CAIRNS 2023
INTERNATIONAL
SYMPOSIUM
4TH - 7TH SEPTEMBER

Symposium
Paper

## Paper information

| | |
|---|---|
| Paper number | 1455 |
| Paper title | Experiences and Learning on Monitoring Digital Substation Communication Networks |
| Study Committee | SC B5 – Protection and automation |
| Paper Stream | 1. Learning from experience |
| Authors | Paulo Sergio Pereira Junior, Rodolfo Cabral Bernardino, Gustavo Silva Salge, Cristiano Moreira Martins, Gustavo Espinha Lourenço, Paulo Sergio Pereira |
| Affiliations | CONPROVE |
| Email address | psjunior@conprove.com.br |

## Summary

Considering that the basic concept of network monitoring is related to systematic verification in search of anomalies that could compromise its proper functioning, IEC 61850 network monitoring is necessary throughout the life cycle of the digital substation. Which means that monitoring must be carried out in the commissioning test stages such as Factory Acceptance Test (FAT) and Site Acceptance Test (SAT), and maintenance tests.

The importance of network monitoring is related to early detection of errors, network operating conditions, reducing network unavailability by tracking problematic elements, logging all network events, and security and stability of the power system. Specialized devices are necessary to monitor these network aspects, acting as a "network oscillograph" / “digital network recorder”. This monitoring system must be implemented both in hardware and software in order to cover all the time-critical requirements of the GOOSE and Sampled Values protocols.

Several network aspects must be analyzed to guarantee the security, reliability, speed and availability of the information being transmitted, warning potential communication failures or invasions. These network aspects are related to message integrity, configuration and data security, system's time synchronism and the message timing statistics, considering the interval between frames, transfer time, packets losses and etc.

Therefore, this paper aims to carry out an analysis of the importance of monitoring the network in the context of IEC 61850, highlighting the requirements necessary for monitoring and discussing its implementations, disseminating experiences and learning acquired in digital substations, and complying with power system best practices of the Brazilian Transmission System Operator (TSO).

## Keywords

IEC 61850, PACS, network monitoring, monitoring system, GOOSE, Sampled Values, PTP

## Introduction

The Protection, Automation and Control Systems (PACS) are progressing due to the constant innovations provided with the advent of the IEC 61850, whose first edition was launched in 2003. Increasingly, the implementation of the IEC 61850 standard is growing all over the world with the aim to implement fully digital substations, where the Process Bus further highlights how vital the Ethernet communication network performance is in PACS.

According to the data structure established by IEC 61850, it is possible to implement different application functions (F1 and F2) distributed through allocations of Logical Nodes (LN) in different Physical Devices (PD), which will exchange information through a communication network where LN are linked by Logical Connections (LC) and PD are linked by Physical Connections (PC), according to a classical example demonstrated in item 8.4.2 of IEC 61850-5 Ed.2 that is shown in Figure 1 below.

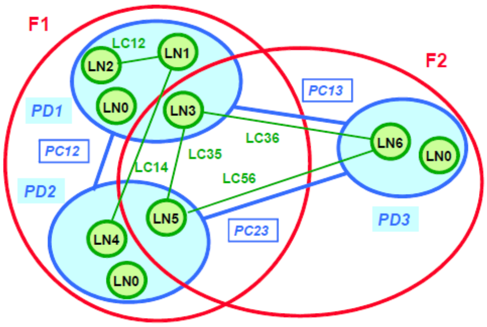


*Figure 1 - The Logical Node and Link Concept*

The description, in details, of this example demonstrates that F1 is implemented in PD1 through LN0, LN1, LN2 and LN3. The same way, F1 is implemented in PD2 through LN0, LN4 and LN5. PD1 and PD2 are connected through PC12. LN1 (PD1) and LN4 (PD2) are connected through LC14. LN3 (PD1) and LN5 (PD2) are connected through LC35.

Thus, this example clearly demonstrates that the performance of the function to be executed depends on the network communication performance, so the communication network and its availability are part of this function. Therefore, it is of vital importance to monitor the network to ensure the correct operation of the PACS.

All data exchange recommended by IEC 61850 is based on these communication protocols: Client/Server (MMS), Sampled Values (SV), GOOSE and Precision Time Protocol (PTP). SV and GOOSE have time-critical requirements, so in order to increase the reliability, a dedicated monitoring system is needed, able to tag the receiving timestamps by hardware. The PTP, in its Power Profile, is the preferred time synchronization protocol as described in IEC 61850 – 9 – 3.

In the IEC 61850 context, the goal of network monitoring is to carry out an in-depth analysis of the entire substation network in search of anomalies, covering both commissioning and maintenance tests. In the case of FAT/SAT tests, the monitoring system can detect errors before the substation is running. Some problems can be detected early like Merging Units (MUs) publishing SV frames with out-of-order samples, or malformed packets, or with time between frames over the sampling rate, or yet drifting its clock pointing to synchronism errors. In maintenance tests, the monitoring system can, for example, perform a network sniffing and find orphan GOOSE or SV frames running on the network, indicating a traffic not foreseen in the SCL file, i.e out of the "White List". This error may even indicate a security issue. Another purpose of monitoring is related to statistical analysis of the network, indicating instantaneous viewing of data like packet delay, transfer time, clock drift and etc.

