Contract No:

This document was prepared in conjunction with work accomplished under Contract No. DE-AC09-08SR22470 with the U.S. Department of Energy (DOE) Office of Environmental Management (EM).

Disclaimer:

Effect of GPS Manipulation to Traditional and Next Generation Relay Protection

A GPS resilient architecture was implemented and tested for differential protective relays through a direct serial fiber connection between the two relays. This allows for one relay to be the master and provide synchronization outside of timestamp for differential protection.

Intellectual Property Review

This report has been reviewed by SRNL Legal Counsel for intellectual property considerations and is approved to be publicly published in its current form.

SRNL Legal Signature

_____ _____

Signature **Date**

Effect of GPS Manipulation to Traditional and Next Generation Relay Protection

Project Team: Klaehn Burkes (Primary) and Ian Webb

Subcontractor: None

Project Type: Standard

Project Start Date: October 1, 2019
Project End Date: September 30, 2021

This project's objective is to test the effect of GPS timing variations on relay protection algorithms to determine vulnerabilities and the associated hazards to the electric grid. This will focus on differential protection which utilizes peer to peer communication between substations to determine if the current is not equivalent. This requires the use of GPS to sync the two substations and can be vulnerable to GPS manipulation. However, the effects of GPS manipulation are not a commonly known risk. Therefore, this LDRD will address the risks of GPS manipulation for such a widely implemented technology. For differential protection a GPS resilient architecture was implemented and tested for differential protective relays through a direct serial fiber connection between the two relays. This allows for one relay to be the master and provide synchronization outside of timestamp for differential protection.

FY2020 Objectives

- Set up SEL-411L differential protection relay within the SRNL-Critical Infrastructure, ICS and Cybersecurity (S-CIIC) lab
- Program protective relays to perform differential protection through controller hardware in the loop platform Typhoon
- Develop IRIG-B code generation and implement in Typhoon platform
- Time shift IRIG-B to perform time manipulation and then conduct faulting sequences

Introduction

The electric power system is upgrading the supervisory control and data acquisition (SCADA) and protective relaying equipment from electromechanical relays to microprocessor-based relays. This has allowed for more advance control through distributed and real time methods, requiring more communication between intelligent electronic devices (IEDs) and remote terminal units (RTUs). These devices are inherently programable logic controllers (PLCs) that resemble the communication protocols of industrial control systems (ICS) [1]. However, the protocols and communication methods specific to the electric power system (traditionally Distribution Network Protocol (DNP3)) are being replaced with International Electrotechnical Commission (IEC) 61850. DNP3 has no timestamped data in its messaging protocol, meaning relay protection algorithms are not affected by GPS time stamps or data [2]. However, IEC 61850 uses many different protocols that are based on fast fiber connections that utilize timing as a key part of the data transfer. These protocols such as Manufacturing Message Specification (MMS), Generic Object-Oriented Substation Event (GOOSE), and Sample Measured Values (SMV) all run over Transmission Control Protocol/Internet Protocol (TCP/IP) networks utilizing high speed switching ethernet

to obtain the necessary response times for millisecond protective relaying controls [3]. Now the future of protective relaying is relying on accurate and synchronized timing to improve the electric power system reliability and stability.

An example of a protection scheme that utilizes high-speed communication is line differential protection, which requires peer to peer communication between substations. This protection scheme compares the current leaving a substation on one end of a transmission line and the current entering into another substation at the other end of the transmission line and compares the values recorded to detect abnormalities that occur in a fault scenario. This requires two substations to be synchronized on an accurate clocking signal, typically a GPS receiver. This project's objective is to research into the effects of GPS signal manipulation between two substations. This will be performed by slowly walking off one substations GPS signal and monitoring how the protection algorithms are affected to determine the failure mechanisms of these millisecond protective relaying functions. SRNL has already proven in previous work that the GPS receivers cannot detect small steps of GPS signal deviations implying that the receiver does not revert to the backup timing source. This project will allow for SRNL to become a leader in the field of GPS timing manipulation with previous knowledge of GPS receiver operation and the knowledge gained through determining the failure mechanisms of the millisecond protective relay functions of differential and time domain protection.

