Testbed for Timing Intrusion Evaluation and Tools for Lab and Field Testing of Synchrophasor System

Mladen Kezunovic[1], *Life Fellow, IEEE*, Cheng Qian[1], *Graduate Student Member*, *IEEE*,
Christoph Seidl[1], *Student Member*, *IEEE*, Jinfeng Ren[2], *Member*, *IEEE*

[1] Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX, USA
[2] Corporate Business Services, Entergy, The Woodlands, TX, USA

***Abstract*—Currently, there are over 2500 phasor measurement units (PMUs) installed in the East, West, and Texas interconnections in the USA, enabling wide-area situational awareness. One of the major concerns in industry is the susceptibility of synchrophasor systems to timing intrusion (TI) attacks. As examples, such TIs may result from compromised timing signal received from Global Positioning System (GPS), malicious attacks associated with the time stamp assigned to the PMU streaming values, or induced latency or other disruptions in the transmission of synchrophasor frames. TI attacks may invalidate measurements of key electrical quantities, and may consequently incapacitate vital control functions. In order to provide a solution to TI detection and mitigation, a TI management testbed is implemented to evaluate the resilience of synchrophasor systems against TI attacks. The functional specifications, implementation details of the TI evaluation testbed, as well as associated testing tools are introduced and discussed. Initial test use cases are defined, the results are presented, and future developments are outlined.**

***Index Terms*—Cyber-physical system, cybersecurity, smart grid, synchrophasor, timing intrusion**

I. INTRODUCTION

The analysis of the causes of the North America blackout on August 14, 2003 has exposed that legacy Energy Management System (EMS) design is inadequate for tracking extreme dynamic events causing major blackouts in the power system [1]. This inadequacy is due to the lack of precise time-synchronization among SCADA measurements, and low scan rate, which together failed to offer effective representation of fast evolving dynamics in the grid. As a result, synchrophasor system technology was introduced for wide area monitoring, protection, and control (WAMPAC) applications. The synchrophasor systems are deployed to supplement EMS at nearly all Independent System Operators (ISOs)/Regional Transmission Organizations (RTOs), and many Transmission Owners (TOs) in the US [2]-[4]. The prominent use of synchrophasor technologies is also evident worldwide in China, and Europe with ambitious deployment plans in India and Brazil [5]-[10].

The synchrophasor system is capable of GPS-time synchronized waveform sampling and calculation of phasor parameters [11]-[13], which enable synchrophasor system to provide a high-fidelity, high-resolution, and real-time reflection of power system operating conditions. A large variety of control applications may benefit from synchrophasor system [14]-[17]. Therefore, the advantage of synchrophasor system over SCADA system substantially depends on the reliable provision of high-precision GPS timing information.

As a cyber-physical system, synchrophasor system is susceptible to TI attacks. Starting from the GPS clock receivers, the timing information in synchrophasor system is transmitted together with phasor parameters in an encapsulated data stream [11],[12] generated by each phasor measurement unit (PMU), or PMU-enabled device such as relays or fault recorders. Timing information is then collected by phasor data concentrators (PDCs), and eventually utilized by end-use synchrophasor applications, as needed. Along this path from the clock receivers and individual PMU to PDCs and end-use application, TI attacks may target the nodes (e.g. GPS receivers, PMUs, PDCs), and/or the links connecting the nodes (e.g. communication channels.

Prior work aims to evaluate the impact of TI attacks on individual component in the aforementioned path of synchrophasor streams. Paper [18] evaluates the impact of instrument transformers on PMU end-to-end testing. Papers [19]-[21] evaluate the impact of TI attacks on GPS clocks. Reference [22] discusses the timing attacks on PMUs, PDCs, and communication links. The aforementioned work focuses on the evaluation of TI attack on individual components. The TI attacks in a synchrophasor system should be detected and located for any other field evaluation strategies can be deployed, and comprehensive approach to TI attack detection and location functionality is missing in prior work.

Moreover, studies have shown that synchrophasor applications can be affected by TI attacks, and the sensitivity of an application under TI attack varies. For example, paper [23] illustrated how undetected TI attacks may adversely affect linear state estimation application. Reference [24] demonstrat-

978-1-7281-1607-5/19/$31.00 ©2019 IEEE

ed how synchrophasor-based applications can be impaired by GPS spoofing, and this is done by comparing the outcomes of the same synchrophasor application running on two streams of synchrophasors, one from a commercial PMU with reference timing input, and the other one from a commercial PMU with spoofed timing input. This approach assumes that commercial PMU output can be used as the synchrophasor reference. However, despite provision of TI-immune timing input, the quality of commercial PMU output cannot be guaranteed especially when the PMU is subject to non-standardized waveforms from the real power system.

In summary, regardless of various tools and synchrophasor testbeds that are developed so far [25]-[27], comprehensive methodologies for TI attack detection and assessment of the impact on end-to-end synchrophasor system and applications are not readily available. To fill this gap, the work described in this paper offers several benefits. The contribution of this paper are related to the development of a novel testbed setup. In addition, methodologies, testing tools, and test plans for detecting TI attacks on synchrophasor system nodes and links, and evaluating the impact on end-use synchrophasor applications as the faulty timing propagates through the entire system are implemented and utilized.

The rest of the paper is organized as follows: Section II discusses the test methodologies and the TI evaluation testbed features. The nested testing strategy is proposed to locate TI attacks and assess their impacts on synchrophasor applications. The necessary components, including hardware, software, and protocols for the TI evaluation are introduced in Section III. Section IV offers results of initial TI resilience evaluation, including the metrics and use cases. Section V outlines conclusions.

