Using Real-Time Testing Tools to Baseline the Performance of OT Networks for High-Speed Communications

Luca Delli Carpini
E-Distribuzione

Amandeep Kalra, David Dolezilek, Giorgio Vielmini, and Tim Grigg
Schweitzer Engineering Laboratories, Inc.

Presented at the
7th Annual PAC World Americas Conference
Virtual Format
September 1–2, 2020

Originally presented at the
15th International Conference on Developments
in Power System Protection, March 2020

Using Real-Time Testing Tools to Baseline the Performance of OT Networks for High-Speed Communications

Luca Delli Carpini, E-Distribuzione
Amandeep Kalra, David Dolezilek, Giorgio Vielmini, and
Tim Grigg, Schweitzer Engineering Laboratories, Inc.

Email: papers@selinc.com

Italy and USA

1 Introduction

Ethernet networks have gained popularity in the operational technology (OT) world because of the obvious advantages of blending multiple communications protocols on the same cable, allowing for a greater number of devices to exchange information at a higher data exchange rate as compared to serial-based communications protocols. However, using Ethernet for power system applications presents challenges for accurate and precise mission-critical machine-to-machine protection signal exchange via multicast Ethernet packets and requires careful consideration. Ethernet networks are nondeterministic in nature and were designed for dynamic information technology (IT) environments. By contrast, the applications served by OT networks have predictable bandwidth requirements, which necessitate detailed engineering to meet the stringent requirements for power system applications. In addition, the available testing tools have been designed to test the networks from an IT perspective. E-Distribuzione in Milan—having experienced all of these issues—decided to build a laboratory to quantify the performance of the Ethernet networks using international standards as references.

In this paper, we discuss the following:

- Different standards that can be used as references to design Ethernet networks for OT applications.
- Various key performance indicators for network performance.
- Real-time test tools that quantify Ethernet network performance.

2 E-Distribuzione Smart Grid

E-Distribuzione manages the electricity distribution network and is responsible for the delivery of electrical energy to customers in Italy. E-Distribuzione has been updating distribution substations with remote control and automation to reduce failures and create a “smart” electricity network.

The electric network is typically composed of a primary substation (PS) with high-voltage-to-medium-voltage (HV-MV) transformation as well as MV lines that feed three automated and remotely controlled secondary substations (SS1, SS2, and SS3), as shown in Fig. 1. SS3 is connected to a neighboring circuit via a normally open breaker in a border station (SSB). Breakers are controlled by intelligent electronic device (IED) relays protecting the MV lines in the PS and the secondary substations. The protection devices in both are compliant with IEC 61850 and communicate protection signals via Generic Object-Oriented Substation Event (GOOSE) messages across the substation local-area networks (LANs) and the wide-area network (WAN).

The WAN communications network, based on Long-Term Evolution (LTE) wireless technology, has a hub-spoke architecture, as shown in Fig. 1, and is promoted for use in performing smart fault selection (SFS) logic via multicast messages among secondary stations and between the primary and secondary substations.

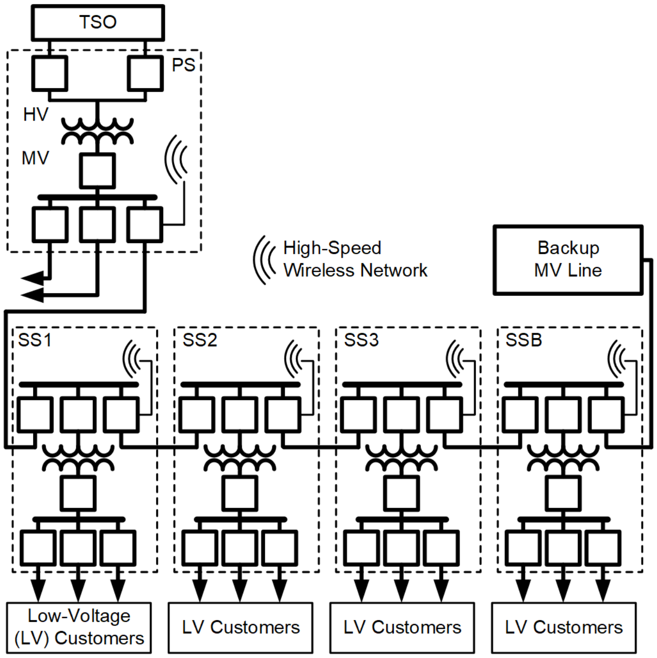


Fig. 1. Example portion of the E-Distribuzione electric network.

