IMPROVED PROTECTION RELIABILITY WITH PTP MASTER IMPLEMENTATION IN PROTECTION RELAYS

Harjinder Sidhu	***Harsh Vardhan***	***Chu Cheng***	***Emmoji Vundekari***
AltaLink	*GE Grid Solutions*	*AltaLink*	*GE Grid Solutions*
Canada	USA	*Canada*	*India*

1. ABSTRACT

Advanced power-system, protection-and-control applications using IEC 61850 sampled values (SV) require a time-synchronization accuracy of 1 microsecond and better. Any inconsistency in the time-reference among the merging units results in phase-angle errors, which might lead to mis-operation of protection functions and harmonic measurement inaccuracies.

IEC 61869-9 recommends using either Precision Time Protocol (PTP) or one pulse per second (1PPS) inputs to achieve the required accuracy. PTP has emerged as the preferred synchronization method because it offers several advantages over 1PPS. These advantages are an in-built mechanism to switch seamlessly between multiple master clocks, and PTP distributes easily over a substation Ethernet network.

Generally, the PTP synchronization requires one or more Global Navigation Satellite System (GNSS) clocks, which synchronize the merging units and protection-and-control devices to a common global reference. This makes GNSS clocks a critical component in protection-and-control systems. Failure/loss of these GNSS devices has adverse effects on related power-system applications.

This paper discusses implementing PTP master-clock functionality in protection relays and how it simplifies the substation protection-and-control architecture and increases reliability and availability of protection-and-control applications.

Note: In this paper, the terms "protection-and-control device", "IED" and "relay" are used interchangeably.

2. IMPORTANCE OF TIME SYNCHRONIZATION IN PROCESS BUS

In process-bus applications, all the merging units and protection relays must have the capability to accept an external time reference so that the sampled values from different merging units are synchronized to a common time reference [2]. The measuring phase-angle error depends on the degree of deviation in the time reference among the merging units. The applications such as protection, control, metering, and synchrophasors are sensitive to the measured phase-angle difference among different merging units and require that the sampled values from these merging units must be synchronized to a common time reference. The preferred time synchronization methods to achieve the required accuracy for protection and monitoring applications are the following [1] [2]:

Precision Time Protocol (PTP)

1 PPS

IRIG-B

An IED using sampled values from multiple merging units, must have all the sampled values synchronized to a common time reference.

If the protection, measurement and control applications are distributed across the power system or depend on the absolute date and time, then the common time reference should be a "global time-traceable" time source such as a "locked" GNSS clock; e.g., applications based on phasor measurement units (PMUs), travelling-wave fault location (TWFL), line-differential protection, etc., must have all the required sampled values synchronized to a common global reference. If the global time source becomes unavailable for any reason, these applications become unavailable or are blocked.

For other protection, measurement and control applications that need only the sampled values from the local site, the common time reference need not to be a "global time-traceable" source; these applications continue to operate as long as there is a common time source. Unavailability of satellites, loss of GNSS antenna, etc., would not affect these applications.

Applications that require only sampled values from a given merging unit do not need the sampled values to be synchronized at all. If, for a distance protection relay the required currents and voltages are published from a given merging unit, then the merging unit is not required to be synchronized to any time reference.

Merging units indicate the state of synchronization using the "SmpSynch" field in the sampled values. If the sampled values are not synchronized, then "SmpSynch" is set to "0." When the sampled values are synchronized to a "global" clock at the required accuracy range, then "SmpSynch" is set to "2." When the sampled values are synchronized to a "local" clock at the required accuracy range, then "SmpSynch" is set to either "1" or to a clock-unique identifier number, ranging from "5 to 254." [2]

2.1 PROCESS-BUS TIME SYNC REQUIREMENTS

IEC 61850 specifies a standard communications model to facilitate interoperability across vendors. IEC 61850 Part 9-3 covers the timing protocol requirements, particularly in process bus, which was built on top of the IEC 61588 – Standard precision clock synchronization protocol for networked measurement and control systems (PTP). Over time, PTP has evolved as a common method of time synchronization across the digital substation network. This protocol leverages the dedicated PTP hardware that time stamps the packets on ingress to and egress from the device ports, which enables more accurate propagation delay calculations in the network.

