# Using Software-Defined Network Technology to Precisely and Reliably Transport Process Bus Ethernet Messages

D. J. Dolezilek
*Schweitzer Engineering Laboratories, Inc.*

Presented at the
14th International Conference on Developments in Power System Protection
Belfast, United Kingdom
March 12–15, 2018

# Using software-defined network technology to precisely and reliably transport process bus Ethernet messages

**D. J. Dolezilek***

*Schweitzer Engineering Laboratories, Inc., 2350 NE Hopkins Court, Pullman, WA 99163 USA,
dave_dolezilek@selinc.com

**Keywords:** Digital messaging, protection signals, GOOSE, SV, copper reduction.

## Abstract

The implementation of a digital process bus using IEC 61850 Sampled Values (SV) is a challenging task. Protection engineers are comfortable with traditional protection systems where copper conductors bring analog secondary signals directly from substation voltage and current transducers to the relay terminals. To begin using SV systems, these engineers must learn about digital system components and their effects on relaying applications. New SV components include merging units, high-accuracy time sources, process bus Ethernet switches, and SV relays. The focus of this paper is on maximizing the performance of process bus Ethernet communications.

## 1 Introduction

The availability of electric power is important to both developed and developing countries, but it is arguably more important in the latter where its impact on improving standards of living is much more dramatic. However, planning and implementing enhancements to the electric power system is much more complicated in developing countries. Limited financing must be balanced among improvements to economic development, energy conservation efforts, and power system additions. Power system improvements are often the most capital-intensive efforts under consideration and may require the majority of a country's scarce financial resources. Therefore, investments in power system modernization and expansion must be made in the most cost-effective manner possible to maximize the immediate effects and reduce system lifecycle costs.

One of the major costs in any energy control system, including electric power systems, is the installation of traditional copper wiring between the control and automation devices and the field sensors and actuators. Many exciting technologies for wire reduction have been used for years and have field-proven results. However, these digital technologies should be applied with great care so as to ease the installation and ongoing maintenance of these technologies in remote and high-priority systems. One such application, wire reduction via digital communications, requires great precision so as not to adversely affect power system protection, monitoring, and control. These applications replace expensive traditional methods of information exchange via energy transfer across copper wires with digital messages across fiber cables.

Capital expenditures can be reduced when devices called intelligent merging units (IMUs) are co-located with the sensors and actuators. These IMUs digitize the field signals, publish them in IEC 61850 Sampled Values (SV) messages over communications cables, and reduce the amount of copper wiring needed. Several Ethernet communications technologies exist to effectively communicate digitized values from the IMUs at the process level with the sensors and actuators, but their success depends entirely on the performance of the packet delivery system across the local-area network (LAN). During the past decade, while the specifications of the international communications standards for IEC 61850 SV over Ethernet have been evolving, a new technology called software-defined networking (SDN) has become available. SDN dramatically improves LAN behavior to perform LAN packet delivery, fault detection, and recovery of data exchange, and it therefore improves SV applications.

Protection system redundancy is best achieved with two independent systems, such as dual-primary protective relays communicating using robust dual-primary LANs. In this way, when there is a fault present in the Primary A system, the Primary B system remains in service. This is an N-1 condition. When this happens, it is quite clear that the communications network must be resilient and detect, isolate, and reconfigure around a communications failure in order to preserve the operation of the Primary B protection functions. This becomes an N-2 requirement for the entire system and also an N-1 for either dual primary in the presence of a fault on the other primary. Process bus Ethernet-based communications introduce new challenges because of the high message rate and the distributed nature of SV systems. Similar to GOOSE-assisted protection schemes, SV applications require redundant paths or messages to support an N-2 system requirement and N-1 failure recovery scheme in either dual primary in the presence of a permanent fault on the other primary. This resiliency is accomplished with new protocols or engineering designed to perform fast detection, isolation, and reconfiguration of the process bus Ethernet network. Protection engineers need to ensure that the Ethernet-based process bus is fast, secure, and reliable, capable of meeting their most stringent protection application requirements.

Methods to quantify, characterize, and manage the delivery of protection signals via process bus are important in addressing engineers' concerns. Process bus communications call for a

new, yet practical, approach for verifying communications speed, security, and reliability during factory acceptance, site acceptance, and commissioning testing.

