

CE-B5 - Análise do monitoramento de rede no contexto da norma IEC 61850

*Paulo Sergio Pereira Jr – Rodolfo Cabral Bernardino – Gustavo Silva Salge –
Cristiano M. Martins – Paulo Sergio Pereira – Gustavo E. Lourenço*

CONPROVE



Brasil

Objectives



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

Introduction



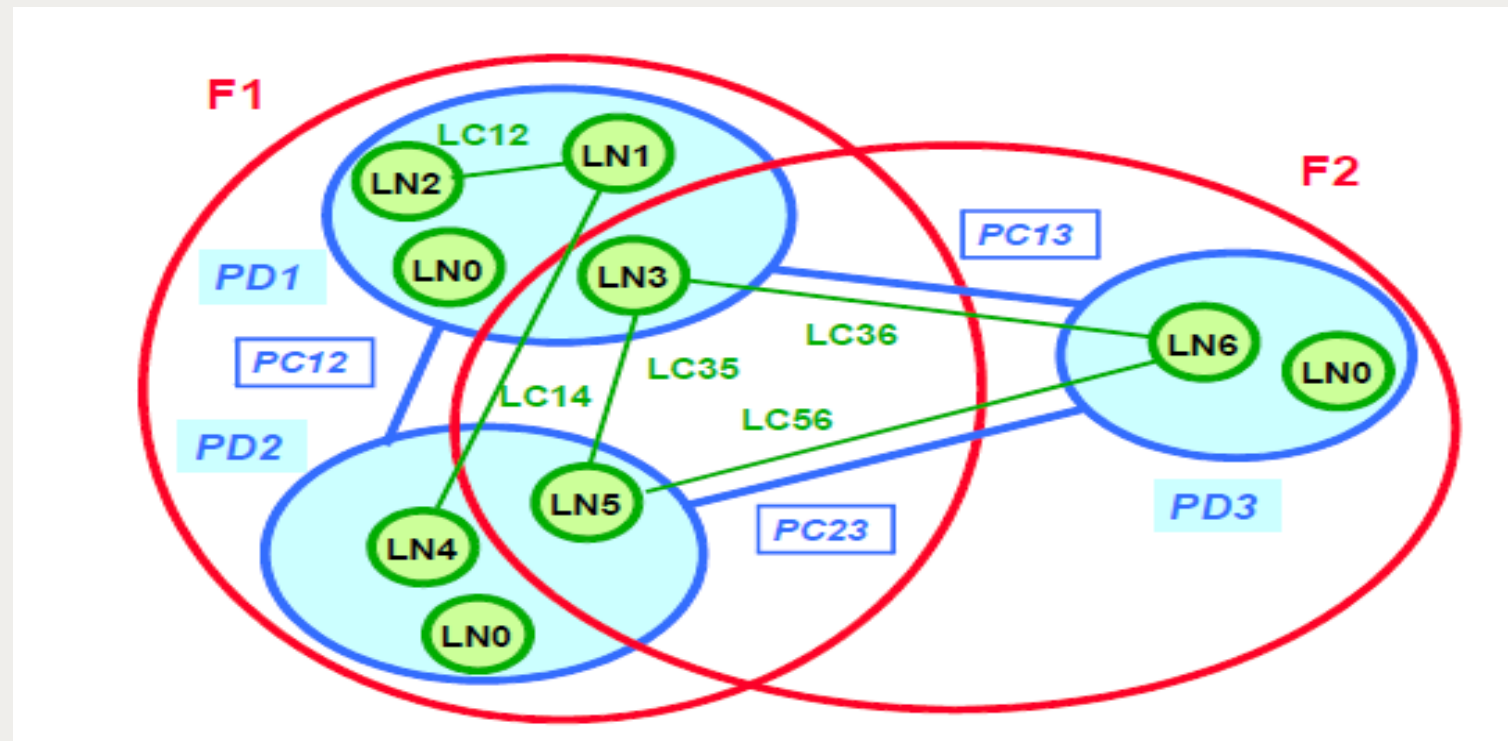
- **Fully digital substations based on IEC 61850:**
 - **Process Bus highlights Ethernet communication network performance.**

- **C/S, SV and GOOSE:**
 - **Network aspects: reliability, speed, availability and security of the information.**

Introduction



- 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.



