Abstract—The numerous time synchronization performance requirements in the Smart Grid necessitates a set of common metrics and test methods. The test methods help to verify the ability of the network system and its components to meet the power industry’s accuracy, reliability and interoperability criteria for next-generation substations. In order to develop viable metrics and test methods, an IEEE 1588 Testbed for the power industry has been established. To ease the challenges of testing, monitoring and analysis of the results, a software-based testing dashboard was designed and implemented. The dashboard streamlines the performance testing process by converging multiple tests for accuracy, reliability and interoperability into a centralized interface. The dashboard enables real-time visualization and analysis of the results. The paper details the design and implementation of the IEEE 1588 Power Industry Performance Testing Dashboard as well as an update of the preliminary findings from the testbed.

Keywords—IEEE 1588, time synchronization, test methods, conformance testing, PMU

I. INTRODUCTION

Enabling the next-generation automated substation’s ability to gather multitudes of data from intelligent electronic devices (IEDs) will require sufficient contextual data quality. Improved data quality will minimize uncertainty when processing the data to establish situational awareness for more efficient and reliable substation control. The impact of data quality on distributed control algorithms over an asynchronous network have been shown to impact the quality of state estimation [1]. In order to merge the data from heterogeneous sources, accurate timestamps play an essential role in determining cause and effect. The network of substation end devices will require time synchronization with worst-case accuracy on the order of ±1 μs [2]. Reliable, high accuracy time synchronization continues to be difficult to achieve in complex systems [3]. Wide-Area Monitoring Systems (WAMS) can benefit from monitoring the accuracy of time synchronization and assessing the quality of the WAMS applications based on timing accuracy achieved [3]. Similarly, substation monitoring and control applications, which propagate information to the wide area network, also need to have accurate time synchronization as one factor in achieving high quality control models by reducing measurement uncertainty. The IEEE 1588 Precision Time Protocol (PTP) provides a promising solution for enabling network time synchronization over the data line within a substation network. However, IEEE 1588 is a nascent standard. Concerns regarding the ability to reliably maintain 1 μs accuracy need to be addressed. The IEEE 1588 testbed for the power industry provides a neutral venue to characterize factors impacting IEEE 1588 performance and to develop test methods to verify the metrics.

In order to streamline the testing process against the numerous requirements with respect to accuracy, reliability and interoperability, a software-based IEEE 1588 performance testing dashboard has been developed. The dashboard, through a Graphical User Interface (GUI), enables performance monitoring of the IEEE 1588 devices on the network, while providing centralized execution of the test methods, data visualization and analysis of the synchronization accuracy, reliability and interoperability. The dashboard is designed to readily integrate into any IEEE 1588-compatible network as it is based upon the Management Node messages in the 1588 version 2 standard [4]. The metrics used are based on industry requirements [1,5]. This paper introduces a novel means of enhancing the management node features to provide an automated testing dashboard for assessing conformance to the IEEE 1588 standard and IEEE 1588 power industry profile requirements. Additionally, the paper details test methods and results from new test scenarios including ring topology, ring topology link failure, traffic load, interoperability, and security.

II. PERFORMANCE CRITERIA

The dashboard test suites assess the performance of IEEE 1588 devices on the network based where the performance criteria are accuracy, reliability and interoperability as depicted in Figure 1. The implementation currently focuses on the ability of IEEE 1588 devices to reliably maintain the required synchronization under a variety of plausible scenarios.

Factors impacting reliability include the implementation’s capability to maintain synchronization over time in all conditions ranging from ideal, stressed to failure conditions in substation topologies such as linear, star and ring. Stressed
conditions include traffic bursts on the network that could create packet delay variation (PDV), which significantly degrade the synchronization accuracy. Failure modes include loss of network connectivity, during which the substation must maintain synchronization of its network for as long as possible and as close to UTC (Coordinated Universal Time) as possible. The current metrics used to assess the reliability of the synchronization include synchronization offset with respect to the GM, mean path delay between the GM and the OC, and out-of-specification probability of $10^{-4}$. Additionally, the number of security vulnerabilities is also considered a reliability metric.