IEC 61869-9 is a standard describing general requirements for instrument transformers. It specifies IEC 61588-based time synchronization in accordance with the profile specified in IEC 61850-9-3 (Power Utility profile), which further clarifies that a total network accuracy of 1 μs must be achieved with approximately 15 transparent clocks and 3 boundary clocks in the communication path [5]. IEC61869-9 specifies that the "time error" caused by a network element is the deviation from the reference signal to the generated synchronization messages and the "time inaccuracy" is the time error not exceeded by 99.7 % of the measurements evaluated over a series of 1,000 measurements, when the clock is in a steady state [2]. The requirements about time inaccuracy for various clock types are the following [5]:

- Grand Master (GM) clock shall have time inaccuracy smaller than 250 ns
- Transparent clock (TC) shall have a device time inaccuracy smaller than 50 ns, which is measured between the synchronization messages at ingress and egress ports
- Boundary Clock (BC) shall have a device time inaccuracy smaller than 200 ns, between the port in SLAVE state and any port in the MASTER state

However, a rigorous network design is required to achieve the required time inaccuracy considering the placement and number of BCs and TCs. A larger time inaccuracy might lead to deviations among the merging-unit time references and can cause protection misoperation.

IEC61869-9 specifies how a grandmaster capable clock adjusts its clockClass parameter in PTP messages to indicate the traceability to a GPS reference. While the grandmaster is synchronized to the primary time reference signal the clockClass is set to 6. When the global time reference signal is lost and the clock switches to the holdover mode, the clockClass is set to 7 [5]. In the holdover period, the clock internal oscillator drives the required accurate time. Internal oscillators drift over time. When the clock time error exceeds 250 ns, the clockClass is set to 52. When the clock time error exceeds 1 μs, the clockClass is set to 187 [5]. When the primary reference is restored, the clockClass switches back to 6.

With network-based time distribution protocols, it is common to experience a disturbance/loss in the network path or switching device and clock-source failure. To mitigate the failure modes in the networking layer, different redundancy protocols are in practice, which include parallel redundancy protocol (PRP), and high-availability seamless redundancy protocol (HSR). Each of these protocols has its own merits and demerits, and the choice of protocol depends on the application needs. To adopt to these redundancy protocols all the clocks must be doubly attached to redundant network paths.

3. ISSUES WITH EXISTING ARCHITECTURES

The process-bus implementations (both IEC 61850 9-2LE [1] and IEC 61869-9 [2]) have been in use for a while and many utilities have successfully implemented digital substation solutions by different vendors. A simplified and commonly used process-bus network hierarchy is shown in Figure 1.

The major components of the process bus network are the following:

- Merging unit
- Time synchronization source
- Ethernet switch
- Protection relay or IED

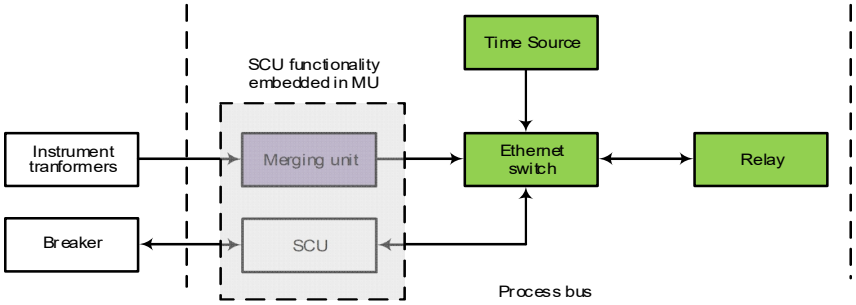

Figure 1. Simplified process bus

While the process-bus-based solutions provide several benefits, it brings a distinct set of issues for overall reliability and availability of the Ethernet-based protection and control functions.