Introduction



- **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**.

Network monitoring system and cybersecurity for PACS



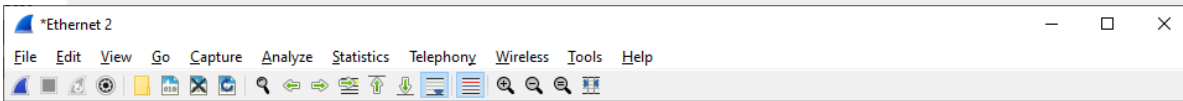
- **PACS network** must incorporate **monitoring functions** able to:
 - Detect and point out **anomalies** or **lacking** of messages;
 - Detect **lacking of synchronism** signal;
 - Verify and point out **abnormal propagation time**;
 - **Independent system**;
 - **Storing event records**.
- **PACS network** must incorporate **mechanisms** that offer **cybersecurity** to ensure:
 - **Confidentiality**;
 - **Integrity**;
 - **Availability**;
 - **Authenticity**.

Network monitoring system and cybersecurity for PACS



- 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 **Application ID**.

Network monitoring system and cybersecurity for PACS



No.	Time	Source	Destination
855857	3.114660	Dell_87:a4:5b	Iec-
855859	0.000000	Dell_87:a4:5b	Iec-
855862	0.000000	Dell_87:a4:5b	Iec-

> Frame 477400: 234 bytes on wire (1872 bits), 234 by
Ethernet II, Src: Dell_87:a4:5b (f0:4d:a2:87:a4:5b)
> Destination: Iec-Tc57_01:00:57 (01:0c:cd:01:00:57)
> Source: Dell_87:a4:5b (f0:4d:a2:87:a4:5b)
Type: IEC 61850/GOOSE (0x88b8)

> GOOSE
APPID: 0x0390 (912)
Length: 220
> Reserved 1: 0x0000 (0)
Reserved 2: 0x0000 (0)

> goosePdu
gocbRef: CONPROVEMaster/LLN0\$GO\$GoCB01
timeAllowedtoLive: 40000
datSet: CONPROVEMaster/LLN0\$TT6DataSet2
goID: CONPROVE_GO1
t: May 10, 2023 17:35:09.764996647 UTC
stNum: 2
sqNum: 0
simulation: False
confRev: 1
ndsCom: False
numDatSetEntries: 24
allData: 24 items

Arquivo Início Exibir Opções Software

Importar SCL Adicionar IED Remover Orfão -> IED Teste Múltiplo Comparar SCL Orfãos

