



## **GRUPO DE ESTUDO DE PROTEÇÃO, MEDIÇÃO, CONTROLE E AUTOMAÇÃO EM SISTEMAS DE POTÊNCIA - GPC**

### **DIAGNÓSTICOS E MONITORAMENTO DE REDES DE COMUNICAÇÃO EM SUBESTAÇÕES DIGITAIS**

**PAULO SERGIO PEREIRA JUNIOR(1); PAULO SERGIO PEREIRA(1); CRISTIANO MOREIRA MARTINS(1); RODOLFO CABRAL BERNARDINO(1); GUSTAVO ESPINHA LOURENÇO(1); GUSTAVO SILVA SALGE(1) CONPROVE INDÚSTRIA E COMERCIO DE PRODUTOS ELETROELETRONICOS LTDA(1)**

#### **RESUMO**

O conceito básico de monitoramento de rede está relacionado à verificação sistemática desta em busca de anomalias que possam comprometer seu correto funcionamento. Desta forma, o monitoramento da rede IEC 61850 é necessário durante todo o ciclo de vida da subestação digital. Isto significa que o monitoramento deve ser realizado nas etapas de comissionamento como Factory Acceptance Test (FAT) e Site Acceptance Test (SAT), e testes de manutenção.

A importância do monitoramento de rede está vinculada à detecção precoce dos erros, às condições de operação da rede, à redução da indisponibilidade da rede através do rastreamento dos elementos problemáticos, ao registro de todos os eventos de rede, e à segurança e estabilidade do sistema de energia. Dispositivos especializados são necessários para monitorar estes aspectos, atuando como "oscilógrafos de rede" ou "registrador digital de rede". Esse sistema de monitoramento deve ser implementado em hardware e software de forma a abranger todos os requisitos de tempo crítico dos protocolos GOOSE e Sampled Values (SV).

Diversos aspectos de rede devem ser analisados para garantir a segurança, confiabilidade, velocidade e disponibilidade das informações a serem transmitidas, alertando potenciais falhas de comunicação ou invasões. Estes aspectos de rede estão relacionados à integridade da mensagem, configuração e segurança dos dados, sincronismo de tempo do sistema e às estatísticas de tempo da mensagem, considerando intervalo entre frames, transfer time, perda de pacotes e etc.

Sendo assim, este artigo tem o objetivo de realizar uma análise da importância do monitoramento de rede no contexto da IEC 61850, destacando os requisitos necessários para o monitoramento e discutindo suas implementações, abordando estudos de casos em subestações digitais.

#### **PALAVRAS-CHAVE**

IEC 61850, PACS, monitoramento de rede, GOOSE, Sampled Values, PTP

#### **1.0 INTRODUÇÃO**

Os sistemas de Proteção, Automação e Controle (PACS) estão evoluindo devido às constantes inovações ocorridas com o surgimento da norma IEC 61850, cuja primeira edição foi lançada em 2003. Progressivamente, a utilização da norma está aumentando em todo o mundo com o objetivo de implementar subestações totalmente digitais, onde o Barramento de Processos destaca ainda mais a importância da performance da rede de comunicação no PACS.

De acordo com a estrutura de dados estabelecida pela IEC 61850, é possível executar diferentes funções de aplicação (F1 e F2) distribuídas através de alocações de Logical Nodes (LN) em diferentes Physical Devices (PD), que trocarão informações pela rede, onde os LNs estão conectados através de Logical Connections (LC) e PDs estão conectados através de Physical Connections (PCs), de acordo com o exemplo clássico demonstrado no item 8.4.2 da IEC 61850-5 Ed.2, demonstrada na Figura 1 abaixo:

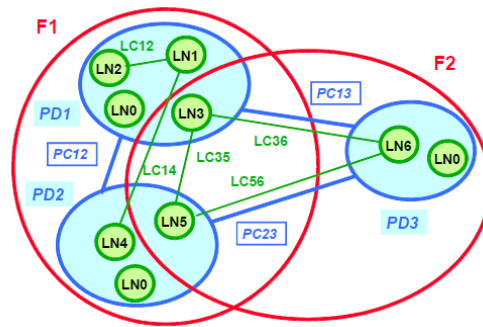


Figura 1 - Conceitos de Logical Node e Conexões

A descrição em detalhes deste exemplo demonstra que F1 está implementado em PD1 através de LN0, LN1, LN2 e LN3. Da mesma forma, F1 está implementado em PD2 através de LN0, LN4 e LN5. PD1 e PD2 estão conectados através de PC12. LN1 (PD1) e LN4 (PD2) estão conectados através de LC14. LN3 (PD1) e LN5 (PD2) estão conectados através de LC35.