II. Test Methodology for Detecting TI Attacks and Evaluating their Impacts

A. Timing Intrusion Definitions

Timing intrusion refers to the situations where one or more of the timing requirements in a synchrophasor system are violated. Compromised timing information can be intentionally exploited, putting the synchrophasor system and application integrity at risk. Malicious attacks on timing information paths, as well as other types of cyber-attacks, may be aimed to disrupt, destroy, and shut down the power system. The TI attacks may be initiated through GPS spoofing, breaching into secure network by lures (e.g. spam emails) to install Trojan horses, malware, etc. An example of a sophisticated malintended intrusion is the 2015 cyber-attack on the Ukrainian power grid [28].

The TI attack surfaces consist of the components of the infrastructure nodes (devices) and links (communication channels between nodes). The two locations most vulnerable to TI attack are the substation and control center. At each location, there are different nodes and links open to a TI attack. In a substation, there are GPS clock receivers, PMUs, PDCs, and network hardware, and in a control center, there may also be GPS clock receivers, PDC, and front-end processor, as well as applications.

TI attacks may be carried out by numerous methods including blocking/spoofing/meaconing GPS clock signal, falsifying timestamps, altering the synchrophasor streams, injecting junk packet or delaying original packets, and so on. Figure 1 illustrates TI attack surfaces and some attack vectors in synchrophasor nodes and links.

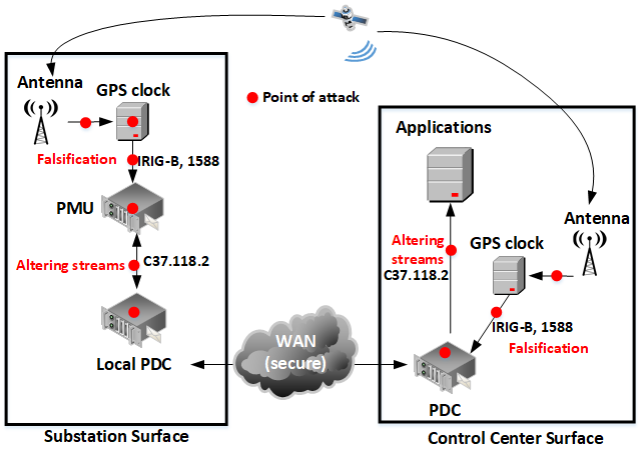

Figure 1. TI Attacks on synchrohpasor nodes and links

The resilience of a synchrophasor system should be evaluated end-to-end, starting from individual GPS clock receivers and PMUs, through the synchrophasor streaming network, to PDCs, all the way to the end-use applications. If any component in this end-to-end chain is susceptible to TI attacks, the synchrophasor system's trustworthiness should be deemed ineffective. The contribution of this paper is in describing developed testbed features and methods for detecting and evaluating the impact of TI in both laboratory and field environment.

B. TI Intrusion Detection and Evaluation Procedure

A hierarchical description of the proposed TI detection and evaluation methodology is illustrated in Figure 2. The details of each block will be discussed in the corresponding subsections.

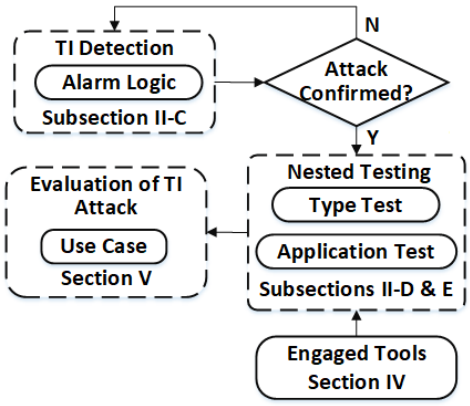

Figure 2. Schematic of proposed methodology for TI detection and evaluation

C. TI Detection and Confirmation

The synchrophasor measurements collected from the outputs of GPS clock receivers and PMUs/PDCs under test in a substation and/or in a control center are assessed by comparing them with outputs from the reference PMU/PDC tools that are installed temporarily or permanently at a given substation

for evaluation purposes. Their timing source is provided by a separate timing module capable of detecting GPS intrusions as well as creating an accurate holdover and is therefore considered free from attack. This timing module is also being developed as part of the same project and is described in a companion paper [29]. The reference PMU, also called "Gold PMU" is developed using specialized synchrophasor algorithms [30]-[35], and reference communication protocol model is also developed for the most common communication protocols. The reference PDC is implemented using a commercial PDC with a reference timing module which is capable of detecting and mitigating TI attacks and provides uncompromised time-reference to the PDC.

Figure 3 shows a simplified view of the lab test system which is an exact replica of the production system running in parallel with the reference system. When irregularities are detected, the test system is switched to the troubleshooting stage, in which a portable test set is used to replay known voltage and current waveforms to locate the discrepancy by performing nested end-to-end testing.

In normal operation, the reference timing source, reference PMU, reference communication protocol model, reference PDC and reference application, as well as the associated comparison and alarming software are running in parallel with the production system by monitoring in real time corresponding module inputs and outputs. Alarm is generated by reference timing module when such comparison show discrepancies and TI attack is suspected. If tampered clock or timestamps are detected, they are corrected and used by reference PMU and PDC as reliable timing information.

End-to-end testing using the test set can be performed when new synchrophasor equipment is commissioned in field, or new applications are deployed in a control center. The test can also be implemented periodically, i.e. as a maintenance test, to detect any hidden anomalies, such as dormant timing intrusion. The test set is also used when the TI detection logic suspects an intrusion.