Arquivo SCL Multi Teste Verificações

Origen Geral Comparação SCL x Rede Orfão Estatística Supervisão Gravação

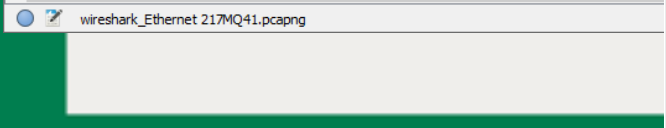
Sistema

GO/SV Todos

IED

- CONPROVE
- GOOSE
 - LD Master
 - GoCB01
 - GoCB02
 - GoCB03

Defined	Found
Control Block	Control Block
Control Block CONPROVEMaster/LLN0\$GO\$GoCB01	Control Block CONPROVEMaster/LLN0\$GO\$GoCB01 ✓
MAG Destino 01:0c:cd:01:00:57	MAG Destino 01:0c:cd:01:00:57 ✓
AppID 57	AppID 912 ⚠
GOOSE ID CONPROVE_GO1	GOOSE ID CONPROVE_GO1 ✓
DataSet CONPROVEMaster/LLN0\$TT6DataSet2	DataSet CONPROVEMaster/LLN0\$TT6DataSet2 ✓
VLAN ID 2213	VLAN ID 2213 ✓
VLAN Priority 6	VLAN Priority 6 ✓
Needs Commissioning False	Needs Commissioning False ✓
Config Rev 1	Config Rev 1 ✓
Simulation False	Simulation False ✓
Time to Live 40000 ms	Time to Live 40000 ms ✓
Nº de DataSets 24	Nº de DataSets 24 ✓
DataSet	DataSet
Nome Tipo	Nome Tipo
FlxLgcGAPC1.Ind003.stVal Boolean	FlxLgcGAPC1.Ind003.stVal Boolean ✓
> FlxLgcGAPC1.Ind003.q Quality	> FlxLgcGAPC1.Ind003.q Quality ✓
FlxLgcGAPC1.Ind004.stVal Boolean	FlxLgcGAPC1.Ind004.stVal Boolean ✓
> FlxLgcGAPC1.Ind004.q Quality	> FlxLgcGAPC1.Ind004.q Quality ✓
FlxLgcGAPC1.Ind005.stVal Boolean	FlxLgcGAPC1.Ind005.stVal Boolean ✓
> FlxLgcGAPC1.Ind005.q Quality	> FlxLgcGAPC1.Ind005.q Quality ✓
FlxLgcGAPC1.Ind006.stVal Boolean	FlxLgcGAPC1.Ind006.stVal Boolean ✓
> FlxLgcGAPC1.Ind006.q Quality	> FlxLgcGAPC1.Ind006.q Quality ✓
FlxLgcGAPC1.Ind007.stVal Boolean	FlxLgcGAPC1.Ind007.stVal Boolean ✓
> FlxLgcGAPC1.Ind007.q Quality	> FlxLgcGAPC1.Ind007.q Quality ✓
FlxLgcGAPC1.Ind008.stVal Boolean	FlxLgcGAPC1.Ind008.stVal Boolean ✓
> FlxLgcGAPC1.Ind008.q Quality	> FlxLgcGAPC1.Ind008.q Quality ✓
FlxLgcGAPC1.Ind052.stVal Boolean	FlxLgcGAPC1.Ind052.stVal Boolean ✓
> FlxLgcGAPC1.Ind052.q Quality	> FlxLgcGAPC1.Ind052.q Quality ✓
FlxLgcGAPC1.Ind053.stVal Boolean	FlxLgcGAPC1.Ind053.stVal Boolean ✓
> FlxLgcGAPC1.Ind053.q Quality	> FlxLgcGAPC1.Ind053.q Quality ✓
FlxLgcGAPC1.Ind054.stVal Boolean	FlxLgcGAPC1.Ind054.stVal Boolean ✓
> FlxLgcGAPC1.Ind054.q Quality	> FlxLgcGAPC1.Ind054.q Quality ✓