Compared to the conventional hard-wired system, the additional components required for a process-bus-based system impact the reliability of the system, and in turn impact availability of the system. Usually, system failure is related to the unavailability of the time-synchronization sources. The loss of GNSS reference, failure of the time synchronization source or a communications failure with the clock source might lead to unavailability of the protection-and-control system. The clock source could be unavailable because of many internal or external factors, such as jamming or spoofing. There have been many papers discussing the vulnerability of GNSS to spoofing and jamming, and how it adversely affects the power industry.

One of the other growing concerns in utilities is cyber-attacks on communications-based, protection-and-control infrastructures. Within process bus, one of the vulnerable components for cyber-attacks and RF interference is the time source as these receive time information from a GNSS receiver using low-power radio frequency (RF) signals from satellites in the L band (between one and two GHz). Thorough cybersecurity and NERC CIP compliance considerations should be made when designing the process-bus system.

4. PTP MASTER CLOCK FUNCTIONALITY IN PROTECTION RELAYS

Synchronization-source failure can be mitigated by introducing redundancy in the timing network. However, adding redundancy impacts the overall cost of the project. This paper discusses implementation of the PTP master clock functionality in protection-and-control IEDs to reduce dependency on external time clocks and improve the overall system reliability and availability.

In general, protection-and-control devices only implement PTP “Slave-only” functionality (a state machine for slave-only implementation, described in IEC 61588 [4]). When the PTP grandmaster is not reachable or not usable, the substation IEDs run freely based on an internal oscillator, and the protection-and-control functions might become unavailable, as per Section 2 of this paper.

In this implementation, the protection-and control-device (IED) implements the full PTP state machine (state machine for full implementation, as described in IEC 61588 [4]). In this case, the IED becomes a PTP “Ordinary clock;” the IED serves as a source of time or might synchronize to another clock.

“Ordinary clock” or “Master-Slave” configuration is generally used when the IED is configured to be the primary PTP grandmaster clock.

“Ordinary clock” or “Master-Slave” configuration could also be used when the IED is connected to an Ethernet network with other PTP master-capable clocks. In this case, the IED runs the Best Master Clock Algorithm (BMCA) on its ports and if a better master is found on the network, the IED becomes the PTP slave and synchronizes to the available grandmaster clock. In the event of failure of the existing grandmaster, the IED takes over as the PTP grandmaster.

Therefore, “Ordinary clock”/ “Master-Slave” configuration could be used to define the protection-and-control IED as a backup PTP grandmaster. As soon as a better grandmaster becomes available again, the operation mode of the IED is forced to be “slave.”

Also, it is possible to force the IED to be a “Slave-only” clock. In the “Slave-only” mode, the IED behaves as a typical protection-and-control IED and synchronizes to the available PTP grandmaster clock.

A simplified PTP Ordinary clock (Master-Slave) state machine is illustrated in Figure 2 [4]. For simplicity, the rest of the PTP states (INITIALIZING, FAULTY, DISABLED, UNCALIBRATED, PASSIVE and PRE_MASTER) in BMCA are not shown.

- When the IED starts, the PTP state machine is in the LISTENING state
- If ANNOUNCE messages are received from an existing grandmaster clock, the recommended PTP state is SLAVE, and all the process-bus clocks are synchronized to the grandmaster
- If no ANNOUNCE messages are received from the grandmaster, the recommend PTP state is MASTER and the IED starts sending the ANNOUNCE and SYNC messages using its own local clock. In this case, the rest of the clocks are synchronized to the IED clock

