This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2665461, IEEE Transactions on Smart Grid

Vulnerability of Synchrophasor-based WAMPAC Applications' to Time Synchronization Spoofing

M. S. Almas, L. Vanfretti, R. S. Singh and G. M. Jonsdottir

***Abstract*—This paper experimentally assesses the impact of time synchronization spoofing attacks (TSSA) on synchrophasor-based Wide-Area Monitoring, Protection and Control applications. Phase Angle Monitoring (PAM), anti-islanding protection and power oscillation damping applications are investigated. TSSA are created using a real-time IRIG-B signal generator and power system models are executed using a real-time simulator with commercial phasor measurement units (PMUs) coupled to them as hardware-in-the-loop. Because PMUs utilize time synchronization signals to compute synchrophasors, an error in the PMUs' time input introduces a proportional phase error in the voltage or current phase measurements provided by the PMU. The experiments conclude that a phase angle monitoring application will show erroneous power transfers, whereas the anti-islanding protection mal-operates and the damping controller introduces negative damping in the system as a result of the time synchronization error incurred in the PMUs due to TSSA.**

The proposed test-bench and TSSA approach can be used to investigate the impact of TSSA on any WAMPAC application and to determine the time synchronization error threshold that can be tolerated by these WAMPAC applications.

***Index Terms*— Phasor measurement unit (PMU), power system protection, smart grid, spoofing, synchrophasors, time synchronization attack**

I. Introduction

Synchrophasor measurements are necessary for a large number of existing and potential synchrophasor-based Wide-Area Monitoring, Protection and Control (WAMPAC) applications, as identified in [1]. The reliability of these applications depends largely on the accuracy of the phasors computed by the Phasor Measurement Units (PMUs) [2] [3], for which timing plays a critical role.

Commercially available PMUs are capable of receiving time-synchronization signals in a number of ways. Almost all the PMUs support the IRIG-B time synchronization format where a substation clock with an antenna receives the GPS signals from satellites and modifies them to the desired time-code format for timing signal distribution [4]. Some PMUs are capable of receiving GPS signals directly with the help of a GPS antenna as a source for time-synchronization. Recently, the Precision Time Protocol (PTP) governed by the IEEE Std. 1588 is being used to distribute time-synchronization signals to the PMUs via Ethernet [5]. The PTP time is synchronized to one Pulse per Second (PPS) signal generated by any master clock (atomic or radio clock) available at the server level. The generated PPS signal synchronizes the time at the PMU (slave) with the reference time (master clock) [6]. The GPS generates and distributes the timing signal over wide-area, whereas PTP only aims to distribute the timing signal over a small geographic area.

A. Paper Motivation

PMU technology is vulnerable to cybersecurity threats. Most of the vulnerabilities are due to the fact that synchrophasors are streamed out using TCP/IP and UDP/IP as a transport layer protocol, which makes it susceptible to interception attacks such as packet sniffing, side channel attacks and man-in-the-middle attacks, modification attacks like malicious code injection, and fabrication attacks in the form of synchrophasor data spoofing [7-9]. Denial of Service (DoS) attacks at the physical layer is also possible by either disconnecting the power supply to the PMU, cutting the cable connecting a PMU with the communication network (switch/router) or jamming the GPS signals that provide time-synchronization input to the PMUs. However, most of the PMUs synchronize their internal local oscillator with the time-synchronization signal and in case of absence of time-synchronization signal due to DoS, the internal oscillator takes over and provides reliable time for several minutes.

Recently, Time-Synchronization Spoofing Attacks (TSSAs) have become a relevant concern. The GPS receiver of a substation clock or a PMU can be deceived by broadcasting counterfeit GPS signals or by simply rebroadcasting the GPS signals captured at another time [10]. This results in wrong computation of synchrophasors by the PMUs and therefore leads to false operation of synchrophasor-based WAMPAC applications.

The IEEE standard for Synchrophasor Measurements for Power Systems (IEEE C37.118.1-2011) [11] specifies requirements for PMUs for both steady state and dynamic operating conditions. The Total Vector Error (TVE) factor assures that the PMUs uncertainty in both magnitude and time synchronization error is bounded within a certain limit. This limit is specified in the standard to 1% and corresponds to a phase angle error of 0.573^0 (degrees) or a time synchronization inaccuracy of 31.8 μs at 50 Hz. It is therefore important to analyse the impact of time-synchronization signal

This work was supported in part by Nordic Energy Research through the STRONg^{2}rid project and by Statnett SF, the Norwegian TSO.

M. S. Almas, R. S. Singh, G. M. Jonsdottir and L. Vanfretti are with KTH Royal Institute of Technology, Stockholm, Sweden. (e-mail: {msalmas, luigiv, rssingh, gmjon}@kth.se)

L. Vanfretti is with Statnett SF, Research and Development, Oslo, Norway (email: luigi.vanfretti@statnett.no)

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2665461, IEEE Transactions on Smart Grid

spoofing on synchrophasor-based applications, to understand their potentially negative consequences in the power system.

B. Literature Review

Unintentional threats to GPS signals in the form of Radio Frequency (RF) interference and space weather events (solar flares) results in timing errors or loss of signal reception [12]. Reference [13] reports that the relatively weak GPS signals can be jammed by transmitting enough noise on the same frequency to overwhelm satellite signals. GPS spoofing tests conducted at Pacific Northwest National Laboratory (PNNL) conclude that GPS receivers of commercially available PMUs can lock themselves to a spoofed GPS signal resulting in wrong calculation of phase angle by 70 degrees and thus, violate the TVE criteria specified by IEEE Std. C37.118.1 [11]. In [14], a GPS spoofer implemented on portable software-defined radio platform with a DSP is used to spoof the IRIG-B output of a GPS receiver. The spoofer in this case induced a timing error of 1 μs resulting in an error of 0.314 mrad (18 mdeg) by a PMU for a 50 Hz measurement. The spoofer in this case achieved PMU phase angle computation error exceeding 10^0 (degrees) within 15 minutes by spoofing the time synchronization signal by 2 μs relative to the authentic signal.

In [15], a time synchronization attack based on two-stage GPS spoofing [16] is analyzed, where the spoofer interferes with a GPS receiver to obstruct authentic GPS signal reception followed by the generation of a spoofed GPS signal, to which the PMU locks. The effect of this GPS spoofing on transmission line fault detection, voltage stability monitoring and fault location is studied. The GPS spoofing resulted in deteriorating performance of fault location, grossly over-estimating power margins for voltage stability detection and imprecise event location in the power grid.

In [17], the GPS spoofing attack is formulated as an optimization problem with an objective of maximizing the difference between PMU's receiver clock offset before and after the attack. The effect of GPS spoofing on a voltage stability algorithm that relies on the phase angle computed by a PMU was analyzed and it was concluded that by GPS spoofing, the error in PMU phase angle computations can increase beyond 10^0 (degrees), which leads to false voltage instability alarms.

According to the authors, the impact of GPS time spoofing has only been performed on monitoring and post-fault analysis applications, and not on more time-critical applications such as synchrophasor-based protection and feedback control.

C. Paper Contribution

This paper presents the impact of time synchronization spoofing attacks (TSSA) on synchrophasor-based monitoring, protection and feedback control applications through numerous laboratory experiments. The experiments were conducted using real-time (RT) hardware-in-the-loop (HIL) simulation, including actual PMUs, Phasor Data Concentrator (PDC) and SW/HW applications in the loop with the real-time simulator. The TSSA is modeled through real-time IRIG-B signal generator and spoofing impacts are analyzed on standard power system synchrophasor use cases. The IRIG-B signal generator model and power system model are executed in real-time using Opal-RT's eMEGAsim Real-Time Simulator (RTS) [18].

As illustrative examples, the impacts of the TSSA on WAMPAC applications that depend on the PMUs' phase measurements are analyzed. Synchrophasor-based Phase-Angle Monitoring (PAM), passive anti-islanding protection and feedback damping control applications are analyzed.

The proposed real-time hardware-in-the-loop (RT-HIL) approach together with TSSA methodology can be utilized to experimentally and quantitatively evaluate the maximum time synchronization error that can be tolerated by any WAMPAC application.

The aim of this paper is to perform experiments using actual field equipment, associated communication protocols and time synchronization technology in a controlled laboratory environment to study, understand and analyze the potential impacts of TSSA on WAMPAC applications. The RT-HIL test-bench, experimental results and the insights obtained through this study, will enable the researchers to delve further into the challenges in wide-area precision clock synchronization in current and future power systems.