To ensure correct message transportation, E-Distribuzione required the WAN to satisfy the following criteria [1]:

- Secure transport of the IEC 61850 GOOSE messages and Manufacturing Message Specification commands over a wireless WAN.
- Reliable transport of multicast IEC 61850 GOOSE messages.
- Latency of message delivery as low as possible between all combinations of protection devices, and small enough to be sufficient for the applications.
- Support of up to 100 devices in each substation.

3 Design of E-Distribuzione SFS

SFS is based on the multicast and interrupt-driven exchange of fault information via GOOSE messages between protection devices.

The GOOSE messages transport topological information, which is expressed by a unique number calculated by the supervisory control and data acquisition (SCADA) system based on the real-time network topology. The payload of the GOOSE message changes when the power system network changes configuration for operation, maintenance, or faults.

The subscription of GOOSE messages is based on the various connections to each secondary substation. For example, SS2 in Fig. 1 subscribes to GOOSE messages from the relays installed in SS1 and SS3.

The operating principle of SFS is done in three steps: fault selection, isolation of the faulted network branch, and closing the breaker at the border (SSB) to connect the backup hot-standby line.

4 Example Operation of E-Distribuzione SFS

For a fault between SS2 and SS3, the fault is detected by the protective relay IEDs installed in the PS and SS1 and SS2. Using the SFS logic selectivity scheme, each relay determines if it should trip immediately or delay to allow a different breaker to separate the faulted segment. After the fault is detected, the protection devices in SS1 and SS2 send a GOOSE message with the fault detection information to the relays in each station. Each subscribing relay evaluates this information; then, based on its own geographic position, each relay decides to use a short delay time (allow fast trip operation) or prolonged delay time (block fast trip operation).

In this example, the result is that relays in the PS and SS1 are in the block state (prolonged delay), the relay in SS2 is not delayed, and the relays in SS3 and SSB do not detect the fault. Afterward, the breaker in SS2 is opened by the protection command.

The second step of SFS logic is to isolate the fault. The relay in SS2 checks the open state of the breaker and the absence of the line voltage. If these conditions are met, and the protection device is aware of the direction of the fault, the relay sends a GOOSE remote-trip command to the neighboring protection devices in SS3. The relay that receives the remote-trip checks the absence of the voltage. If the condition is validated, then it sends an open command to the associated breaker. As shown in Fig. 1, opening the breaker in SS2 and SS3 isolates the branch of the network affected by the fault.

The third step of SFS is to close the SSB. The relay that has isolated the fault sends a GOOSE remote-close signal to the relay in the SSB. This relay checks the absence of the voltage and sends the close command to the breaker. At this stage, the border breaker routes an alternative power source to the section of the electric network that has been isolated from the fault.

SFS follows the same steps if the fault occurs between the PS and SS1 or between SS1 and SS2. If the fault occurs between SS3 and SSB, the border breaker is not closed by the SFS logic. In this case, the relay in SS3 opens the breaker but restoration via the alternative source is not possible.

5 IEC 61850 GOOSE Exchange Service-Level Specifications

Communications-assisted applications need to satisfy numerous service level specifications, including many related to the performance of the underlying application. The IEC 61850-90-4 Technical Report provides advice on network engineering and commissioning. Section 5.3.17 describes network testing, recommending that a network's communications design be verified and that network performance be tested for requirement compliance during both factory and site-acceptance testing [2]. This technical report also requires that an appropriate subset of the tests should continue to monitor the network during operation, to detect and mitigate failures and ensure conformance to the service level agreements (SLAs) that the service provider has agreed to meet. Since relays that publish GOOSE message data are unaware of multicast message delivery, signal exchange between those and data subscribers must be monitored by each subscriber.

6 Signal Exchange SLA Based on International Standards

The list of international standards necessary to define IEC 61850 GOOSE signal message delivery performance and quality are described in [3].