Cybersecurity is pertinent to the Smart Grid. The National Institute of Standards and Technology (NIST) has developed guidelines for Smart Grid cybersecurity [6]. Therefore, reliability of the synchronization is also dependent upon the ability of the slave node and network to detect and defend against cybersecurity attacks. Thus far, the dashboard includes test methods for Denial of Service (DoS), masquerade, delay, and multicast poisoning.

Interoperability among the IEEE 1588 nodes not only impacts accuracy and reliability, but also has implications on ease of system integration and interchangeability of substation devices. The IEEE 1588 standard specifies many requirements. As a proof of concept, a few have been selected for the current testbed. Among the interoperability specifications that can impact performance, one IEEE 1588 parameter selected for testing is the synchronization (sync) interval. The evaluation method would include a scorecard of the required and optional functions for a specific IEEE 1588 node. Other interoperability metrics include ease of integration and ease of interchangeability.

III. DASHBOARD DESIGN AND IMPLEMENTATION

The dashboard, shown in Figure 2, provides a centralized monitoring interface, automated means of executing test scenarios, visualizing the data in real-time, as well as real-time analysis statistics of the key metrics identified for the IEEE 1588 Power Systems profile [2]. The dashboard enables remote configuration of IEEE 1588 nodes in the network.

A. Management Node

The foundation of the test dashboard relies on the management messages. The IEEE 1588 management messages provide the ability to set and obtain data regarding the performance and status of the IEEE 1588 devices in the network. The management messages provide the ability to remotely and dynamically monitor and configure the network and each IEEE 1588 device.

B. Traffic Simulation

Another component of the testbed that is integrated into the dashboard is the traffic generator. The dashboard enables execution of the traffic generator through the GUI. In order to provide practical test methods, traffic loads representative of next-generation substations need to be simulated. As the traffic characteristics of next-generation substations are not yet available, the first set of simulations is based upon G.8261 Timing and Synchronization Aspects in Packet Networks [7]. The traffic patterns include static, square and ramp. The simulator can generate traffic at up to 100 percent of the network bandwidth using a specified traffic model. The objective is to inject traffic based on the IEC 61850 standard [8] and to simulate networks under heavy duress during a fault occurrence. It is expected that during a fault occurrence, the network will experience frequent traffic bursts. It is imperative to have good synchronization during a fault occurrence to be able to accurately correlate the cause and effect.

C. Graphical User Interface (GUI)

The dashboard monitors the offset of synchronization and mean path delay between the Grandmaster and the ordinary clocks. To see the reliability over time, a histogram displaying the distribution of the synchronization offset is enhanced with color-coded outliers to determine the frequency of occurrence. When nodes are in peer-to-peer (P2P) mode, the delays between the peers are also displayed. The dashboard monitors the current status of the IEEE 1588 devices including the current elected Grandmaster and whether the ordinary clock is synchronized. The status of all the IEEE 1588 nodes, synchronization offsets over time, the distribution of the offsets, and mean path delays are visualized through the GUI in real-time as shown in Figure 2. The dashboard alerts the user when the offset approaches 75 ns and 100 ns, by color-coding the points yellow and red, respectively. The alert thresholds are configurable by the user via the GUI.

![Figure 2. IEEE 1588 Dashboard using an enhanced management node for network configuration, test scenario deployment and results analysis.](image-url)
the slave are also automatically generated for each test scenario.

E. Scalability through simulation

The simulation aims to incorporate virtual versions of common Smart Grid devices, specifically the PMU (phasor measurement unit), into the testbed. PMUs are becoming increasingly important in wide area monitoring and protection schemes. PMUs provide voltage and current phasor measurements to detect anomalies in the grid [9]. PMUs depend on synchronized time for accurate measurements. Therefore accurate clock synchronization on the order of 1 μs of UTC is needed, which is within PTP capabilities. The simulation provides the ability to incorporate realistic synchrophasor traffic into the network [10].