Based on item 11.1.1.4 of IEC 61850-5 Ed.2, the transfer time is defined as the complete frame´s transmission time including the processing of publisher and subscriber. In details, it is the sum of three times: *ta*, *tb* and *tc*, where:

- *ta* is the time counted from the moment the publisher puts the frame on top of its transmission stack (coding) to the moment it is sent to the network;

- *tb* is the network latency time;

- *tc* is the time counted from the frame´s incoming moment at the subscriber to the frame is extracted from the receiving stack.

Copied from IEC 61850-5 Ed.1, Figure 2 illustrates the transfer time´s concept.

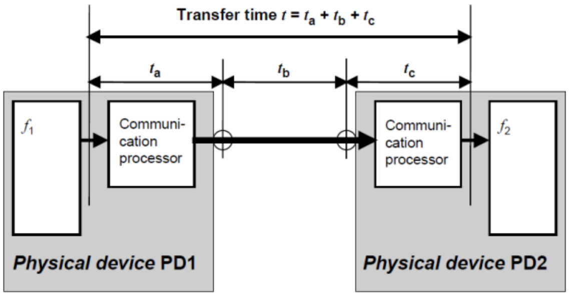
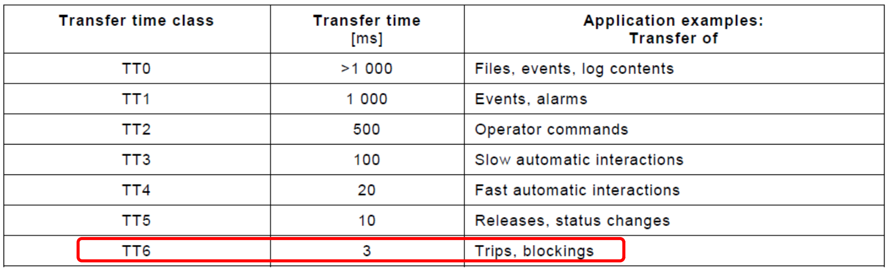


*Figure 2 - The Concept of Transfer Time*

For protection systems, the transfer time class for Trip applications is "TT6" and the transfer time must be smaller than 3ms. Copied from IEC 61850-5 Ed.2, Table 1 shows the classes for transfer times.

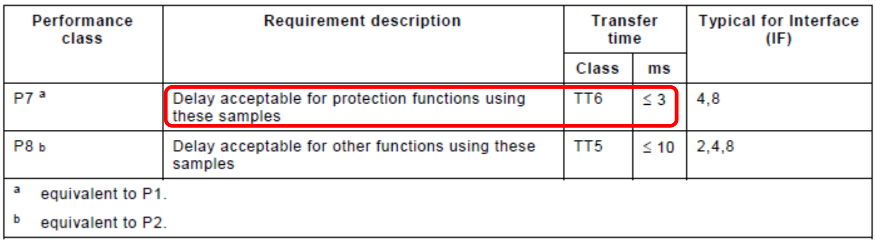
*Table 1 - Classes For Transfer Times*



| Transfer time class | Transfer time [ms] | Application examples: Transfer of |
|---|---|---|
| TT0 | >1 000 | Files, events, log contents |
| TT1 | 1 000 | Events, alarms |
| TT2 | 500 | Operator commands |
| TT3 | 100 | Slow automatic interactions |
| TT4 | 20 | Fast automatic interactions |
| TT5 | 10 | Releases, status changes |
| TT6 | 3 | Trips, blockings |

In the same way, according to IEC 61850-5 Ed.2, item 11.2.4 Type 4 – Raw data messages ("Samples"), the transfer time for synchronized samples from Merging Units for protection functions is also of TT6 class, so it must be smaller than 3ms. Table 2, based on this edition of IEC 61850-5, shows this:

*Table 2 - Transfer Times Classes for Synchronized Samples*



| Performance class | Requirement description | Transfer time | | Typical for Interface (IF) |
|---|---|---|---|---|
| | | Class | ms | |
| P7 [a] | Delay acceptable for protection functions using these samples | TT6 | ≤ 3 | 4,8 |
| P8 [b] | Delay acceptable for other functions using these samples | TT5 | ≤ 10 | 2,4,8 |

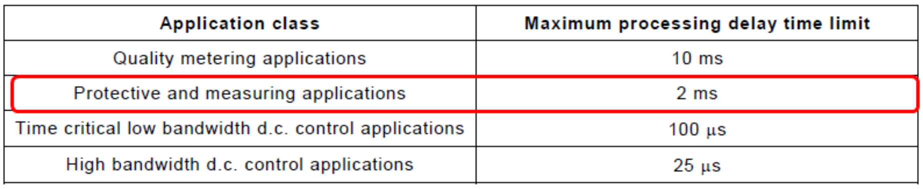
[a] equivalent to P1.

[b] equivalent to P2.

Therefore, both GOOSE and SV transfer times for Trip and protection applications, respectively, must be smaller than 3ms.

Furthermore, IEC 61689-9 Ed.1, item 6.902.2 - Maximum processing delay time requirement deals with the concept of "Processing Time" of Merging Units, which is the time MU takes from the digitization of analogical inputs signals until SV's publication. So, this processing time must to be verified in the MU's network output, in order not to take into account the network latency time. The maximum processing time in this case is 2ms. Table 3, based on this edition of IEC 61869-9, shows this:

Table 3 - Maximum Processing TIme for *Merging Units*



| Application class | Maximum processing delay time limit |
|---|---|
| Quality metering applications | 10 ms |
| Protective and measuring applications | 2 ms |
| Time critical low bandwidth d.c. control applications | 100 µs |
| High bandwidth d.c. control applications | 25 µs |

In the following topics a network monitoring system requirements, composed by hardware and software, will be approached sharing experiences and learning about digital substation monitoring.