Identified in the related standards, above, communications acceptance criteria have become the founding basis of the SLAs that are provided to end users. The SLAs that satisfy protection and distribution automation criteria are quite strict. Ongoing fulfillment of these SLAs is necessary for the safe and reliable operation of communications-assisted automation, so the values are used to understand performance degradation and associated risk. Problematic outliers are used to provoke root-cause analysis and service improvements. Designers may choose to request stricter acceptance criteria; however, IEC 61850 GOOSE exchange SLA, based on these standards, must at minimum do the following:

- Document a signal exchange success rate greater than 99.99 percent.
- Document configuration and real-time details to support diagnosis and troubleshooting of substandard signal exchanges.
- Achieve an expected LAN signal transfer time between devices of less than 3 milliseconds.
- Achieve an expected signal transit via LAN of less than 1 millisecond.
- Document a maximum data delivery time between devices within a substation LAN of less than 0.25 cycles.
- Document a maximum data delivery time between devices external to a substation, across a WAN, of between 8 and 12 milliseconds, as illustrated in Table I.

Table I
Substation Line Protection and Control Communications Performance Requirements

Data/Application	Maximum Delivery Time
Breaker tripping and breaker failure initiate	0.25 cycles*
Backup breaker tripping (after breaker failure time-out)	8 to 12 ms
Break reclosure, including voltage-supervised and multiple	8 ms
Send/receive trip command	2 to 8 ms
Initiate lockout function (not in mechanical lockout)	16 ms
Motor-operated disconnect	16 ms
Indicator control (on, off, blink, etc.)	1 s
Testing of trip and block channels	1 s

*Actual breaker operation may take 1.5 to 8 cycle*s*

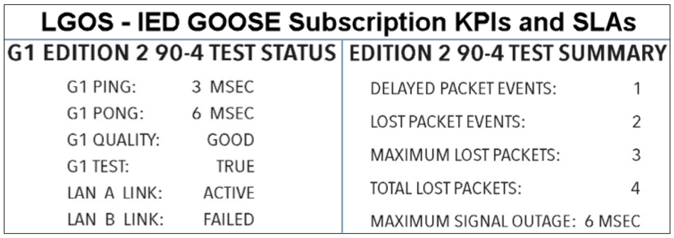
7 Key Performance Indicators to Verify IEC 61850 GOOSE SLA

Each subscribing relay must uniquely monitor and validate each protection signal exchange. In the case of GOOSE messages, each exchange is supervised in real time to confirm its integrity before its contents are used for communications-assisted protection, automation, and control. The metrics necessary to confirm satisfaction of an SLA are referred to as key performance indicators (KPIs). The IEC 61850 GOOSE KPIs and related SLA, monitored by GOOSE subscribing relays, include the following:

- Subscriber devices detect and document delayed GOOSE messages for each subscription (SLA 1).
- Subscriber devices detect and document undelivered, lost GOOSE messages for each subscription (SLA 1).
- Subscriber devices detect and document maximum quantity of packets lost in a single event, total aggregate quantity of packets lost, and maximum outage time as the duration of time in which GOOSE messages are not received for each GOOSE subscription (SLA 1).
- Subscriber devices create and store GOOSE message receipt reports containing message configuration information as well as message status, including priority tag, virtual LAN (VLAN), state number, time-to-live (TTL) value, sequence number, and error code for each subscription. In this case, the TTL value is recalculated in real time and represents the expected time duration before receipt of the next GOOSE message (SLA 2).
- Subscriber devices create and store a TTL count (SLA 1).
- Subscriber devices create and store an out-of-sequence count (SLA 1).
- Subscriber devices create and store a decode error count (SLA 1).

8 E-Distribuzione SFS Initial KPIs and Tests

In-service subscriber relay KPIs, as illustrated in Fig. 2 and summarized by Table II, provide important metrics that are measured on a regular basis. SLA reports include the metric, target performance level, and interval for the report. An example KPI metric design for a GOOSE signal exchange and IEC 61850 logical node for GOOSE service subscription (LGOS) with extensions is shown in Table II.