Este exemplo demonstra claramente que a performance da função a ser executada depende do desempenho da rede de comunicação, sendo assim a rede e sua disponibilidade fazem parte desta função. Portanto, é de vital importância monitorar a rede para garantir a correta operação do PACS.

Toda a troca de dados recomendada pela norma é baseada nos seguintes protocolos de comunicação: Cliente/Servidor (MMS), Sampled Values (SV), GOOSE e Precision Time Protocol (PTP). SV e GOOSE possuem requisitos de tempo crítico, então a fim de aumentar a confiabilidade, um sistema de monitoramento dedicado é necessário, capaz de marcar as estampas de tempo do recebimento destes frames por hardware. O PTP, no seu Power Profile, é o protocolo de sincronismo de tempo preferido pela norma como descrito na IEC 61850-9-3.

No contexto da IEC 61850, o objetivo do monitoramento de rede é realizar uma análise profunda de toda a rede de comunicação da subestação em busca de anomalias, envolvendo tanto testes de comissionamento quanto de manutenção. No caso de FAT/SAT, o sistema de monitoramento pode detectar erros antes de a subestação entrar em operação. Alguns problemas podem ser detectados precocemente como Merging Units (MUs) publicando frames SV fora de ordem, ou pacotes mal-formados, ou com tempo fora da taxa de amostragem, ou ainda escorregamento de clock indicando erros de sincronismo. Em testes de manutenção, o sistema de monitoramento pode, por exemplo, realizar um sniffer da rede e encontrar frames GOOSE ou SV órfãos, apontando para um tráfego não previsto no arquivo SCL, ou seja, fora da "White List". Este tipo de erro pode indicar problemas de segurança também. Outro objetivo do monitoramento é realizar uma análise estatística da rede, mostrando, em tempo real, dados como atraso de pacote, transfer time, escorregamento de clock e etc.

Baseado no item 11.1.1.4 da IEC 61850-5 Ed.2, o transfer time é definido como o tempo de transmissão completo de um frame incluindo o tempo de processamento no processador de comunicação dos dispositivos publicador e assinante. Em detalhes, é a soma de três tempos:  $t_a$ ,  $t_b$  e  $t_c$ , onde:

- $t_a$  é o tempo contado a partir do momento em que o publicador coloca o frame no topo da pilha de transmissão até o momento em que ele é enviado pela rede;
- $t_b$  é o tempo de latência da rede;
- $t_c$  é o tempo contado a partir da chegada do frame no assinante até o momento em que ele é extraído da pilha de recebimento.

De acordo com a IEC 61850-5 Ed.1, a Figura 2 ilustra o conceito de transfer time:

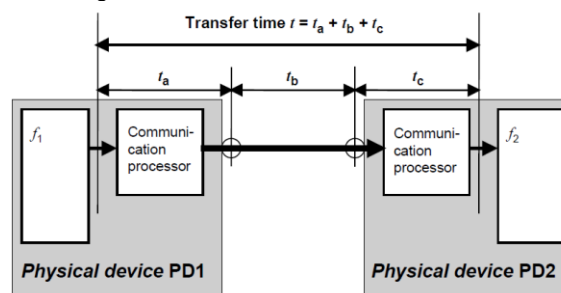


Figura 2 - O Conceito de Transfer Time

Para os sistemas de proteção, a classe de transfer time para aplicações de Trip é "TT6" e deve ser menor que 3ms. De acordo com a IEC 61850-5 Ed.2, a Tabela 1 abaixo mostra as classes para transfer times:

Tabela 1 - Classes para 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

Da mesma forma, de acordo com a IEC 61850-5 Ed.2, item 11.2.4 “Type 4 – Raw data messages (“Samples”)”, o transfer time para amostras sincronizadas de Merging Units para funções de proteção também são de classe TT6, então devem ser menor que 3ms. A Tabela 2, baseada nesta edição da IEC 61850-5, mostra:

Tabela 2 - Classes de Transfer Times para Amostras Sincronizadas

Performance class	Requirement description	Transfer time		Typical for Interface (IF)
		Class	ms	
P7 <sup>a</sup>	Delay acceptable for protection functions using these samples	TT6	≤ 3	4,8
P8 <sup>b</sup>	Delay acceptable for other functions using these samples	TT5	≤ 10	2,4,8
<sup>a</sup> equivalent to P1.				
<sup>b</sup> equivalent to P2.				