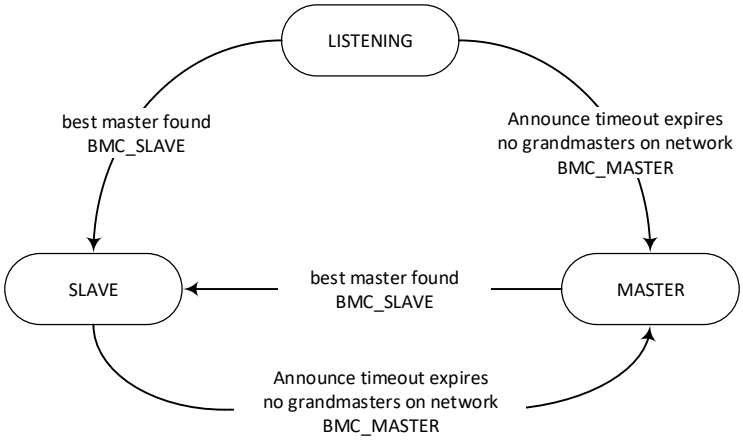

Figure 2. Simplified Master-Slave PTP state machine

- While the protection and control IED is acting as the local PTP master, and the ANNOUNCE messages are received from another grandmaster (or from any master better than the IED local clock), the BMCA recommend state is SLAVE and the relay stops publishing the ANNOUNCE messages. Then, all the clocks in the process bus switch to the new grandmaster

The relay’s default PTP dataset attributes (defaultDS.priority1, defaultDS.priority2 and defaultDS.clockQuality) are initialized in such a way that the relay becomes grandmaster only when no dedicated grandmaster clocks (with GPS reference) are available in the network [7].

5. RELIABILITY AND ARCHITECTURES

This section compares the net mean time between failure (MTBF), reliability and availability for some basic-substation, protection-and-control architectures. In this analysis the protection relay requires data from four merging units to protect the system without any degradation. Unavailability of data from any of the merging units renders the protection system unavailable.

Typical architectures with protection relays having PTP Master functionality are illustrated in systems (a) and (a’) in Figure 3, and systems (b) and (b’) in Figure 4.

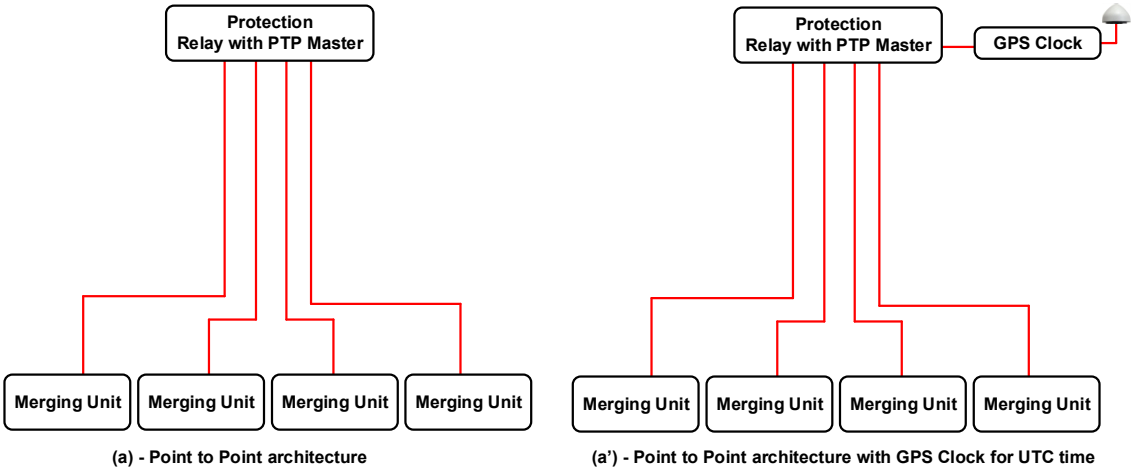

Figure 3. Point-to-point architecture

System (a) in Figure 3 is a point-to-point architecture in which all the merging units are connected to the protection relay using direct fiber cables. The protection relay has a built-in PTP master clock, which synchronizes all the connected merging units using IEEE 1588 power [6] (or power utility [5]) profile and drives the common clock reference.

System (a') Figure 3 is an extension of system (a), where an external GNSS-based, time-sync source is added for UTC time keeping. The relay global time could be provided by using either IRIG-B or PTP, and is used only for timestamping events, files etc. Unavailability of the GNSS clock does not compromise the protection availability and reliability of the system. However, cybersecurity remains a concern.