LGOS - IED GOOSE Subscription KPIs and SLAs

G1 EDITION 2 90-4 TEST STATUS		EDITION 2 90-4 TEST SUMMARY	
G1 PING:	3 MSEC	DELAYED PACKET EVENTS:	1
G1 PONG:	6 MSEC	LOST PACKET EVENTS:	2
G1 QUALITY:	GOOD	MAXIMUM LOST PACKETS:	3
G1 TEST:	TRUE	TOTAL LOST PACKETS:	4
LAN A LINK:	ACTIVE	MAXIMUM SIGNAL OUTAGE:	6 MSEC
LAN B LINK:	FAILED		

Fig. 2. Example subscriber IED GOOSE KPIs displayed on IED front panel.

Table II
Example KPI Metric Design

KPI Component	Description
Metric	Availability of communications-assisted protection scheme measured as successful receipt of each Ethernet GOOSE packet from publisher
Target performance level	Zero undelivered GOOSE messages received from publisher since last IED reset
Format1	Message failure indication in real time as IED front-panel human-machine interface (HMI) alarm
Interval1	Updated in real time
Format2	Message failure indication in real time as status to substation monitor and SCADA via digital messages
Interval2	Updated in real time, and interrupt-driven messages
Format3	GOOSE event report, including out-of-sequence count, TTL count, decode error count, buffer overflow count, message lost count, maximum message lost count, total downtime, and maximum downtime notification
Interval3	Updated in real time, and report available on demand
Format4	History of GOOSE event reporting
Interval4	Updated in real time, report available on demand, and most recent 32 detailed events stored in IED

The essential KPIs were not available in the existing E-Distribuzione relays, so test engineers chose to use a separate test device that could provide them. Since the latency measurement requires distributed time synchronization, they decided to perform an initial test of a subset of SLA 1 KPIs and then add more KPIs for SLAs 2–6 in the future. The plan was to create a baseline for the GOOSE exchange on a LAN in the laboratory, then compare it to the substation LAN, and finally compare it across the LTE WAN.

9 E-Distribuzione OT Testing and Real-Time Monitoring Tools

E-Distribuzione required a tool that could provide the data used to quantify the network performance (based on the KPIs identified in previous sections) independent of the publishing relay's manufacturer. Each unique subscribing relay had to be monitored to validate each protection-signal exchange. E-Distribuzione located a tool that has the following capabilities.

9.1 GOOSE Repetition Monitor

The tool stores certain values when the message state number increments by one. For a fixed, user-selected time interval, the values stored include the sequence number, packet arrival time, and the time difference between the current and the last sequence—if there is no other state change. If the state does otherwise change within that user-selected time interval, then that value is stored instead.

9.1.1 Jitter

The tool calculates the time differences between consecutive packets to determine if there is any jitter in the network.

9.1.2 Report

The tool generates a report with repetition number, time stamp, time difference, and the log of state changes for each user-defined fixed time interval.