IV. PERFORMANCE RESULTS

The testbed is comprised of redundant PTP Grandmasters (denoted as GM1 and GM2) synchronized to the Global Positioning System (GPS). For the results described in this paper, we used four PTP switches with two different implementations. The PTP switches can be configured as Transparent Clocks (TCs) or Boundary Clocks (BCs). The PTP network currently has five ordinary clocks (OCs) configured in slave mode. OC2, OC3 and OC4 are based upon the same implementation. OC3 has an oven-controlled crystal oscillator (OCXO), while OC2 and OC4 have temperature-controlled crystal oscillators (TCXOs).

Figures 4 and 5 provide a comparison of the results from the link failure scenario between the two protocols. The area shaded in red denotes the time, which port 2 is closed for three minutes and opened and subsequently, port 4 is closed for 3 minutes and opened such that all nodes in the ring would be affected at least once. With RSTP, the network did not maintain the accuracy and reliability requirements. When the link fails in RSTP, packets are not routed correctly, leading to packet loss. The protocol takes about tens of seconds to be able to recover from the failure scenario. The poor synchronization performance is due to lost packets during the link failure. Regardless of the quality of the quartz, the synchronization accuracy of the slave node can be impacted by the loss and re-route of the packets. The re-route of the packets can introduce PDV depending on the location of the node. In Table 1, the maximum offset and out-of-specification probability are shown. For a single run, one OC did not meet the 10⁻⁴ out-of-specification requirement. In contrast, with MRP, where there is a guarantee to respond to a link failure on the order of tens of milliseconds, the results after a link failure expectedly show a consistent synchronization offset within the hundreds of nanosecond range after 50 runs. When a link failure occurs in an MRP ring, the topology is able to maintain the synchronization performance over the network of four switches. Packet loss is minimized, thus maintaining the communication between the GM and the OC. Therefore, the accuracy of the synchronization is not affected.

Table 1. Synchronization accuracy and reliability using RSTP in ring topology with link failures in a 2 hour test

| OC2 | OC3 | OC4 | OC5 |
|-----|-----|-----|-----|
| Maximum Offset (μs) | 1206 | 186 | 191 | 262 |
| 1 μs out-of-specification probability | 4.15x10⁻⁴ | 0.00x10⁻⁴ | 0.00x10⁻⁴ | 0.00x10⁻⁴ |

Figure 4. Ring topology scenario with two link failures at ports 2 and 4.

Figure 5. Synchronization offset with link failure in ring topology using RSTP.
B. Network traffic bursts

Due to fault conditions in the substation, which may result in short but frequent bursts of traffic, this test scenario emulates what would occur when substation data is sampled at high frequencies in order to detect transient fault occurrences. We conjectured that static heavy traffic loads would not impact IEEE 1588 because TCs are able to compensate for the jitter by time-stamping at the ingress and egress ports, therefore removing the PDV. An accurate implementation of the TC should be able to maintain the synchronization accuracy over the four hops. The traffic bursts occur over the duration of two hours. The traffic is injected as square steps, with a period of 1 h, where the minimum network load threshold is at 5 percent and a maximum network load threshold is at 95 percent with each load lasting for 30 minutes. The traffic injected is based upon the traffic model 1 of G.8261/Y.1361 [7]. As shown in Figure 7, the IEEE 1588 devices were configured in a linear topology with three hops, with the slave nodes on the last hop to assess the synchronization performance. The traffic generator node injects packets at the specified percentages into the first hop and absorbs the extraneous traffic from the third hop. To ensure the correct level of traffic is being generated, a network packet analyzer was used to verify the quantity and sizes of the packets. We tested two device implementations on the third hop, TC A and TC B. Results from both TCs indicate that there were no significant time synchronization performance setbacks due to the bursts of traffic as shown in Figure 8. The slaves were able to maintain similar variation in mean path delay with a maximum offset of less than 200 ns. Heavy traffic, with use of TCs, did not have impact on the synchronization of the slaves and the ability of the TCs to time-stamp the messages.