This paper (a shortened version of [1]) describes the components of the SV system and discusses communications network engineering challenges, solutions, and tools available to provide and verify a reliable Ethernet packet transport in the process bus system. Special attention is given to the design of large substations, which need to securely merge the station bus and the process bus into a single, substation-wide network.

This paper explains the technical issues that have been addressed during the past decade of SV technology development and explains how these issues are resolved with the use of SDN for process LAN packet switching and fault recovery. The resulting technical advances lead to improved performance, fewer faults in the power system, and reduced maintenance efforts, which result in lower lifecycle costs for electric power improvements. By maximizing the effect of the financial resources expended in electric power system enhancements, these power system improvement projects also help make developing economies more self-sufficient while improving local standards of living.

## 2 Substation Ethernet wire reduction via digital messaging

Several types of digital messages exist to digitize and bidirectionally communicate process-level data and controls across fiber cables. Protocols that are typically used for digital message communications include MIRRORED BITS® communications, IEC 61850 GOOSE, IEC 61158 EtherCAT®, IEEE C37.118 synchrophasor messages, and IEC 61850 SV [2]. The associated communications network for any and all of these message types is referred to as the process bus.

The reliability and performance of a process bus Ethernet LAN relies on packet switching in normal situations and on Ethernet fault detection, isolation, reaction, and reconfiguration during a failure. To achieve high availability requires a packet switching and fault recovery method that continues to work in the presence of one or more faults in the system.

Although very comprehensive, IEC 61850 was created to standardize power system management and the associated information exchange, and it intentionally does not define power system apparatus requirements or expected behavior. This leaves the need and opportunity for further standardization of Ethernet networking, diagnostics, and test procedures to other technical committees.

## 3 Process bus intelligent device development

The block diagram in Fig. 1 illustrates the logical separation of the process level, the bay or unit level, and the station level related to the instrumentation and control of the protection, control, and monitoring process with digital messaging via a shared Ethernet LAN. In this example, the process-level LAN and station-level LAN are separated and are managed by different Ethernet switches. This clearly illustrates the apparent complexity of this method compared with simply installing the relay at the process level. This traditional process bus merging unit concept requires the correct operation of four devices in the process level (rather than that of a single microprocessor-based multifunction relay): an intelligent breaker controller, a time synchronization source, a merging unit, and an Ethernet switch or several switches interacting as a process LAN [3].

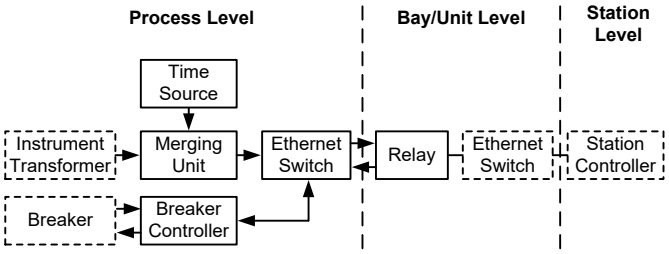


Fig. 1. Simplified substation block diagram indicating core devices and their traditional associated logical levels

The block diagram in Fig. 2 illustrates several key elements of a modern process bus installation. The changes to the process level include combining the functionality of the merging unit, breaker controller, and breaker-related protection functions into the same physical device. This improves the reliability of the system by having fewer devices and simplifies the process of installing redundant functionality. Further, it provides breaker-related protection availability even if the process bus LAN should fail [4].

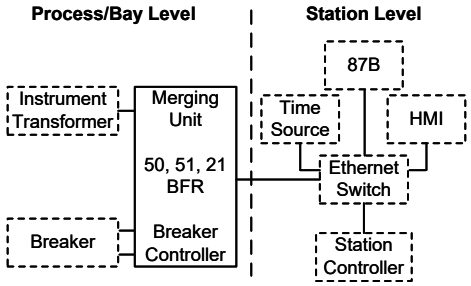


Fig. 2. A modern, full-featured merging unit installation with local protection and control

Changes to the station level include the multicasting of digital messages containing instrumentation and control information to several devices. These devices include other relays on the substation bus, such as a differential bus protection relay that needs information from several locations and therefore requires several merging units. Other devices include the operator human-machine interface (HMI) and the station-level controllers. This message multicast behavior and the numerous sources and destinations for the digital messages require a shared-bandwidth Ethernet network.