## Network Monitoring System for PACS

The monitoring system is an essential tool for troubleshooting the digital substation network, so the Brazilian TSO – ONS – discussed several requirements and included, in the power system best practices, the IEC 61850 network monitoring.

According to that, PACS network must incorporate monitoring functions able to:

1) Detect and point out anomalies or lacking of messages, like GOOSE or SV, or yet unforeseen messages;

2) Detect lacking of synchronism signal;

3) Verify and point out abnormal propagation time, i.e. latency, and asymmetry or excessive variation, i.e. jitter, of messages propagation times;

4) Be implemented in an independent way of protection devices or local teleprotection devices;

5) Have resources for storing event records of detected anomalies.

Also, PACS network must incorporate mechanisms that offer cybersecurity to ensure the following topics:

1) Confidentiality: to limit data access to authorized users only;

2) Integrity: to ensure that are no unauthorized modifications of messages data or information steals;

3) Availability: to ensure authorized access to data or services;

4) Authenticity: to ensure that the data comes from a legitimate source.

Therefore, the monitoring system will be able to log substation hardware or software issues, and must also generate files that register all the network traffic, such as PCAP format, very popular among network protocol analysers, for evaluating time-synchronized events.

In order to ensure that all these features cited in the topics above will be covered by the monitoring system, some network aspects must be analysed. One of these is related to the integrity of the messages, that is, if there are no packet losses or corrupted packets. Also, the configuration and security of the data, i.e. verify that all messages contained in the substation's SCL file are present in the network and if there are any messages running that were not foreseen, and related to frame´s structure comparing fields like MAC source address and destination address, VLAN ID and priority tag.

Another aspect of the network to be considered is related to the system's time synchronism, through the traffic check of PTP messages.

Finally, the message timing statistics in the network must be checked, considering the interval between frames, Transfer Time, Propagation Delay and etc. In addition, it must been evaluated how the monitoring system will behave in a Test/Simulation configuration when there are two SV streams: simulated and the real one coming from a Merging Unit.

These checks will allow to increase the reliability, security and, consequently, the availability of the network, alerting potential communication failures (caused by an IED network adapter bug, for example) or invasions. The checks will generate event logs that can be stored and consulted, making it possible to track the problem and to locate its source. In addition, event logs can be used in reports to facilitate comprehension of the failure. To further optimize the evaluations, PCAP files can be recorded for more detailed checks of the events in the pre-trigger and post-trigger stages. In practice, network monitoring can be performed either through a Trunk Port on the network Switch or through Port Mirroring, to have access to all substation traffic, regardless of VLANs.

The digital substation monitoring system must implement features that meet some analyse modes. In SCL validation mode, the main purpose is to compare all the SCL file and verify if there any field not complying with IEC 61850 standard, like frames fields length, multicast destination MAC addresses range recommendation, best settings practices such as one destination MAC address per GOOSE or SV streams, and others. In sniffer mode, the main purpose is to scan the network and check if there is traffic not foreseen by the SCL files, that is, any GOOSE or SV frames not included in the "White List", known as "orphans", and confirm that all frames expected are running on the network. With these ones, a complete field-by-field frame verification must be performed in order to compare the frame is running on the network with the respective one described in the SCL file. The goal is to find setting differences such in Application ID and Configuration Revision.

In supervision mode, the main purpose is to evaluate the network for errors. Several “supervision events” can be configured depending on which protocol is to be supervised. In case of GOOSE, there are some examples of events:

- Time Allowed to Live (TTL) is Expired: this event occurs if the GOOSE message is not running on the network for a time equal to or greater than the maximum allowed, according to the definition of the TTL field by the IEC 61850 standard;
- Frames Out Of Order: this event occurs if the sequence number or even state number is out of the sequence defined by the IEC 61850 standard;
- Malformed Packets: this event occurs if the GOOSE frame format does not comply to the IEC 61850 standard definition;
- Never Seen Frames: this event occurs if a GOOSE frame has not been running on the network long enough to conclude that it has never been seen;
- GOOSE Quality Events: these events occur if the Validity bits are different from “good” or even if Test bit has changed its value;
- Time Quality Events: these events occur if the “TimeQuality” byte of TimeStamp field has changed any of its bits, or even if the “ClockFailure” or “Clock not synchronized” bit is set;
- Transfer Time Event: this event occurs if the transfer time is longer than expected.

If case of PTP, there are some examples of events:

- Synchronization is Lost: this event occurs if the Slave has lost Master´s messages;
- PTP Clock Drift: this event occurs if Slave clock is drifting more than expected related to Master clock;

- Grandmaster Accuracy has Changed: this event occurs if is detected that grandmaster has changed its clock accuracy;
- Synchronization is Established: this event occurs if Slave clock has synchronized with Master clock within a defined accuracy range;
- Grandmaster ID has changed: this event occurs if is detected that there is another grandmaster as PTP time synchronization source;
- Grandmaster Current UTC Offset has Updated: this event occurs when is detected that the grandmaster current UTC offset has changed. The UTC offset valid flag must be verified by the monitoring system in order to present the validity of this offset update.

