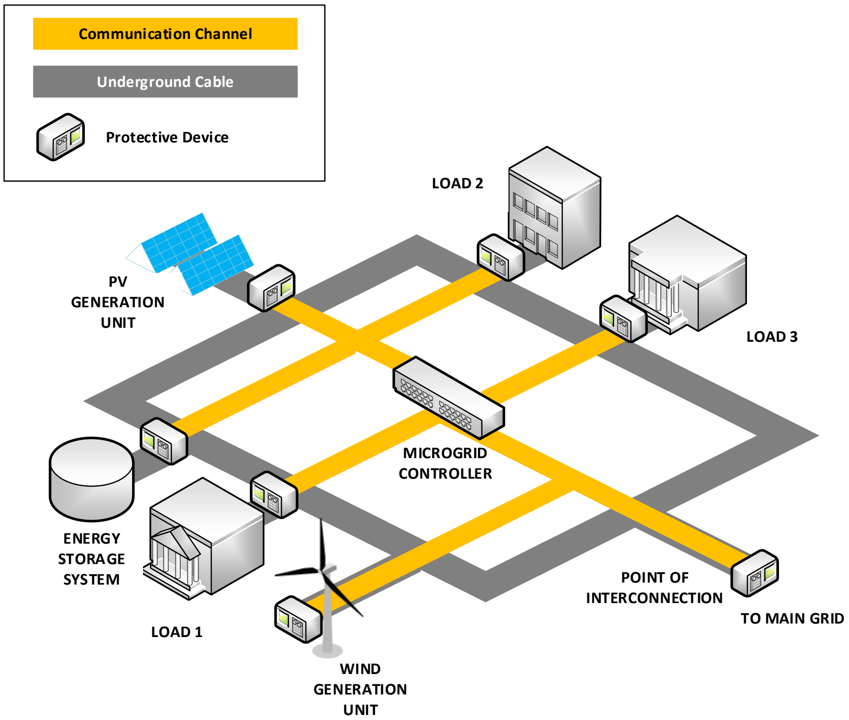

Figure 3. A microgrid with distributed renewable energy generation and communication-aided protection schemes.

As shown in Figure 3, there are three loads in this example and a protective device at every site, including the point of interconnection (POI) with the main grid. Transformers, measuring devices, switches, and circuit breakers are not shown in the figure. The microgrid controller (MGC) has two-way communication with all protective devices within the microgrid. When the switch at the POI is open, the microgrid enters into the islanded operating mode. Otherwise, it is in the grid-connected mode.

The microgrid controller should receive the status of the POI switch via the communication channel and transmit a signal to each of the relays in the microgrid to force them to switch to a certain settings profile when the operating mode changes. For example, the settings profile with lower overcurrent pickup settings would be used in the islanded operating mode. Additionally, there is communications between the relays to enhance the protection coordination. This involves the transmission of signals such as blocking or transfer trip. Lastly, certain fault scenarios necessitate the use of detailed logic within the relays.

The dynamic switching of profiles, communication between microgrid relays, and advanced logic schemes are difficult to model using traditional software modelling approaches. This proves detrimental to the design and testing of microgrid protection systems. Without a software model, protection engineers are blind to the validity of their design until the testing stage with the physical relays. Such tests could be done with devices such as real-time digital simulators (RTDSs) at the hardware level, which in practice should only be used as the final stage prior to commissioning. This restricts engineers from developing more complex logic and schemes since the effort to verify these designs is significant and costly at the hardware level.

However, the pilot relay can be utilized to model the above-mentioned features in a software environment. It can connect to any element in any setting group in the local relay and can also read the status of equipment such as circuit breakers. It can connect to other pilot relays to simulate the transmission and receival of communication signals. Lastly, it is capable of being programmed with any logical expression desired using the local and communications-based elements.

In the hypothetical microgrid presented in this paper, a pilot relay would be modelled alongside the protective device at each of the sites. The pilot relay at the POI would transmit the status of its local circuit breaker to the other pilot relays. Each pilot relay chooses a protection setting profile in the main protective devices based on the operating mode. Each pilot relay would contain a tripping expression using elements from each setting group ANDed with the bit that enables that profile. This would model the switching and utilization of setting profiles in the microgrid relays. The pilot relays at each site could also transmit bits to one another to represent transfer trip or blocking signals. A complex logical expression can be produced within the pilot relay, so that custom schemes can easily be modeled and analyzed.

