Contract No:

This document was prepared in conjunction with work accomplished under Contract No. 89303321CEM000080 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

Klaehn Burkes
Cybersecurity and Threat Assessments
Savannah River National Laboratory
Aiken, SC 29808, USA
klaehn.burkes@srnl.doe.gov

Ian Webb
A-3 Technology Applications
Los Alamos National Laboratory
Los Alamos, NM 87545, USA

***Abstract*—This paper discusses the work performed to test and evaluate the effect of GPS manipulation on protective relay algorithms which require precision clocks to operate. Specifically, two algorithms were tested: line differential protection and traveling wave line protection. Controller hardware in the loop test networks were set up utilizing RTDS and Typhoon HIL hardware. For the line differential protection test, Typhoon simulated both the grid and the spoofed GPS signals. For the traveling wave protection test, a grid was modeled using an RTDS and a Typhoon HIL system simulated the spoofed GPS signals. GPS was spoofed to a single relay and a fault on the protected line was applied. Each relay was able to identify that a fault occurred and tripped their breakers because in each scenario one of the relays were configured as a slave relay. However, the time differences between the spoofed signal and the non-spoofed signal were evident and identified in the event reports. This shows that with a secure and proper configuration, GPS spoofing does not compromise the capabilities of these relay algorithms.**

***Index Terms*—GPS, GNSS, Protective Relays, IRIG-B, RTDS, Typhoon, RSCAD, Differential Protection, Traveling Wave Protection**

I. Introduction

This work was supported by the Laboratory Directed Research and Development (LDRD) program within the Savannah River National Laboratory (SRNL). This document was prepared in conjunction with work accomplished within the U.S. Department of Energy (DOE) Office of Environmental Management (EM)

The electrical power grid is the largest industrial control system in the country that interconnects every single industry within the U.S. It is composed of three distinct systems: generation, transmission, and distribution. This consists of over 20,000 generators, 642,000 miles of high voltage transmission lines, 6.3 million distribution lines, and serves 150 million customers [1]. The transmission system acts as the backbone of the electric power grid, transmitting electricity generated at large power plants down to the residential and commercial customers. Within the transmission network there are over 55,000 substations that are interconnection points between generation, transmission, distribution, and end users. Figure 1. These substations provide redundancy in flow paths, reliability in fault protection, and efficiency in voltage transformation. Within a substation are programable logic controllers (PLCs) and intelligent electronic devices (IEDs) that allow for advanced control. These devices offer logging, event reporting, and a snapshot of the conditions in the grid back to the Supervisory Control and Data Acquisition (SCADA) system in a central control center.

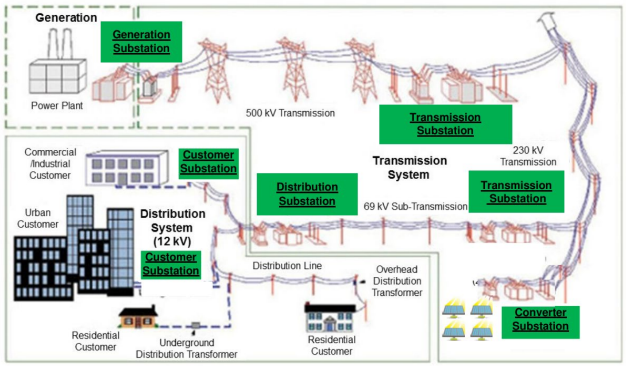

Figure 1: Different Types of Substations found in an Electric Power System [2]

Generally, most substations are geographically separated, but new control algorithms, phasor measurement units, wide area protection algorithms and new research are requiring accurate synchronization between distributed substations to allow for new functionalities, new topologies, enhanced power flow and voltage control. Therefore, accurate timing has become a focus to synchronize the electrical grid due to the geographically dispersed nature of power. Being that most substations are geographically remote, they often lack network connectivity, meaning that GPS has become the standard time source for substations. Thus, most substations are equipped with a satellite-synchronized network clock that receives global navigation satellite system (GNSS) time signals and distributes precise time via multiple output time codes: inter-range instrumentation group (IRIG-B), precision time protocol (PTP), and network time protocol (NTP).