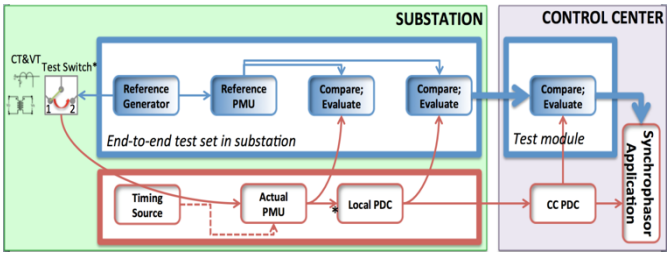

Figure 3. The use of reference tools for TI detection and confirmation

D. *Nested End-to-End Testing*

To evaluate the end-to-end integrity of a synchrophasor system, this paper introduces the concept of nested testing for synchrophasor applications. While the basic idea is somewhat trivial, the complexity of this testing methodology is in developing the detection logic for accurately evaluating all components of a system layer by layer with a top-to-bottom approach, as shown in Figure 4.

Starting with the timing clock reference, i.e. GNSS clock receiver, the span of the test loop is gradually increased to include PMUs, PDCs, communications network and finally the end-user application. We have not only developed a test strategy, but also the comparison logic, the portable test set and hardware/software reference modules, as well as a calibration laboratory to determine the impact of TI on a synchrophasor system using nested testing. The developed synchrophasor testbed used for PMU testing and calibration consists of a timing reference comparison and confirmation system, including a GPS antenna and receiver (timing reference), a signal generator, power amplifiers for grid simulator interfacing, data management and result analytics tools. The timing system provides a reference of an uncompromised GPS signal and time-code to both the calibration system and device under test. The lab setup is used to calibrate and characterize both the Field Test Set as well as some commercial PMUs and PDCs before their performance is evaluated in a field setup.

Figure 4. Nested testing strategy enabling End-to-End testing of synchrophasor system

A simplified version of the test setup is depicted in Figure 5. The Field Test Set, served as reference signal generator, provides analog waveforms corresponding to a specific test scenario to feed both the Device Under Test (DUT) and a reference PMU. As mentioned earlier, the reference PMU, termed Gold PMU described in III.B, is a phasor measurement unit providing accurate (reference) synchrophasor data by utilizing a set of reference algorithms. The data stream out of both devices are aggregated and sent to the TI detection logic software to perform the comparison. For the full extent of the nested testing scheme shown in Figure 4, test switches are included in the loop as shown in Figure 5 to allow the use of two different GPS clock inputs to each module and consecutively evaluate TI impact at the timing source. Similarly, test switches are available to choose either the field waveforms or replayed waveforms from FTS when feeding PMUs in the field. The test system also meets the requirements outlined in the IEEE Test Suite Specification (TSS) [36].

E. *Type Test vs. Application Test*

Once the possibility of TI is detected, two categories of tests are used to determine the TI impact on the system, namely type tests and application tests. Due to the time-sensitive nature of synchrophasors, it is imperative to ensure precisely timed waveform replay by the reference signal generator also called Field test Set (FTS), as well as measuring or time-stamp aligning of data by the PMU and PDC, respectively. The system can only be evaluated accurately if the timing precision of each element used for evaluation is warranted. The impact of inaccurate replay emulating the GPS clock delay in a steady state test is simulated in Figure 6 as a function of phase displacement. TVE is defined in the IEEE standard [11] as:

$$TVE(n) = \sqrt{\frac{\left(\left[\hat{X}_r(n) - X_r(n)\right]^2 + \left(\hat{X}_i(n) - X_i(n)\right]^2\right)}{\left(X_r(n)\right]^2 + \left(X_i(n)\right]^2}}$$

Where $\hat{X}_r(n)$ and $\hat{X}_i(n)$ are the sequence values estimated by the unit under test. $X_r(n)$ and $X_i(n)$ are the theoretical sequence values of the input signal at time (n).

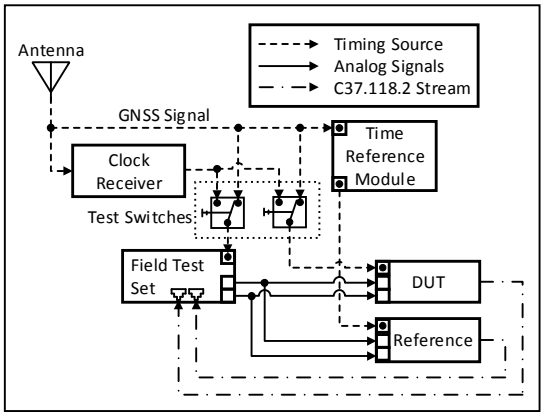

Figure 5. Simplified block diagram of test setup

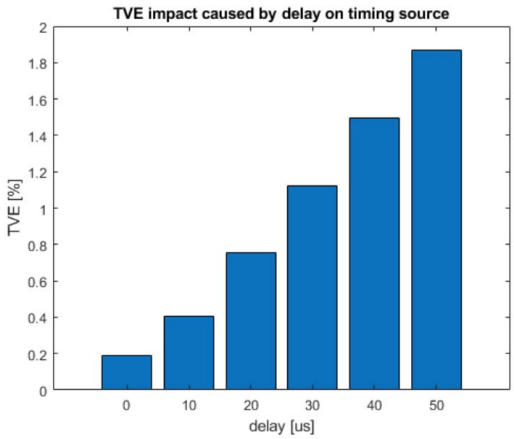

Figure 6. TVE impact caused by timing source delay

Type tests are standardized according to [11], [12] and intended to verify the quality of the internal design of a PMU. Figure 7 shows the test set connected to the synchrophasor system components being attacked. By comparing the outputs from each component with the outputs from reference GPS clock, PMU and PDC, and communication and application models the TI impact can be evaluated starting from the timing source, PMU, substation PDC, and to control center (CC) PDC and eventually the power system application at hand.