D. Paper Organization

The paper is organized as follows: Section II provides a brief overview of the IRIG-B time-code, its real-time modeling, and real-time IRIG-B signal generation. Section III presents the RT-HIL experimental setup. The effect of TSSA on synchrophasor-based monitoring, protection and control applications is discussed in Section IV, V and VI respectively. The impact of loss of time synchronization signal on PMUs from different vendors and the impact of TSSA on PMU's internal oscillator is discussed in Section VII. Finally, conclusions are drawn in Section VIII.

II. Real-Time IRIG-B Signal Generation and Manipulation

A. IRIG-B Overview

To analyze the impact of TSSA on WAMPAC applications, an Inter-Range Instrumentation Group Code B (IRIG-B) time signal [19] was simulated and controlled in real-time. Each frame of IRIG-B time code is one second long and has a pulse rate (or bit rate) of 100 pulses per second (PPS) providing time of day and day of year information. The two most common formats of IRIG-B time codes are unmodulated "DC Level Shifted (DCLS) pulse width code" and "Amplitude Modulated (AM)" based on 1 kHz sine wave signal. The unmodulated DCLS IRIG-B can provide a timing accuracy of the order of ± 500 ns, which is better than the accuracy range of ± 10 µs provided by its amplitude modulated counterpart. For this reason, the unmodulated DCLS IRIG-B time signal was modeled and generated in real-time to carry out this study.

B. Unmodulated DCLS IRIG-B

In the unmodulated DCLS IRIG-B time code, the width of logic zero is set to be 20% of the index interval (2 ms), the width of logic one is 50% of the index interval (5 ms). Position markers which define the end of one cycle and beginning of the consecutive cycle are 80% of the index interval (8 ms). This means that every (new) one-second time frame is identified by two consecutive 8 ms pulses [19]. The

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2665461, IEEE Transactions on Smart Grid

second 8 ms pulse in this case is triggered along with the rising edge of the 1 PPS signal from GPS.

C. DCLS IRIG-B Real-Time Modeling and Signal Generation

The unmodulated DCLS IRIG-B time code was programmed in MATLAB and embedded in a Simulink model as a MATLAB function. The code includes an option to set the initial time from where time starts rolling. Other control parameters like daylight saving, leap seconds and time quality can also be set and modified. This IRIG-B time signal generator model was executed in real-time using Opal-RT's eMEGAsim Real-Time Simulator (RTS) [18], the generated IRIG-B time code pulses were acquired from the analog output of the RTS and fed to the IRIG-B input of the commercial hardware PMUs.

D. Time Synchronization Attack Strategy

In the developed IRIG-B signal generation model, it is possible to delay the time synchronization signals from microseconds to milliseconds as per user settings. In this study, the time errors were varied in the precise steps of 10 µs. Figure 1 shows the one second simulation output of the real-time IRIG-B time code generation in the RTS. The structure of an IRIG-B frame is presented below:

<synch>SS:MM:HH:DDD:YY<Control><Binary Seconds>

where:

SS: The second of the minute [00 to 59 (60 during leap seconds)] in Binary Coded Decimal (BCD)
MM: The minute of the hour (00 to 59) in BCD
HH: The hour of day (00 to 23) in BCD
DDD: The day of year (001 to 366) in BCD
YY: Counts year and cycles to the next year on January 1st of each year and will count to year 2099
Control: Leap second, daylight saving, quality information and a parity bit included in a block of 27
Binary Seconds: Second of the day in 17 bits

Figure 2 shows a screenshot from an oscilloscope before and during the spoofing attack. As shown in Fig. 2a, before the spoofing attack, the reference and spoofed IRIG-B signals are time aligned with the 1 PPS signal from the GPS. The spoofed IRIG-B signal is then controlled in the real-time causing a spoofer-induced error of exactly 10 ms (Fig. 2b). This confirms that the real-time IRIG-B model and signal generator can precisely control the timing to launch a TSSA.

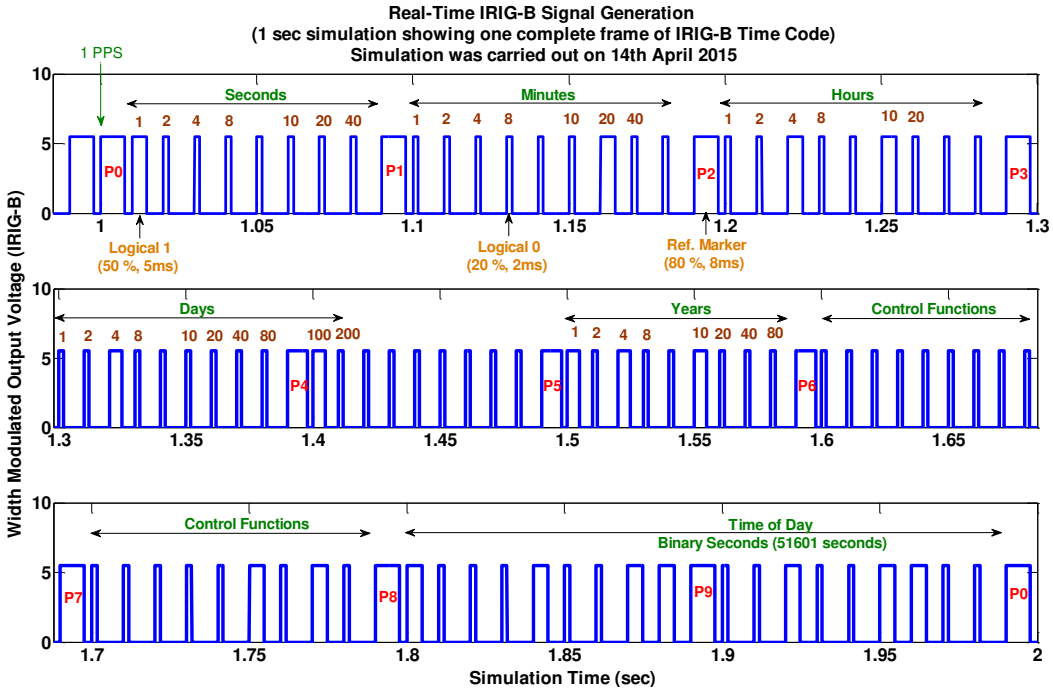


Fig. 1. IRIG-B time code format which is implemented in real-time in RTS. Time at this point equals 104 Days, 14 Hours, 20 Minutes, 1 Second, 15 Years (14th April 2015, 14:20:01).

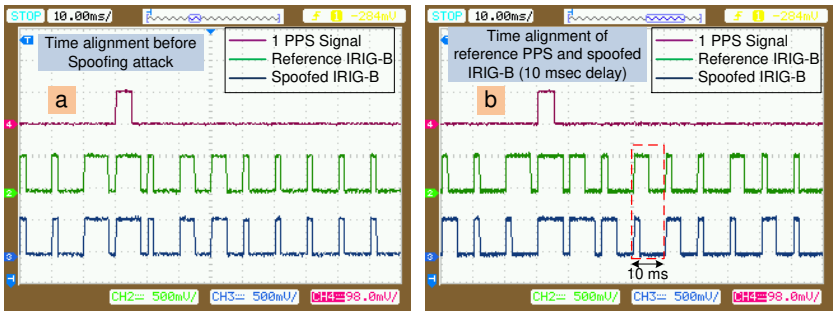


Fig. 2. Screenshots from an oscilloscope showing time alignment to the reference PPS (top trace), reference IRIG- B (middle trace) and spoofed IRIG-B (bottom trace) for pre-spoofing (Fig. 2a) and during spoofing (Fig. 2b) attack. During TSSA, spoofed IRIG-B signal was controlled to induce timing-error of 10 ms.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2665461, IEEE Transactions on Smart Grid

E. Assumptions

The proposed strategy of launching TSSA requires the attacker to connect the output of the IRIG-B signal generator (spoofed signals) to the time synchronization signal input of the PMU under attack. Therefore, it is assumed that the attacker has physical access to the PMU.