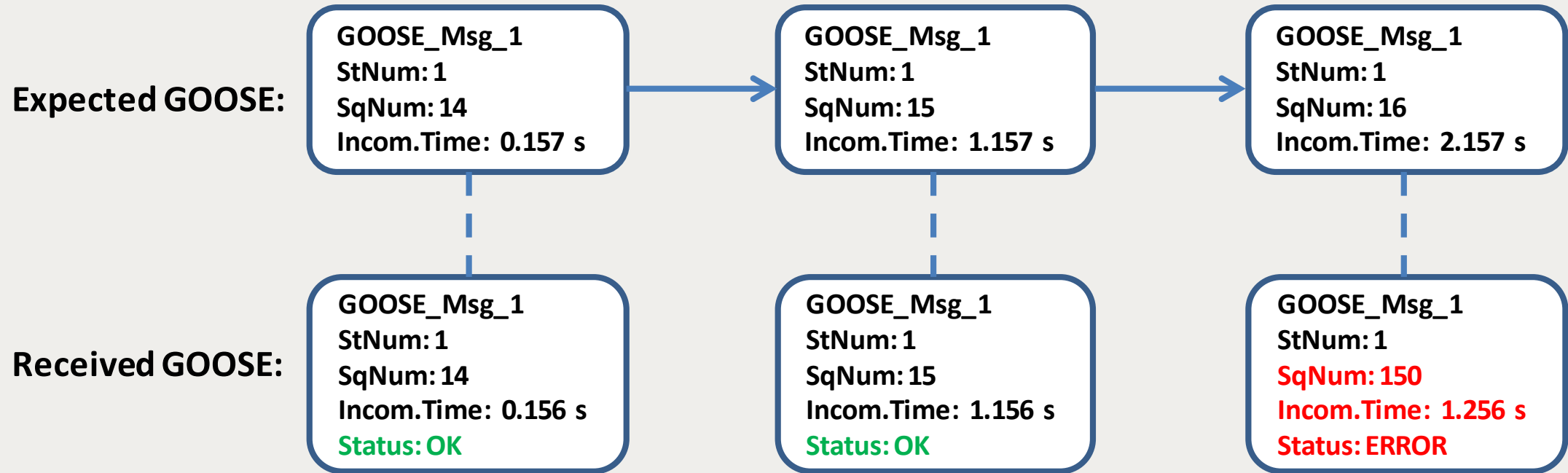


Network monitoring system and cybersecurity for PACS



- 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**.

Network monitoring system and cybersecurity for PACS



- **Blind spot:** invader is able to publish malicious GOOSE frames in the right retransmission time and sequence order.

Network monitoring system and cybersecurity for PACS



- **PTP** (Precision Time Protocol):
 - **BMCA**: used to choose the **best node** in the network in order to become the **GM**;
- **Monitoring system**:
 - To verify if **GM** messages are **running** on the Ethernet network;
 - Must analyze **Announce and Sync**.

Network monitoring system and cybersecurity for PACS



*Ethernet 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ptp

No.	Time	Source	Destination	Protocol	Length	Info
153737	0.003839	RuggedCo_58:0b:00	IEEEI&MS_00:00:00	PTPv2	60	Follo...
172120	2.354194	RuggedCo_58:0b:02	LLDP_Multicast	PTPv2	68	Peer_...
206329	0.647823	RuggedCo_58:0b:00	IEEEI&MS_00:00:00	PTPv2	136	Annou...
206505	0.003231	RuggedCo_58:0b:00	IEEEI&MS_00:00:00	PTPv2	60	Svnc...

> Frame 206329: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits) on interface \

> Ethernet II, Src: RuggedCo_58:0b:00 (00:0a:dc:58:0b:00), Dst: IEEEI&MS_00:00:00 (01:1b:19:

> Precision Time Protocol (IEEE1588)

0000 = majorSdoId: Unknown (0x0)

.... 1011 = messageType: **Announce** message (0xb)

0000 = minorVersionPTP: 0

.... 0010 = versionPTP: 2

messageLength: 122

domainNumber: 0

minorSdoId: 0

> flags: 0x021c

> correctionField: 0,000000 nanoseconds

messageTypeSpecific: 0

> ClockIdentity: 0x000adcfffe580b00

SourcePortID: 1

sequenceId: 5095

controlField: Other Message (5)

logMessagePeriod: 0

originTimestamp (seconds): 1683741620

originTimestamp (nanoseconds): 73520282

originCurrentUTCOffset: 36

priority1: 128

grandmasterClockClass: 6

messageType (ptp.v2.messageType), 1 byte(s)

*Ethernet 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ptp

No.	Time	Source	Destination
153737	0.003839	RuggedCo_58:0b:00	IEEEI&MS_00:00:00
172120	2.354194	RuggedCo_58:0b:02	LLDP_Mu
206329	0.647823	RuggedCo_58:0b:00	IEEEI&MS_00:00:00
206505	0.003231	RuggedCo_58:0b:00	IEEEI&MS_00:00:00

> Frame 206505: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \

> Ethernet II, Src: RuggedCo_58:0b:00 (00:0a:dc:58:0b:00), Dst: IEEEI&MS_00:00:00 (01:1b:19:

> Precision Time Protocol (IEEE1588)

0000 = majorSdoId: Unknown (0x0)

.... 0000 = messageType: **Sync** Message (0x0)

0000 = minorVersionPTP: 0

.... 0010 = versionPTP: 2

messageLength: 44

domainNumber: 0

minorSdoId: 0

> flags: 0x0200

> correctionField: 0,000000 nanoseconds

messageTypeSpecific: 0

> ClockIdentity: 0x000adcfffe580b00

SourcePortID: 1

sequenceId: 6315

Config. PTP

Configuração

Config. OCS

Endereço MAC Orig: 00:50:56:C0:00:01

< VLAN

Habilitado	Sim
ID	1
Prioridade	4
Máx PathDelayReq	1s
Nº Domínio	0
Precisão Desejada	1ms