II. Precision Timing in Protective Relays

With precision time being provided at each substation by time clocks, more advanced protective relaying algorithms can be developed taking advantage of nano-second time synchronization over geographically large distances such as between transmission lines. From this, differential protection and the new traveling wave protection were developed. Each of these requires a highly accurate IRIG input for the protection to be initiated. In the next sections both protection algorithms will be explained and the IRIG waveform described.

A. Line Differential Relay

The differential relay operates on the premise of comparing two different measured quantities from two physically separate ends of a device. For example, under steady-state operating conditions the current measured at opposite ends of a short transmission line will be the same in magnitude and phase, hence the relay does not close. However, a fault may occur on the protected transmission line and the current from either side of the transmission line is not the same, hence the breaker will trip the line out of service. This type of protection requires that both relays are in constant contact with high-speed communication because the response time required to clear a fault to maintain grid stability must be sub-millisecond. This constant high-speed high-quality communication is costly to implement for long stretches of transmission line but is still used for sensitive systems. This type of relay is widely used for transmission lines but is also used for distribution level voltages in devices such as substation bus bars, transformers, and large industrial motors. An example of differential line protection is shown below in Figure 2, protecting the line in between both relays and displaying the communication line.

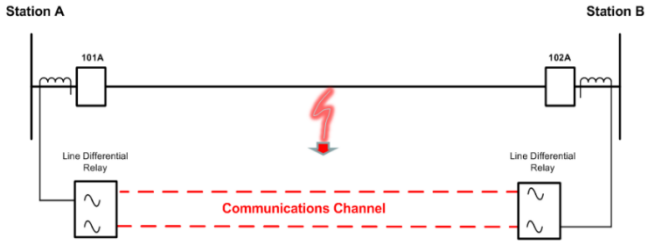

Figure 2: Line Differential Protection Traveling Wave [5]

B. Traveling Wave Relay

The traveling wave relay is an advanced technology that has, until recently, not been as widely used in the protection industry. When a fault occurs on a power line, a temporary pulse or step change in voltage and current is created and travels along the line in both directions from the point of origin. One method of detecting and determining fault location utilizes precise measurement equipment that calculates the difference of the traveling waves measured at each end of a line and can then determine the precise location to the tower of where the fault occurred. [6] [7] Modern traveling wave (TW) fault locators use a common time reference for the calculation of the location of the TW. The TW receive time is recorded and exchanged between the TW relays devices using a high-speed communication transmission medium (often fiber optic cabling), which is then used to calculate the location of the fault. Figure 3 shows the measurement at 2 ends of the transmission line where current magnitude is inverse on the different ends.

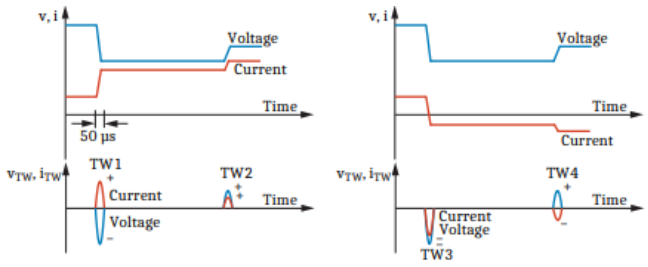

Figure 3: Traveling Wave Protection [8]

C. IRIG-B Timecode

The IRIG timecodes, version B demodulated specifically, is the most utilized method for delivering accurate time communication down to ±500ns for the electrical grid. The timecode was developed by the US military in the 1960's and has many variations based on rate. [9] This time code provides a 1 second pule train of 100 bits per frame where a position bit every 10 Hz provides 10 sections of 9 bits of data, providing seconds, minutes, hours, days, years, and control functions. An example of an IRIG train is show in Figure 4.

