10150 Session 2022
B5 – PROTECTION & AUTOMATION
PS3 - INTEGRATION OF INTELLIGENCE ON SUBSTATIONS

Analysis of Network Monitoring in the Context of IEC 61850

Paulo S. Pereira JUNIOR*	Rodolfo Cabral BERNARDINO	Gustavo Silva SALGE	Cristiano Moreira MARTINS	Paulo Sergio PEREIRA	Gustavo Espinha LOURENÇO
Conprove Brazil	Conprove Brazil	Conprove Brazil	Conprove Brazil	Conprove Brazil	Conprove Brazil

*** psjunior@conprove.com.br**

SUMMARY

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 messages integrity, configuration and data security, system's time synchronism and the messages timing statistics, considering the interval between frames, Transfer Time, Propagation Delay and the Processing Time.

Due to increased deployment of IEC 61850 based digital substations, cybersecurity vulnerabilities are increasing the same way. These vulnerabilities are related both to the Process Bus and to the Station Bus, so that Sampled Values messages, GOOSE messages or MMS messages are all subject to cyber attacks.

Therefore, it is noteworthy that the protection performance of power systems depends on the communication network performance. This way, it must be trusted and safety.

In this paper, the reason for monitoring will be described and also discussed how to do this for each network requirement aspect. The monitoring issues that are not able to be verified will also be analyzed. Finally, it will be discussed how the network monitoring will behave in relation to the test conditions, since in maintenance tests there will be two SV streams: one simulated by the test set and the other from an MU / SAMU, for example.

Thus, the paper aims to perform an analysis on the importance of monitoring the network in the context of IEC 61850, highlighting the network requirements necessary for monitoring and discussing its implementations.

KEYWORDS

Monitoring, IEC 61850, Test Set, Network, Cybersecurity.

1. INTRODUCTION

The Protection, Automation and Control Systems (PACS) are progressing due to the constant innovations provided with the advent of the IEC 61850 standard, whose first edition was launched in 2003. Increasingly, the implementation of the IEC 61850 standard is growing in 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.

All data exchange recommended by the standard is based on three communication protocols: Client / Server (MMS), GOOSE and Sampled Values (SV). In this context, several network aspects must be analyzed to guarantee reliability, speed, availability and security of the information being transmitted.

IEC 61850 standardizes the exchange of information between IEDs (Intelligent Electronic Devices) of one or more substations, allowing the implementation of SAS (Substation Automation System). The standard's architecture is based on the object-oriented data model, abstracting attributes and functions from IEDs, called Physical Devices. Each Physical Device has a set of Logical Devices that are the different functionalities implemented by the IED (System, Control, Protection, among others). Each Logical Device has a set of Logical Nodes that are the functional elements of the Logical Device. Examples of protection Logical Nodes: PDIS (distance protection), PTOC (overcurrent protection), PDIF (differential protection), etc. Finally, each Logical Node has a set of Functional Constraints with their Data Objects and Data Attributes.

Thanks to the data structure established by the 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.

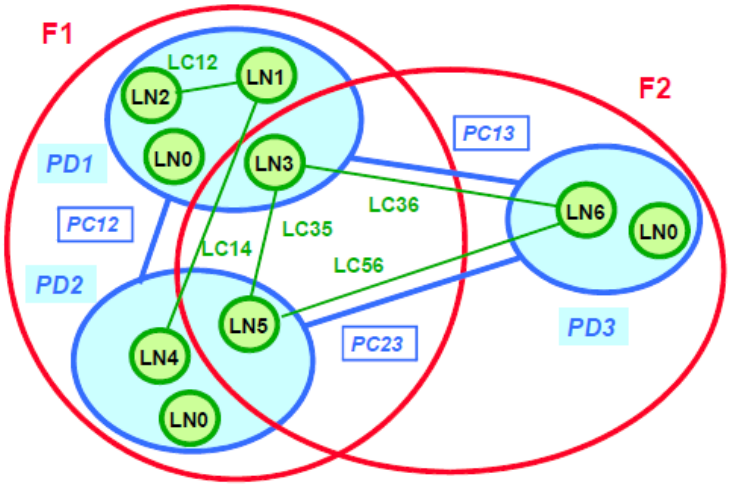

Figure 1 - The Logical Node and Link Concept

The description, in details, of this example demonstrates that F1 is implemented in PD1 through LN0, LN1, LN2 and LN3. LN1 and LN2 are connected through LC12. 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 functioning of the PACS.