Application tests may be used for analysis of an impact on an end-user application, such as fault location [14], small signal stability [15], voltage stability [16], and model validation [17]. This form of testing is based on replaying waveforms that are either simulated or recorded and directly correspond to an event relevant for a specific application. To illustrate the test concept, we use the fault location application as an example. A known waveform from a pre-selected fault scenario is replayed to the system under test while running a fault-location application at the control center. A compromised GPS signal, or rigged timestamps in data stream will lead to an unexpected error (gross mis-location) of the fault, which can be used to evaluate how much this form of intrusion impacts the application.

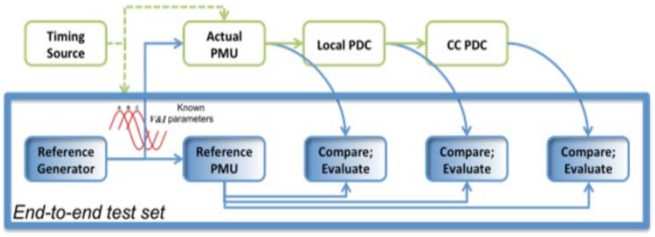

Figure 7. End-to-end testing paradigm for type test

Another benefit for this form of testing can be found in the assessment of dynamic behavior of PMUs exposed to dynamic waveforms or fault scenarios, which unlocks a whole new potential of dynamic testing capable of revealing insufficient ability of PMUs to capture complex waveform changes on much more realistic signal interaction time-scale than conventional type tests. The underlying test signals for the application tests are stored as analog waveform samples, which may capture many unfolding time domain details of measured or simulated power system conditions that can profoundly affect the phasor calculation, including DC offset subharmonic, harmonics and high frequency transients. Learning about the application performance under such dynamic conditions can help in setting the thresholds for detecting the measurement errors to help differentiate TI attacks.

III. Calibration Lab and Field Testing

The aforementioned tests can be performed on a production system in a lab as well as in the field, i.e. substation, control center or other synchrophasor test environment. The purpose of each test environment is quite different. We developed a calibration system whose function is similar to Figure 4, which has been assessed by NIST to define uncertainties needed to meet calibration standards according to the IEEE ICAP program [36]. The reference signal generator provides nominal analog test signals, which are 70V and 5A for voltage and current respectively. The main purpose of this form of testing is to evaluate the behavior of the devices under test and monitor the impact of TI for known input signals under the attack scenarios. This exposes possible device malfunctions and helps tune test parameters for the field test.

The FTS is a portable version of the calibration laboratory with additional functionality to meet the requirements imposed by tests performed in a field environment. Small power signal waveforms are used to suspend the need for amplifiers to maintain a portable design, which bypasses the auxiliary transformers and feeds directly into the PMUs secondary input. This eliminates the uncertainty introduced by the transformers and amplifiers. The basic setup of the test loop is the same as in Figure 3. The procedure is constrained by factors imposed by the uncertain nature of field measurements. As opposed to the lab, the main purpose is to detect impacts linked to TI attacks and locate the intrusion accordingly. The field equipment and the status of all its components when in-

stalled and after continued service for an extended period is usually unknown. In addition, some updates of the system may include adding new components or reconfiguring existing ones, introducing slightly different base performance. The associated standards, guides and recommendations for field-testing may also evolve. For that reason, field-testing methodology has three different steps:

- Commissioning Test: This test characterizes and calibrates an installed system with all its components to establish the reference system condition for any future TI testing. It usually consists of a full suite of type- and possibly some applications tests, and is performed in controlled non-attack environment.
- In-field Test: Also referred to as a periodic maintenance test may be performed during normal operation or periodically recurring system maintenance sessions to ensure safe and reliable operation. This test can be used to re-calibrate the system and detect any hidden anomalies, i.e. dormant timing intrusion by comparison with the commissioning test results.
- Troubleshooting Test: Being aware of a certain problem in the system either by performing an In-field test or through some TI detection approach, the test scheme and especially the replayed analog waveforms can be tailored to accurately locate the source and/or extent of a TI impact by troubleshooting the problem to determine the counter measures.

IV. Implementation of TI Management Testbed

To achieve the aforementioned functionalities of TI management testbed, TI evaluation tools including hardware modules and software packages that integrate the hardware modules are developed. They are described next.

A. Field Calibrator

The Field Calibrator uses a National Instruments CompactRIO (cRIO) 9082 with the following modules to achieve its functionalities:

- NI 9567 – GPS receiver: This card is connected to GPS antenna when using GPS/GNSS as the primary timing source.
- NI 9263×2– Analog Outputs: These cards are used for the analog waveform generation necessary to perform the different kinds of testing and can provide a small voltage signal in the range of ±10V. Sampling rate: 100KS/s/ch simultaneously, 16Bit resolution [37]
- NI 9402 – Digital In/Outputs: This card is used for synchronizing the system with an IRIG-B or 1PPS timing source. It may also be used to provide trigger signals to the system under test or forward a 1PPS signal to other modules.

The cRIO setup is packaged in a NI 9919 enclosure. The card inputs and outputs are internally connected to the back-panel of the enclosure, where all cables in the field environment, i.e. substation 19" rack, are connected to. The overall setup of the Field Calibrator hardware platform is shown in Figures 8 and Figure 9.

The Field Calibrator is uniquely designed to facilitate nested testing strategy, with GPS time-synchronization, communication with PMU/PDC, and central analysis module functionalities. These functionalities cannot be achieved by any commercial product, such as [38].