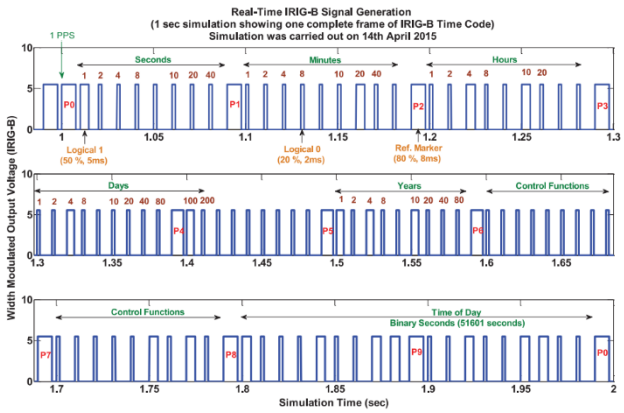

Figure 4. IRIG-B Signal Generation [10] [11] [12]

The IRIG time code is preferred within an industrial control environment because it is an analog signal that does not present added cyber security vulnerabilities in networks, unlike IEEE-1588/PTP or NTP. Further, most substations within the electric power grid are in remote locations, typically communicating back through cellular, or satellite communications. These wireless communications methods do not provide direct network connections and can reduce the accuracy of network-based timing. Most installations have local GPS clocks installed that provide a stratum 1 time server to output to the protective relays and controllers. This allows for improved accuracy at the edge of the grid, but also relies heavily on GPS to be present and reliable.

III. Test Setups for GPS CHIL

A. Differential Protection Approach

The approach taken for implementing and testing differential protection algorithms reliance on GPS was 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 a variety of protective relays. This allows for the execution of multiple scenarios to get repeatable, controlled results. To implement GPS spoofing on protective relays the Typhoon platform was used to emulate the electric power grid, outputting waveforms of voltage and current to the protective relays. The Typhoon was also used to both calculate and output IRIG-B timing signals to the relays via digital outputs, [8] [9] [10], as well as take contactor digital 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 allowed for implementing and testing multiple differential protection topologies, examining their vulnerabilities to GPS time walk off. Figure 5 shows a diagram of the differential CHIL test setup.

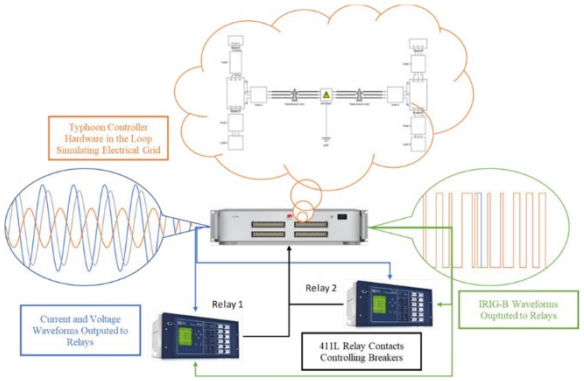

Figure 5. Line Differential Protection CHIL Diagram

The goal of the differential CHIL testing was to determine what the vulnerabilities differential protection algorithms had in regard to GPS timing manipulation. The two relays were 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 current measurement signals from the Typhoon were fed into the low voltage testing inputs to the relay. A high accuracy IRIG-B output from Typhoon was integrated into both relays and then a series of faults were performed, with the IRIG signal being spoofed in one of the relays.

B. Traveling Wave Approach

The approach for implementing and testing the traveling wave protection scheme's dependance on GPS was through a very similar CHIL test bed. However, the electrical grid simulations were produced via the software RSCAD, [13] [14] running on an RTDS Novacor stack. The RSCAD software recently added traveling wave components to its library to allow for precise emulation of an electrical power grid physics that can output current waveforms consistent with the traveling wave simulation. These outputs would be passed at a low signal level to the protective relay, which would interpret the signals to correspond to a "real" power system scenario via appropriate gain settings. The simulation used in this set of experiments consisted of varying lengths of transmission line between two simulated power generation plants, with the protective relays virtually placed at either end of a 100 mile transmission line between the generation plants, as shown in Figure 6. RSCAD/RTDS additionally utilized digital inputs from the protective relays to take contactor inputs to control the virtual breakers within the simulation.