In case of SV, there are some examples of events:

- Timeout has Expired: this event occurs if the frames of a MU are not running on the network for a determined time;
- Frames Out Of Order: this event occurs if the sample counter is out of the sequence defined by the IEC 61850 standard;
- Malformed Packets: this event occurs if the SV frame format does not comply to the IEC 61850 standard definition;
- Never Seen Frames: this event occurs if a SV frame has not been running on the network long enough to conclude that  it has never been seen;
- SV Quality Events: these events occur if the Validity bits are different from "good" or even if Test bit has changed its value;
- SV Clock Drift: this event occurs if the MU clock is drifting more than expected;
- Digitization + Transfer Times Event: this event occurs if the time that MU took to process and publish the SV frame added by the network latency time is longer than expected;
- Sample Sync Flag Changed Event: this event occurs if the Sample Sync flag field has changed its value, indicating some alteration of synchronization type.

In all of these events explained above, a PCAP recording must be triggered to make the network traffic available considering the pre-trigger and post-trigger steps. This way, the monitoring system will act as a "network oscillograph" or "network digital recorder".

In statistics mode, the main purpose is to perform a statistical analysis of GOOSE and Sampled Values frames in order to carry out a specific and objective check with statistical data on these network traffics. This analysis covers all frame´s fields, including data and qualities.

In case of GOOSE, the statistical analysis must verify the time when packet was received, and some counters such as: packets received, state number changes, state and sequence numbers changes that were lost and duplicated frames.  Besides, it must show if some GOOSE frame has its Time Allowed To Live expired and a counter of how many times it happened. Related to transfer time analysis, the monitoring system must calculate the maximum, average and minimum values found during the process. In addition, it must verify a counter that shows how many times the transfer time was longer than a given value as determined by the IEC 61850 standard.

In case of SV, the statistical analysis must verify the time when packet was received and the counters: SV packets received and sample counters that were lost. Besides, it must show the quantity of: out of sequence and duplicated frames. In addition, monitoring system must verify the time when received the last sample count zero frame, the current drift of the MU clock as also as this clock drift since the process has started. If the SV frames were not running on the network for a given time, it needs also been verified by the monitoring system and how many times this occurred. Also, related to digitization + transfer times analysis, the monitoring system must calculate the maximum, average and minimum values during the process. The counter with how many times this sum of times was longer than a given value as determined by the IEC 61850 standard, also needs to be verified. Besides that, the maximum, average and minimum values of the interval between SV frames also need to be calculated.

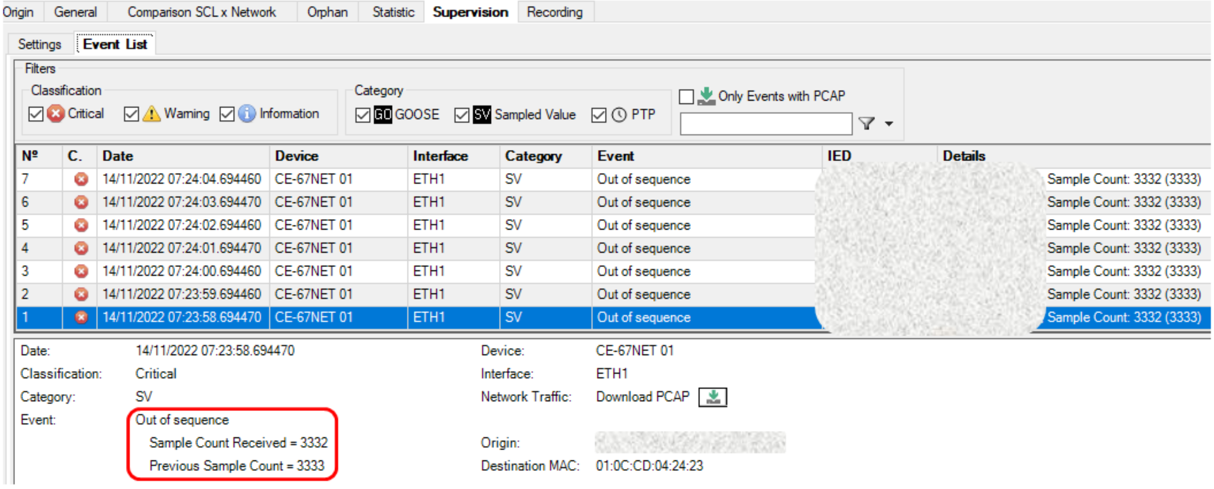
It is important to highlight that when in test/simulation conditions, i.e. with two GOOSE or SV streams running on the network with the same identification but one coming from a real device and other simulated, the monitoring system must consider two different filters, which implies in two different message configurations: one with the simulation bit set to false and the other with simulation bit set to true.

## Study Cases: Experiences and Learning

In this topic, some cases of network issues in Brazilian digital substations will be discussed, as well as how monitoring system can detect and identify these problems to help find a solution.

The first case is related to duplicate Sampled Values frames errors due to a RedBox (Redundancy Box) problem. This fact happened in a digital substation with 13 Merging Units and about 168 GOOSE streams inserted into the network architecture.

The SV frames were being published at the IEC 61869-9 preferred sampling rate, at 4800 samples/second and 2 ASDUs. The duplication issue was happening every second on the same sample counters, and on the RedBox output, i.e., the frames were being published in the right order from the Merging Unit. This error could be detected by the monitoring system as an out of sequence event in supervision mode, evidencing that the current sample counter is not the one unit increment of the previous one, as shown in the Figure 3.