9.2 GOOSE Reception Monitor

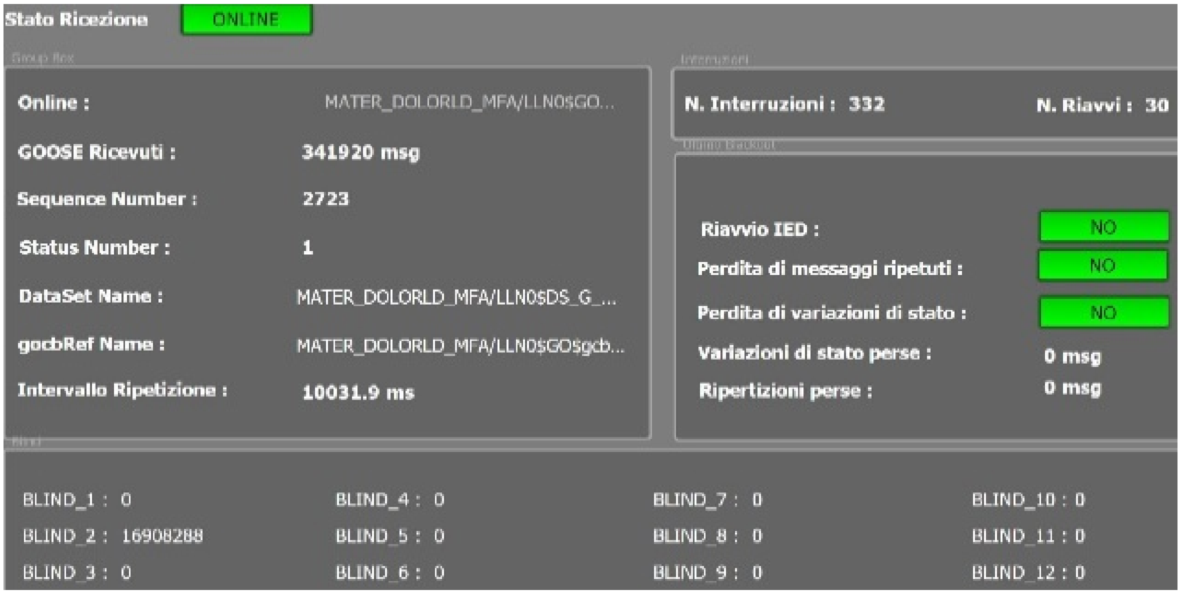
The tool records the time stamp of the first GOOSE message (GOOSE Online). It also has two counters—one for GOOSE missed and one for GOOSE received. The GOOSE message counters increment by one as follows:

- IF [$\text{sqNumn}_{I-1} + 1 \neq \text{sqNumn}_I$ AND $\text{stNumn}_{I-1} + 1 = \text{stNumn}_I$] OR [$\text{sqNumn}_I = 0$ AND $\text{stNumn}_{I-1} + 1 \neq \text{stNumn}_I$], then the GOOSE missed counter increments by 1.
- WHEN [$\text{sqNumn}_{I-1} + 1 = \text{sqNumn}_I$ AND $\text{stNumn}_{I-1} + 1 = \text{stNumn}_I$] OR [$\text{sqNumn}_{I-1} = 0$ AND $\text{stNumn}_{I-1} + 1 = \text{stNumn}_I$], then the GOOSE missed counter has to be stored with time stamps and then reset.
- WHEN [$\text{sqNumn}_{I-1} + 1 = \text{sqNumn}_I$ AND $\text{stNumn}_{I-1} + 1 = \text{stNumn}_I$] OR [$\text{sqNumn}_{I-1} + 1 = 0$ AND $\text{stNumn}_{I-1} + 1 = \text{stNumn}_I$], then the GOOSE received counter increments by 1.
- WHEN [$\text{sqNumn}_{I-1} + 1 \neq \text{sqNumn}_I$ AND $\text{stNumn}_{I-1} + 1 = \text{stNumn}_I$] OR [sqNumn + 1I-1 = 0 AND $\text{stNumn}_{I-1} + 1 \neq \text{stNumn}_I$], then the GOOSE received counter has to be stored with time stamps and then reset.

9.3 Further Requirements

The tool also uses the real-time utility Subscribe to “blind” GOOSE messages used for logic selectivity. It stores GOOSE time stamp and data set information for new messages each time there is a new status number. All collected data are stored in a single file.

The tool has a web-based HMI, shown in Fig. 3 to provide users with real-time information, such as the name of the IED, GOOSE control block reference, and GOOSE received and GOOSE missed counters. These GOOSE counters are color-coded: green when GOOSE received is incrementing and red when GOOSE missed is incrementing. In addition, the HMI provides information such as logical nodes and values transported by GOOSE and time differences between the first ten GOOSE messages. Fig. 4 shows how the tool provides detailed information about all the parameters associated with a GOOSE control block, including GOOSE ID, VLAN, GOOSE control block reference, and so on. It also highlights any anomaly information using the color-coded scheme.