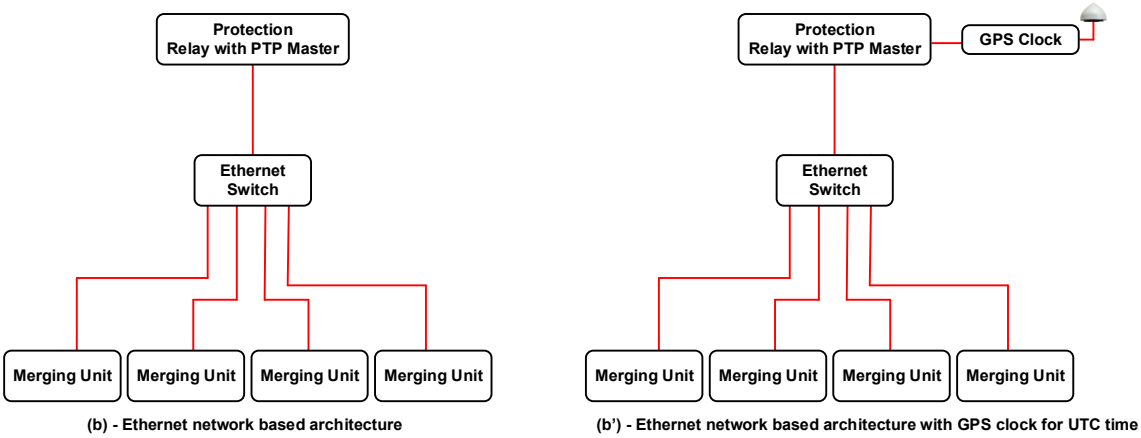

Figure 4. Ethernet network-based architecture

System (b) in Figure 4 is an Ethernet network-based architecture, which is an extension to system (a) shown in Figure 3. All the merging units and protection relays are connected using an Ethernet switch. The protection relay synchronizes the merging units using IEEE 1588 over the Ethernet network.

System (b') in Figure 4 is an extension to system (b) where an external GNSS-based, time-sync source is added to the network for UTC time keeping. Unavailability of the GNSS clock does not compromise the protection availability and reliability of the system.

System (c) in Figure 5 is a standard Ethernet network-based, process-bus architecture. An external clock synchronizes all the devices. Unavailability of the time-sync signal causes unavailability of the protection system. System (d) in Figure 5 is an extension to system (c), where a redundant time-sync source is added to remove the protection dependency on a single clock.

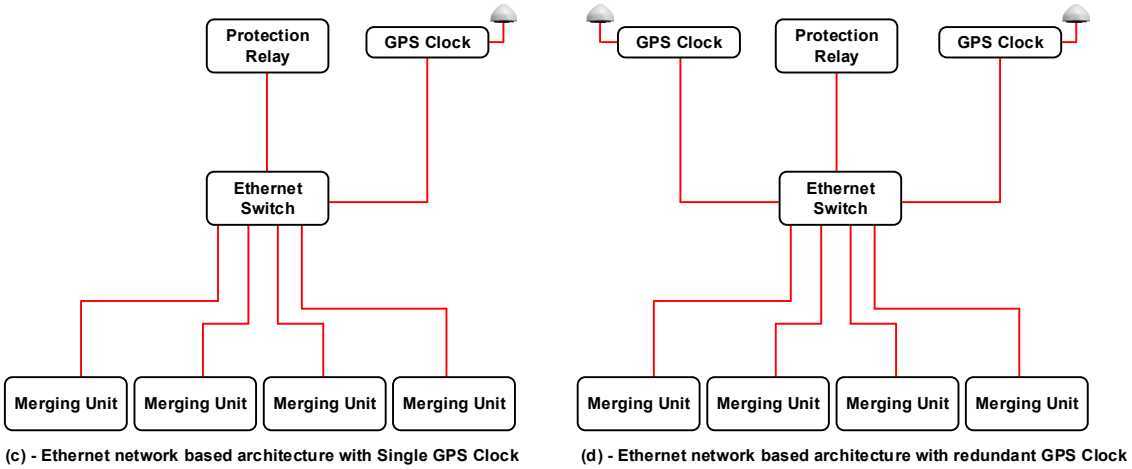

Figure 5. Ethernet network-based architecture with GPS clock(s)

For simplicity, all IEDs such as protection relays, Ethernet switches, merging units and GNSS clocks (including antenna) are considered to have an MTBF of 100 years and mean time to repair (MTTR) of one day. The net system MTBF, reliability and availability after 10 years for different system architectures are presented in Table 1.