III. RT-HIL Experimental Setup

The overall experimental test setup for RT-HIL simulation is shown in Fig. 3. The power system test-case model was executed in real-time using 4 cores of Opal-RT's eMEGAsim Real-Time Simulator (RTS) [18]. One of the cores of the RTS was dedicated to execute the IRIG-B time code signal generation model presented in Section-II. IRIG-B signals and the three phase voltage and current signals from the desired buses in the test-case model were acquired from the analog outputs of the RTS. The time synchronization signals were fed to the IRIG-B input terminal of the PMUs from Schweitzer Engineering Laboratories (SEL) [20]. As shown in Fig. 3, two PMUs were configured with identical settings and their CT and VT modules were bypassed to eliminate any difference in phasor calculation due to internal filtering and A/D converters, instead, PMUs were coupled to the RTS using a low-level interface. The only difference in configuring the hardware is that PMU-A is fed with the authentic IRIG-B signals, and is used as a reference PMU, while PMU-B is targeted with TSSA by spoofing the IRIG-B signals.

The synchrophasor-based anti-islanding protection algorithm was deployed internally in the PMU using protection logic equations, which are supported by proprietary PMUs [21]. The deployed protection algorithm utilizes the computed synchrophasors and generates trip signals based on the protection logic. In this study, the trip command is generated by the PMU as an IEC 61850-8-1 GOOSE message [22], which offers a faster response time than using wired signaling as shown in [21]. This GOOSE message was published by the PMU that has a subscription from the RTS that is configured to open a circuit breaker when the status of the GOOSE message changes. For the synchrophasor-based feedback control application, the synchrophasors from the PMUs are received in an external embedded controller (a National Instrument's Compact Reconfigurable I/O Controller (NI-cRIO)). The controller executes an oscillation damping algorithm and feeds the damping signal to the RTS where, it is configured as a supplementary signal in the voltage controller of a Static VAR Compensator (SVC).

The PMUs are configured to stream out all computed phasors at a rate of 50 frames/s. Important states of the protection algorithm and the tripping signal are configured as digital outputs within the PMU streams as specified by the IEEE Standard for Synchrophasor data transfer for Power Systems (IEEE Std. C37.118.2-2011) [11]. These PMU streams are concentrated by a Phasor Data Concentrator (PDC) and the concentrated output stream is received in a workstation using Statnett's Synchrophasor Software Development Kit (S3DK) [23], which provide real-time synchrophasor data in the LabView environment. Within

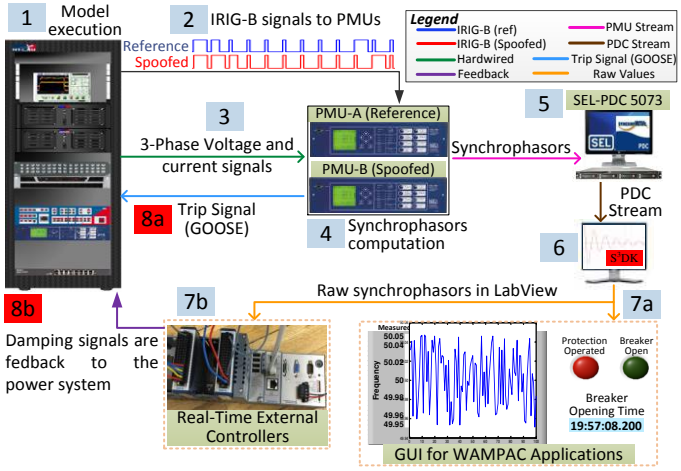


Fig. 3. Experimental setup for analyzing the impact of time synchronization spoofing attacks on synchrophasor-based protection and control applications.

LabView, these raw measurements are presented in real-time displays for monitoring purposes and archived for further analysis.

The important components and the data-flow of the experimental setup shown in Fig. 3 are summarized below;

1. Power system and IRIG-B signal generation models are executed in real-time in separate cores of Opal-RT's RTS.
2. Reference and spoofed IRIG-B time code pulses acquired from RTS are fed to respective PMUs.
3. 3-phase voltage and current signals of the desired buses are acquired from the analog output of the RTS and fed to the low-level interface of the PMUs.
4. PMUs compute synchrophasors based on their respective voltage/current and IRIG-B input signals.
5. PDC time-aligns and concentrates the streams from both PMUs.
6. Protocol parser (S3DK) unwraps PDC stream and provides raw values of phasors, analogs and digitals wrapped in IEEE C37.118 format in LabView environment.

7a. GUIs of the monitoring, protection and control applications utilize these synchrophasors for visualization.

7b. External controller executes oscillation damping algorithm based on the selected input synchrophasor measurements.

8a. The output of the protection algorithm executing in PMU-B is a trip signal which is published as a GOOSE message to open circuit breaker in the power system model.

8b. The output of the controller which is a damping signal is configured as a supplementary control of an SVC in power system model being executed in RTS.

IV. Synchrophasor Based Phase Angle Monitoring (PAM) Vulnerability To TSSA

An important application of synchrophasor measurements is phase angle monitoring (PAM). Monitoring phase angle differences between ends of transmission corridors reveals valuable information related to loading, power transfer through the corridor, etc.

The impact of TSSA on PAM is analyzed on a variant of the Nordic-32 power system model [24], which is shown in Fig. 4. PMU-A and PMU-B are receiving three phase voltages and currents from Bus-38 and Bus-43, respectively which allow monitoring a major corridor between the North and the Central part of the network.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2665461, IEEE Transactions on Smart Grid

A. *Total Vector Error (TVE)*

Firstly, the impact of TSSA on TVE is analyzed. The voltages and currents at Bus-43 of test system (Fig. 4) were fed to the PMU-B and the TSSA was launched by injecting a time error in steps of 10 µs. Fig. 5a shows the impact of TSSA on synchrophasor voltage phase angle error. It is observed that the TSSA resulted in an error in voltage phase angle computation beyond 0.573^0 mark as soon as the time error increases beyond 30 µs, thus breaching the maximum allowable TVE limit. Once the TVE is violated, these measurements are considered imprecise and uncertain to be used for any further analysis. Figure 5b and 5c show the actual synchrophasors as computed by the PMU before and after time spoofing by 1000 µs, thus resulting in a phase angle error of about 18^0.

B. *Phase Angle Monitoring (PAM)*

Figure 6 shows the GUI of the synchrophasor-based PAM application. From t = 30 s, the TSSA is launched on PMU-B (connected at Bus-43) to introduce a time synchronization error in steps of 10 µs at precisely every 5 seconds. This results in an inaccurate phase angle computation by PMU-B (Bus-43), and consequently leading to inaccurate computations of power transfer and line loading between the North and the Central part. As the PAM application shows, the TSSA results in an erroneous increase in line loading of 12 % and corrupts the power transfer between Bus-38 (North) and Bus-43 (Central) by showing an increase from 630 MW to 765 MW. The impact on the PAM application occurs within a span

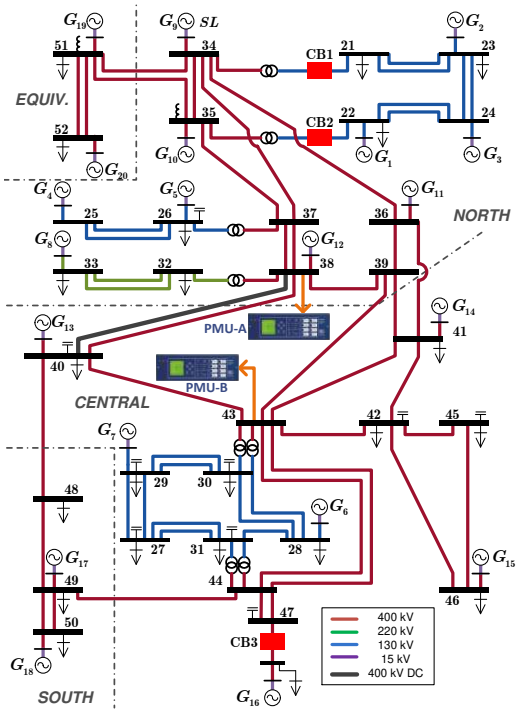


Fig. 4. Real-Time Nordic-32 power system model. PMUs are located at Bus-38 and Bus-43 which are feeding synchrophasors to PAM application.

