





Study Committee B5

**PROTECTION & AUTOMATION** 

## 10150

### Analysis of Network Monitoring in the Context of IEC 61850

Paulo Sérgio Pereira Junior, Rodolfo Cabral Bernardino, Gustavo Silva Salge, Cristiano Moreira Martins, Paulo Sergio Pereira, Gustavo Espinha Lourenço

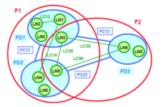
CONPROVE

### Objectives

- Importance of monitoring the IEC 61850 network;
- Network requirements necessary for monitoring;
- Implementation of monitoring techniques.

### Introduction

- Fully digital substations based on IEC 61850:
  - Process Bus highlights Ethernet communication network performance.
- C/S, SV and GOOSE:
  - Network aspects -> reliability, speed, availability and security of the information.
- Item 8.4.2 of IEC 61850-5 Ed.2:
  - Different application functions distributed through allocations of LNs in different PDs: exchange information through a communication network.



- Performance of the function to be executed depends on the network communication performance:
  - Communication network and its availability are part of this function: monitoring is vital.
- Vulnerabilities of SAS based on IEC 61850:
  - As the complexity of the system increases, more vulnerable to cyber attacks it becomes;
  - External and Internal threats.
- COVID-19 pandemic scenario:
  - Power utility staff have been working from home and accessing the substation's internal network through remote access: one of the reasons for opening security holes for threats.

## **Considerations about IEC 62351**

- Elaborated by WG 15 of IEC TC 57;
- Security aspects related to series of standards covered by TC 57, including IEC 61850 series;
- IEC 62351-6 "Security for IEC 61850":
  - Security matters of IEC 61850 communication protocols;
  - Contributions to GOOSE and SV security: addition of "Authentication Value" and optional encryption methods;
  - Performance issues in case of time-critical requirements of GOOSE and SV;
  - Encryption methods are recommended whenever it does not cause problems.
- IEC 62351-7:
  - Network and System Management (NSM);
  - NSM Data Objects (NSM Dos);
  - Management Information Base (MIBs).
- IEC 62351-14:
  - Implementation of security logs Syslog;
  - Importance of security logs for the cybersecurity operation centers.
- Detection mechanism on the IEC 62351:
  - SNMP defined on part 7: operational monitoring;
  - Syslog defined on part 14: security operation center.

### Network monitoring system and cybersecurity for PACS

- PACS network must incorporate monitoring functions able to:
  - Detect and point out anomalies or lacking of messages;
  - Detect lacking of synchronism signal;
  - Verify and point out abnormal propagation time;
  - Independent system;
  - Storing event records.







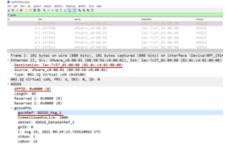
Study Committee B5

**PROTECTION & AUTOMATION** 

### 10150

# Analysis of Network Monitoring in the Context of IEC 61850 continued

- **PACS network** must incorporate **mechanisms** that offer **cybersecurity** to ensure:
  - Confidentiality;
  - Integrity;
  - Availability;
  - Authenticity.
- Some requirements may not be foreseen in the monitoring system – blind spot;
- Monitoring deal with: Test/Simulation configuration
   -> two SV streams: simulated and the real one;
- Monitoring system -> event logs to be stored and consulted;
- Trunk Port on the network Switch or through Port Mirroring;
- · GOOSE frames carrying as data a Trip command:
  - Not delivered to the SCU -> the protection system is compromised,
  - Monitoring system must detect this anomaly:
    - Is the GOOSE there?
    - Analyzing all IEDs instances through SCL file (SCD or ICD);
    - Filters like Destination MAC Address, GOOSE Control Block Reference and



- An invader could publish malicious GOOSE frames:
  - To open or to close a circuit breaker;
  - Causing a **network overload**.

Monitoring system must detect this anomaly:

- Retransmission times too different from what is configured or with wrong SqNum (out of order);
- Analyzing reception times of the frames and verifying the time difference, also SqNum.



- Blind spot: invader is able to publish malicious GOOSE frames in the right retransmission time and sequence order.
- PTP (Precision Time Protocol):
  - BMCA.

#### Monitoring system:

- To verify if **GM** messages;
- Analyzing Announce and Sync.

•					A.A.O. g90a7be11a4	
She hat you for	Capture Analyse Stati	intics Talephony Souls	premius (pip			
	IN DX CIS		000000	0 4 10 5 14 10	8	
Alter pla			Therein. Car A	uto Sana		
in New	Searce .	Outination	Protocol	Langth Info		
6 0.415299	Reppeter, McRell	0 Texes ( 01,00,00.0	10 #19942	1.16 Annual	CA Passage	
8.5.045592					white the second s	
- Ethernet II., 1 - President File	vies on white Comm ris Ruggedin, 58-58 Protocol (DAREASE transportiges)fic	100 (0000x0405810 40	captured (1088 bits) b:00), but: leex10r	1.00-00-00 (01-18-18	00.00.00)	
0010 -	versionits: 2	a secondar control				
messaget engl subdang treas	desti D	4				) (Birehan 2A4 (i2A4-0-g)
# flags: dwills	A DOUBLE PARTY AND	the Lot yes Go	Capture Analyse State	to heatery Josh in		
e locksdare in	an dwittladefffate	00482		******		🗰 50 🥵 56 🛛 22
boar conservation is testamentali tota constrain other message (O) inspressionapper tail 0 originitiestamp (secondo): 140 originitiestamp (secondo): 140 originitiestamp (secondo): 1 originitiestamp (secondo): 1 originitiestamp (secondo): 1 originitiestamp (secondo): 1 originitiestamp (secondo): 1 originitiestamp): 1 originitiestamp): 1 secondo originitiestamp): 1 secondo originitiestamp): 1 secondo originitiestamp): 1 secondo originitiestamp): 1 secondo originitiestamp): 1 originitiestamp):		Filter yes			Equation. Our Apply	See
		2 0.040115 3 0.064776 6 0.415100 6 3.040197	Instant England on J. A. (A. (A. (A. England on J. A. (A. (A. England on J. A. (A. (A. England on J. A. (A. (A. Rugged on J. A. (A. (A. (A.			Langh Info III Profit, John Lay, Jr. III Profit, John Lay, Jr. III Antoning Pro- IIII Antoning Pro- IIII Antoning Pro- IIII Antoning Pro- IIII
priority21 1		Ethervet II. or Precision Time	rc: Ruggedca, 38:06 Protocol (1668358 CramportIgec(F1c)	00 (00:0a)dc158:06: 0	red (480 bits) on in DO), Dut: Inex18r5_D	terface 0 0:00:00 (01:130:139:00:00)
		Clocksdentity BourcePort20 sequence3d: Byne Tognessagere ortgintimesta	hi A4 her:0 2,000000 ranosecore 21 0x000adcffffc3400 1 1 154 0 Message (2)			