Última Leitura

Refresh

Config. OCM

Endereço MAC Orig: 00:0A:DC:58:0B:00

< VLAN

ID	0
Prioridade	4
Nº Domínio	0
< Flag_Field_Octet1	
Flag_Leap61	Não
Flag_Leap59	Não
Flag_CurrentUTCOffsetValid	Sim
Flag_PTPTimeScale	Sim
Flag_TimeTraceable	Sim
Flag_FrequencyTraceable	Não
< Source Port Identity	
Clock Identity	00:0A:DC:FF:FE:58:0B:00
Port Number	1
Current UTC OffSet	36
< Grand Master	
Priority	128

Status OCS: Offset: 5224 ns Delay: 5286 ns (SINC OK)

Ok Cancelar

Network monitoring system and cybersecurity for PACS

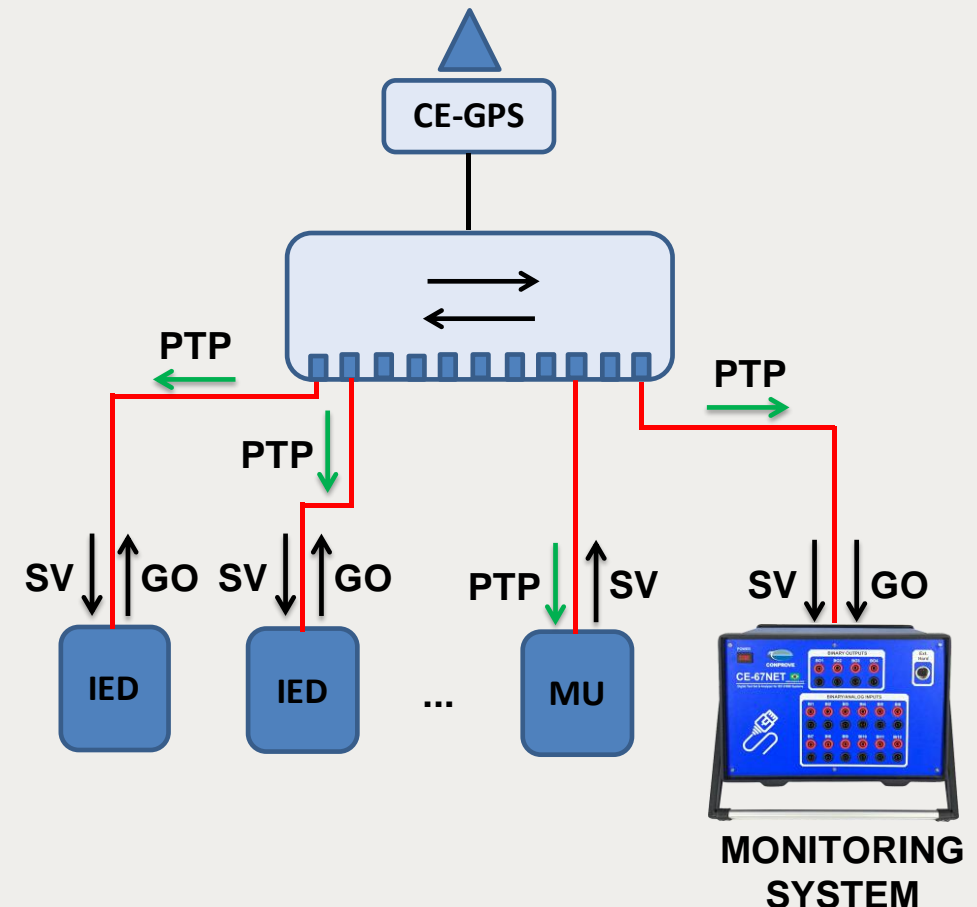


- **Loss of time synchronism -> threat in the Process Level;**
- **Monitoring system:**
 - Must be a **PTP slave**;
 - **To verify** if the slave **clock jitter** is increasing in relation to **master clock**.
- **If time synch is lost -> two possibilities**
 - **Some interference**;
 - **Hardware problem** 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”**.