C. Holdover and convergence

The holdover tests provide a view of how the IEEE 1588 nodes would fare without a Master clock. The holdover durations tested include 10 s, 100 s, and 1000 s. With accurate time-stamping in the TC, the IEEE 1588 OCs were able to support holdover between 10 to 100 s while remaining within 1 μs accuracy. Table 2 provides a sample of the synchronization offsets after the node establishes contact with the Grandmaster. OC3 holdover ranged from 200 ns to 2.5 μs, whereas a less stable clock, OC4, drifted 448 ns in 10 s to a drift of 4.7 μs in 1000 s. OC5, which is compromised by a TC introducing a large timing error drifted significantly with a 2.6 μs offset at 10 s. At 1000 s, the maximum offsets of all three OCs went significantly above the 1 μs threshold. It is important to note that since the dashboard relies on the offset responses from the IEEE 1588 slave nodes, it is currently not recording data when it is not synchronized to a Grandmaster. The dashboard will integrate the hardware measurement to be able to provide data during the holdover. In contrast to results from [5], the automation of test deployment enabled more data to be obtained on holdover and convergence patterns. Figure 9 indicates a consistent convergence pattern and duration within seconds over ten iterations, with an hour stabilization period. The holdover dispersion between runs indicates a large range of uncertainty in the behavior of the OC. While the pattern is consistent, the amount of drift can vary significantly. The variation is due to conditions such as ambient temperature, which can contribute to the variation in the drift rates. To address the issue of ambient temperature, using more robust quartz such as an OCXO would guarantee a smaller margin of error. Analyzing and isolating the factors impacting the variation could ensure greater repeatability. However, the initial results indicate devices could benefit from robust shielding to be able to handle ambient conditions within the substations without adversely affecting the synchronization performance.
The method of testing IEEE 1588 security is by exposing the network to attacks and detecting vulnerabilities. Several security vulnerabilities of the IEEE 1588 protocol have been identified [11], [12], [13] and [14]. The attacks implemented include masquerade, DoS, and multicast poisoning. Masquerade enables the attacker to control the synchronization, while DoS and multicast poisoning would leave the slave clocks without a master. The dashboard provides a basic framework to readily deploy the security tests and can be readily extended to include more test methods. Using default configurations, the devices tested succumbed to masquerade, but not the basic DoS attack.

The goal of the masquerade attack is to become the best master clock such that all the IEEE 1588 devices synchronize with the rogue clock. In order for the best master clock algorithm to select this clock, the rogue clock sends an announce message describing itself as the best clock within the network. Once it has been selected as the best master clock it becomes the GM. It can disrupt the accuracy of the time synchronization by periodically sending the sync messages and responding to the delay request. The results have repeatedly indicated the nodes, by default, would synchronize to the new GM. The rogue GM can introduce both obvious offsets, which can be verified by other clocks or it can introduce subtle variations. With IEEE 1588 slaves in default configuration, the vulnerability existed on all devices in the network.

For multicast poisoning, IEEE 1588 is using multicast packets to communicate between the devices. This attack aims at isolating a device from the IEEE 1588 multicast group. It continuously sends Internet Group Management Protocol (IGMP) Leave packets, which notify the network that a device is leaving a multicast group. The vulnerability would prevent an OC from receiving any multicast IEEE 1588 messages, and therefore compromise the synchronization. The multicast poisoning attack will only work if the IEEE 1588 BCs and TCs are taking into account the IGMP messages. The testbed is currently configured for broadcast messages, so the vulnerability does not exist by default.

To realize the DoS attack, the test overloads the Grandmaster with IEEE 1588 delay request messages from different slave nodes, which prevent the Grandmaster from sending the Sync packets to synchronize the other devices. This attack was partially successful on our testbed, some transparent clocks were able to detect the DoS attack and close the port where it was coming from. A more advanced DoS attack, where the packets are disguised as originating from multiple sources, was successful on all the nodes.