 Loss of time synchronism, -> threat in the Process Level;

Monitoring system:

- Must be a PTP slave;
- To verify if the slave clock jitter is increasing in relation to master clock.
- · If time synch is lost -> two possibilities
  - · Some interference;
  - Hardware problem with Transparent Clock or calibration of GM clock.
- Invader pretends to be the GM and break down the time synchronism:
  - With the same Clock Identity of the current GM - blind spot for monitoring systems;
  - With different Clock Identity can be verified by the monitoring system through a "White List".







Study Committee B5

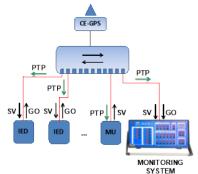
**PROTECTION & AUTOMATION** 

## 10150

# Analysis of Network Monitoring in the Context of IEC 61850 continued



Monitoring system -> statistical analysis of SV and GOOSE frames;



Sampled Values:

- Propagation delay;
- Processing time;
- Time between frames;
- Errors in the network;
- Synchronism flag.

Inputs Bin, GOOSE and Analog Waveform Accumulations Phasors Harm
Download Download after stop
B-Report
- SVID: Conprove_MU01
<ul> <li>Maximum number of subsequent errors set: 80</li> </ul>
<ul> <li>Maximum number of errors per second set: 80</li> </ul>
<ul> <li>Maximum number of subsequent errors registered at end of test: 0</li> </ul>
<ul> <li>Maximum number of errors per second registered at end of test: 0</li> <li>Table endered existence area at end of best. 0</li> </ul>
<ul> <li>Total number of registered errors at end of test: 0</li> <li>Error</li> </ul>
R-Statistics
Synchroniam
- 16-09-2021 14:15:39,000009 - (0) SV not synchronized by an external clock signal.
Processing time
- No. of Samples: 116
Min: 54,927 us
Med: 56,365 us
Max: 57,948 us
Time between frames
No. of Samples: 553972 Min: 200.583 us
- Med: 208 333 us
- Max: 214.854 us

#### GOOSE:

- Transfer time.
- LN for monitoring IEC 61850-7-4 Ed.2.1 :
  - LGOS;
  - LSVS.
- Monitoring system -> two SV frames running: one simulated and other real:
  - Test set -> to publish SV with simulation bit set x MU/SAMU -> to publish real SV frames;
  - 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.

	34	have	Industry	Poled	angle 1
	2.0.000200	Dell_fc:df:53	Ist-Tc57_04:00:00		
	3.0.000418	Dell_fc:df:53	Isc-Tc57_84:88:88	TECGLES.	
	4.0.000554	Dell_fc:df:53	Isc-Tc57_84:88:88	TECGLES.	
	5.0.000334	Dell_fc:df:53	Isc-Tc57_04:00:00	TECHIRS.	
	6.0.001041	Dell_fc:df:53	Isc-Tc57_04:00:00	TECHLES.	
APPID Lengt Reser	0 Sampled Values : 0x4000 h: 111 ved 1: 0x8000 (327 ved 2: 0x0000 (0)	<u>68)</u>			
APPID Lengt Reser Reser - sauAd nok	: 0:4000 h: 111 ved 1: 0:8000 (327 ved 2: 0:0000 (0) u SDU: 1 SDU: 1 item	<u>88)</u>			
4910 Lengt Reser Reser - savAd nok - sasj - AS	: 0:4000 h: 111 yed 1: 0:80000 (327 yed 2: 0:00000 (8) u SDU: 1 SDU: 1 SDU: 1 iten SDU: 1 iten SUD: Congrove_MUB suDD: 1 3743 confRef: 1	1			
APPID Lengt Reser - savPd nok - sep - AS	: 0x4000 h: 111 vad 1: 0x8000 (327 vad 2: 0x8000 (0) v EDU: 1 EDU: 1 EDU: 1 iten DU supO: Comprove_MUE supOrt: 3763	1			

### Conclusions

- It was possible to evaluate the requirements for the monitoring of the network and the failure identification methodologies;
- Aspects not foreseen by network monitoring were also addressed (blind spots);
- The deployment of a digital substation can be more reliable with the implementation of the monitoring system:
- Any failure event will be alarmed and logged so that will be possible to trace its causes.
- It is expected that this work contributes to enable proper operation of communication networks, as this is the only way to ensure safe and reliable traffic of information.