Stato Ricezione ONLINE

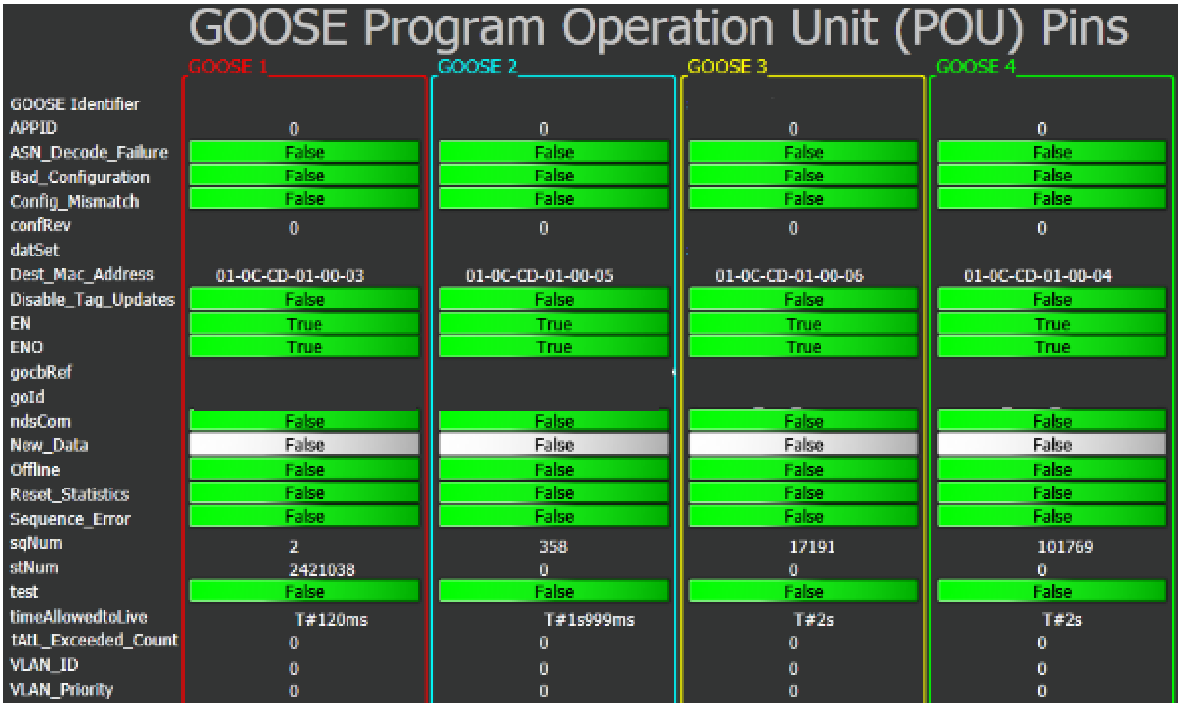
Online : MATER_DOLORLD_MFA/LLN0$GO...
GOOSE Ricevuti : 341920 msg
Sequence Number : 2723
Status Number : 1
DataSet Name : MATER_DOLORLD_MFA/LLN0$DS_G_...
gocbRef Name : MATER_DOLORLD_MFA/LLN0$GO$gcb...
Intervallo Ripetizione : 10031.9 ms

N. Interruzioni : 332
N. Riavvi : 30

Riavvio IED : NO
Perdita di messaggi ripetuti : NO
Perdita di variazioni di stato : NO
Variazioni di stato perse : 0 msg
Ripertizioni perse : 0 msg

BLIND_1 : 0	BLIND_4 : 0	BLIND_7 : 0	BLIND_10 : 0
BLIND_2 : 16908288	BLIND_5 : 0	BLIND_8 : 0	BLIND_11 : 0
BLIND_3 : 0	BLIND_6 : 0	BLIND_9 : 0	BLIND_12 : 0

Fig. 3. E-Distribuzione HMI.



GOOSE Program Operation Unit (POU) Pins

	GOOSE 1	GOOSE 2	GOOSE 3	GOOSE 4
GOOSE Identifier				
APPID	0	0	0	0
ASN_Decode_Failure	False	False	False	False
Bad_Configuration	False	False	False	False
Config_Mismatch	False	False	False	False
confRev	0	0	0	0
datSet				
Dest_Mac_Address	01-0C-CD-01-00-03	01-0C-CD-01-00-05	01-0C-CD-01-00-06	01-0C-CD-01-00-04
Disable_Tag_Updates	False	False	False	False
EN	True	True	True	True
ENO	True	True	True	True
gocbRef				
goId				
ndsCom	False	False	False	False
New_Data	False	False	False	False
Offline	False	False	False	False
Reset_Statistics	False	False	False	False
Sequence_Error	False	False	False	False
sqNum	2	358	17191	101769
stNum	2421038	0	0	0
test	False	False	False	False
timeAllowedtoLive	T#120ms	T#1s999ms	T#2s	T#2s
tAtL_Exceeded_Count	0	0	0	0
VLAN_ID	0	0	0	0
VLAN_Priority	0	0	0	0

Fig. 4. Received GOOSE information.