Filters

Classification: ☑ Critical ☑ Warning ☑ Information

Category: ☑ GO GOOSE ☑ SV Sampled Value ☑ PTP

☐ Only Events with PCAP

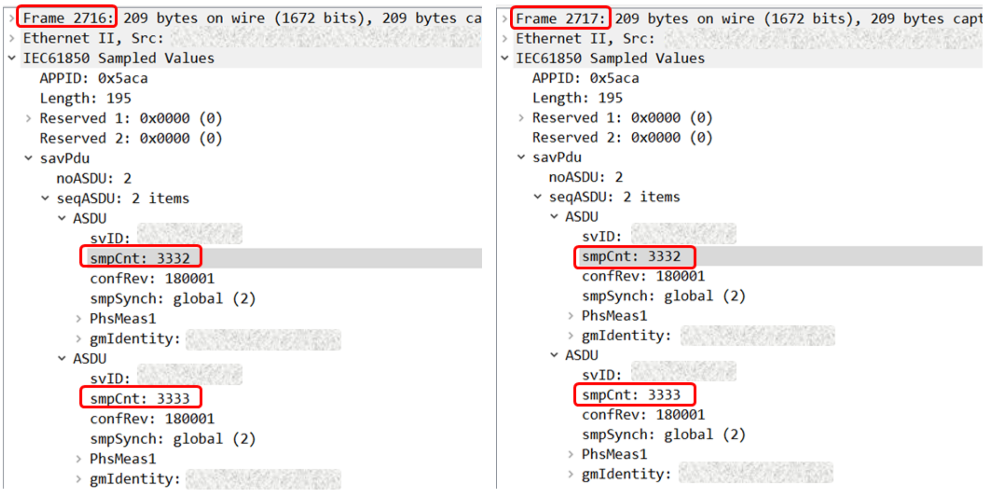
| Nº | C. | Date | Device | Interface | Category | Event | IED | Details |
|---|---|---|---|---|---|---|---|---|
| 7 | ✖ | 14/11/2022 07:24:04.694460 | CE-67NET 01 | ETH1 | SV | Out of sequence | [redacted] | Sample Count: 3332 (3333) |
| 6 | ✖ | 14/11/2022 07:24:03.694470 | CE-67NET 01 | ETH1 | SV | Out of sequence | [redacted] | Sample Count: 3332 (3333) |
| 5 | ✖ | 14/11/2022 07:24:02.694460 | CE-67NET 01 | ETH1 | SV | Out of sequence | [redacted] | Sample Count: 3332 (3333) |
| 4 | ✖ | 14/11/2022 07:24:01.694470 | CE-67NET 01 | ETH1 | SV | Out of sequence | [redacted] | Sample Count: 3332 (3333) |
| 3 | ✖ | 14/11/2022 07:24:00.694460 | CE-67NET 01 | ETH1 | SV | Out of sequence | [redacted] | Sample Count: 3332 (3333) |
| 2 | ✖ | 14/11/2022 07:23:59.694460 | CE-67NET 01 | ETH1 | SV | Out of sequence | [redacted] | Sample Count: 3332 (3333) |
| 1 | ✖ | 14/11/2022 07:23:58.694470 | CE-67NET 01 | ETH1 | SV | Out of sequence | [redacted] | Sample Count: 3332 (3333) |

Date: 14/11/2022 07:23:58.694470
Classification: Critical
Category: SV
Event: Out of sequence
Sample Count Received = 3332
Previous Sample Count = 3333

Device: CE-67NET 01
Interface: ETH1
Network Traffic: Download PCAP
Origin: [redacted]
Destination MAC: 01:0C:CD:04:24:23

*Figure 3 - Out Of Sequence in SV Supervision Event*

The duplicated frames were related to sample counters 3332 and 3333 in the frames 2716 and 2717, as shown in the PCAP file in Figure 4.

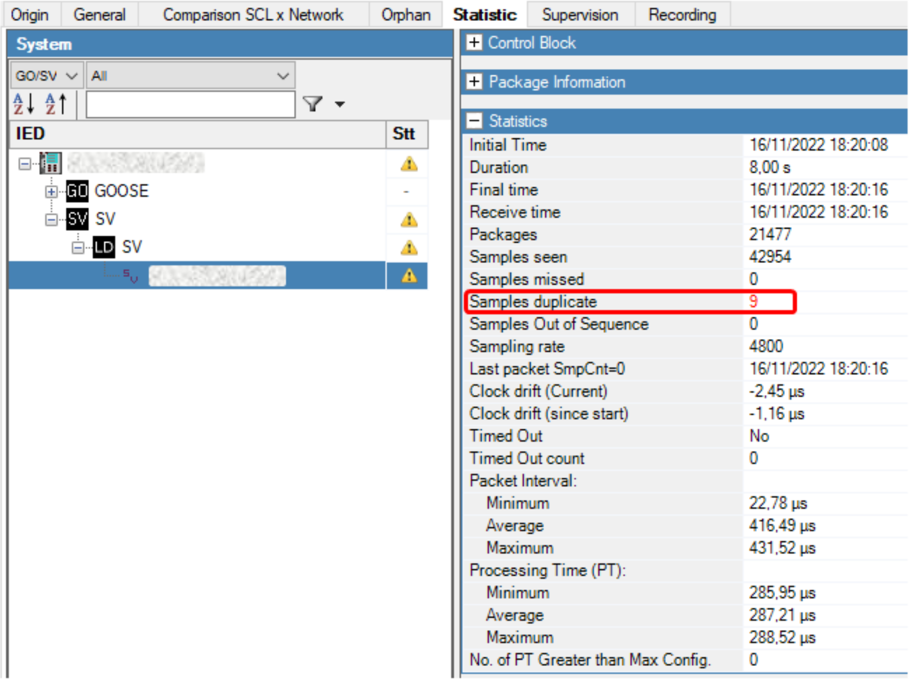


```
› Frame 2716: 209 bytes on wire (1672 bits), 209 bytes ca
› Ethernet II, Src: [redacted]
˅ IEC61850 Sampled Values
    APPID: 0x5aca
    Length: 195
  › Reserved 1: 0x0000 (0)
    Reserved 2: 0x0000 (0)
  ˅ savPdu
      noASDU: 2
    ˅ seqASDU: 2 items
      ˅ ASDU
          svID: [redacted]
          smpCnt: 3332
          confRev: 180001
          smpSynch: global (2)
        › PhsMeas1
        › gmIdentity: [redacted]
      ˅ ASDU
          svID: [redacted]
          smpCnt: 3333
          confRev: 180001
          smpSynch: global (2)
        › PhsMeas1
        › gmIdentity: [redacted]
```

```
› Frame 2717: 209 bytes on wire (1672 bits), 209 bytes capt
› Ethernet II, Src: [redacted]
˅ IEC61850 Sampled Values
    APPID: 0x5aca
    Length: 195
  › Reserved 1: 0x0000 (0)
    Reserved 2: 0x0000 (0)
  ˅ savPdu
      noASDU: 2
    ˅ seqASDU: 2 items
      ˅ ASDU
          svID: [redacted]
          smpCnt: 3332
          confRev: 180001
          smpSynch: global (2)
        › PhsMeas1
        › gmIdentity: [redacted]
      ˅ ASDU
          svID: [redacted]
          smpCnt: 3333
          confRev: 180001
          smpSynch: global (2)
        › PhsMeas1
        › gmIdentity: [redacted]
```