IEC 61850 plays a key role in power system protection, automation and control. However, as the complexity of this system increases more vulnerable to cyber attacks it becomes. Cyber attacks can occur not only from external source, but internal too, for example: unsatisfied ex-employees, vendors,

third part maintenance staff, employees who may open messages from an untrusted source in corporate email, etc.
Since 2020, due to the current COVID-19 pandemic scenario, a considerable increase in the number of power utility staff have been working from home and accessing the substation's internal network through remote access. This is one of the reasons for opening security holes for threats. So, power system operators in several countries are examining a number of requirements to include, in their standard network procedures, IEC 61850 network monitoring.

2. CONSIDERATIONS ABOUT IEC 62351

The IEC 62351 standard was elaborated by WG (Working Group) 15 of IEC TC (Technical Committee) 57, aiming to deal with security stuff of TC 57 series of standards, including IEC 61850 series.
IEC 62351-6, whose title is “Security for IEC 61850”, addresses security matters of IEC 61850 communication protocols. The main contributions of IEC 62351-6 to GOOSE and SV security are the addition of an extra message field named “Authentication Value”, used to check integrity, and optional encryption methods. This one is not mandatory due to performance issues in case of time-critical requirements like in GOOSE (Type 1A “Trip”, performance class P2/3) and Sampled Values, because of additional processing time for cryptography, and in case of CPU with low processing power. Thus, encryption methods are recommended whenever it does not cause problems.
IEC 62351-7 describes the security monitoring of the PACS communication network infrastructure, referring to it as Network and System Management (NSM). This part of the standard defines the necessary data objects for this function, named NSM Data Objects (NSM DOs), whose goal is to get security monitoring information.

3. NETWORK MONITORING SYSTEM AND CYBERSECURITY FOR PACS

PACS network must incorporate monitoring functions, considering cybersecurity stuff, 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 a 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 any hardware/software issues in addition to cyberattacks aspects.
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 analyzed. 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 messages timing statistics in the network must be checked, considering the interval between frames, Transfer Time, Propagation Delay and the Processing Time.

Some requirements may not be foreseen in the monitoring system and this is an important issue to be addressed. 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 increasing 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. In practice, network monitoring can be performed either through a Trunk Port on the network Switch or through Port Mirroring.
Considering GOOSE frames carrying as data a Trip command, if these messages are not delivered to the SCU (Switchgear Control Unit) so that circuit breaker can take an act, the protection system is compromised, severely affecting substation operation. Before this situation happens, the monitoring system must detect this anomaly and point it to the supervisory as an alarm, indicating that a GOOSE frame that should be running is not there and register this event as a log to be analyzed by the user. A way for the monitoring system to implement this function is to analyze all IEDs instances (publishers and subscriber devices), through SCD file (or even ICD files), verifying if all the GOOSE messages are running on the substation network. For this, can be used some filters like Destination MAC Address, GOOSE Control Block Reference and Application ID from GOOSE frame structure. Figure 2 highlights these fields from a Wireshark capture.