Thus, the proposed pilot relay would allow protection engineers to quickly and accurately test possible designs with adaptive protection or telecommunications. Users can model their initial design in a software environment, verify it, and adjust the design until it is acceptable. This gives them a greater confidence when arriving at the hardware level testing. Additionally, more complex logic can be explored at the design stage. Sophisticated logic can improve the security and dependability of the protection system, and reduce equipment cost when used intelligently.

REAL-WORLD EXAMPLE

The approaches presented in this paper have been applied to a real-world large-scale system comprised of more than 600 lines and 500 transformers. While the proposed tools and methods can be used to capture several protection issues, in this section one real-world example is given. Figure 4 represents the mho plot of a local distance relay's Zone 2, shown in red.

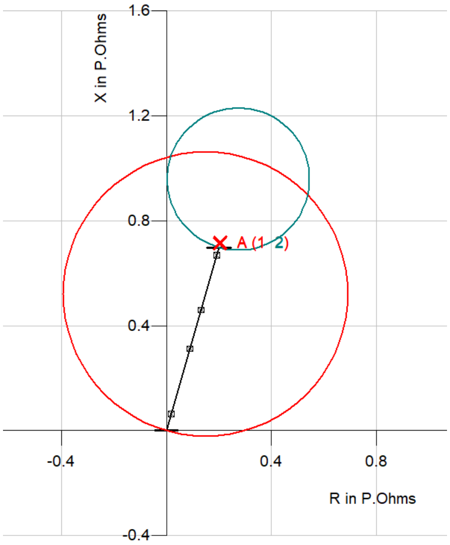

Figure 4. Software-generated R-X plot of a fault on a neighbouring line superimposed on reach of the local distance Zone 2 and remote reverse-facing Zone 3.

As shown in Figure 4, the teal circle represents the coverage of a reverse-facing Zone 3 in a distance relay at the remote terminal of the line. The red X marks the apparent impedance of a fault on a neighbouring line to the remote terminal. By solely assessing this model without the context of telecommunication-based protection schemes, an engineer sees no potential miscoordination. Zone 2 has a timer which prevents it from tripping before the Zone 1 on the neighbouring lines. If a secure DCB scheme is assumed to be on the line, the fault on the neighbouring line (as seen in Figure 4) is seen by the remote Zone 3 and a blocking signal should be sent to the local relay, preventing instantaneous Zone 2 operation. This may be enough for the engineer to have confidence in the DCB scheme.

The Zone 2 may trip instantaneously, however, if it does not receive a blocking signal before the DCB coordination delay ends. This depends on the communication medium, which may be incapable of transmitting the blocking signal in time. Further, Figure 5 shows the hidden coordination issue for a DCB scheme with insufficient DCB coordination delay.