Figure 8. Field calibrator hardware setup

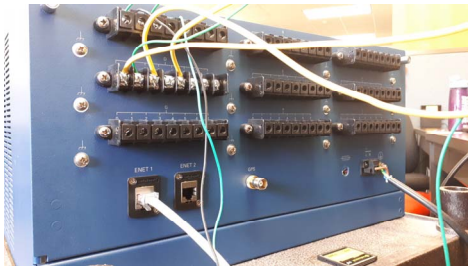

Figure 9. Field calibrator back-panel

B. Gold PMU

The reference synchrophasor stream in the test strategy is provided by a dedicated device termed Reference PMU, or Gold PMU, indicating its superior synchrophasor estimation accuracy. Gold PMU receives uncompromised timing code described in [29].

As shown in Figure 10, the Gold PMU consists of a GPS receiver, voltage/current measurement hardware modules and is empowered by high accuracy synchrophasor algorithms. Optionally, Gold PMU can be configured to accept alternative timing protocols, such as IRIG-B. The high accuracy of Gold PMU is enabled by an algorithm selection mechanism [30], allowing the most accurate algorithm associated with a particular type of input waveform to be leveraged. For each type of waveform, signal models are meticulously chosen to match the waveform, and algorithms are used or developed to achieve accurate phasor parameter calculation [31]-[35]. By doing so, reporting latency in various test conditions can be managed and minimized at the same time.

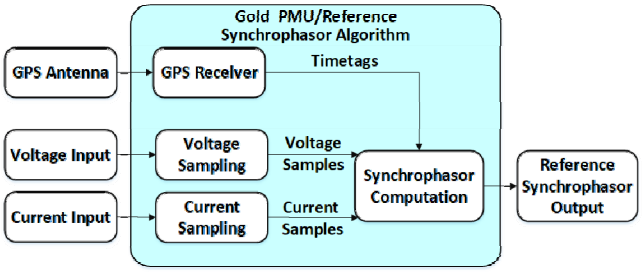

Figure 10. Structure of Gold PMU

The Gold PMU is implemented in National Instruments CompactRIO (cRIO) platform, shown in Figure 11, with removable modules achieving the aforementioned functionalities.

- Host computer/Chassis is the enclosure for computation unit, data processing center, and slots where modules can be plugged in.
- GPS card receives the raw timing code from GPS receiver, and decodes the information into 1PPS pulses and absolute timestamps. Alternatively, the GPS module can be replaced with digital I/O module if IRIG-B timecode is desired.
- Data acquisition cards samples analog voltage and current waveforms, digitize the samples, and interface with Host Computer.

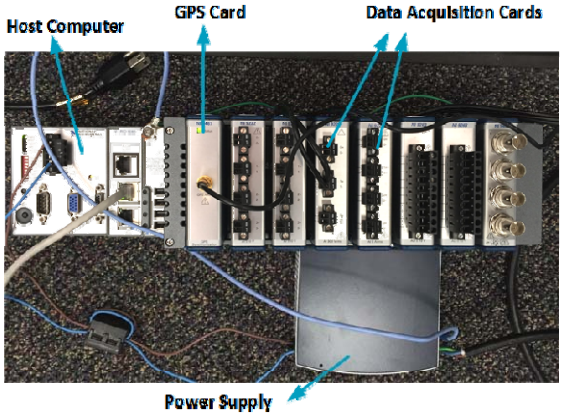

Figure 11. Gold PMU implementation

C. Integration of Field Calibrator and Gold PMU

When a possible instance of an intrusion is detected, a nested testing scheme is performed to check the accuracy of PMUs and PDCs. The field calibrator generates the test signals for both Type test and Application test that are mentioned in previous section and feeds corresponding waveforms to the PMUs under test and the Gold PMU. The accuracy indices are calculated by comparing the outputs from PMUs, and PDCs with the Gold PMU and reference PDC respectively. The implementation diagram of the field-testing scenario is shown in Figure 12. In Nested testing, the synchrophasor system components are tested layer by layer from substation PMUs to control center PDCs to accurately locate the source of errors and evaluate the impact on the synchrophasor applications.

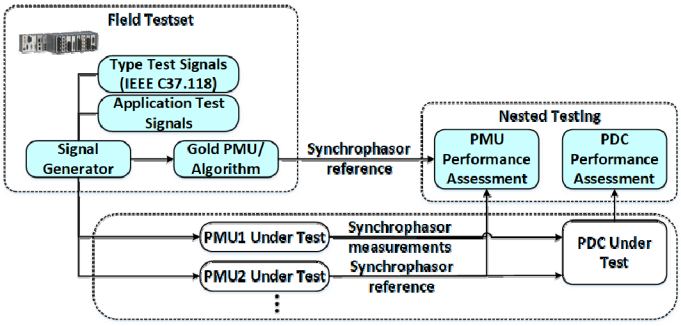

Figure 12. Synchrophasor test system instrumented with FTS and Gold PMU

V. Methodology for Evaluating Impacts of TI Attack on Synchrophasor Applications

This section introduces the metrics, lab and field use cases where the aforementioned TI attack evaluation system and strategies are deployed. The impact of TI on a synchrophasor system is evaluated using type test and application test. A fault location algorithm is selected to evaluate the impact [14]. Examples of preliminary test results are provided below.

A. Metrics for Evaluation of TI Detection Modules

The goal of the developed modules is to correctly and effectively detect timing attacks without interfering with other functionalities of the system. When a TI attack occurs, indication of the occurrence of TI attack as well as any relevant information should be provided by the testbed modules. The metrics used to evaluate the TI impacts are:

- TI detection trustworthiness. Quantified in detail by accuracy, false positive rate, and false negative rate.
- TI detection latency. Control center should be notified when the synchrophasor system is subject to timing attacks. The latency between the initiation of timing attack and attack detection should be minimized so that TI impact could be mitigated.
- TI location. The knowledge of exactly where the TI attack takes place will facilitate quicker recovery of synchrophasor system after it has been attacked.