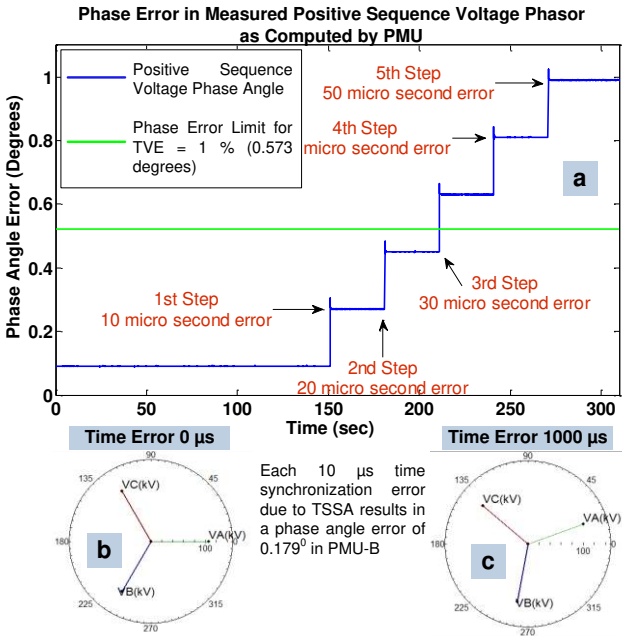


Fig. 5. (a) shows the phase angle error with respect to allowable TVE limit, (b,c) shows actual phasor as computed by PMU-B before and after the TSSA.

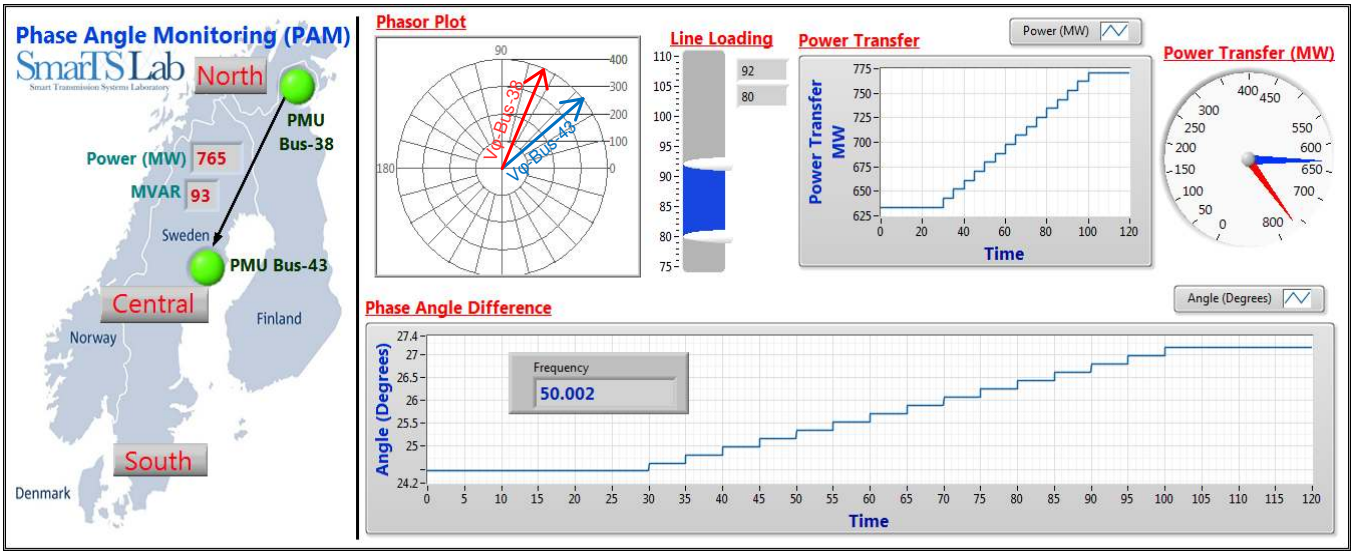


Fig. 6. (Left) shows the map of the Nordic region and the location of the PMUs. (Right) shows the phasor plot for positive sequence voltage phasor from bus-38 and bus-43, transmission line loading, power transfer through the line, phase angle difference at the ends of line (38-43) and frequency.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2665461, IEEE Transactions on Smart Grid

of 70 s once the TSSA is launched on PMU-B. By the end of the TSSA at t = 100 s, the error in phase angle differences is 2.69^0 due to a time synchronization error of 150 µs.

V. Synchrophasor Based Anti-Islanding Protection Vulnerability to TSSA

This section presents the impact of TSSA on a wide-area synchrophasor-based passive anti-islanding protection scheme. The TSSA is launched at PMU-B to introduce a time synchronization signal error that results in erroneous tripping times for the scheme and further leading to false protection tripping. Thus, due to TSSA, the protection scheme misinterprets the healthy state as a faulty condition and subsequently issues a trip command.

A. *Power System Model*

The impact of TSSA on the synchrophasor-based anti-islanding protection scheme is analyzed on a variant of IEEE 3-machine 9-bus system [25] modeled for real-time execution. The single line diagram of the system is shown in Fig. 7.

B. *Wide-Area Passive Anti-Islanding Protection*

The power system shown in Fig. 7 is used to study the impact of TSSA on the synchrophasor-based passive anti-islanding scheme. If CB-1 opens due to a protection operation or malfunction, this results in an islanding condition with G1 supplying electric power to Load A at Bus-4. Once the breakers are opened and the island is formed, this condition needs to be detected and G1 needs to be disconnected from the isolated network within 2 seconds as specified by the IEEE Std. 1547-2008 [26].

PMU-B is considered as a local PMU (in the vicinity of G1) being fed with currents and voltages from Bus-4, while PMU-A is a remote PMU installed at Bus-7 and streaming out synchrophasors at the same rate of 50 frames/s. A wide-area anti-islanding protection algorithm based on voltage phase angle estimates is deployed using protection logic equations within PMU-B. This is achieved by configuring PMU-B as a client for PMU-A, and using direct relay-to-relay communication between them [21]. Thus, PMU-B processes the remote synchrophasor data internally, time aligns them with local data and makes them available for the passive islanding detection algorithm. The important steps of the experimental setup shown in Fig. 7 are summarized below;

1. Reference PMU-A is installed at Bus-7 (remote bus).
2. Spoofed PMU-B is installed at Bus-4 (local bus).
3. Direct relay-to-relay communication is established between PMU-A and PMU-B.
4. This allows PMU-B to receive internally the remote synchrophasors from PMU-A and utilize them in anti-islanding algorithm executing inside PMU-B.
5. The output of the anti-islanding algorithm is a trip command issued by PMU-B as a GOOSE message to disconnect generator G1 by opening circuit breaker CB-2.

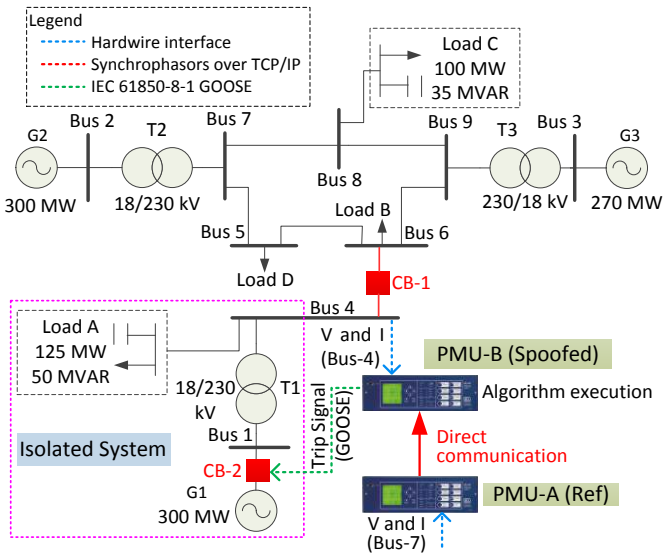


Fig. 7. Modified IEEE 3-machine, 9-bus system. PMU-B computes synchrophasors of Bus-4 and receives synchrophasors of Bus-7 through PMU-A. Angle-based anti-islanding protection is incorporated within PMU-B.

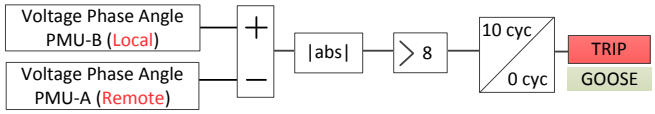
This anti-islanding scheme detects an islanding condition and opens CB-2 if the difference between phase angles computed by local and remote PMUs exceeds 8^0 and this condition persists for 10 cycles. The phase angle threshold is computed by assessing the phase variation between G1 and the rest of the network during different operating conditions. The 10 cycle time delay takes into account that during major system transients, the phase angle variation may briefly fall outside the normal phase variation of $\pm 6^0$. Figure 8 shows the logic diagram of the phase angle-based passive islanding detection algorithm and its respective logic equation programmed in PMU-B. This scheme is analyzed for the following cases:

Case-A: Both PMUs receive reliable time-synchronization signals from the IRIG-B generator and the islanding scenario is initiated at t = 60 s.