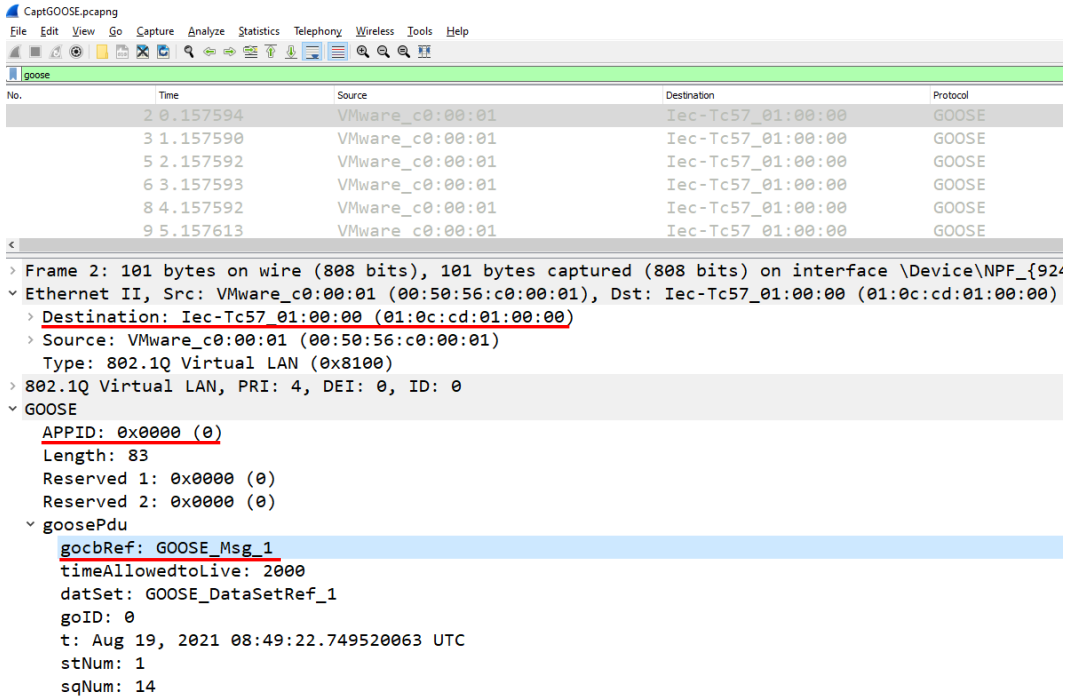

Figure 2 - Fields Suggestions for Analyzing GOOSE Running on the Network

Another damage situation possible to occur is an invader is able to publish malicious GOOSE frames on the network with two purposes : to open or to close a circuit breaker causing serious damages or causing a network overload in order to delay the legitimate GOOSE frames. In this case, the monitoring system must detect this anomaly, i.e. GOOSE frames expected according to SCD file, however, with retransmission times too different from what is configured or with wrong Sequence Number (SqNum) early or later than the expected one (out of order). To develop this functionality, monitoring system can analyze the frames incoming times and verify if the time difference between them are correct, also can check if SqNum is right. Figure 3 exemplifies this case : the fields highlighted in red demonstrate what must be checked by the monitoring system.

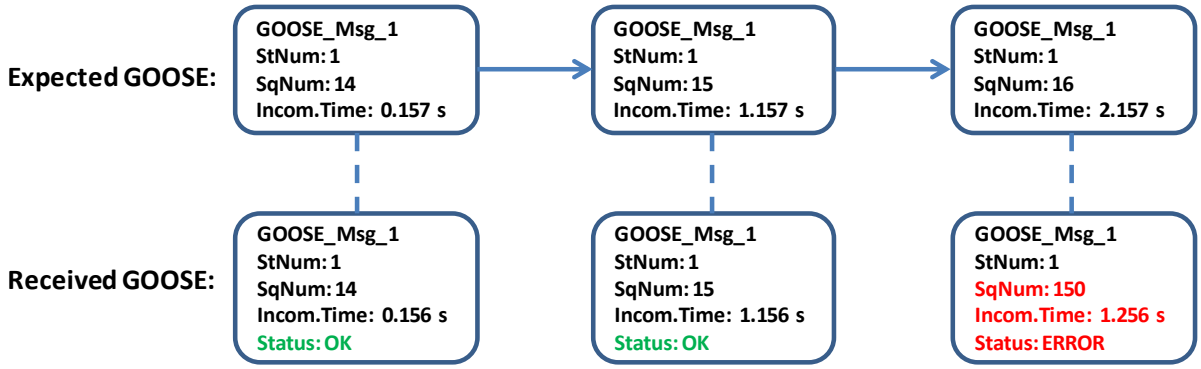

Figure 3 - Monitoring System Analyzing GOOSE Retransmission Times and Out of Order

A blind spot to monitoring system in the case described above is if the invader is able to publish malicious GOOSE frames in the right retransmission time and sequence order.