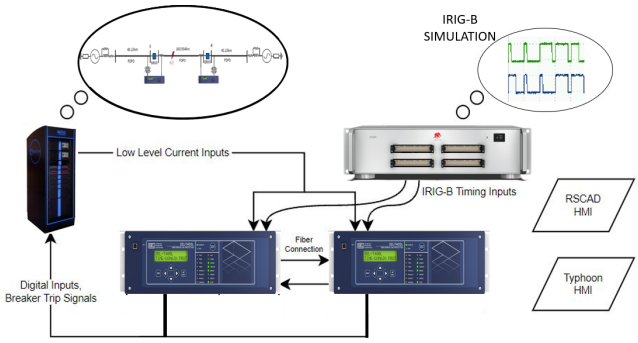

Figure 6. Traveling Wave CHIL Setup

Similar to the differential protection scheme experiments, the Typhoon system simulated IRIG-B time code outputs to supply to the protective relays. Typhoon then added time delay to one time code to simulate a GPS signal manipulation. This simulates the effect of a threat actor spoofing GPS locally at a substation miles away from the other substation and slowly walking off the time.

IV. Results from GPS CHIL Testing

The overall results from the two tests were very promising and showed how the protective algorithms would respond in a resilient manner to a real GPS attack. Both protective relays' 87L (differential) and TW87 (traveling wave) functions detected the fault applied to the line and operated the breaker within the programmed time. However, during the analysis of the event files the time shift was detected in the waveforms. The next two sections will describe the results from both sets of experiments.

A. Differential Protection Results

For the line differential protection testing, a phase-to-ground fault was applied on the line without any GPS spoofing being applied to the test network. Both relays 87L logic tripped on the fault and cleared the breaker. The event file's fault current wave forms from a phase A to ground fault are shown in Figure 7.

Figure 7. Line Differential Fault Current

The single phase-to-ground fault allows for a clearer look at the fault current as there is not another phase's fault current to consider. 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 time to clear the fault is 54 ms or about 3.3 cycles, and the time to detect the fault was 25 ms or about 1.5 cycles. This verifies that the differential protection algorithm is working and functioning properly.

After the control experiment was performed, a 1ms delay was placed on Relay 1's IRIG-B signal. The timing source (Typhoon HIL) 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-to-ground fault to show a comparison to the baseline presented with no time shift. Figure 8 shows the fault current for both Relay 1 (blue) and Relay 2 (yellow). The waveforms no longer are inverse images of each other, and Relay 1 current is shifted from Relay 2's. However, both relays continue to operate and perform their required tripping functions, it just takes longer for the relays to clear the fault.

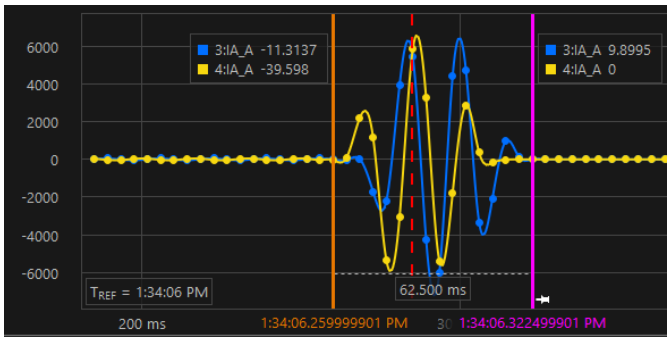

Figure 8. Line Differental Fault Current with GPS Shift

The reason why the differential relay algorithm still operated with the mismatched currents is because the Relay 1 was configured to be a timing-slave to Relay 2. Both relays still recorded all data with their respective time stamp, but the logic to trip required a second communication or ping-pong between Relay 1 and Relay 2 before Relay 1 could make the trip decision. Therefore, there was a delay in tripping for relay 1 by 8.33 ms. This can be seen in Figure 9, 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 1 ms time change, and yellow is relay 2 with 1 ms time change. The trip differential is 8.33 ms.