Case-B: PMU-A receives a reliable time-synchronization signal while PMU-B is subjected to TSSA at t = 30 s. The islanding scenario is initiated at t = 60 s.

The performance of this scheme for *Case-A*, i.e. with no TSSA, is shown in Fig. 9. The plots shown in Fig. 9 correspond to 10% active power mismatch between G1 and Load A. The important states of the anti-islanding algorithm execution as shown in Fig. 9 are;

1. At 60 s, circuit breaker CB-1 opens, resulting in an island.
2. The phase angle difference (blue trace) starts increasing and at 60.43 s, it goes beyond 8^0, resulting in timer initiation (grey trace).




```
PMV53 := V1YPMA % Storing Local Positive sequence synchrophasor voltage angle in user defined analog
PMV54 := RTCAP01 % Storing remote Positive sequence synchrophasor voltage angle in user defined analog
PMV55 := 8.00000 % Store threshold value of 8 degrees in user defined analog
PSV01 := abs (PMV53 - PMV54) > PMV55 % SET if measured synchrophasor synchrophasor voltage phase angle difference is greater than 8 degrees
PCT01IN := PSV01 % Input for conditioning timer. Timer tracks PSV01
PCT01PU := 10.000000 % Pickup is set to 10 cycles i.e. When PSV changes state from 0 to 1, the timer picks it up only if state of PSV01 stays 1 for 10 cycles
PCT01Q : Timer output SET to 1 when time exceeds 10 cycles after PSV01 is set
```

Fig. 8. Logic diagram and protection logic equations used for the synchrophasor phase angle based islanding detection.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2665461, IEEE Transactions on Smart Grid

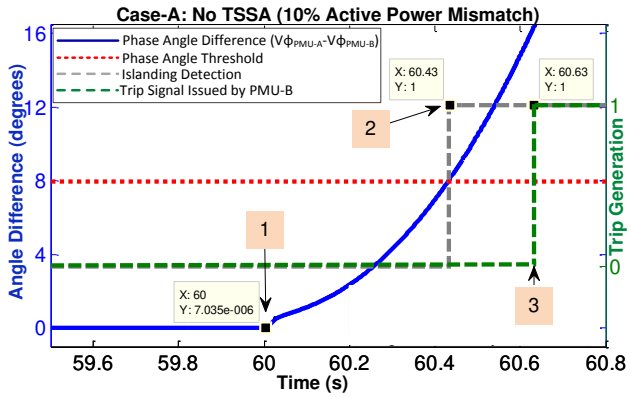


Fig. 9. Performance assessment of the wide-area anti-islanding scheme for 10% active power mismatch (*Case A:* No TSSA). Operating time is 0.63 s.

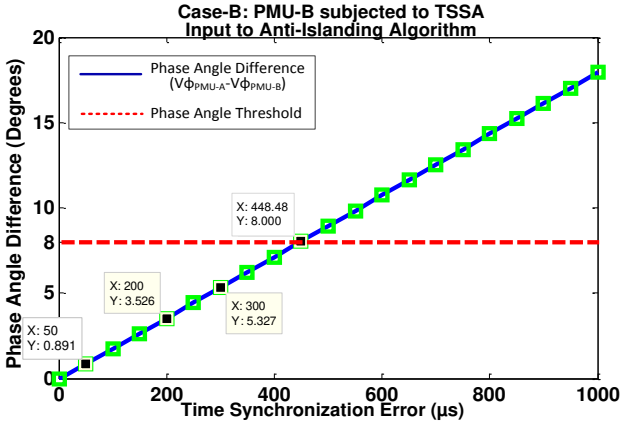


Fig. 10. Input to the anti-islanding protection scheme when PMU-B is subjected to TSSA (*Case-B*).

3. Once the timer elapses 10 cycles and while the phase angle difference condition is sustained, the PMU-B issues a trip command published as a GOOSE message [22] that opens the circuit breaker CB-2 at 60.63 s to disconnect the DG from the isolated island (green trace).

Thus, the total operation time for this scheme with 10% active power mismatch is 0.63 s.

Figure 10 shows the synchrophasor positive sequence voltage phase angle difference as computed by PMU-B ($V\varphi_{PMU\text{-}A}$-$V\varphi_{PMU\text{-}B}$) when subjected to TSSA. As the GPS spoofing is increased beyond 448.48 µs, the phase angle difference computed by PMU-B goes above 8^0 and the anti-islanding protection scheme initiates false tripping instantly. For this 50 Hz system, the phase measurement error of PMU- B, ϵ_φ , is related to the time synchronization error due to TSSA, t_{TSSA}, as follows:

$$\epsilon_\varphi = 50 \times t_{TSSA} \times 360^0 \quad (1)$$

For a 50 µs time synchronization error, (1) yields a phase measurement error of 0.9^0, which complies with the experimentally acquired values as shown in Fig. 10.

The comparison of the operation time of the implemented scheme for different active power mismatches when subjected to TSSA is shown in Fig. 11a. These operation times include the anti-islanding algorithm processing time, PMU phasor computation time and GOOSE communication delay [21].

The operation time of the scheme reduces with an increase in time synchronization error to a stage where it initiates false tripping beyond 448.48 µs due to the erroneous computation of the synchrophasor voltage phase angle by PMU-B. The operation time also reduces with an increase in active power mismatch between generator G1 and Load-A for all cases i.e. with and without TSSA. To further elaborate the impact of TSSA on anti-islanding protection scheme, the comparison of protection operation time is made between *Case-A* i.e. no TSSA and *Case-B* with 400 µs of TSSA (Fig. 11b).

VI. Synchrophasor Based Feedback Control Application Vulnerability to TSSA

To analyze the impact of TSSA on synchrophasor-based control applications, the performance of a Wide-Area phasor-[27] was implemented in a National Instrument's Compact based Oscillation Damping (WAPOD) controller is investigated. The phasor-based oscillation damping algorithm Reconfigurable I/O controller (NI-cRIO). This NI-cRIO receives local and/or remote synchrophasors as inputs, it processes them and separates the resulting controller input signal into average and oscillatory content using a recursive least square filter. The oscillatory content of the signal is phase shifted to create the damping signal. This damping signal is provided as a supplementary control signal to the Static VAR Compensator (SVC) executing in real-time in the RTS to provide damping.

The 2-area 4-machine Klein-Rogers-Kundur power system model as shown in Fig. 12 is used for this analysis. This power system model is inherently unstable due to an un-damped 0.64 Hz mode. The three phase voltages and currents of Bus-1 and Bus-2 are fed to the low-level interfaces of PMU-A and PMU-B, respectively. These synchrophasor streams are concentrated using PDC and then unwrapped using Statnetts' Synchrophasor Software Development Kit (S^3DK) [24] which provides raw phasors data to the WAPOD controller deployed

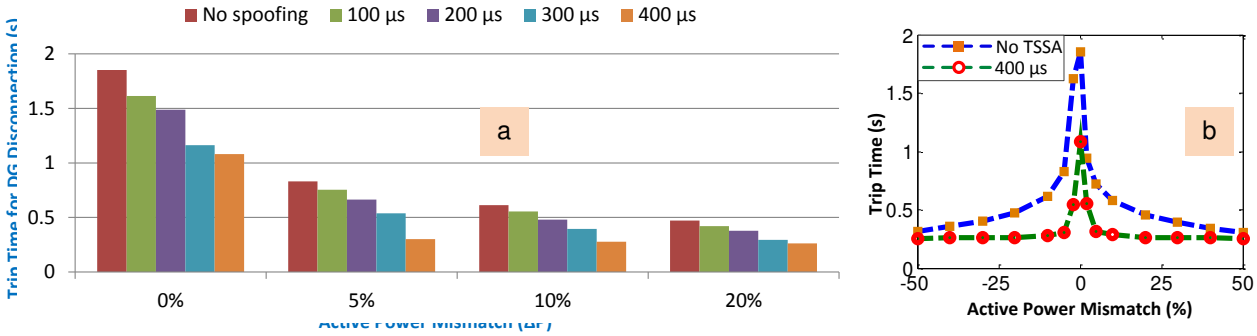


Fig. 11. Operation time of passive anti-islanding protection scheme for different active power mismatch and in presence of different TSSA

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2665461, IEEE Transactions on Smart Grid