PTP (Precision Time Protocol) time synchronism is an aspect pretty important for monitoring system to check, i.e. must be able to verify if GM (Grand-Master) messages are running on the Ethernet network. It is a threat the loss of time synchronism, considering that MUs or SAMUs in the Process Level depend on it to operate properly; otherwise protection system may be compromised, because merging units will not sampling in the correct frequency. One way to analyze that GM messages are running is to verify if there are two main ones: Announce and Sync. Figure 4 is a Wireshark capture exemplifying the fields to identify these messages.

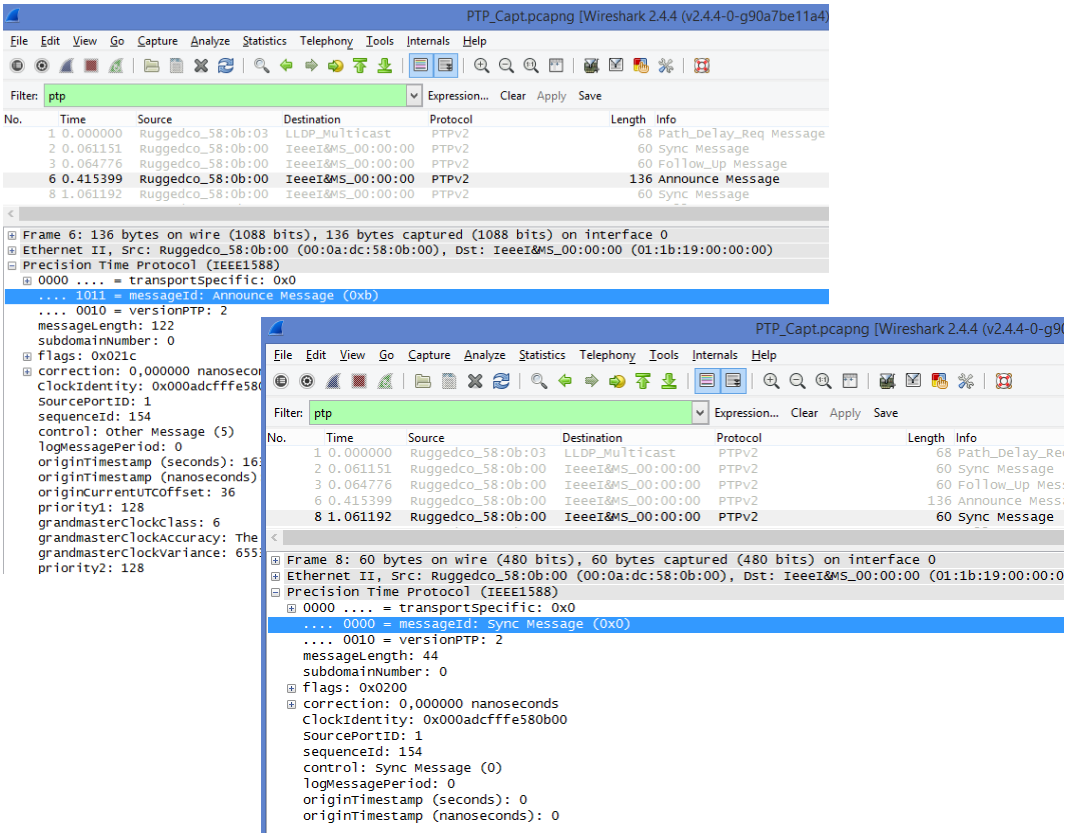

Figure 4 - Monitoring System Identifying Announce and Sync PTP Messages

The Best Master Clock Algorithm (BMCA) is used to choose the best node in the network in order to become the GM. This algorithm is dynamic and works this way : when no Announce was received for a defined time interval, all nodes (that implement BMCA) become master and send their own Announce messages. All nodes listen Announce message and verify its quality information of the clock (class, priorities and qualities fields). If a node concludes that the Announce received contains quality information better than their own, it stops sending Announce and becomes Slave ; but if a node