10 Real-Time OT Network Troubleshooting Tools

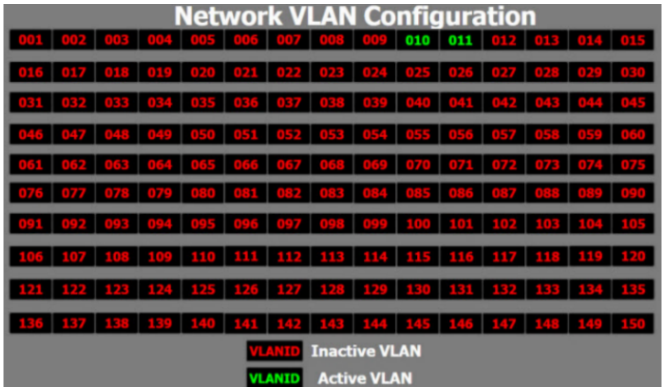
IT tools used by substation engineers are capable of capturing and archiving Ethernet traffic for forensic analysis. However, they are only able to verify traffic on the network port to which they are connected. The tools cannot verify if any multicast protection traffic reaches the intended IED subscriber on a different network port. In some cases, port mirroring can approximate this traffic but cannot ensure genuine data.

Another issue that arises when using IT tools is that they are susceptible to inaccuracies imposed by different operating systems. These errors affect the true timing, due to inaccurate time stamps, and sometimes even the sequence of the messages. These errors prevent IT tools from providing the reliable information needed to troubleshoot OT networks.

Apart from monitoring network performance, OT tools are often required to verify the configuration of the network either at commissioning or during troubleshooting. Fig. 5 illustrates a tool developed to do just that. VLANs are very popular for segregating traffic over OT networks; however, an incorrectly configured VLAN can pose problems. This tool monitors the IEEE 802.1Q VLAN configuration of Ethernet-based networks using two devices: one that is connected to one end of the network and publishing Layer 2 messages and another device subscribing to those messages on the opposite end of the network, as shown in Fig. 6. This collection of information is viewed by connecting a laptop to the second, subscribing device.

The tool specifically validates permission for Ethernet packets to traverse a LAN and egress through a specific port according to an IEEE 802.1Q VLAN tag. It can also be used to validate and troubleshoot LAN configurations. Correct results displayed on the simple HMI, as shown in Fig. 5 quickly demonstrate a properly working LAN and configured egress port. Incorrect results indicate that at least one network configuration or functionality issue exists and needs to be corrected.

This tool is also helpful when addressing network security, as it helps users verify which VLANs are enabled on which sections of the network. VLANs are a part of OT applications network design best practices because they allow the user to segregate network traffic. By allowing only the verified, network-required VLANs, networks can be made secure against cyberattacks.



Network VLAN Configuration

001	002	003	004	005	006	007	008	009	010	011	012	013	014	015
016	017	018	019	020	021	022	023	024	025	026	027	028	029	030
031	032	033	034	035	036	037	038	039	040	041	042	043	044	045
046	047	048	049	050	051	052	053	054	055	056	057	058	059	060
061	062	063	064	065	066	067	068	069	070	071	072	073	074	075
076	077	078	079	080	081	082	083	084	085	086	087	088	089	090
091	092	093	094	095	096	097	098	099	100	101	102	103	104	105
106	107	108	109	110	111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130	131	132	133	134	135
136	137	138	139	140	141	142	143	144	145	146	147	148	149	150

VLANID Inactive VLAN

VLANID Active VLAN

Fig. 5. HMI screen showing VLAN 10 and VLAN 11 enabled on network egress.