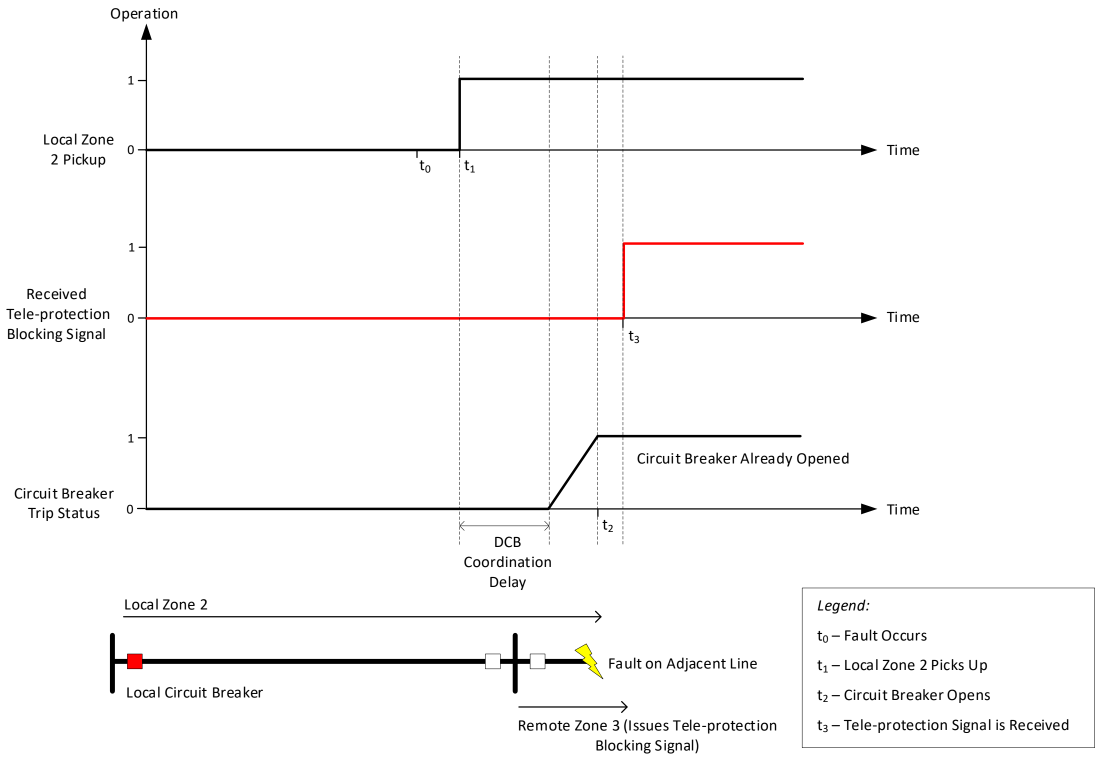

Figure 5. A hidden coordination issue for a directional comparison blocking scheme with insufficient coordination delay.

The issue demonstrated in Figure 5 might be hard to determine from the mho plot and in simulations of the system lacking the complete pilot scheme. Such issues have been discovered after the implementation of the pilot relay and through wide-area coordination studies on the completed protection model.

The pilot relays used in the real-world studies have been developed to replicate certain common tele-protection schemes, such as DCB, POTT and transfer trip. Figure 6 demonstrates how the internal logic in the pilot relay can recreate the DCB scheme in an actual relay.

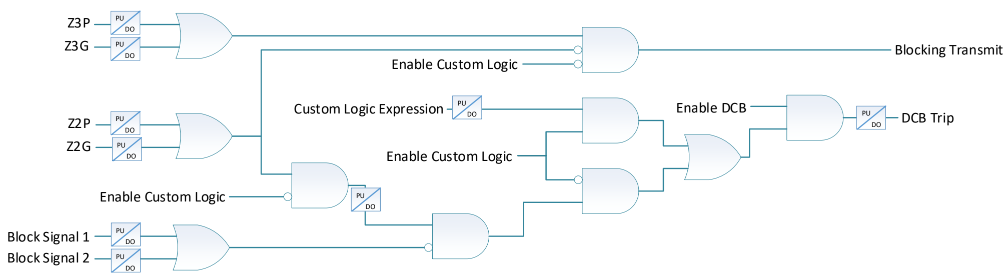

Figure 6. Pilot relay transmitter and tripping logic for directional comparison blocking scheme.

As shown in Figure 6, the elements Z2P and Z2G are mapped to the local relay's Zone 2 phase and ground elements. Similarly, Z3P and Z3G are mapped to the reverse-facing Zone 3 elements of the local relay. The Block Signals are represented by the receivers which are connected to the remote terminal's Blocking Transmit. There are timers with pickup and dropout settings before each element. These are used in the Block Signals to simulate communication delay.

As per the DCB scheme, the Zone 2 elements (with a timer for DCB coordination delay) are NANDed with the blocking signals to generate DCB Trip. The Enable DCB bit is a tap in the pilot relay, set to true when the DCB scheme is used. There is an Enable Custom Logic bit as well, which when active will use the custom logic expression written by the user in the pilot relay instead of the hard-coded logic. This expression can use any of the elements mapped to the pilot relay. Lastly, the local Blocking Transmit is turned on with the pickup of Zone 3 elements.

Figure 7 details the internal logic in the pilot relays for the POTT scheme, which operates when the Enable POTT tap is true.