*Figure 4 - PCAP File with SV Duplicated Frames*

Also, the monitoring system could have detected this duplicated SV frames as a duplicated frame feature in statistical mode, showing that the duplicated frame counter was incremented, as shown Figure 5.



| | |
|---|---|
| Initial Time | 16/11/2022 18:20:08 |
| Duration | 8,00 s |
| Final time | 16/11/2022 18:20:16 |
| Receive time | 16/11/2022 18:20:16 |
| Packages | 21477 |
| Samples seen | 42954 |
| Samples missed | 0 |
| Samples duplicate | 9 |
| Samples Out of Sequence | 0 |
| Sampling rate | 4800 |
| Last packet SmpCnt=0 | 16/11/2022 18:20:16 |
| Clock drift (Current) | -2,45 µs |
| Clock drift (since start) | -1,16 µs |
| Timed Out | No |
| Timed Out count | 0 |
| Packet Interval: | |
| Minimum | 22,78 µs |
| Average | 416,49 µs |
| Maximum | 431,52 µs |
| Processing Time (PT): | |
| Minimum | 285,95 µs |
| Average | 287,21 µs |
| Maximum | 288,52 µs |
| No. of PT Greater than Max Config. | 0 |

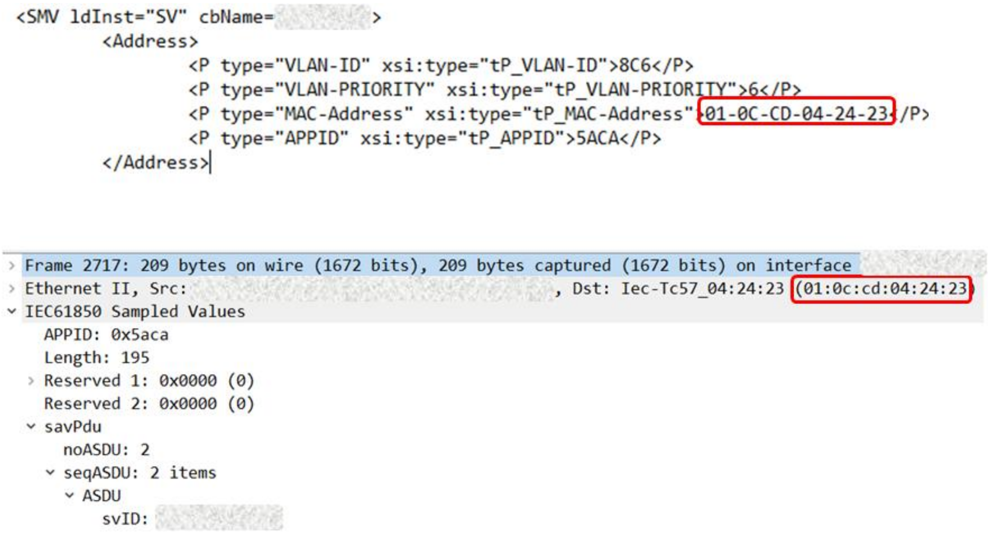
*Figure 5 - Duplicated Frames in SV Statistics Mode*

Still analysing this same digital substation, it was verified a SCL file compliance error with the IEC 61850 standard requirements related to the multicast destination MAC addresses range. In the IEC 61850-9-2 Ed. 2, Annex B, it is possible to verify the recommended multicast addressing, according to each communication protocol, as shown in Table 4.