Table 1. MTBF, reliability and availability comparison

MTBF = 100 Years; MTTR = 1 Day			
System	**System MTBF**	**Reliability at 10 Years**	**Availability**
System (a), (a')	21.15 years	62.3 %	99.9869 %
System (b), (b')	18.16 years	57.8 %	99.9846 %
System (c)	15.10 years	51.8 %	99.9820 %
System (d)	17.30 years	56.1 %	99.9845 %

As shown in Table 1, the architectures (a) and (a') have the largest MTBF, reliability and availability. However, this does not mean that these architectures are always the most optimized solution. The availability and reliability of the other architectures could be improved significantly by using redundant clocks and networks with PRP/HSR. This added reliability comes at the price of increased cost of equipment, complexity of the system, and increased engineering, testing and commissioning time.

Generally, the cost of the IEDs and other aspects are not the main driving factors for large transmission stations. Moreover, a protection relay has the greatest probability of being taken out of service for testing, troubleshooting, setting changes, and logic changes than a standalone GNSS clock. Therefore, having PTP Master clock functionality might not add much value to transmission architectures. However, there is a good business case for distribution substations, where reducing capital cost and system complexity are the main concerns.

5.1 USE CASES

A typical distribution substation and corresponding network architecture are shown in Figure 6 and Figure 7, respectively. Two fully redundant, multi-feeder, protection relays manage the entire substation; the relays connect to the merging units using point-to-point architecture. All the merging units are synchronized using IEEE 1588 PTP with protection relays acting as the PTP Grandmaster and the merging units acting as the slave-only devices. The merging units run the Best Master Clock Algorithm (BMCA) to select the best master, as per IEC 61850-9-3.

A global time-sync source is connected to the relays using IRIG-B or PTP to maintain the UTC time in the relays for time stamping of events and files. This architecture can be extended for several feeders.