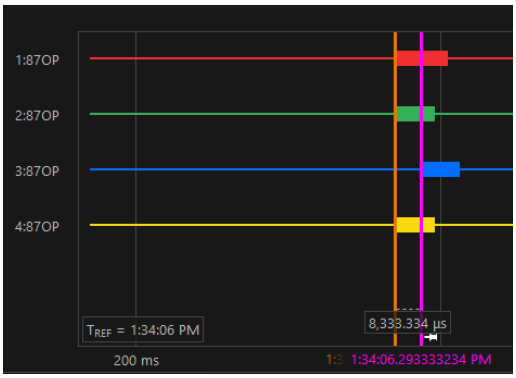

Figure 9. Line Differential Trip Logic Comparison

B. *Traveling Wave Protection Results*

For the traveling wave testing a phase-to-ground fault was applied to the line without GPS spoofing. This fault was not applied at the middle of the line to see the effectiveness of the traveling wave detection. In this instance, the traveling wave at each location are not proportionally inverse- but rather based on transmission line impedance. In this test, Relay 2 had the simulated spoofed GPS and is represented by the green and yellow waveforms. The red and blue waveforms are Relay 1 and can be seen in Figure 10 that they match under repeated fault scenarios.

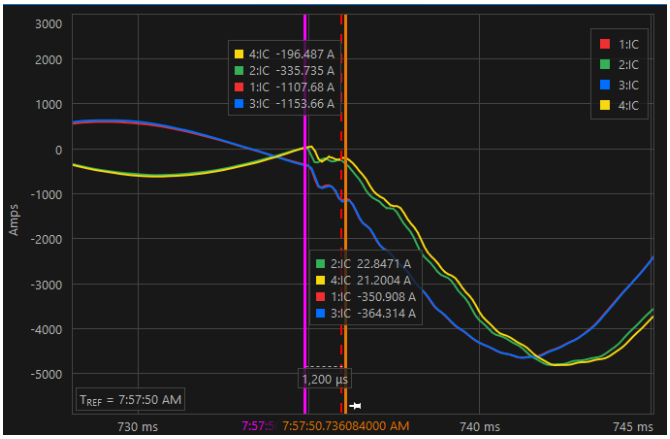

Figure 10. Traveling Wave Fault Waveforms

The yellow and green waveforms represent Relay 2 with and without the spoofing. Both waveforms have similar shapes and if their trip signals were alined they would be identical. However, there is a small delay can be seen on the yellow waveform. This is attributed to the GPS spoofing. There is a much less identifiable delta between the waveforms compared to the with the traveling wave. These relays were only configured with TW87 trip logic and both relays tripped on the fault and cleared the falt just the same as the line differential. This, as before with the differential, is because of the timing master-slave configuration in the relays. However, there was a delay in the trip logic, where relay 2 is delayed by 100 µs when GPS was spoofed as compared to when not spoofed. This can be seen in Figure 11

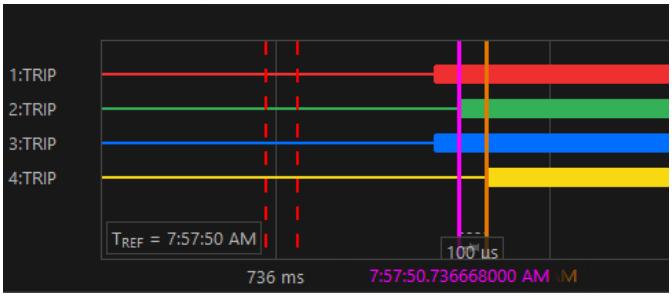

Figure 11. Traveling Wave Trip Logic

V. CONCLUSION

The results from this research show that with a secure configuration, both line differential and traveling wave protection algorithms can still operate in the presence of a fault- even under GPS spoofing attacks. Both relays tripped due to the