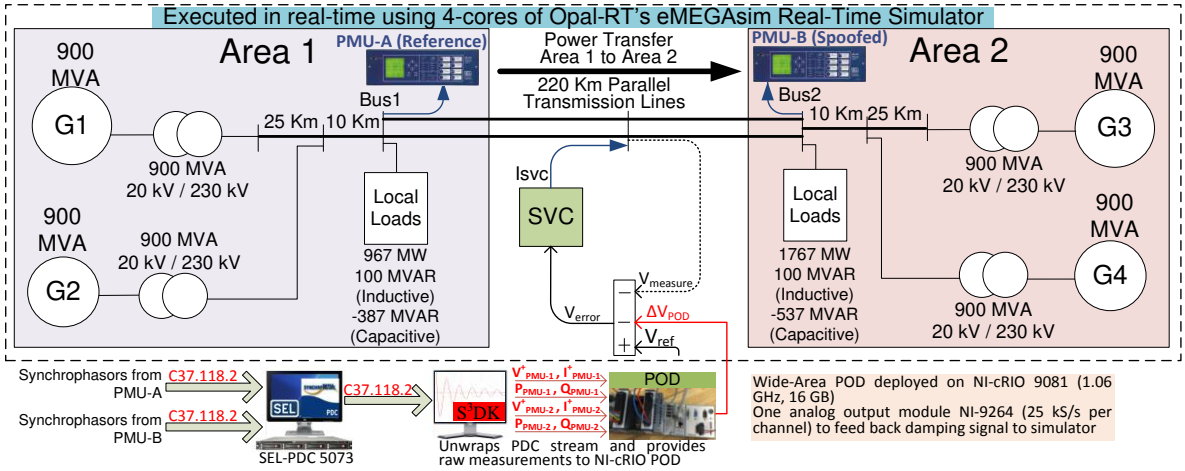


Fig.12. 2-area 4-machine Klein-Rogers-Kundur power system modelled in MATLAB/Simulink. PMU-A and PMU-B receives three phase voltage and currents from Bus-1 and Bus-2. These synchrophasors are received in WAPOD controller which provides damping signals to the supplementary control of an SVC.

on a NI-cRIO. The WAPOD executes damping algorithm using the synchrophasor measurement selected as an input, and provides a damping signal as an output through its analog output module. This damping signal is fed back to the RTS as an additional input to the SVC connected at mid-point of the test-case system to provide damping.

In order to analyze the performance of the WAPOD, the voltage phase angle difference ($V\varphi_{PMU\text{-}A}$-$V\varphi_{PMU\text{-}B}$) is selected. The same strategy of launching TSSA on PMU-B, as in the previous section, is carried out. As shown in Fig. 13, the performance of the WAPOD to damp the 0.64 Hz inter-area oscillation degrades as the time synchronization error in PMU-B due to TSSA increases. This performance degradation is primarily because of the erroneous phase angle computation by PMU-B when subjected to TSSA.

To further investigate the impact of TSSA on the performance of the WAPOD, the following control performance metrics are analyzed.

Decay Ratio: The ratio by which the oscillation is reduced in one complete cycle.

Overshoot / Undershoot: Maximum / minimum deviation of the signal from its post-disturbance steady-state value.

Settling Time: Time at which the oscillations are damped to a value that is within ±1 % of the post-disturbance steady-state value.

Table I shows the computation of above mentioned performance metrics for different time synchronization error values introduced in PMU-B as a result of TSSA. As the time synchronization error in PMU-B increases, its error in phase angle computation escalates. This results in rise in decay ratio, prolonged settling times and surge in overshoot/undershoot. As the TSSA increases beyond 1500 µs, the WAPOD introduces a negative damping and the overall system becomes unstable due to the undamped 0.64 Hz oscillation.

VII. Discussion

A. *Impact of Loss of Time Synchronization Signal on PMUs*

As discussed in Section-I, a TSSA is launched by interfering with a GPS receiver to obstruct authentic GPS signal reception followed by the generation of a spoofed GPS signal, to which the PMU locks. When the GPS signal is lost, the PMUs rely on their local oscillator to compute synchrophasors. The local oscillator frequency drifts due to temperature variations and mechanical vibrations, thus providing inaccurate time stamps for synchrophasor computation, which is reflected in the form of erroneous phase angle computation by PMUs.

The loss of time synchronization signal due to intentional interference can be considered as a jamming attack on the physical layer (GPS receiver) [28]. In order to investigate the impact of loss of time synchronization signals (GPS / IRIG-B) on synchrophasor-computation by PMUs from different vendors, RT-HIL simulation was carried out by utilizing PMUs from 4 different vendors. Identical three phase voltage

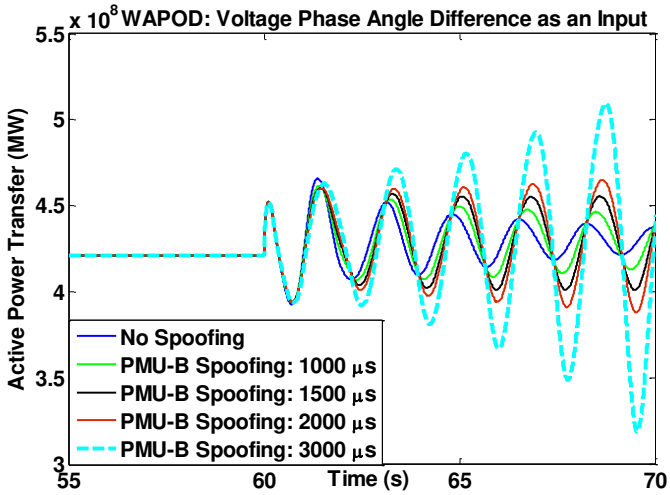


Fig. 13. Performance of synchrophasor-based WAPOD controller when subjected to Time Syncrhonization Spoofing Attack (TSSA)

TABLE I
WAPOD's CONTROL PERFORMANCE METRICS

Spoofing (µs)	Decay Ratio	Overshoot / Undershoot (%)	Setting Time (s)	Phase Error (deg)
0	0.964	10.35	11.75	0
200	0.966	10.61	11.93	3.526
400	0.969	11.08	12.15	7.104
600	0.975	11.70	13.56	10.730
800	0.977	11.95	15.79	14.335
1000	0.990	12.25	17.18	17.937
1500	0.997	14.17	31.48	26.755
2000	1.02	unstable	unstable	35.573
3000	1.05	unstable	unstable	53.652

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2665461, IEEE Transactions on Smart Grid

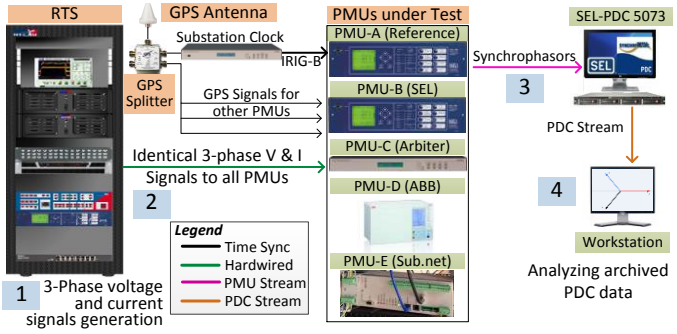


Fig. 14. RT-HIL test-setup for analyzing impact of loss of time synchronization signal on PMUs from different vendors.

and current signals were accessed through analog outputs of the RTS and fed to VT and CT modules of each of the PMUs respectively. All the PMUs were configured to stream out a similar synchrophasor datasets, i.e. voltage and current three phase phasors and their positive sequences. These PMU streams were concentrated and time-aligned in a Phasor Data Concentrator and were outputted as a concentrated PDC stream for archiving and analyzing. The overall experimental test-setup is shown in Fig.14.

PMU-A is considered as a reference PMU and it receives time synchronization signals in the form of IRIG-B pulses through substation clock. The rest of the PMUs (B-E) receive GPS signals through a single output of a GPS splitter by daisy-chaining. In order to analyze the impact of time synchronization signal loss, the output of the GPS splitter feeding PMUs (B-E) was disconnected at a given point in time. Due to this loss of time synchronization input signal, PMUs (B-E) utilize their respective internal oscillators to provide time reference which is used to compute synhrophasors. This results in imprecise synchrophasors computations by PMUs (B-E) as compared to the reference PMU-A, which is continuously receiving IRIG-B signals from the substation clock.