Network monitoring system and cybersecurity for PACS



- **Monitoring system -> statistical analysis of SV and GOOSE frames;**
- **Sampled Values:**
 - Propagation delay;
 - Processing time;
 - Time between frames;
 - Errors in the network;
 - Synchronism flag.



Network monitoring system and cybersecurity for PACS



Arquivo Início Exibir Opções Software

Importar SCL Adicionar IED Remover Orfão Teste Múltiplo Comparar SCL Orfãos Iniciar Estatística Iniciar Supervisão Iniciar Gravação Parar Limpar Direc Canais Config Hrd Config Sync Apresentar Relatório Restaurar Layout

Arquivo SCL Multi Teste Verificações Limpeza Hardware Relatório Layout

Origem Geral Comparação SCL x Rede Orfão **Estatística** Supervisão Gravação

Sistema

GO/SV Todos

IED

- SES2DMUP1
 - GO GOOSE
 - SV SV
 - LD SV
 - SES2DMUP1SV1

IEDs: 1 (GO: 2, SV: 1)

GO (Default) **SV (Default)** Item Sel. Hab. Padrão

Habilitar Avaliação

Avaliar Sincronismo

Temp. Processamento (TP) máx permitido: 3,00 ms

Escoregamento do Clock máx permitido: 5,00 µs

Nº máx - Amostras Perdidas: 0

Nº máx - Amostras Duplicadas: 0

Nº máx - Amostras Fora de Sequência: 0

Nº máx - Time Outs: 0

Nº máx - TP maior que máx permitido: 0

Control Block

Informações do Pacote

MAC Origem: F0:4D:A2:87:A4:5B

Status Sincronização: (1) SV sincronizado por um sinal de clock de uma área local não especificada.

Grandmaster Clock ID

Estatísticas

Tempo Inicial	31/03/2023 10:40:59	-
Duração	8,00 s	-
Tempo Final	31/03/2023 10:41:07	-
Tempo Último Recebimento	31/03/2023 10:41:07	-
Nº Pacotes	19439	-
Nº Amostras Recebidas	38878	-
Nº Amostras Perdidas	0	✓
Nº Amostras Duplicadas	8	⚠
Nº Amostras Fora de Sequência	0	✓
Taxa de amostragem	4800	-
Último pacote SmpCnt=0	31/03/2023 10:41:07	-
Desvio Clock (Atual)	1,01 µs	✓
Desvio Clock (Acumulado)	1,64 µs	-
Time Out	Não	-
Nº de Time Outs	0	✓
Intervalo dos Pacotes:		-
Mínimo	22,78 µs	-
Médio	416,49 µs	-
Máximo	431,34 µs	-
Tempo de Processamento (TP):		-
Mínimo	286,30 µs	-
Médio	287,54 µs	-
Máximo	288,48 µs	✓
Nº TP Maior que Máx Config.	0	✓

DataSet

Nome	Tipo	Valor
ASDU 1		

Network monitoring system and cybersecurity for PACS



- **GOOSE:**
 - Transfer time, out of order, quality not good
- **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 (simulation bit set) x MU/SAMU -**
 - > to publish real SV frames;

Network monitoring system and cybersecurity for PACS



Control Block	
Control Block	CONPROVEMaster/LLN0\$GO\$GoCB01
MAC Destino	01:0C:CD:01:00:57
AppID	57
GOOSE ID	CONPROVE_GO1
DataSet	CONPROVEMaster/LLN0\$TT6DataSet2
VLAN ID	2213
VLAN Priority	6
Needs Commissioning	False
Config Rev	1
Simulation	False
Time to Live	40000 ms
Nº de DataSets	24

Control Block	
Control Block	CONPROVEMaster/LLN0\$GO\$GoCB01
MAC Destino	01:0C:CD:01:00:57
AppID	912
GOOSE ID	CONPROVE_GO1
DataSet	CONPROVEMaster/LLN0\$TT6DataSet2
VLAN ID	2213
VLAN Priority	6
Needs Commissioning	False
Config Rev	1
Simulation	True
Time to Live	40000 ms
Nº de DataSets	24

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**.



MUITO OBRIGADO!!!

Paulo Sergio Pereira Junior



CONPROVE
E N G E N H A R I A

www.conprove.com.br