When a relay or other device with capabilities beyond analog-to-digital conversion is used as a merging unit, it is referred to as an IMU. The difficulty and expense of building IMU devices to survive harsh environments for 20-plus-year lifespans led to the existence of less functional, nonintelligent merging units. As with communications-assisted logic via protection signal exchange in the station bus, process bus designers must

consider the desired distribution of functions when choosing merging units, IMUs, relays, and controller devices.

Modern process bus solutions, which require three to four times as many devices as traditional methods, provide wire reduction and additional functionality but increase the cost and potentially reduce the reliability of the systems. However, when designed and managed correctly, these modern methods can provide a wealth of new station-wide functions and features. These functions and features can be achieved and maintained if the new digital messaging and Ethernet packet switching system is made to be as precise and available as the rest of the protection system. The following sections of this paper analyze new methods of process bus message monitoring and diagnostics as well as LAN designs for deterministic message exchange.

IEC 61850-9-2 describes the SV messaging technology for process bus applications and introduces the information that is now available via digital messaging to support the development of new and improved applications. The SV solution based on switched Ethernet packets requires specific attention to detail to overcome existing issues of signal loss and delay, creates more confidence in reliable packet delivery, and has become more widely accepted. In order to be effective, any process bus technology solution based on IEC 61158 EtherCAT, IEC 61850-9-2 SV, or IEC 61850 GOOSE must satisfy the following requirements:

- Easily support both digital SV communications interfaces and traditional analog, hardwired terminations on the merging units, IMUs, and other devices.
- Allow the flexibility to meet new and existing user expectations.
- Meet and exceed industry and user requirements for availability, reliability, and resilience.

Allow logic to be distributed among various merging units, IMUs, and other devices.

## 4 IEC 61850 Edition 2: Validating correct publication of all Ethernet packet signal messages

The IEC 61850 communications standard describes the use of multicast Ethernet frames to exchange sensor and actuator information and protection automation signals via GOOSE and SV messages. Multicast Ethernet packet exchange works in a publish-subscribe pattern where data providers, called publishers, create and publish GOOSE and SV messages. These messages are received by data consumers, called subscribers. Multicast messages are not addressed to specific subscribers so that they can be delivered to multiple subscribers based on the configuration of the LAN. Also, data consumers can subscribe to multiple publication streams in order to obtain information from numerous publishers in the system. This system supports the reuse of information by sending it to multiple subscribers and provides scalability of the system size and features.

Each publisher is unaware of the message delivery to the intended subscribers. Therefore, the validation of the message publication can only confirm the behavior of the publisher and the contents of the digital message being published. To validate SV publication, each publishing device must maintain and produce information about the message configuration and real-time performance of the outgoing SV publications. The publisher calculates and stores information for each of the SV messages that it publishes. This information is available in a human-readable format report via an engineering access connection and via a poll-and-response interaction with a data concentrator [5].

The SV transmit message report contains configuration information including the SV control reference, multicast address media access control (MAC), priority tag, virtual LAN (VLAN), application identifier (AppID), data set reference, SV identifier, and test SV mode state [5].

## 5 IEC 61850 Edition 2: Validating correct reception of all Ethernet packet signal messages

The only accurate way to monitor the correct delivery of Ethernet packet messages is to keep track at the receiver. Ethernet packet messages for protection and high-speed automation signal transfer include GOOSE, SV, and line current differential (87L) [5] [6].

In order to validate SV subscriptions, each subscribing device maintains and produces information about the message configuration and the real-time performance of the incoming SV subscriptions. The publisher calculates and stores information for each of the SV messages to which it is subscribing. This information is available in a human-readable format report via an engineering access connection and via a poll-and-response interaction with a data concentrator. The subscriber uses the following SV message configuration information to validate that the SV message is from the intended source and matches the engineered subscription design. SV messages that do not match a pre-engineered configuration are discarded. The SV receipt message report must contain information including the following [6]:

- Message configuration information, including the SV control reference, multicast address MAC, AppID, data set reference, and SV identifier.
- Message status, including the priority tag received with message, VLAN received with message, publisher error code received with message, SV ID error, sample count error, SV configuration revision mismatch, sample synchronization mismatch, protocol data unit (PDU) length error, and status indicators (such as SV stream is lost, failed message quality, SV message received late, SV message received out of sequence, SV simulation mode, SV test mode, and network delay).