concludes that the Announce received is worse by its quality, the node stays in Master and continues to send Announce. So, in the network can only be one node as Master, receiving the name of Grand-Master.
It is important to consider that monitoring system must be a PTP slave, in order to synchronize with GM and to be in the same time base of all substation´s devices. Thus, monitoring system can also analyze if there is loss of time synchronism, by verifying if the slave clock jitter is increasing in relation to master clock. This situation may indicate two possibilities : Ethernet link is lost or, if link is healthy, some hardware problem may have occurred with Transparent Clock or even with calibration of GM clock and BMCA was yet unable to choose other GM.
Still on the PTP time synchronism issue, there is a possibility of an invader pretend to be the GM and break down the time synchronism of the substation. This attack can be performed in two ways : the invader may force sending GM messages with the same Clock Identity of the current GM or with different Clock Identity. The first case is a blind spot for monitoring system due to there is no way to differentiate the real GM messages from fake GM messages, because the Clock Identity is the same in both. The second case can be verified by the monitoring system through a “White List”, i.e. a list with all the possible Clock Identity of GM nodes in the substation´s network. As the Clock Identity of the threat is different from the current GM, monitoring system must verify if it is not on the “White List” to take some action like signaling by an alarm. Figure 5 shows where to find Clock Identity in Sync and Announce messages.

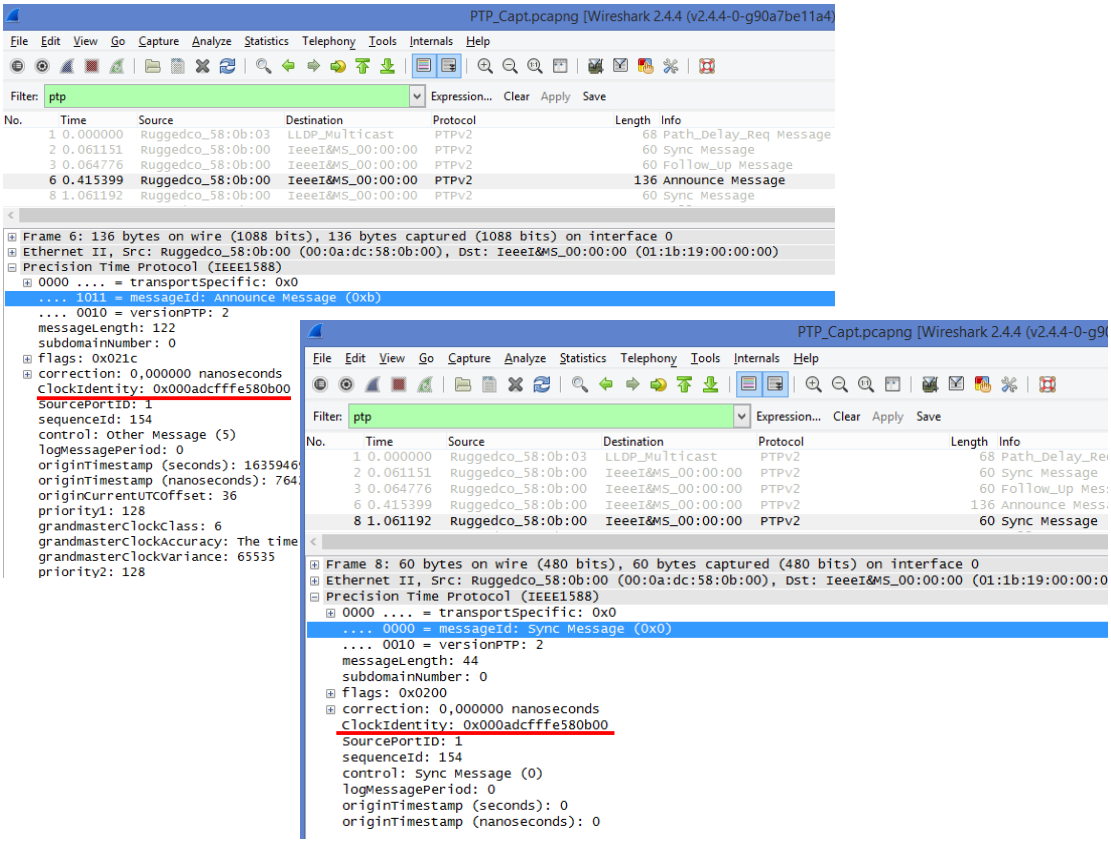

Figure 5 - GM Clock Identity in Sync and Announce Messages

An important function that monitoring system must implement is related to statistical analysis of SV and GOOSE frames.
In the case of Sampled Values, the goal is to verify propagation delay, processing time and time between frames. The first one is the time that a message takes to leave one device´s Ethernet port and enter another device´s Ethernet port, i.e. the network latency time. It is important the monitoring system to verify the propagation delay and to analyze if there is a network overload.
The processing time is the time a MU/SAMU takes to sampling the signals that are coming from instrument transformers, to encapsulate them into the standard frame and to publish them, plus the