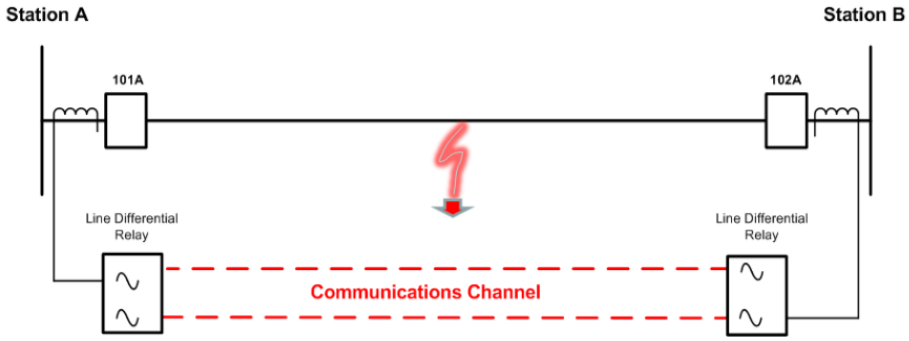

Figure 1: Differential Protection Concept

Approach

The approach for implementing and testing this is through setting up a controller hardware in the loop (CHIL) test bed for the protective relays. CHIL testing allows for controllable and repeatable testing of different protective relays. This allows for running many different scenarios to get precise controlled results. To implement GPS spoofing on protective relays the Typhoon platform was used to emulate the electric power grid, output waveforms of voltage and current to the protective relays, calculate and output IRIG-B timing signals to the relays, and finally take contactor inputs to control breakers in the simulation. Through this method every input and output to the protective relays were controlled through the Typhoon platform and allowed for testing the protective relay as if they were deployed in the field. This all allowed for implementing and testing multiple differential protection architectures and examining their vulnerabilities to GPS time walk off. Specifically, directly related to the different IRIG-B inputs for the relays. Figure 2, represents the test network established in the S-CIIC.