This impact of loss of time synchronization signal on phase angle computation by PMUs from different vendors is shown in Fig. 15. At t = 00:05:40, the time synchronization input signal to PMUs (B-E) was disconnected. This resulted in phase angle computation error by PMUs (B-E) with respect to PMU-A which keeps receiving authentic time synchronization signals. For all the PMUs, the phase angle computation error goes beyond 1 % TVE (0.573^0 or 31.8 µs) within 24 minutes of the disconnection of time synchronization input signal. Figure 16 shows the same analysis carried out for 4 hours which resulted in maximum phase angle error of 390^0 (21.64 ms) corresponding to PMU-D and a minimum phase angle difference of 10.45^0 (0.58 ms) corresponding to PMU-E.

B. Impact of TSSA on PMU's Internal Oscillator

In case of a TSSA, the PMU's internal clock synchronizes itself to the spoofed time synchronization signal. If the authentic time synchronization signal is replaced with the spoofed signal instantly, the PMU's internal oscillator takes some time to re-synchronize itself to the spoofed signal. This is shown in Fig. 17 where at t = 65.82 s, the TSSA is launched on PMU-B by replacing authentic time synchronization signal with spoofed signals instantly, to introduce time synchronization error of 50 µs. As the TSSA is launched instantly, the internal oscillator takes around 10 s to re-synchronize to the spoofed signal and during this period, the phase angle computation error goes beyond 8^0. After 10 s, the internal oscillator re-synchronizes itself to the spoofed signal which results in a phase angle computation error of 0.892^0 (TSSA = 50 µs). Such a TSSA is relatively easy to identify as the compromised PMU shows large phase angle deviations for a few seconds.

By slightly modifying the TSSA methodology, a more sophisticated TSSA can be launched. This approach is similar to the 2-stage GPS spoofing presented in [16]. This involves jamming the authentic GPS signals for a small duration before feeding the spoofed signals to the PMU. In this way, the internal oscillator of the PMU undergoes a smooth transition to the spoofed signal and does not result in large phase angle deviations. Such an attack can be hard to detect especially when the induced time synchronization error is very small. As shown in Fig. 18, the increase in jamming duration before feeding the spoofed signals results in smaller overshoot in the phase angle computation by the PMU. For a jamming period of 14 s, the overshoot for phase angle computation error is 0.106^0 (0.998^0 - 0.892^0) which is much smaller as compared to over 8^0 overshoot in case of instant TSSA without jamming (Fig. 17).

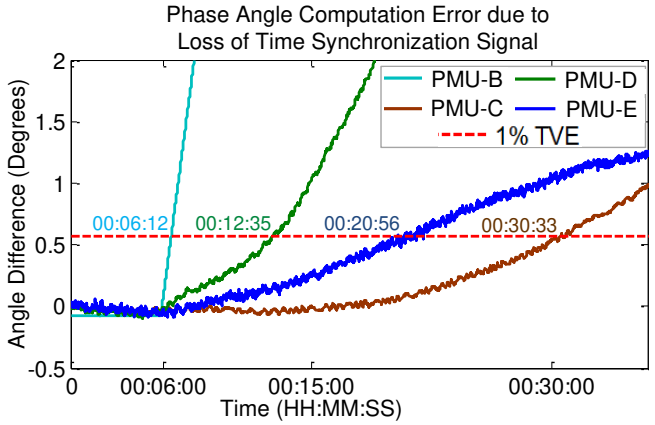


Fig. 15. Impact of loss of time synchronization input signal on phase angle computation by PMUs from different vendors (30 minute analysis)

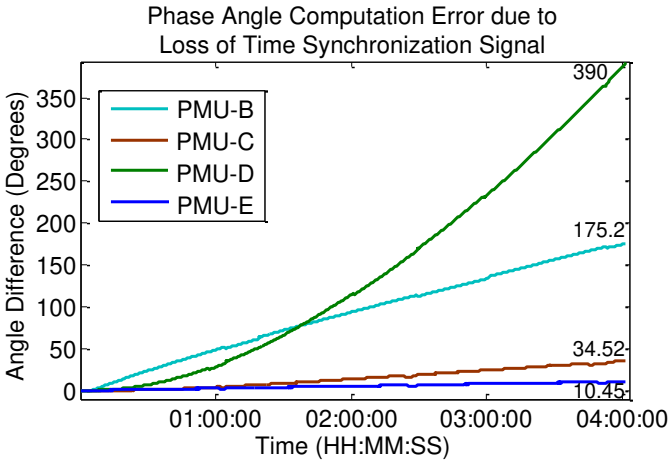


Fig. 16. Impact of loss of time synchronization input signal on phase angle computation by PMUs from different vendors (4 hours analysis)

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2665461, IEEE Transactions on Smart Grid

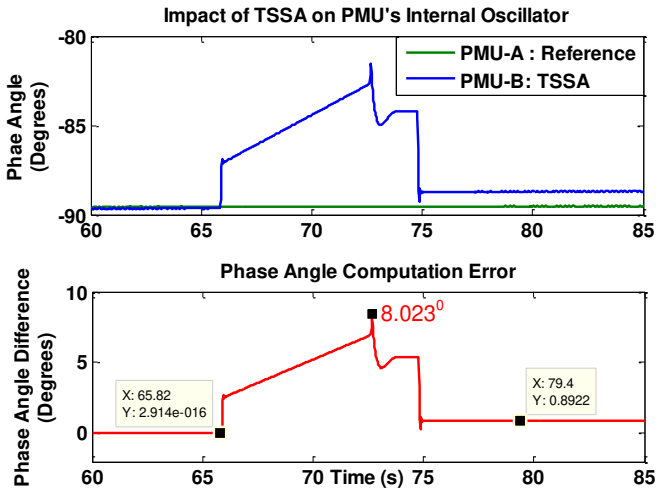


Fig. 17. Impact of instant TSSA on PMU's phase angle computation.

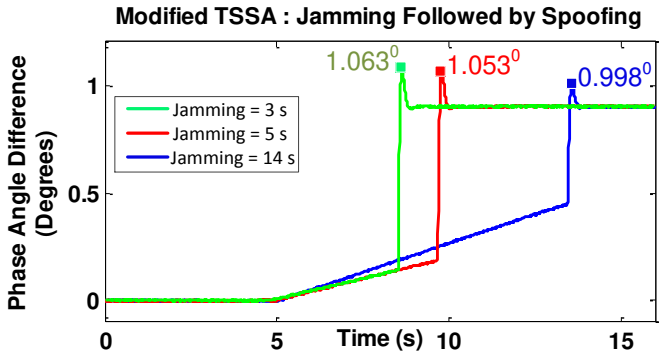


Fig. 18. Impact of modified TSSA on PMU's phase angle computation.

C. *Synthesis of Results*

The results obtained in this study can be synthesized as follows:

1. Monitoring Applications: *Any application which requires phase angle measurements will provide misleading information when PMUs are subjected to TSSA*. Section-IV deduced this for the specific case of Phase Angle Monitoring (PAM) application. Such misleading information can result in false corrective actions either automatically or manually (through operators' action).

2. Protection Applications: *The TSSA can result in faulty activation of a protection scheme*. Section-V deduced this for the specific case of anti-islanding protection where a TSSA of around 450 µs (phase angle computation error of 8^0) resulted in false activation of the scheme and separation of the DG from the rest of the power system.

3. Feedback Control Applications: *The TSSA results in a delay in the feedback control loop. If the delay is not compensated, this degrades the controller's performance.* Section-VI deduced this for the specific case of oscillation damping control where a TSSA of 1500 µs resulted in negative damping contribution by the controller.

4. *PMU's Internal Oscillator*: *Each PMU has a different internal oscillator and therefore results in different phase angle computation error when its external time synchronization signal is lost.* When subjected to a TSSA instantly, the internal oscillator of the PMUs needs to resynchronize to the spoofed time synchronization signal which requires additional time. During this period, the PMUs report a large phase angle computation error, which can result in mal-operation of the associated monitoring, protection and control applications.

As shown in Table-II, in order to provide a quantitative metric for the TSSA's tolerance level of each application, the aspects to consider include, but are not limited to:

- Threshold settings, for example the phase angle difference value above which the application would initiate a trip / control action. These thresholds are system dependent and are unique for each application.
- For the specific case of oscillation damping, the change in system topology results in a shift in the mode's frequency and damping, thus resulting in different damping requirement for the controller.