network latency time. One way for the monitoring system to implement this functionality is, once all devices are synchronized, to calculate the time difference between 1PPS and the SV frame´s incoming time on the network board with Sample Counter 0. Thus, the users can analyze if it is going out of the ordinary time of processing. Also, it can be verified number of SV frames errors in the network, and the synchronism flag.
The time between frames indicates if the MU/SAMU is sampling properly according to what was set. This functionality can be implemented by the monitoring system just marking the frame's incoming time on the network board and getting the difference between them.
Figure 6 exemplifies these statistical analysis of SV frames.

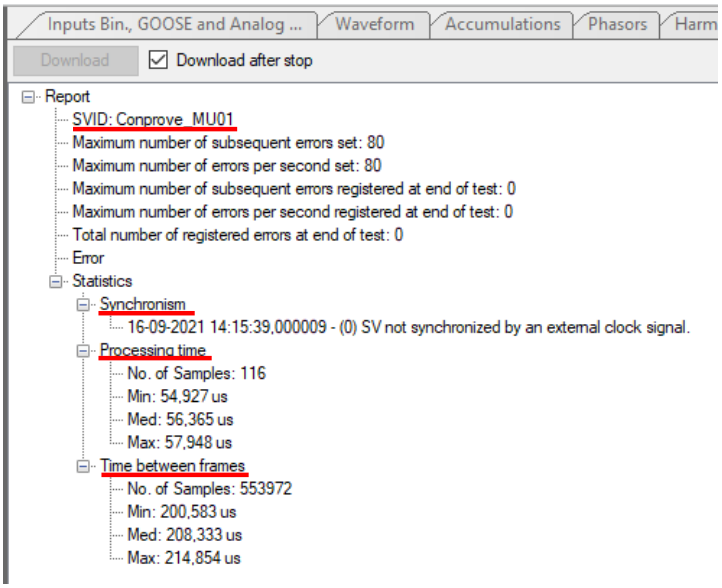

Figure 6 - Example of Statistical Analysis of SV Frames

In the case of GOOSE, the goal is to calculate the transfer time and to verify if it was under the limits defined by the IEC 61850-5 according to the performance classes defined in IEC 61850-8-1.
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: t_a, t_b and t_c, where:

- t_a 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;
- t_b is the network latency time;
- t_c is the time counted from the frame´s incoming moment at the subscriber to the frame is extracted from the receiving stack.

Printed from IEC 61850-5 Ed.1, Figure 7 illustrates the transfer time´s concept.

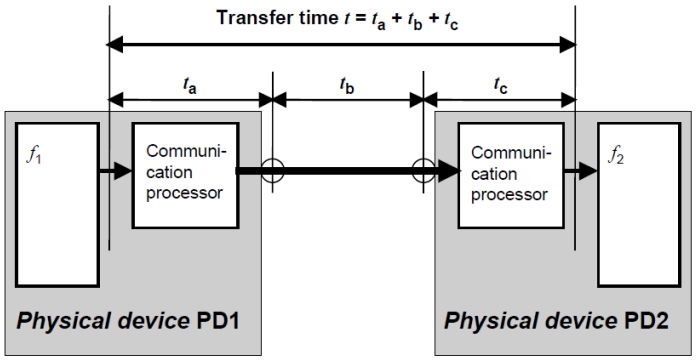

Figure 7 - The Concept of Transfer Time

For protection systems, the transfer time class for Trip applications is “TT6” and the transfer time must be up to 3ms. Printed 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

Based on that, it is very important the monitoring system to detect and to report any time greater than 3ms, considering GOOSE messages of protection trip.
An important monitoring functionality of GOOSE messages due to their retransmission time is related to the Time Allowed to Live field. This information can be used to alarm if packet losses occur.
IEC 61850 defined two logical nodes with specific data objects for monitoring of GOOSE and SV messages. The LNs LGOS and LSVS defined by IEC 61850-7-4 Ed.2.1 on items 6.3.5 and 6.3.6, respectively, can be analyzed by the monitoring system as a client of an IED as a server through MMS communication protocol.
LGOS has data objects specific for GOOSE monitoring purposes as they define subscription status information. Table 2, printed from the standard, shows these data objects in details.