### E. Interoperability

Interoperability test methods are being developed by implementing the IEEE 1588 management messages for retrieving and configuring IEEE 1588 parameters. Additionally, requirements specified by the profile can also be included into the dashboard conformance test method suite. The purpose is to determine whether the required or optional functions are available to enable both improved performance and ease of management. The interoperability tests evaluate both the percentage of required functions available as well as the percentage of optional functions available. To extend to the power industry requirements, the performance of the IEEE 1588 devices can be compared against the IEEE 1588 Power Profile requirements.

In addition to verifying the existence of the required features, the dashboard provides additional analysis capabilities to verify the implementation performs to the specified configuration. For example, one interoperability test includes the ability to query the synchronization frequency available and then for each frequency determine the actual number of synchronization packets received within a specified window of time. Figure 10 displays the results from the synchronization rate where the left column is the specified log sync interval, the middle column show the rates and actual number of packets received when the test goes from a log interval of -3 to 3, and the last column show the rates and actual number of packets where the interval range is 3 to -3 to ensure the ability for rapid transition between interval specifications in both directions.

![Figure 10](image-url) Interoperability test for synchronization rate.

### V. Conclusion and Future Work

The IEEE 1588 Test Dashboard enables network time synchronization performance monitoring and streamlines performance testing through a centralized GUI. It automates the execution of test methods for evaluating the accuracy, reliability and interoperability performance criteria against the
IEEE 1588 version 2 standard and IEEE 1588 profile for the power industry. The dashboard is also easily extensible to include IEEE 1588 profiles from other industries. The dashboard has significantly eased the testing and data acquisition process. It enables the deployment of a series of test scenarios and the ability to readily repeat the series of tests to optimize the consistency of the different iterations by minimizing the variables introduced when running the tests manually. Increasing the number of repeatable runs ensures sufficient data can be collected and statistically analyzed. The dashboard can also be utilized by vendors and customers to measure the performance of their network of IEEE 1588 devices based on the criteria discussed. An open-source version of the IEEE 1588 dashboard software is planned for release to allow testing against the IEEE 1588 standard as well as the power profile.

Additional test scenarios were implemented and investigated through the new dashboard software. The dashboard enables remote configuration of a ring network allowing automated testing of a ring topology by opening and closing the ring to simulate link failures. Additionally the traffic generator was integrated into the testbed network, where the dashboard can execute the script to enable various types of traffic loads to deploy various traffic patterns and models.

Furthermore, the dashboard provides a prototype of how vulnerability testing can be developed and deployed. Though only a limited number of devices were available for test, by default, each node was vulnerable to at least some of the cybersecurity attacks. Therefore, it is imperative for the network administrator to ensure perimeter security for the IEEE 1588 devices in the network given the cybersecurity requirements of the Smart Grid [6]. To protect the network against these attacks, one solution is to implement Annex K of IEEE 1588 [6]. However, vulnerabilities have also been found and must be addressed [15]. A complete solution would be a secure protocol along with a security policy for the entire network [6].

Interoperability can also be a significant challenge to achieving the performance and reliability necessary to meet the power industry requirements. The dashboard implementation provides a prototype of how conformance testing can be executed via the Management Node messages in addition to profile requirements. In addition to verification of IEEE 1588 capabilities required in the profile, such as the accuracy requirement, the dashboard can also serve as a means to display the status of all the IEEE 1588-enabled based on the Management Base Information (MIB) Objects [2].