- Period of time over which the statistics were collected—the statistics must be collected and displayed for each SV subscription including the accumulated downtime duration, maximum duration of continuous downtime, out-of-sequence count, and the total number of discarded frames for any of the previously described error codes.
- Message status history, which must retain statistics for the last several failure events for each SV subscription.

SV subscription list, including the AppID, the control block reference, and the subscription status with error codes (if applicable) for all the configured SV subscriptions.

## 6 Process bus LAN packet switching acceptance criteria

The previous sections indicate the numerous features of SV messaging used to observe all of the characteristics of message exchange behavior in order to confirm correct power system operation and to diagnose problems. Publishers and subscribers must be designed to work as a system to achieve and monitor appropriate performance. The LAN packet switching devices must also be designed to work as a system to achieve and monitor the necessary performance in order for them to be part of the SV application. The system of LAN packet switching devices must satisfy the following acceptance criteria:

- The network delay is designed to be 1 ms and must never exceed 7 ms.
- The network message delivery is designed to be 100 percent, and the worst-case delivery failure caused by the LAN packet switching devices must not exceed two consecutive undelivered messages in each SV message exchange.
- The network message delivery is designed to be 100 percent, and the worst-case message corruption caused by the LAN packet switching devices must not exceed two consecutive corrupted messages in each SV message exchange.

SV messages are published every 208.3 µs. A network downtime duration of greater than 417 µs due to reconfiguration prohibits the delivery of two consecutive SV messages in an exchange. A network downtime duration of greater than 625 µs due to reconfiguration prohibits the delivery of three consecutive SV messages in an exchange. Therefore, a network downtime duration due to the reconfiguration of the LAN packet switching devices is designed to be zero, and the worst-case network downtime duration due to reconfiguration must not exceed 600 µs so that the LAN packet switching devices can reestablish packet delivery in fewer than 625 µs.

## 7 SDN for process bus LAN

SDN provides a fundamental change to Ethernet packet switching and fault recovery within communications networks by decoupling the part of the system that determines what to do with packets (i.e., the control plane) and the parts that actually switch and forward the packets (i.e., the data plane) [6]. Spanning tree algorithms (STAs), supported by Rapid Spanning Tree Protocol (RSTP) Bridge Protocol Data Unit (BPDU) messages, are the traditional method for managing Ethernet LAN switching and fault recovery. With careful attention to detail, data flow engineering, and precise configuration, settings, and topologies, these traditional Ethernet mechanisms satisfy mission-critical communications applications. However, even at their best, STAs cannot guarantee packet delivery of the process bus protocols. More importantly, STAs require extensive staging and testing to identify the packet switching behavior and determine if it is satisfactory. The complexity of STAs arises from the fact that each packet switching device is running its own algorithms to perform the control decisions and the data-forwarding actions. This increases the time required to detect and isolate a fault and then perform recovery of the data flow. Also, each device must be individually configured initially as part of an interactive system design and then reconfigured individually when changes need to be made to the network. When applications change, this may require changing the configuration of many end devices and packet switching devices. A logical illustration of the separation of the devices making the control decisions and performing the data-forwarding actions (based on SDN) is shown in Fig. 3. SDN dramatically improves the ability to predesign data flow rules and greatly simplifies the configuration of the packet switching devices within the network. SDN also provides numerous and important packet monitoring and diagnostic functions that do not exist in traditional STA networks.

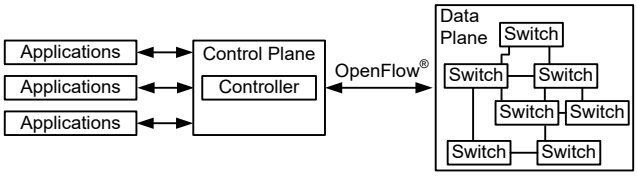


Fig. 3. SDN architecture overview

When using an STA, designers plan and configure the bridge priority, port priority, path cost, and port behavior settings for the STA logic. The STA creates shared-bandwidth paths with combined data flows based on the devices and the physical cables. STA logic forces the network to disable all but one active connection to each end device. Each STA switch individually and continuously attempts to decide the best course of action to forward each packet based on STA logic and BPDU exchange. These choices influence the outcome of the STA logic, but the few settings available in STA technology within information technology-class (IT-class) switches do not provide the control or determinism required for station bus or process bus communications. The settings in operational technology-class (OT-class) switches *do* satisfy the control and determinism required for station bus communications via STA logic but not for process bus communications. An OT STA switch detects and isolates a failure, reroutes the data flows, and reestablishes packet delivery in fewer than 7 ms within a switch and in fewer than 15 ms among multiple switches in a well-designed network.