*Table 4 - Recommended Multicast Addressing*

| Service | Recommended address range assignments | |
|---|---|---|
| | Starting address (hexadecimal) | Ending address (hexadecimal) |
| GOOSE | 01-0C-CD-01-00-00 | 01-0C-CD-01-01-FF |
| GSSE | 01-0C-CD-02-00-00 | 01-0C-CD-02-01-FF |
| Multicast sampled values | 01-0C-CD-04-00-00 | 01-0C-CD-04-01-FF |

In this SCL file, the destination MAC addresses range were out of the recommendation mentioned in Table 4, as shown in Figure 6, composed with the SCL file and a PCAP captured.



```
<SMV ldInst="SV" cbName=[redacted]>
        <Address>
                <P type="VLAN-ID" xsi:type="tP_VLAN-ID">8C6</P>
                <P type="VLAN-PRIORITY" xsi:type="tP_VLAN-PRIORITY">6</P>
                <P type="MAC-Address" xsi:type="tP_MAC-Address">01-0C-CD-04-24-23</P>
                <P type="APPID" xsi:type="tP_APPID">5ACA</P>
        </Address>
```

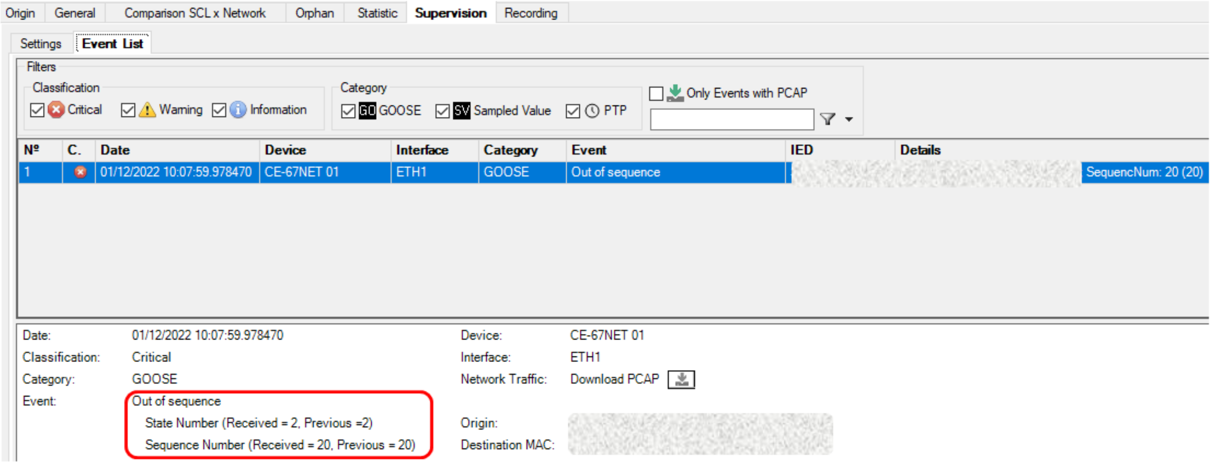
```
> Frame 2717: 209 bytes on wire (1672 bits), 209 bytes captured (1672 bits) on interface [redacted]
> Ethernet II, Src: [redacted], Dst: Iec-Tc57_04:24:23 (01:0c:cd:04:24:23)
v IEC61850 Sampled Values
    APPID: 0x5aca
    Length: 195
  > Reserved 1: 0x0000 (0)
    Reserved 2: 0x0000 (0)
  v savPdu
      noASDU: 2
    v seqASDU: 2 items
      v ASDU
          svID: [redacted]
```

*Figure 6 – SCL: IEC 61850 Compliance Verification*

The monitoring system could have detected this SCL non-compliance with the IEC 61850 standard through the SCL validation mode.

The second case happened also in a Brazilian digital substation with four different IEDs vendors, where there were GOOSE and Sampled Values streams being published. Network issues related to duplicated GOOSE frames and lost of MUs' synchronism occurred. Monitoring system could verify these two errors both in supervision mode feature and statistical mode feature.

In a supervision mode, monitoring system could verify the duplicated GOOSE frames as an out of sequence event as shown in Figure 7.



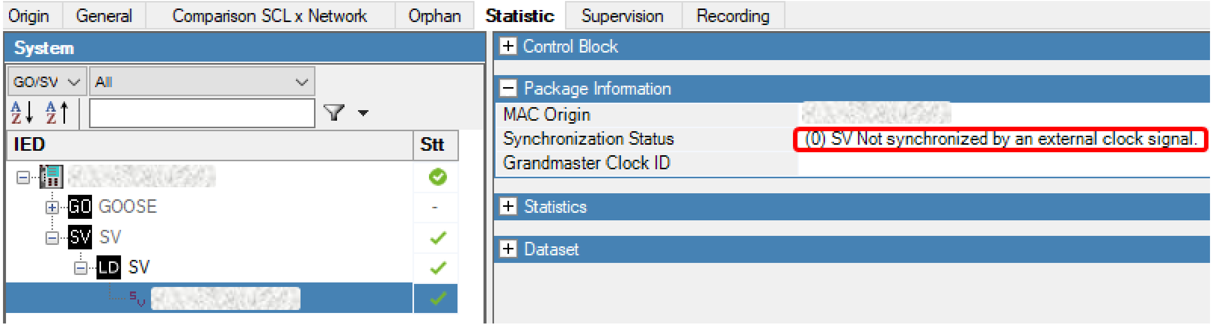
| Nº | C. | Date | Device | Interface | Category | Event | IED | Details |
|---|---|---|---|---|---|---|---|---|
| 1 | ☒ | 01/12/2022 10:07:59.978470 | CE-67NET 01 | ETH1 | GOOSE | Out of sequence | [redacted] | SequencNum: 20 (20) |

Date: 01/12/2022 10:07:59.978470
Classification: Critical
Category: GOOSE
Event: Out of sequence
State Number (Received = 2, Previous =2)
Sequence Number (Received = 20, Previous = 20)

Device: CE-67NET 01
Interface: ETH1
Network Traffic: Download PCAP
Origin: [redacted]
Destination MAC: [redacted]