fault for the 87L and TW87 protection and operated the breaker to clear the fault. The line differential took much longer to clear the fault than the traveling wave but that is inherent to the nature of the two protection algorithms. However, with GPS spoofing, the line differential trip delta was 8ms versus the 100µs traveling wave delta. These deltas did not cause substantially longer clearing of the fault current and were only detectable in the event files. These would be detected by an Engineer if reviewing the fault information but did not cause the relay to trip, keeping the true functionality of the relay operational. The reason for testing just the 1 ms time delta is that anything larger would cause the GPS clock to fall back onto its internal clock and disregard the time source as legitimate, thus, the 87L and TW87 protective elements would be disabled. This results in the differential and traveling wave 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.

REFERENCES

[1] U.S. Department of Energy, "Electricity baseline report for the US power system," 2016.

[2] Transformer Resilience and Advanced Components Program, "Solid State Power Substation Technology Roadmap," U.S. DOE Office of Electricity, Washington DC, 2020.

[3] testguy.net, "Electrical Device Numbers ANSI/IEEE," testguy.net, [Online]. Available: https://testguy.net/content/148-ANSI-IEEE-Device-Numbers#ansiprint. [Accessed 3 March 2020].

[4] K. Damron and B. Andrews, *DISTRIBUTION PROTECTION OVERVIEW,* Pullman, Washington: Avista Utilities, 2017.

[5] "SEL-411L advanced line differential protection online: www.selinc.com".

[6] E. O. Schweitzer, B. Kasztenny, A. Guzman, V. Skendzic and M. Mynam, "Speed of line protection -can we break free of phasor limitations?," in *2015 68th Annual Conference for Protective Relay Engineers*, College Station, TX, USA, 2015.

[7] E. O. Schweitzer, A. Guzman, M. V. Mynam, V. Skendzic, B. Kasztenny and S. Marx, "Locating faults by the traveling waves they launch," in *2014 67th Annual Conference for Protective Relay Engineers*, College Station, TX, USA, 2014.

[8] "SEL-T400L time-domain line protection online: www.selinc.com".

[9] Timing Committee: Telecommunications and Timing Group, "IRIG Serial Time Code Formates," Range Commanders Council, U.S. Army White Sands Missle Range, New Mexico, 2016.

[10] M. S. Almas, L. Vanfretti, R. S. Singh and G. M. Jonsdottir, "Vulnerability of Synchrophasor-based WAMPAC Applications' to Time Synchronization Spoofing," *IEEE Transactions on Smart Grid,* vol. 9, no. 5, pp. 4601-4612, 2017.

[11] R. Singh, H. Hooshyar and L. Vanfretti, "Laboratory test set-up for the assessment of PMU time synchronization," in *2015 IEEE Endhoven PowerTech*, Endhoven, Netherlands, 2015.

[12] R. Singh, H. Hooshyar and L. Vanfretti, "Assessment of time synchronization requirements for Phasor Measurement Units," in *2015 IEEE Endhoven PowerTech*, Endhoven, Netherlands, 2015.

[13] R. Mirzahosseini, Y. Chen, Y. Zhang and R. Kuffel, "Closed-Loop Traveling-Wave Relay Testing (TWRT) using RTDS Real-TIme Simulators," in *2019 IEEE 8th International Conference on Advanced Power System Automation and Protection (APAP)*, Xi'an, China, 2019.

[14] R. Mirzahosseini, R. Iravani and Y. Zhang, "An FPGA-based Digital Real-Time Simulator for Hardware-In-The-Loop Testing of Traveling-Wave Relays," *IEEE Transactions on Power Delivery,* vol. 35, no. 6, pp. 2621-2629, Dec. 2020.

[15] 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.

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

[17] M. Silveria and P. Franco, "IEC 61850 Network Cybersecurity: Mitigating GOOSE Message Vulnerabilities," in *6th Annual PAC World Americas Conference*, Raleigh, North Carolina, 2019.