Future work on the test dashboard will include integration with the hardware synchronization offset measurement [5]. The focus will also include development of test methods for security, interoperability as well as adherence to the IEEE 1588 Power Profile industry requirements. Additional security tests, such as replay and delay attacks, as well as countermeasures will be implemented. The performance impact of the countermeasures will also be analyzed. A substation network simulation will also be integrated. The current IEEE 1588 simulation is limited in to replicating the effect of the synchronization protocol on each node's simulated local time. Future work will involve replicating the IEEE 1588 protocol down to each individual packet within the simulation. Along with the bridge between the physical testbed and simulation, this will allow the virtual nodes to act as IEEE 1588 slaves, exchanging synchronization messages with a real world grandmaster clock. The simulation would transition towards building a virtual substation network model synchronized with IEEE 1588. The testbed will also continue to expand to characterize new metrics impacting the performance criteria of IEEE 1588.

ACKNOWLEDGMENT

We would like to thank Jerry Stenbakken, James Gilsinn, Kevin Brady, Galina Antonova, Kang Lee and the IEEE PSRC WG, and numerous others who provided support and suggestions on the development of the testbed.

REFERENCES

[1] D. Anand, J.G. Fletcher, Y. Li-Baboud, and J. Moyne, “A practical implementation of distributed system control over an asynchronous Ethernet network using time stamped data,” IEEE Conference on Automation Science and Engineering, August 21-24, 2010, Toronto, Canada.

[2] IEEE Standard Profile for use of IEEE 1588™ Precision Time Protocol in Power System Applications, IEEE Power System Relaying Committee and Substations Committee, July 2011.

[3] S. Meliopoulos and A. Bose, “Substation of the Future: A Feasibility Study,” Power System Engineering Research Center Publication 10-17, October 2010.

[4] IEEE 1588-2008, Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems, IEEE Instrumentation and Measurement Society, TC-9, The Institute of Electrical and Electronics Engineers, Inc., New York, NY, 24 July 2008.

[5] J. Amelot, J. Fletcher, D. Anand, C. Vasseur, Y. Li-Baboud, and J. Moyne, “IEEE 1588 Testbed,” IEEE International Symposium on Precision Clock Synchronization, September 2010, Portsmouth, NH.

[6] NISTIR 7628, Guidelines for Smart Grid Cybersecurity, September 2010.

[7] G.8261/Y.1361 Timing and Synchronization Aspects in Packet Networks. ITU-T Recommendation.

[8] IEC 61850 Communication Networks and Subsystems in Substations.

[9] R.E. Wilson, “PMUs”, IEEE Potentials, vol. 13, pp. 23-26, 1994.

[10] M. Chenine, Wide Area Monitoring and Control Systems – Application Communication Requirements and Simulation. PhD Thesis, KTH Royal Institute of Technology, 2009.

[11] A. Treytl, G. Gaderer, B. Hirschler, R. Cohen, “Traps and pitfalls in secure clock synchronization,” Precision Clock Synchronization for Measurement, Control and Communication, 2007. ISPCS 2007. IEEE International Symposium on , vol., no., pp.18-24, 1-3 Oct. 2007.

[12] J. Tsang, K. Beznosov “A Security Analysis of the Precise Time Protocol,” Technical Report, Vancouver, Canada, Laboratory for Education and Research in Secure Systems Engineering (LERSSE), University of British Columbia, LERSSE-TR-2006-02, 4 December, 2006, pp.20.

[13] G. Gaderer, A. Treytl, and T. Sauter, "Security Aspects for IEEE 1588 based Clock Synchronization Protocols," IEEE International Workshop on Factory Communication Systems (WFCS06), Torino, Italy, pp. 247-250, June 2006.

[14] Ullmann, M.; Vogeler, M.; "Delay attacks-Implication on NTP and IEEE 1588 time synchronization," IEEE International Symposium on Precision Clock Synchronization for Measurement, Control and Communication, Brescia, Italy, pp.97-102, Oct. 12-16, 2009.

[15] Treytl, A.; Hirschler, B.; “Security flaws and workarounds for IEEE 1588 (transparent) clocks,” IEEE International Symposium on Precision Clock Synchronization, Brescia, Italy, pp.1-6, Oct. 12-16, 2009.