B. Field Validation Use Case

The field validation resembles the lab validation when the performance of the system under test as well as the form of attack is unknown. The following Use Cases are defined:

- System characterization and calibration – Perform calibration testing on the system using type and application tests to characterize the systems behavior, and establish the thresholds to prevent false TI detection.
- Intrusion vs. failures in Timing Infrastructure – The TI detection modules should be able to differentiate the intrusion from failures in regular operation conditions using FTS and reference PMU as described in Section II.B.
- Integrity of Control Center Applications – Evaluate accuracy and behavior of fault location (example) application (or other corresponding events) using waveform reply testing.

C. TI Impact Evaluation Using Type and Application Test

As discussed in previous sections, TI attacks may be carried out in various forms. One of the forms may be offsetting the timestamps in synchrophasor data stream. Amplitude modulation test, which is one of the dynamic tests in IEEE Standard [11], is used as an instance to show the impact. The total vector error (TVE in %) measures the accuracy of synchrophasor calculation. Designate N_{offset} as the number of data frames being offset and F_s as the PMU data reporting rate, the time of offset is calculated as N_{offset} / F_s.

The evaluation results when offsets are 1 and 2 are given in Figure 13. Comparing to the 3% required in standard the timestamp offset introduces significant error in data accuracy. This irregularity may indicate a TI. It can be used to trigger the troubleshooting mode in nested testing as described in Section II.

A fault location (FL) method described in [14] is used to evaluate the TI impact on the application result. The FL method uses synchrophasor measurements during disturbances obtained from PMUs sparsely located in the network. A simplified power network model of Idaho Power Company

(IPC) is used to simulate the synchrophasor data during faults. The model was calibrated by comparing measurements from field recording devices to the simulated waveforms for the same event and the model was tuned to minimize any discrepancies. The measurements are obtained at Bus 1, 4 and 7. The one-line diagram is shown in Figure 14. Three-phase fault scenarios are simulated on Line 1-2 with fault distance from 0 to 99% looking from Bus 1 in increment of 1%.

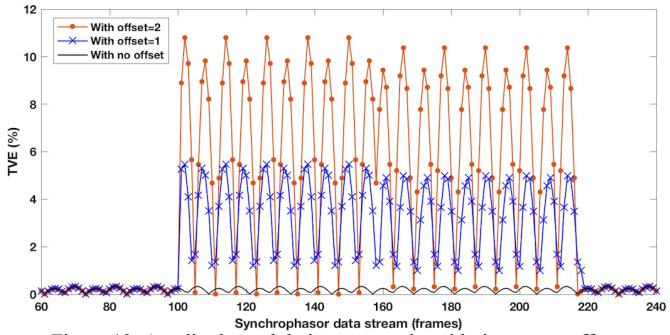

Figure 13. Amplitude modulation test results with timestamp offset

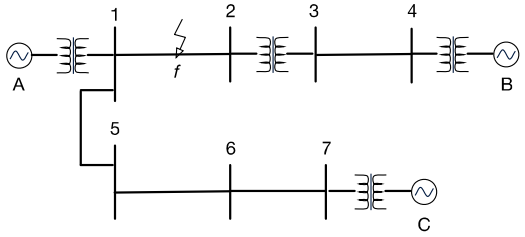

Figure 14. One-line diagram of simplified IPC system

In evaluation of the application test, timestamps in PMU data stream during faults are offset by certain amount of time to simulate a scenario of timestamp falsification. Positive and negative time offsets are planted in consecutive data frames. The impact on estimated fault location result are evaluated when N_{offset} is 5 and 10, respectively. For the report rate of 60 frames per second, the time offsets are 83 ms and 167 ms. The test results with and without TI are given in Figure 15 and 16, in which the impact is obvious. The maximum errors caused by the TI are 22% and 40% of line length. As an example, for a line of 50 miles, the error in FL result may end up to show 11 miles and 20 miles in the mentioned scenarios respectively. This also demonstrates that the proposed method for evaluating the impact of TI on applications is effective.

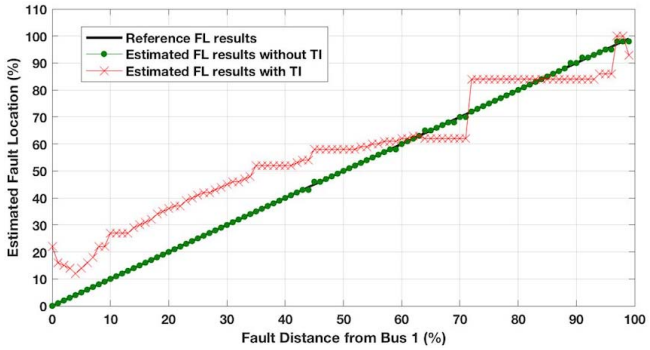

Figure 15. Estimated fault location results when N_{offset}=5

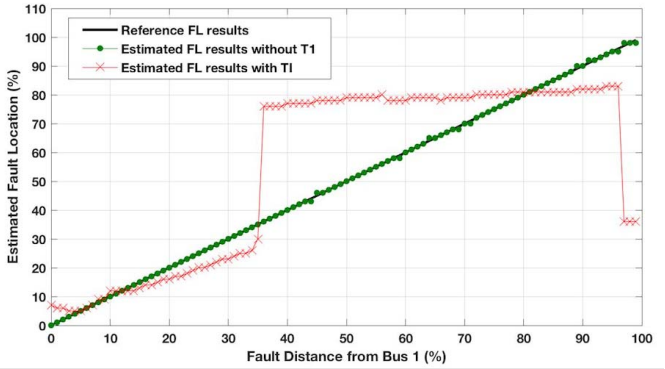

Figure 16. Estimated fault location results when N_{offset}=10

VI. CONCLUSIONS

In this paper, a testbed infrastructure to evaluate synchrophasor system resiliency against timing intrusion is introduced. Test tools for performing lab and field tests are developed and described. The contributions are summarized as follows:

- Novel timing intrusion management testbed, associated test tools and methods are developed for both lab and field environment to detect and evaluate the impact of TI.
- The impact of TI on a synchrophasor application is illustrated through a "nested testing" strategy, where the TI resiliency can be assessed at a device-by-device, layer-by-layer in the synchrophasor system hierarchy.
- In order to realize TI evaluation strategies, necessary tools and test protocols include Field End-to-End Calibrator, Gold PMU, communication protocol models, and test plans for the integral testing of synchrophasor system.
- Use cases for TI resiliency evaluation are designed for both lab and field-testing environments. The preliminary test methodology and results illustrate the use of type and application test, the efficacy of the synchrophasor testbed, and various features of the test method.

ACKNOWLEDGMENT

This work was performed under the DOE/NETL CEDS program funding of the "Timing Intrusion Management for Enhanced Resiliency-TIMER" project. The authors would like to acknowledge the collaboration with our project partners: Milorad Papic and Erik Schellenberg from Idaho Power Company (IPC), Beverly Johnson, Seemita Pal and Chris Bonebrake, from Pacific Northwest National Lab (PNNL), Iknoor Singh from Electric Power Group (EPG), and Prof. Steve Liu, Prof. Alex Sprinston and John Lusher, as well as their students from Texas A&M University.

REFERENCES

[1]. U.S.-Canada Power System Outage Task Force, "Final report on the August 14, 2003 blackout in the United States and Canada: Causes and Recommendations", April 5, 2004. [Online]. Available: http://www.nerc.com.

[2]. NASPI Control Room Solutions Task Team. Using Synchrophasor Data for Phase Angle Monitoring. [Online]. Available: https://www.naspi.org/sites/default/files/reference_documents/0.pdf?fileID=1567. May 2016.

[3]. SR Mix, H. Kirkham, A. Silverstein. Recommended Guidelines for NERC CIP Compliance for Synchrophasor Systems. [Online]. Available:https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-27062.pdf. Nov 2017.

[4]. JD Taft. Assessment of Existing Synchrophasor Networks. [Online]. Available: https://gridarchitecture.pnnl.gov/media/white papers/ Synchrophasor_net_assessment_final.pdf. Apr 2018.

[5]. Synchrophasor Applications in Transmission Systems. [Online]. Available:https://www.smartgrid.gov/recovery_act/program_impacts/applications_synchrophasor_technology.html.

[6]. A. Silverstein, J. E. Dagle, "Successes and Challenges for Synchrophasor Technology: An Update from the North American Synchro-Phasor Initiative," System Science (HICSS), 2012 45th Hawaii International Conference on, Maui, HI, 2012, pp. 2091-2095.

[7]. A. von Meier, D. Culler, A. McEachern and R. Arghandeh, "Micro-synchrophasors for distribution systems," Innovative Smart Grid Technologies Conference (ISGT), 2014 IEEE PES, Washington, DC, 2014, pp. 1-5.

[8]. M. Wache and D. C. Murray, "Application of Synchrophasor Measurements for distribution networks," Power and Energy Society General Meeting, 2011 IEEE, San Diego, CA, 2011, pp. 1-4.

[9]. M. Kezunovic, S. Meliopoulos, S. Venkatasubramanian, V. Vittal, "Application of Time-Synchronized Measurements in Power System Transmission Networks," Springer, ISBN 978-3-319-06218-1, 2014.

[10]. A. Mingotti, L. Peretto, R. Tinarelli, A. Angioni, A. Monti and F. Ponci, "Calibration of Synchronized Measurement System: from the Instrument Transformer to the PMU," 2018 IEEE 9th International Workshop on Applied Measurements for Power Systems (AMPS), Bologna, 2018, pp. 1-5.

[11]. IEEE Standard for Synchrophasor Measurements for Power Systems -- Amendment 1: Modification of Selected Performance Requirements," in IEEE Std C37.118.1a-2014 (Amendment to IEEE Std C37.118.1-2011), vol., no., pp.1-25, April 30 2014.

[12]. IEEE Standard for Synchrophasor Data Transfer for Power Systems," in IEEE Std C37.118.2-2011 (Revision of IEEE Std C37.118-2005), vol., no., pp.1-53, Dec 28. 2011.

[13]. P. Castello, C. Muscas, P. A. Pegoraro and S. Sulis, "Trustworthiness of PMU data in the presence of synchronization issues," 2018 IEEE International Instrumentation and Measurement Technology Conference (I2MTC), Houston, TX, 2018, pp. 1-5.

[14]. A Esmaeilian, M. Kezunovic, "Fault Location Using Sparse Synchrophasor Measurement of Electromechanical Wave Oscillations," IEEE Trans. Power Delivery, vol. 31, no. 4, pp. 1787-1796, Aug. 2016.

[15]. NASPI Control Room Solutions Task Team. Using Synchrophasor Data for Oscillation Detection. [Online]. Available: https://www.naspi.org/sites/default/files/reference_documents/crstt_oscillation_detection_20180129_final.pdf. Oct 2017.

[16]. Bonneville Power Administration. Synchrophasor Technology at BPA: from Wide-Area Monitoring to Wide-Area Control. [Online]. Available: https://www.bpa.gov/Doing%20Business/TechnologyInnovation/Documents/SYNCHROPHASORS%20AT%20BPA%20Nov%202017.pdf. Oct 2017.