SDN provides many more settings and much better and faster control over the packet switching functions for each data flow, not just each cable.

The SDN control plane is designed prior to installation with knowledge of all the system communications, connections, and switches. This design serves as a packet switching and fault recovery system model that is staged in a laboratory and then tested with a battery of real-time fault scenario simulations to verify correct behavior. This is similar to the process of using real-time digital simulation to test power system models for short circuits and other fault scenarios. After testing and commissioning, the switches are loaded with the rules from the pre-engineered control plane, and then they simply execute the data flow rules after each LAN fault event instead of determining what to do via logic.

SDN eliminates the need to force physical links to be inactive if they create redundant packet flows, which are not allowed in STA LANs. The ability to define and design data flows onto specific cable and switch paths with SDN means that it is not necessary to leave any cables unused to prevent packet loops, as is necessary in STA LANs. Therefore, each cable and switch combination can be used for both primary and failover paths. Also, the two Ethernet connections to an end device can function simultaneously in numerous modes, including failover, isolated, and pass-through. The network and end devices can be designed to publish and deliver duplicates of a single packet of signal information or redundant packets with two different payloads of signal information. Based on this different functionality, SDN can be used to create redundant active and fast failover data paths within one physical network, whereas an STA LAN cannot.

Using a variety of methods, SDN technology uses the pre-engineered design to calculate data flow settings. Efficient execution of these settings allows for the detection of and reaction to LAN faults to quickly create a fast failover path. Once loaded into the SDN switches, these settings effectively become if-then-else statements that are meant to be executed in real time. These pre-engineered rule sets detect and isolate failures, reroute data flows, and reestablish packet delivery in fewer than 100 µs. This means that the network experiences no packet loss, or at the most it loses the frame that is actively being transmitted from a buffer at that instant. This behavior confirms that SDN satisfies all of the process bus LAN packet switching acceptance criteria. Also, any fault in an SDN network is quickly isolated to a small section of the LAN and does not affect other parts of the network. Fast failover groups are predesigned and sent to the SDN switches, which then use the egress port in the group with the highest priority to forward the packet. If that port is in a fault state, the SDN switch immediately detects this without the need for an STA and immediately uses the port with the next highest priority. If both of those ports are unavailable, the SDN switch uses the egress port with the third highest priority to forward the packet, and so forth. By forwarding a packet to this group of three ports, the SDN device can detect and react to a fault based on pre-engineered rules within microseconds, as shown in Fig. 4.

In this example, a fast failover group in the switch on the left is designed to use Port 3 to transmit SV messages from the IMU to the relay. If Port 3 or the cable connected to it fails, the switch detects the failure immediately and executes if-then-else rules to decide within 100 µs to transmit the packet out Port 4 instead.

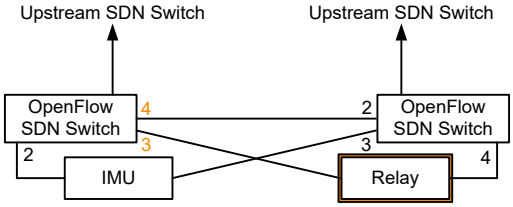


Fig. 4. SDN fast port failover

SDN works on the deny-by-default principle, meaning that no packets are forwarded unless they meet a pre-engineered data flow rule. This function is also referred to as "whitelisting," and it is the basis for firewall functionality at geographic or functional LAN boundaries. All non-whitelisted packets are dropped so that they do not consume network bandwidth and do not reach any end devices or network boundaries. Alternatively, all non-whitelisted packets can be sent to an intrusion detection system for further analysis. Also, maintenance rules can be sent to the network to seamlessly reroute data flows around specific pieces of hardware. This allows those devices to be removed and serviced without affecting the data flow or the applications that it serves [6].