Table 2 – Logical Node LGOS and Data Objects

LGOS				
Data object name	Common data class	T	Explanation	PresCond nds/ds
Descriptions				
NamPlt	LPL		inherited from: DomainLN	MONamPlt / na
Status information				
LastStNum	INS		Last state number of the received GOOSE message.	O / na
NdsCom	SPS		inherited from: SubscriptionSupervisionLN	O / na
St	SPS		inherited from: SubscriptionSupervisionLN	M / na
SimSt	SPS		inherited from: SubscriptionSupervisionLN	O / na
ConfRevNum	INS		inherited from: SubscriptionSupervisionLN	O / na
RxConfRevNum	INS		inherited from: SubscriptionSupervisionLN	O / na
Beh	ENS (BehaviourModeKind)		inherited from: DomainLN	M / na
Health	ENS (HealthKind)		inherited from: DomainLN	O / na
Mir	SPS		inherited from: DomainLN	MOcond(1) / na
Controls				
Mod	ENC (BehaviourModeKind)		inherited from: DomainLN	O / na
Settings				
GoCBRef	ORG		Object reference of subscribed GOOSE control block.	M / na
InRef	ORG		inherited from: DomainLN	Omulti / na

LSVS has data objects specific for Sampled Values diagnose and monitoring purposes as they define subscription status information. Table 3, printed from the standard, shows these data objects in details.

Table 3 - Logical Node LSVS and Data Objects

LSVS				
Data object name	**Common data class**	**T**	**Explanation**	**PresCond nds/ds**
Descriptions				
NamPlt	LPL		inherited from: DomainLN	MONamPlt / na
Status information				
NdsCom	SPS		inherited from: SubscriptionSupervisionLN	O / na
St	SPS		inherited from: SubscriptionSupervisionLN	M / na
SimSt	SPS		inherited from: SubscriptionSupervisionLN	O / na
ConfRevNum	INS		inherited from: SubscriptionSupervisionLN	O / na
RxConfRevNum	INS		inherited from: SubscriptionSupervisionLN	O / na
Beh	ENS (BehaviourModeKind)		inherited from: DomainLN	M / na
Health	ENS (HealthKind)		inherited from: DomainLN	O / na
Mir	SPS		inherited from: DomainLN	MOcond(1) / na
Controls				
Mod	ENC (BehaviourModeKind)		inherited from: DomainLN	O / na
Settings				
SvCBRef	ORG		Object reference of subscribed SV control block.	M / na
InRef	ORG		inherited from: DomainLN	Omulti / na

The final aspect monitoring issues worth approaching is related to the behaviour in Test/Simulation scenarios, i.e. how monitoring system must act when there are two SV frames running: one simulated and other real. In this case, a test set is going to publish SV with simulation bit set in the same time a MU/SAMU is going to publish real SV frames, that is with simulation bit reset. Thus, the monitoring system must be able to subscribe the SV frames published and to check the simulation bit field that is the most significant bit of the most significant byte of Reserved 1 field, like is shown in the Figure 8.