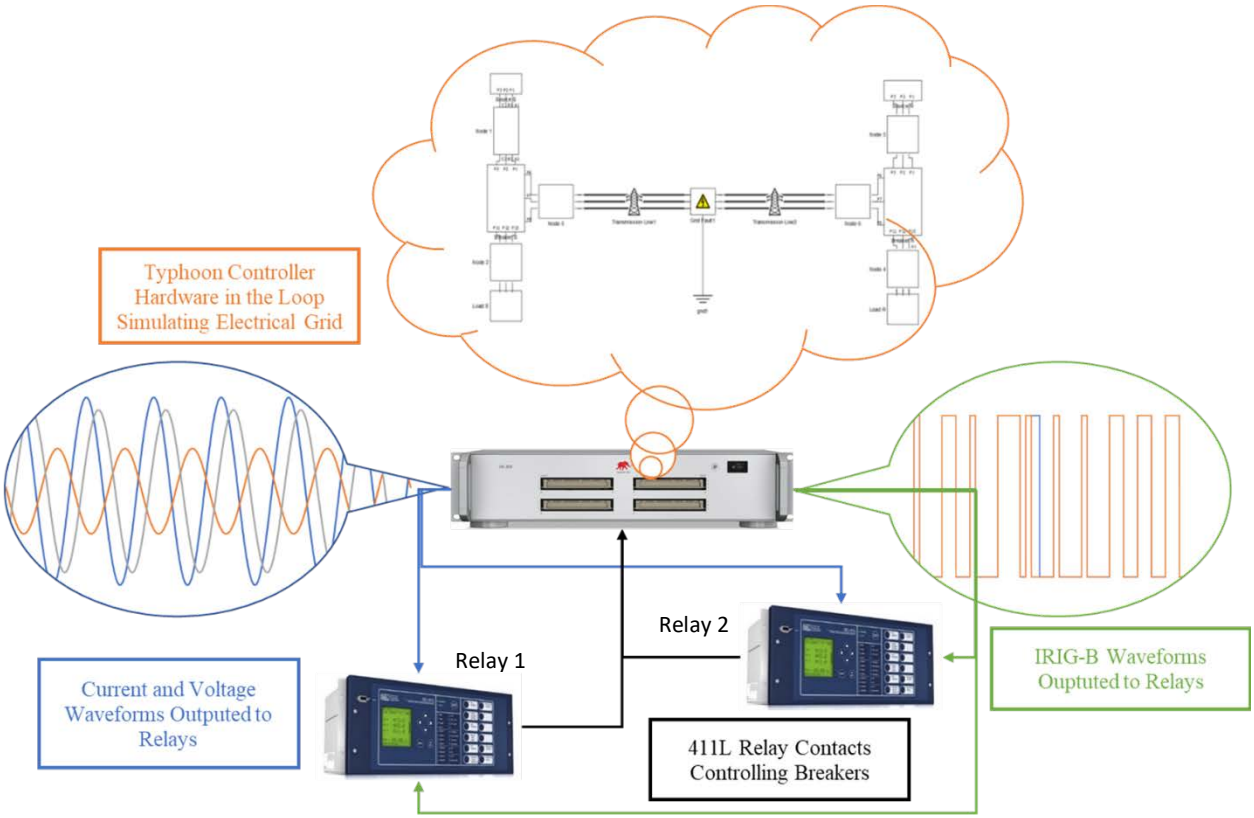

Figure 2: Controller Hardware in the Loop Testing Network

Results/Discussion

The goal of the CHIL testing was to determine what the vulnerabilities differential protection algorithms had in regard to GPS timing manipulation. The two relays were setup and programed to perform only 87L line differential protection and not trip for any other relaying scheme. In Typhoon a simple power system network was established with two sources, two loads and a transmission line between. The voltages and currents were fed into the low voltage testing inputs to the relay. A high accuracy IRIG-B output from Typhoon was established in both relays and then a series of faults were performed and detected by the relay only results from a phase A to ground fault are shown in Figure 3. This allows for a better look at the fault current as there is only one phase. It can be seen that the two currents are equivalent and opposite in polarity as the fault is located in the middle of the line and the impedance is equivalent. The red wave form in Relay 1 The time to clear the fault is 54 ms about 3.3 cycles, and the time to detect the fault was 25 ms about 1.5 cycles. This verifies that the differential protection algorithm is working and functioning properly.

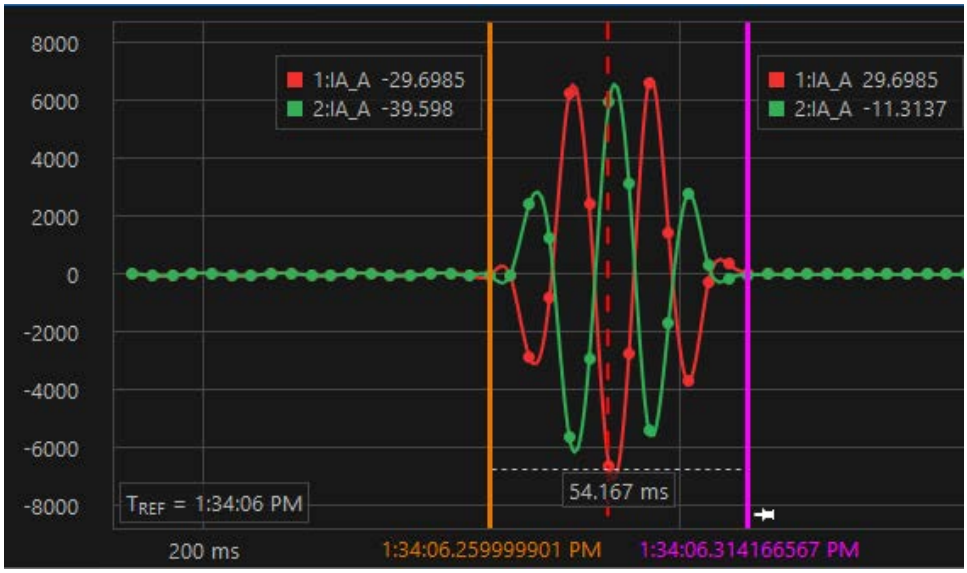

Figure 3: Relay 1 & 2 Current for Phase A to Ground Fault without 1ms Time Spoof

Then a 1ms delay is placed on relay 1's IRIG-B signal. The timing maintained a high quality IRIG-B suitable for PMU timing. Then a series of faults were performed on the CHIL testbed. The following will present the phase A to ground fault to show a comparison to the baseline presented with no time shift. Figure 4 shows the fault current for both Relay 1 (blue) and Relay 2 (yellow). It can be seen that the waveforms no longer are inverse images of each other, and Relay 1 current is shifted from Relay 2s. However, the relays still operate and perform their required tripping functions. It just takes longer for the relays to clear the fault.

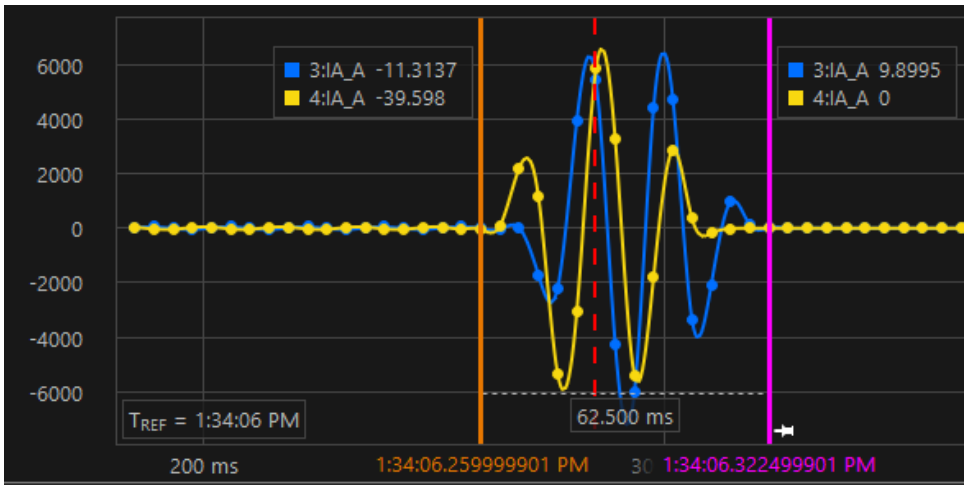

Figure 4: Relay 1 & 2 Currents for Phase A to Ground Fault with 1ms Time Spoof

The reason why the differential relay algorithm still operated with the mismatched currents is because the Relay 1 was configured to be a slave to Relay 2 in reference to timing. Therefore, the relay still recorded all data with its time stamp but the logic to trip required a second communication or ping pong between Relay 1 and Relay 2 before Relay one could make the trip decision. Therefore, there was a delay