*Figure 7 - Duplicated Frames in GOOSE Supervision Mode*

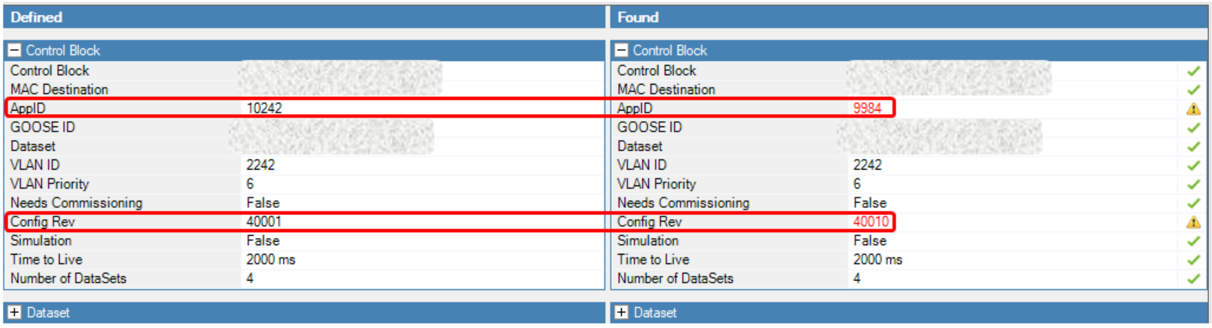
Also, monitoring system could verify lost of MU's synchronism in statistical mode as shown in Figure 8.



| | |
|---|---|
| MAC Origin | [redacted] |
| Synchronization Status | (0) SV Not synchronized by an external clock signal. |
| Grandmaster Clock ID | |

*Figure 8 - Lost Of MU´s Synchronism Detection*

Finally, it is important to analyse the third case of network issues that happened in another Brazilian digital substation, with 26 MUs and about 148 GOOSE streams inserted into the network architecture. In this case, there was SCL files incompatibility issue between IEDs so that processing problems occurred when importing a file in an IED, this file being exported by another IED from the same manufacturer. This errors occurred due to differences between the frames running on the network and the respective ones described in SCL files. The monitoring system could have detected this issue through sniffer mode, identifying differences in the frames´ fields, as shown in Figure 9.



| Defined | | Found | | |
|---|---|---|---|---|
| Control Block | [redacted] | Control Block | [redacted] | ✓ |
| MAC Destination | [redacted] | MAC Destination | [redacted] | ✓ |
| AppID | 10242 | AppID | 9984 | ⚠ |
| GOOSE ID | [redacted] | GOOSE ID | [redacted] | ✓ |
| Dataset | [redacted] | Dataset | [redacted] | ✓ |
| VLAN ID | 2242 | VLAN ID | 2242 | ✓ |
| VLAN Priority | 6 | VLAN Priority | 6 | ✓ |
| Needs Commissioning | False | Needs Commissioning | False | ✓ |
| Config Rev | 40001 | Config Rev | 40010 | ⚠ |
| Simulation | False | Simulation | False | ✓ |
| Time to Live | 2000 ms | Time to Live | 2000 ms | ✓ |
| Number of DataSets | 4 | Number of DataSets | 4 | ✓ |

*Figure 9 - Comparing SCL x Running Frames*

## Conclusions

This paper performed a detailed study of network monitoring in a digital substation context, discussing the requirements necessary for the implementation of a complete monitoring system, which covers all the life cycle of the digital substation: commissioning test stages such as FAT and SAT, and maintenance tests.

The experiences and learning acquired with real cases of network problems occurred in Brazilian digital substations, and with a network monitoring system implemented in hardware and software were disseminated in study cases.

Only when the communication network is properly operating to ensure safe and reliable information traffic will the PACS be executed satisfactorily, making the reliance on communication performance unquestionable.

## Bibliography

[1] Pereira Junior, P. S., Bernardino, R. C., Salge G. S., Martins, C. M., Pereira, P. S., Lourenço, G. E. Analysis of Network Monitoring in the Context of IEC 61850; Cigre Session 49; Paris 2022.

[2] Pereira Junior, P. S., Bernardino, R. C., Martins, C. M., Lourenço, G. E., Pereira, P. S. Analyzing the limits of data transmission in the Process Bus; Cigre Session 48; Paris 2020.

[3] Standard IEC 61850 – Communication networks and systems for power utility automation – Part 9-3: Precision time protocol profile for power utility automation, Ed. 1.0 – 2016-05.

[4] Standard IEC 61850 – Communication networks and systems for power utility automation – Part 5: Communication requirements for functions and device models, Ed. 2 - 2013.

[5] Revisão do Submódulo 2.11 dos Procedimentos de Rede para adequação às subestações digitais - Denise Borges de Oliveira (ONS); Tatiana Maria Tavares de Souza Alves (ONS) – 3ª Reunião de 2021 do Grupo de Trabalho do Cobei IEC TC95-MT04 (Funções de Proteção e Guias de Aplicação).

[6] Standard IEC 61850 – Communication networks and systems in substations – Part 5: Communication requirements for functions and device models, Ed. 1 - 2003.

[7] Standard IEC 61850 – Communication networks and systems for power utility automation – Part 8-1: Specific communication service mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3, Ed. 2 - 2011.

[8] Standard IEC 61850 – Communication networks and systems for power utility automation – Part 7-4: Basic communication structure – Compatible logical node classes and data object classes, Ed. 2.1 – 2020-02.