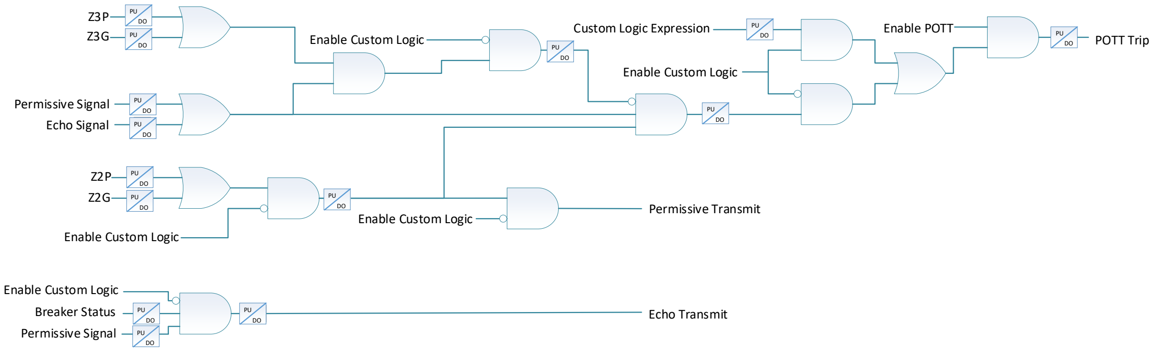

Figure 7. Pilot relay transmitter and tripping logic for permissive overreaching transfer trip scheme.

As shown in Figure 7, the same distance elements are used in this scheme as in the DCB one. Additionally, the Breaker Status is read from the local circuit breaker. The received Permissive Signal and Echo Signal are connected to the Permissive Transmit and Echo Transmit of the remote terminal. Zone 2 elements are ANDed with the received permissive signals and NANDed with the local Zone 3 current reversal guard to activate POTT Trip. The Zone 2 is used to generate the Permissive Transmit, while the received Permissive Signal and Breaker Status are used to generate the Echo Transmit. Custom logic can also replace the hard-coded one if enabled.

CONCLUSION

The authors in this paper argue that in order to come up with a reliable protection design, tele-protection schemes need to be accurately modeled in a software environment and analyzed thoroughly before issued to the field. To that end, new tools are designed that can handle complicated tele-protection schemes in an advanced software environment and allow the user to replicate the behaviour of the real-world protection system. The proposed approaches and tools are utilized for protection modelling, simulation, and analysis in a real-world large-scale system. It is discussed that the proposed pilot relay can be utilized for protection design and analysis in both the conventional and modern applications. It is indicated that the pilot relay can help capture hidden protection coordination issues that would have not been found otherwise. As such, the model can be utilized for designing more robust tele-protection schemes for transmission systems and microgrids. The ability to incorporate more complex logic in the software model enables the user to study and develop more secure and dependable protection schemes than they would be able to do normally. The pilot relay saves a significant amount of effort and cost by allowing testing of the logic in the software environment rather than verifying the design at the hardware level at the initial design stages. As modern power systems become more interconnected, complicated, and reliant on telecommunication, the ever-increasing need for accurate protection models can be partially fulfilled by using the designed pilot relay.

BIBLIOGRAPHY

[1] B. Barman, J. Clack, and V. Padaca, “A Practical Guide to Performing Wide-Area Coordination Analysis”, Western Protective Relay Conference (WPRC), 2014, Spokane, Washington DC, USA.

[2] Saman Alaeddini, et. al, “Comparison of Risk Assessment Approaches in Wide Area Protection Coordination” 2016, CIGRE Paris.

[3] M. N. Alam, “Overcurrent protection of AC microgrids using mixed characteristic curves of relays”, Computers & Electrical Engineering, volume 74, 2019, pages 74-88.

[4] J. Gu, H. Chun, Y. Yen, and M. Yang, “Apply Setting Group Function of IED in Protection Management Systems for Microgrid Reconfiguration,” 2019 International Youth Conference on Radio Electronics, Electrical and Power Engineering (REEPE), Moscow, Russia, 2019, pp. 1-6.

[5] R. R. Ferreira et. al, “Method for identification of grid operating conditions for adaptive overcurrent protection during intentional islanding operation, International Journal of Electrical Power & Energy Systems, volume 105, 2019, pages 632-641.