[17]. NERC Modeling Improvements Initiative Update Technical Report. [Online].Available:https://www.nerc.com/comm/PC/System%20Analysis%20and%20Modeling%20Subcommittee%20SAMS%20201/NERC_Modeling_Improvements_Initiative_Update_Report_-_2018-05-17.pdf. May 2018.

[18]. A. Mingotti, L. Peretto, R. Tinarelli, A. Angioni, A. Monti and F. Ponci, "Calibration of Synchronized Measurement System: from the Instrument Transformer to the PMU," 2018 IEEE 9th International Workshop on Applied Measurements for Power Systems (AMPS), Bologna, 2018, pp. 1-5.

[19]. D. P. Shepard, T.E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks," *Int. J. Crit. Infrastruct. Protect.,* vol. 5, no. 3, pp. 146-153, Dec. 2012

[20]. X. Jian, J. Zhang, B. J. Harding, J. J. Makela, and A. D. Dominguez-Garcia, "Spoofing GPS receiver clock offset of phasor measurement units," *IEEE Trans. Power Syst.,* vol. 28, no. 3, pp. 3253-3262, Aug. 2013.

[21]. G. Fu, T. Holmes, C. Riedel, J. C. Liu, " RAIM and SBAS based Detection of GNSS Spoofing by Timing and Content Consistency Rules," in Proc. of the 30th International Technical Meeting of the Satellite Division of the Institute of Navigation, pp. 2854-2868, Portland, OR, September 2017.

[22]. C. T. Beasley. Electric Power Synchrophasor Network Cyber Security Vulnerabilities.[Online].Available:https://tigerprints.clemson.edu/cgi/viewcontent.cgi?article=2995&context=all_theses.

[23]. S. Barreto, M. Pignati, G. Dán, J. Le Boudec and M. Paolone, "Undetectable Timing-Attack on Linear State-Estimation by Using Rank-1 Approximation," in *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 3530-3542, July 2018.

[24]. L. Vanfretti. Vulnerability of Synchrohpasor-based WAMPAC Applications to Time Synchronization Spoofing. [Online]. Available: https://www.naspi.org/sites/default/files/2018-05/04_Vanfretti_VulnerablitlyWAMPAC_20180425.pdf.

[25]. S. S. Biswas, J. H. Kim and A. K. Srivastava, "Development of a smart grid test bed and applications in PMU and PDC testing," 2012 North American Power Symposium (NAPS), Champaign, IL, 2012, pp. 1-6.

[26]. M. Kezunovic, A. Esmaeilian, T. Becejac, P. Dehghanian, C. Qian, "Life Cycle Management Tools for Synchrophasor Systems: Why We Need Them and What They Should Entail," IFAC Workshop on Control of Transmission and Distribution Smart Grids (CTDSG 2016). Prague, Czech Republic, October 2016.

[27]. M. Yoon, S. Mohan, J. Choi, J. Kim and L. Sha, "SecureCore: A multi-core-based intrusion detection architecture for real-time embedded systems," *2013 IEEE 19th Real-Time and Embedded Technology and Applications Symposium (RTAS)*, Philadelphia, PA, 2013, pp. 21-32.

[28]. Analysis of the Cyber Attack on the Ukrainian Power Grid. [Online]. Available:https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.

[29]. C. Riedel, S. Liu, "Measurement System Timing Integrity in the Presence of Faults and Malicious Attacks", 2019 IEEE International Conference on Smart Grid Synchronized Measurements and Analytics – SGSMA, College Station, TX, May 2019.

[30]. C. Qian, M. Kezunovic, "Synchrophasor Reference Algorithm for PMU Calibration System," 2016 IEEE PES Transmission & Distribution Conference and Exposition, Dallas, TX, pp. 1-5, May 2016.

[31]. C. Qian, M. Kezunovic, "A Power Waveform Classification Method for Adaptive Synchrophasor Estimation," IEEE Transactions on Instrumentation and Measurement, vol. 67, no. 7, pp. 1646-1658, July 2018.

[32]. P. Romano and M. Paolone, "Enhanced Interpolated-DFT for Synchrophasor Estimation in FPGAs: Theory, Implementation, and Validation of a PMU Prototype," in IEEE Transactions on Instrumentation and Measurement, vol. 63, no. 12, pp. 2824-2836, Dec. 2014.

[33]. T. Bi, H. Liu, Q. Feng, C. Qian, and Y. Liu, "Dynamic Phasor Model-Based Synchrophasor Estimation Algorithm for M-Class PMU," IEEE Trans. Power Delivery, vol.30, no.3, pp.1162-1171, June 2015.

[34]. C. Qian, M. Kezunovic "Dynamic Synchrophasor Estimation with Modi-fied Hybrid Method," 2016 IEEE PES Conference on Innovative Smart Grid Technologies, Minneapolis, MN, pp. 1-5, September 2016.

[35]. C. Qian, M. Kezunovic, "Spectral Interpolation for Frequency Measurement at Off-Nominal Frequencies," 2017 IEEE PES General Meeting, Chicago, IL, pp. 1-5, July 2017.

[36]. Test Suite Specification: Synchrophasor – IEEE Synchrophasor Measurement Test Suite Specification (TSS), version 2. September 28, 2015.

[37]. NI 9263 Data Sheet: [Online] Available http://www.ni.com/pdf/manuals/373781b_02.pdf.

[38]. Angilent Technologies, Waveform Playback and Capture Made Easy. [Online] Available: https://cdn.testequity.com/documents/pdf/easy-waveform-capture-playback.pdf.