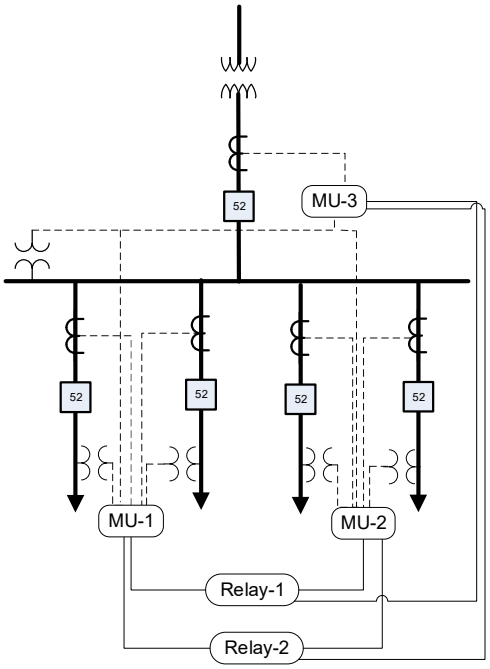

Figure 6. Typical distribution substation

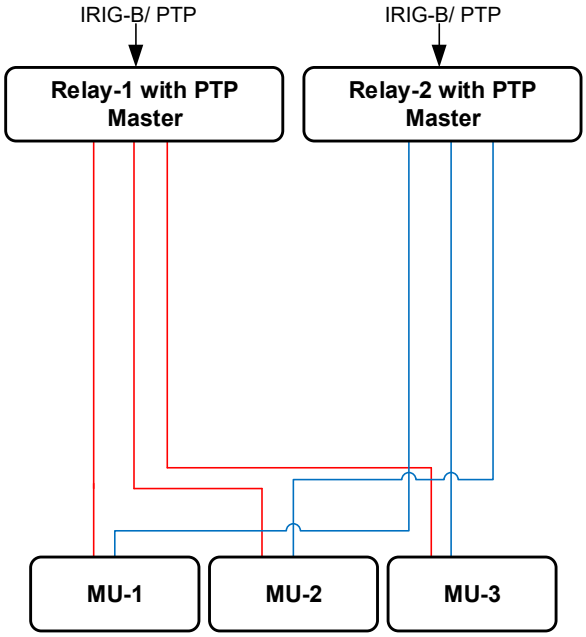

Figure 7. Substation protection-and-control architecture

Another use case is to use the protection-and-control device as the backup grandmaster in the Ethernet based architectures. The protection relay can be configured with required priority 1 and priority 2 fields so that GNSS clock is selected as the grandmaster by BMCA, by default. The protection relay becomes grandmaster only when the primary GNSS clock is lost or is out-of-service.

5.2 INTEROPERABLE POINT-TO-POINT ARCHITECTURES

In the past, most of the point-to-point communications architectures were not interoperable because these were based on proprietary communications protocols and time-sync mechanisms. One of the reasons for the use of proprietary communication was the lack of an industry standard for a high-accuracy, Ethernet-based, time-sync protocol. IEEE 1588 PTP solves this need. With the wide adaptation of PTP and implementation of the PTP

master-clock functionality in protection relays, it is now possible to have point-to-point, vendor-agnostic, and interoperable protection-and-control architectures [7].

6. CERTIFICATION OF PROTECTION RELAYS AS GRANDMASTER CLOCKS

The IEEE Conformity Assessment Program (ICAP) has developed a certification program to certify that clocks meet the requirements of the PTP standard and its associated power-profile specific parameters for IEEE C37.238-2017 and IEC/IEEE 61850-9-3 2016.

At the time of writing this paper, the present version, v1.22, of IEEE 1588 Power Profile Conformance Test Suite Specification (TSS) does not recognize the grandmaster clocks that are not connected to a recognized, standard time source. The authors have requested IEEE and the respective working groups to investigate it and update the TSS accordingly.

7. CONCLUSIONS

This paper focused on the issues related to reliability and availability of protection-and-control functions with existing process-bus architectures when affected by time-synchronization source failure. Implementation of PTP master functionality in protection relays improves the reliability of the process-bus system and reduces the number of devices required and the risk of cyber-attacks. Also discussed are the implementation aspects of PTP master functionality in protection relays. Some typical process-bus architectures, compliant with IEC 61850-9-2LE and IEC61869-9, showed good net MTBF, reliability and availability after a period of 10 years. With the PTP master implementation in protection relays, it is now possible to have the interoperable point-to-point architectures.

REFERENCES.

[1] Implementation Guideline for Digital Interface to Instrument Transformers Using IEC 61850-9-2, Raleigh, NC; UCA International Users Group, 2004.

[2] IEC 61869-9:2016 Instrument transformers –Part 9: Digital interface for instrument transformers, Geneva, SW; IEC, 2016.

[3] IEC 62439-3:2016 Industrial communication networks – High availability automation networks –Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR), Geneva, SW; IEC, 2016.

[4] IEEE Std. 1588-2008. IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems, New York, NY; IEEE, 2008.

[5] IEC/IEEE 61850-9-3 Edition 1.0 2016, Communication networks and systems for power utility automation – Part 9-3: Precision time protocol profile for power utility automation, Geneva, Switzerland; IEC, 2016.

[6] IEEE Std. C37.238-2017, IEEE Standard Profile for Use of IEEE 1588™ Precision Time Protocol in Power System Applications, New York, NY; IEEE, 2017.

[7] "GE D60 Instruction manual", GE publication code: 1601-0089-AL1, Part number: 1601-0089-AK1 (November 2020)