in tripping for Relay 1 by 8 µs. This can be seen in Figure 5 where the differential trip bits are shown for the relays: red is Relay 1 with no time change, green is Relay 2 with no time change, blue is relay 1 with 1ms time change, and yellow is Relay 2 with 1ms time change. Anything greater that 1 ms would cause the relay to fall back onto its internal clock and disregard the time source as legitimate. This results in the differential protection function being resilient to GPS and timing manipulation when utilizing a direct fiber connection and configured properly to perform a ping pong verification of the timestamp with one relay as a slave and other as the master.

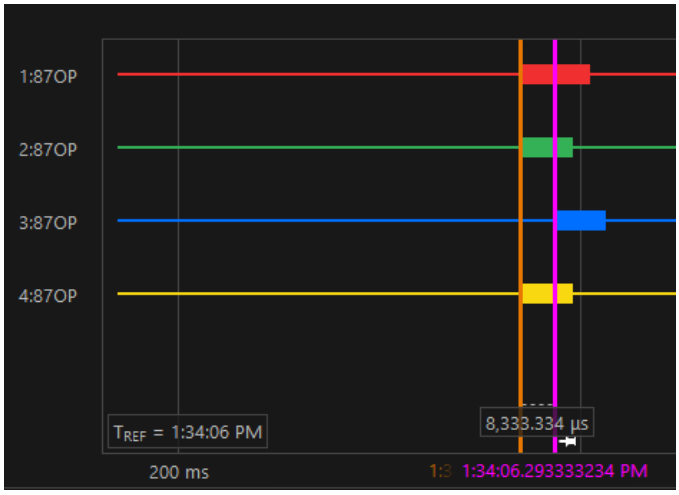

Figure 5: Differential Current Trip Signal

FY2020 Accomplishments

- ✓ Implemented and tested a GPS resilient architecture for differential protective relays through a direct serial fiber connection between the two relays.
- ✓ Received $350k for implementing a PTP timing signal with the protective relays from Office of Electricity
- ✓ Established a relay experimental test bed to function test relays with controllable voltage and current outputs, timing signals, and breaker inputs
- ✓ Developing Journal Publication on Results

Future Directions

SRNL will next be testing the latest type of relay produced the time domain protection relay. This system makes claims of being able to locate the fault to the tower and detect a fault within 1 microsecond. About 30 times faster than line differential protection relays could.

FY 2020 Peer-reviewed/Non-peer reviewed Publications

1. In progress

Presentations

None

Works Cited

[1] S. Ward, J. O'Brien, B. Beresh, G. Benmouyal, D. Holstein, J. Tengdin, K. Fodero, M. Simon, M. Carden, M. Yalla, T. Tibbals, V. Skendzic, S. Mix, R. Young, T. Sidhu, S. Klein and J. Weiss, "Cyber Security Issues for Protective Relays," GE Grid Solutions.

[2] S. East, J. Butts, M. Pap and S. Shenoi, "A Taxonomy of Attacks on the DNP3 Protocol," in *International Federation for Information Processing*, 2009.

[3] M. Gadelha da Silveira and P. Henrique Franco, "IEC 61850 Network Cybersecurity: Mitigating GOOSE Message Vulnerabilities," in *6th Annual PAC World Americas Conference*, Raleighm North Carolina, 2019.

Acronyms

- CHIL – Controller Hardware in the Loop
- DNP3 – Distribution Network Protocol 3
- GOOSE – Generic Object-Oriented Substation Event
- GPS – Global Positioning System
- ICS – Industrial Control System
- IEC – International Electrotechnical Commission
- IED – Intelligent Electronic Device
- IRIG-B – Inter-range Instrumentation Group-B
- MMS – Manufacturing Message Specification
- RTU – Remote Terminal Units
- SCADA – Supervisory Control and Data Acquisition
- SCIIC – SRNL Critical Infrastructure, ICS, and Cybersecurity
- SMV – Sample Measured Value
- TCP/IP – Transmission Control Protocol/Internet Protocol

Intellectual Property

- None

Total Number of Post-Doctoral Researchers

- None

Total Number of Student Researchers

- None

External Collaborators (Universities, etc.)

- None