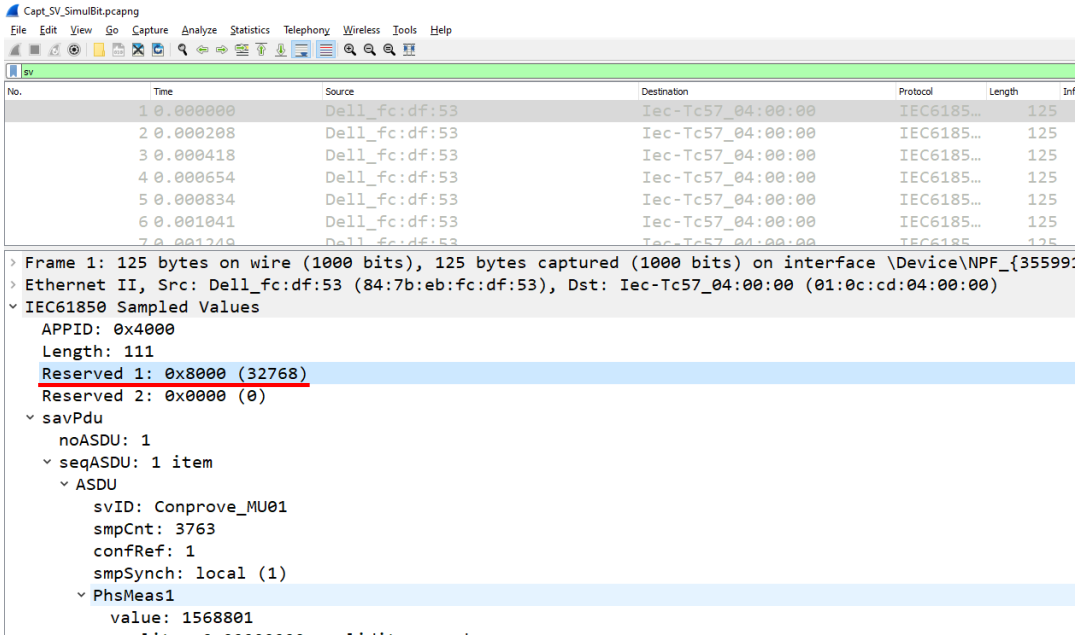

Figure 8 - Simulation Bit Set on SV Frame

If the monitoring system has not been notified that substation is under maintenance, it must report data inconsistency and save this information to a log.

4. CONCLUSIONS

Through this paper, it was possible to evaluate the requirements for the monitoring of the network and to evaluate the failure identification methodologies. Aspects not foreseen by network monitoring were also addressed, like its blind spots in case of the invader is able to publish malicious GOOSE frames in the right retransmission time and sequence order, or in case of the invader is able to send GM messages with the same Clock Identity of the current GM.

The deployment of a digital substation can be more reliable with the implementation of the monitoring system, because any failure event will be alarmed and logged so that will be possible to trace its causes, improving PACS this way.

In this way, it is expected this work has contributed so that the communication network can operate properly, as only in this way to ensure safe and reliable traffic of information, will the PACS be executed satisfactorily, making the dependence on the performance of the communication unquestionable.

5. BIBLIOGRAPHY

[1] Pereira Junior, P. S., Bernardino, R. C., Salge, G. S., Davi, M.Jr. B.B., Martins, C. M., Pereira, P. S., Lourenço, G. E. Avaliação da Performance de Uma Proteção de Linha Implementada com Barramento de Processo (IEC 61850-9-2) Através de Ensaios em Malha Fechada; STPC 2018; Brasil.

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

[3] Security Monitoring of IEC 61850 Substations Using IEC 62351-7 Network and System Management - Abdullah Albarakati; Chantale Robillard; Mark Karanfil; Marthe Kassouf; Mourad Debbabi; Amr Youssef; Mohsen Ghafouri; Rachid Hadjidj – IEEE, 2021.

[4] Cybersecurity Test-Bed for IEC 61850 based Smart Substations - Y. Yang; H. T. Jiang; K. McLaughlin; L. Gaol; Y.B. Yuan; W. Huang; S. Sezer. – IEEE, 2015.

[5] Standard IEC 62351-7 – "Power systems management and associated information exchange – Data and communications security – Part 7: Network and system management (NSM) data object models," 2017.

[6] Standard IEC 62351-6 – "Power systems management and associated information exchange – Data and communications security – Part 6: Security for IEC 61850.

[7] Network and System Management using IEC 62351-7 in IEC 61850 Substations: Desing and Implementation – Chantale Robillard – Concordia University, 2018.

[8] 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).

[9] Introduction to PTP Basics – NetTimeLogic, GMBH.

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

[11] Standard IEC 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.

[12] Standard IEC 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.