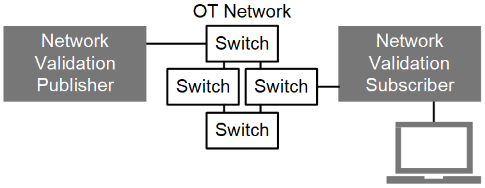


Fig. 6. A typical connection diagram for the network validation tool.

11 Conclusion

This paper describes a case study in which real-time OT tools provided quantified data on network performance to create a baseline of network information as used by OT applications. Using OT networking best practices to engineer and test Ethernet networks provides improved confidence in communications-related issues to the end user, and a specific OT network tool can be used in a continuous real-time monitoring mode or on a case-by-case basis.

12 References

[1] L. Delli Carpini, A. Cammarota, G. Sapienza, and P. Paulon, “Smart Fault Selection Through Smart Protection Devices Using IEC 61850,” proceedings of the 25th International Conference on Electricity Distribution, Madrid, Spain, June 2019.

[2] IEC 61850-5, Communication Networks and Systems for Power Utility Automation – Part 5: Communication Requirements for Functions and Device Models, 2003.

[3] D. Dolezilek, P. Lima, G. Rocha, A. Rufino, and W. Fernandes, “Cost and Performance Comparison of Numerous In-Service Process Bus Merging Unit Solutions Based on IEC 61850,” proceedings of the 10th Annual Protection, Automation and Control World Conference, Glasgow, United Kingdom, June 2019.

13 Biographies

Luca Delli Carpini is with E-Distribuzione in Italy.

Amandeep Kalra is an application engineer with Schweitzer Engineering Laboratories, Inc. (SEL). He has several years of experience in designing automation systems and secure communications networks. He has authored numerous technical papers focusing on IEC 61131-based automation controllers, secure Ethernet networks, cybersecurity, and Ethernet-based communications protocols, as well as IEC 61850 communications standards. He is a patented inventor and has represented SEL at various international conferences and IEC 61850 interoperability demonstrations organized by UCA. He frequently teaches engineering design and application of IEC 61850 solutions. He has a bachelor of technology degree in instrumentation and control engineering from the National Institute of Technology, India, and a master's degree in electrical engineering from California State University, Northridge.

David Dolezilek is a principal engineer with Schweitzer Engineering Laboratories, Inc. and has three decades of experience in electric power protection, automation, communication, and control. David is a patented inventor, has authored dozens of technical papers, and continues to research first principles of mission-critical technologies. Through his work, he has created methods to specify, design, and measure service level specifications for digital communication of signals, including class, source, destination, bandwidth, speed, latency, jitter, and acceptable loss. As a result, he helped coin the term operational technology (OT) to explain the difference in performance and security requirements of Ethernet for mission-critical applications versus IT applications. David is a founding member of the DNP3 Technical Committee (IEEE 1815), a founding member of UCA2, and a founding member of both IEC 61850 Technical Committee 57 and IEC 62351 for security. He is a member of the IEEE, the IEEE Reliability Society, and several CIGRE working groups.

Giorgio Vielmini is a regional technical manager with Schweitzer Engineering Laboratories, Inc. in Italy.

Tim Grigg is an application engineer with Schweitzer Engineering Laboratories, Inc.

Abstract—In this paper, we discuss the various operational technology (OT) tools available for the performance analysis of mission-critical Ethernet-based communications networks. We describe techniques for simple test cases that provide performance quantification of the communications path in terms of determinism, latency, and availability, using as an example tests performed at the Enel Smart Grid Lab (created by E-Distribuzione in Milan) that were conducted to verify the performance of existing Ethernet network technology when exchanging mission-critical information. Due to similar terminology and comparably appearing networks, many end users use software-based information technology (IT) tools to baseline the performance of OT networks. However, OT networks have different design and performance requirements and require specific, real-time OT tools to verify design implementation and performance. Moreover, an important aspect of testing OT networks is verifying cybersecurity, because the security of the network is directly related to its availability and reliability. A nonsecure network cannot be considered for mission-critical applications, as seen by the repercussions of recent cyberattacks on power systems.

20200716 • TP6958