## 8 Process bus LAN and communications engineering design

The engineering design effort for process bus communications is the same regardless of the packet switching and fault recovery mechanism chosen, such as STA or SDN. Unfortunately, some designers do not perform all the necessary design requirements, so the effort appears to be less for STAs than for the deny-by-default and purpose-built data flow design of SDN. However, when the lifecycle of a system for packet switching, fault recovery, segregation, and cybersecurity (from specification and design to building, testing, and maintaining the system) is considered, SDN requires less effort and is lower cost. During the design phase of either an STA or SDN process bus LAN, users must specify the system design and create the following documents to support the design:

- Application requirements.
- Device and connection topology.
- Packet switch topology, packet flow paths, and fault recovery strategy.
- Data flow design.
- Device-specific communications-assisted protection and control master signal I/O lists.
- Truth table matrix of device signals identified as hardwired inputs, hardwired outputs, process bus digital message inputs, and process bus digital message outputs among all devices.

- Truth table matrices of GOOSE and SV messages with process bus digital message inputs to be received and outputs to be transmitted by each device.
- Message-specific control reference information (including intelligent electronic device [IED] name, logical device instance, logical node class, and generic substation event control block name), multicast address MAC, AppID, data set reference, VLAN, priority, and SV identifier list.
- LAN connection list, including switch identification numbers and port numbers for the primary, dual-primary, or failover port connections to the LAN for each port on each publisher and associated subscriber device.
- Cybersecurity segregation and filtering plan.

Segregation plan to isolate the multicast data link layer traffic (referred to as Layer 2 of the Open System Interconnection [OSI] network model) from the network link layer traffic, considered Layer 3.

## 9 Conclusion

Traditional methods of power system information exchange include moving currents and voltages via long runs of copper wiring from field sensors at the process level to terminals directly on the protective relays and control devices in a control building at the station level. These methods are well understood but labor-intensive, time consuming, and expensive. It is necessary to understand and implement appropriate LAN packet transport and recovery technologies for use in electric power system expansions to satisfy increasing global demands. We need new technologies, new standards, and new industry practices. To deploy systems more quickly and with lower expense, we need to rely on fewer but more highly skilled people and shorter deployment times. Cost reduction is predominantly found in the reuse of information once it is digitized by multicasting signals to several subscribers from each publisher. Also, costs are lowered when the digitization of analog values is moved further into the process level and closer to the sensors and primary equipment, which reduces the need for copper wiring.

The data flow for an IEC 61850 GOOSE and SV message solution is a straightforward concept of using digital messaging over a fiber cable or Ethernet packet switching network. These technologies digitize and transmit bidirectional information between equipment in the substation yard and the relay in the control house. However, the less straightforward effort is in determining the appropriate packet switching and fault recovery technology to satisfy process bus messaging requirements, as explained in this paper.

When adding or expanding electric power generation, transmission, and distribution systems, it is imperative that new technologies be used and installed in resilient and cost-effective ways. It is also important that protection, monitoring, and control systems have low installation costs, low lifecycle costs, and high availability and resilience.

## References


[1] D. Dolezilek, "Taking Full Control of Your Process Bus LAN Using New Ethernet Packet Transport Technologies," proceedings of the International Conference and Exhibition – Relay Protection and Automation for Electric Power Systems, Saint Petersburg, Russia, April 2017.

[2] D. Dolezilek, D. Whitehead, and V. Skendzic, "Integration of IEC 61850 GSE and Sampled Value Services to Reduce Substation Wiring," proceedings of the 12th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2010.

[3] V. Skendzic, I. Ender, and G. Zweigle, "IEC 61850-9-2 Process Bus and Its Impact on Power System Protection and Control Reliability," proceedings of the 9th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2007.

[4] D. Dolezilek and F. Ayello, "Collaboration Leads to Modular Protection and Control Solutions That Satisfy IEC Security and Dependability Requirements," proceedings of the CIGRE Study Committee B5 Colloquium, Minas Gerais State, Brazil, August 2013.

[5] D. Dolezilek, J. Dearien, and M. Van Rensburg, "Lessons Learned and Successful Root Cause Analysis of Elusive Ethernet Network Failures in Installed Systems," proceedings of the International Conference and Exhibition – Relay Protection and Automation for Electric Power Systems, Saint Petersburg, Russia, April 2017.

[6] D. Dolezilek, C. Gordon, and D. Anderson, "Fast Fault Detection, Isolation, and Recovery in Ethernet Networks for Teleprotection and High-Speed Automation Applications," proceedings of the Power and Energy Automation Conference, Spokane, WA, March 2016.




20171107 • TP6844