The maximum tolerance for each application can be calculated using the demonstrated RT-HIL setup and the proposed TSSA methodology. These tolerance levels are system and application dependent and therefore will be different for each case.

TABLE II
IMPACT OF TSSA ON ANALYZED WAMPAC APPLICATIONS

Application	Effect	Significance
Phase Angle Monitoring	Misleading information resulting in false control actions either manually or automatic	Major
Anti-Islanding Protection	False activation of protection scheme leading to system separation	Threshold dependent
Oscillation Damping Control	Controller's performance degradation that may result in incorporating negative damping into the system leading to loss of synchronism	Controller and System dependent

D. *Recommendations*

The current PMUs lack the functionalities to identify between authentic and spoofed time synchronization signals. Some of the recent recommendations put forward by North American SynchroPhasor Initiative (NASPI) [29] and National Institute of Standard and Technology (NIST) [30] to address TSSA are;

1. Supplying PMUs with two time synchronization sources (GPS and GALILEO).
2. Relying on GPS-independent networks such as telecom infrastructure to avoid dependence on very low power GPS signals from satellites.
3. Jamming, spoofing and interference detection and correction at the receiver (Substation clock / PMU).
4. Appropriate internal holdover oscillator for PMUs as back-ups for providing accurate time signals in case of absence of external time synchronization signals.

VIII. Conclusion

The GPS system can be interfered both intentionally and/or cosmically. Therefore, it is paramount to investigate the effect of time synchronization spoofing attacks (TSSA) on synchrophasor-based applications. This paper presented the design and implementation of TSSA in the form of IRIG-B signal generator and analyzing the impact of TSSA on WAMPAC applications by performing RT-HIL simulations with commercially available PMUs.

When the TSSA is launched, the time synchronization error is introduced at the PMUs, thus providing inaccurate time stamps for synchrophasor computation, which is reflected in the form of erroneous phase angle computation by PMUs.

Through the analysis of several RT-HIL experiments, this paper concludes that TSSA results in corrupted power system monitoring results, false protection activation and degradation of wide-area controller performance to an extent where the controller has a negative impact on system stability. Though all these applications had different time synchronization error tolerance, beyond which, these applications mal-operate. The RT-HIL experimental setups demonstrated in this paper the advantage it provides in the design, implementation and testing of synchrophasor applications. In contrast, the currently available off-line simulation software for power system computer-aided design provides no realistic insight into the practical design and implementation challenges.

The RT-HIL test setup, experimental results and insight gained through this study can aid other researchers within this domain in identification of the vulnerabilities that exist, their pervasiveness in deployed equipment/systems and evaluating their impact on future power system monitoring, protection, control, prediction and optimization applications. Additionally, this RT-HIL test-bench can be used to perform rigorous testing of timing equipment and timing security assessment which can lead to the development of new technologies in electric sector reliant on precision timing (such as PMUs), resilient to time-synchronization attacks.

REFERENCES

[1] V. Terzija, G. Valverde, D. Cai, et. al, "Wide-Area Monitoring, Protection, and Control of Future Electric Power Networks," Proceedings of the IEEE, vol. 99, no. 1, pp. 80 –93, Jan. 2011.

[2] R. Burnett , M. Butts and P. Sterlina "Power system applications for phasor measurement units", IEEE Comput. Appl. Power, vol. 7, no. 1, pp.8 -13 1994.

[3] J. DeLaRee, V. Centeno, J.S. Thorp, and A.G. Phadke, "Synchronized phasor measurement applications in power systems", IEEE Trans. Smart Grid, vol. 1, no. 1, pp. 20–27, 2010.

[4] K. Behrendt, and K. Fodero, "The Perfect Time: An Examination of Time Synchronization Techniques", Publication, Schweitzer Engineering Laboratories, Inc., pp 1-18, 2006

[5] "IEEE 1588-2008", IEEE Standard for Precision Clock Synchronization Protocol for Networked Measurement and Control Systems, 2008

[6] "C37.238-2011", IEEE Standard Profile for Use of IEEE 1588 Precision Time Protocol in Power System Applications, 2011

[7] B. Sikdar, and J. H. Chow, "Defending Synchrophasor Data Networks Against Traffic Analysis Attacks", IEEE Trans. Smart Grids, vol. 2, no. 4, pp. 819-826, Oct. 2011

[8] O. Kosut, L. Jia, R.J. Thomas, and L. Tong, "Malicious data attacks on smart grid", IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 645–658, 2011.

[9] T. Kim and H. Poor, "Strategic protection against data injection attacks on power grids", IEEE Trans Smart Grid, vol.2, no.2, pp.326–333, 2011.

[10] D. Shepard , T. Humphreys and A. Fansler, "Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks", Proc. Int. Conf. Critical Infrastructure Protection, 2012

[11] IEEE Standard for Synchrophasor Measurements for Power Systems, IEEE Std C37.118.1-2011, Dec. 2011.

[12] R. Johannessen, S. J. Gale, and M.J.A. Asbury, "Potential interference sources to GPS and solutions appropriate for applications to civil aviation", IEEE Aerospace Magazine, vol. 5, no. 1, pp. 3-9, Jan. 1990

[13] C. Bonebrake, and L. R. O'Neil, "Attacks on GPS Time Reliability", IEEE Security & Privacy, vol. 12, no. 3, pp. 82-84, June 2014

[14] D. P. Shepard, et. al, "Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks", 25th Technical Meeting of Satellite Division of Institute of Navigation, pp. 3591-3605, Sept. 2012

[15] Z. Zhang, S. Gong, A. D. Dimitrovski, and H. Li, "Time Synchronization Attack in Smart Grid: Impact and Analysis". IEEE Trans. Smart Grid, vol. 4, no. 1, pp. 87-98, March 2013

[16] A. Jafarnia-Jahromi , T. Lin , A. Broumandan , J. Nielsen and G. Lachapelle "Detection and mitigation of spoofing attacks on a vector-based tracking GPS receiver", Proc. ION ITM, pp.790 -800 2012

[17] X. Jiang, J. Zhang, B. J. Harding, J. J. Makela, et.al, "Spoofing GPS Receiver Clock Offset of Phasor Measurement Units", IEEE Trans. Power System, vol. 28, no. 3, pp. 3253-3262, Aug. 2013

[18] Opal-RT, "eMEGAsim PowerGrid Real-Time Digital Hardware in the Loop Simulator", Available online: http://www.opal-rt.com/.

[19] IRIG Standard 200-98, IRIG Serial Time Code Formats, May 1998. [Online]. Available: http://www.irigb.com/pdf/wp-irig-200-98.pdf

[20] SEL, "Protection Relays by Schweitzer Engineering Laboratories," available on-line: http://www.selinc.com/protection/.

[21] M. S. Almas and L. Vanfretti, "RT-HIL Implementation of Hybrid Synchrophasor and GOOSE-based Passive Islanding Schemes", IEEE Trans. Power Delivery, vol. 31, no. 3, pp. 1299-1309, June 2016

[22] IEC Standard, "Communication networks and systems in substations - Part 8-1: Specific Communication Service Mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3."

[23] L. Vanfretti, et. al , "A Software Development Toolkit for Real-Time Synchrophasor Applications", Powertech 2013, France, June 2013

[24] T. Van Cutsem, "Description, Modelling and Simulation Results of a Test System for Voltage Stability Analysis," IEEE Working Group on Test Systems for Voltage stability analysis, Tech. Rep., July 2010.

[25] P. W. Sauer and M. A. Pai, Power System Dynamics and Stability, 1998 :Prentice-Hall

[26] IEEE Standard for Interconnecting Distributed Resources with Electric Power Systems, IEEE Standard 1547.2-2008, 2009.

[27] L. Angquist and C. Gama, "Damping algorithm based on phasor estimation", IEEE PES Winter Meeting, 2001, Vol. 3, pp. 1160-1165.

[28] M. S. Almas and L. Vanfretti, "Impact of time-synchronization signal loss on PMU-based WAMPAC applications," IEEE Power and Energy Society General Meeting (PESGM), Boston, MA, USA, 2016, pp. 1-5.

[29] NASPI, "Work group meeting", Oct. 19-20. 2016, Seattle, WA, USA. [Online]. Available: https://www.naspi.org/meetings

[30] IEEE NIST "Timing Challenges in the Smart Grid Workshop", Oct. 26. 2016, [Online]. Available: https://www.nist.gov/news-events/events/2016/10/ieeenist-timing-challenges-smart-grid-workshop