Sendo assim, tanto transfer time de GOOSE quanto de SV para aplicações de Trip e proteção, respectivamente, devem ser menores que 3ms.

Além disso, a IEC 61869-9 Ed.1, item 6.902.2 “Maximum processing delay time requirement” trata do conceito de tempo de processamento das MUs, que é o tempo entre a digitalização dos sinais das entradas analógicas até a publicação dos frames SV. Assim, este tempo deve ser mensurado na saída de rede da MU, de maneira a não levar em conta o tempo de latência de rede. O tempo de processamento máximo neste caso é de 2ms. A Tabela 3, baseada nesta edição da IEC 61869-9, mostra:

Tabela 3 - Tempo Máximo de Processamento para 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

Nos tópicos a seguir, os requisitos de um sistema de monitoramento de rede, composto por hardware e software, serão abordados, abrangendo estudos de casos no monitoramento de subestações digitais.

## 2.0 SISTEMA DE MONITORAMENTO DE REDE PARA PACS

O sistema de monitoramento é uma ferramenta essencial para solução de problemas de redes de subestações digitais, então o operador nacional do sistema elétrico brasileiro – ONS – discutiu diversos requisitos e está incluindo, no procedimento de rede, o monitoramento das redes IEC 61850.

De acordo com este documento, a rede PACS deve incorporar funções de monitoramento capazes de:

- 1) Detectar e apontar anomalias ou perda de mensagens, como GOOSE e SV, ou ainda mensagens não previstas;
- 2) Detectar perda de sinal de sincronismo;
- 3) Verificar e apontar tempo anormal de propagação, ou seja, latência, e assimetria ou variação excessiva, isto é, jitter, dos tempos de propagação das mensagens;
- 4) Ser implementado de uma forma independente dos dispositivos de proteção ou teleproteção;
- 5) Ter recursos para armazenar gravações dos eventos de detecção das anomalias.

Também, a rede PACS deve incorporar mecanismos que ofereçam cyber segurança para garantir os seguintes tópicos:

- 1) Confidencialidade: limitar o acesso aos dados apenas para usuários autorizados;
- 2) Integridade: garantir que não há modificações não autorizadas de dados das mensagens ou informações roubadas;
- 3) Disponibilidade: garantir o acesso autorizado aos dados ou serviços;
- 4) Autenticidade: garantir que os dados vêm de uma fonte legítima.

Sendo assim, o sistema de monitoramento deve ser capaz de armazenar os problemas de rede da subestação, e deve gerar arquivos que registrem todo o tráfego de rede, como por exemplo, o formato PCAP, muito popular entre os softwares analisadores de protocolos de rede, para avaliação de eventos sincronizados no tempo.

De forma a garantir que todas as funcionalidades descritas acima serão abrangidas pelo sistema de monitoramento, alguns aspectos de rede devem ser analisados. Um destes aspectos está relacionado à integridade das mensagens, ou seja, se não há perda de pacotes ou pacotes corrompidos. Também, relacionado à configuração e segurança dos dados, deve-se verificar se todas as mensagens previstas nos arquivos SCL da subestação estão presentes na rede e se há tráfego de mensagens não previstas. E, relacionado à estrutura do frame, comparando campos como endereços MAC de origem e de destino, VLAN ID e tag de prioridade.

Outro aspecto de rede a ser considerado é o sincronismo de tempo do sistema, através da verificação do tráfego de mensagens PTP.

Finalmente, as estatísticas de tempo das mensagens na rede devem ser verificadas, considerando o intervalo entre frames, transfer time, e etc. Também, deve ser avaliado o comportamento do sistema de monitoramento em uma configuração de teste/simulação quando houverá, por exemplo, duas streams SV na rede: uma simulada vinda de um dispositivo de teste e outra real vinda de uma MU.

Essas verificações permitirão aumentar a confiabilidade, segurança e, conseqüentemente, a disponibilidade da rede, alertando potenciais falhas de comunicação (causadas por um erro no adaptador de rede do IED, por exemplo), ou invasões. Logs de eventos deverão ser gerados para armazenamento e consulta, tornando possível rastrear o problema e localizar sua origem. Além disto, os logs de eventos podem ser utilizados em relatórios para facilitar a compreensão da falha. Para otimizar as avaliações, arquivos PCAP podem ser armazenados para uma análise mais detalhada dos eventos com etapas de pré-trigger e pós-trigger. Na prática, o monitoramento de rede pode ser realizado através da porta trunk do switch ou por espelhamento de portas, para ter acesso a todo o tráfego da rede a despeito de VLANs.

O sistema de monitoramento deve implementar funcionalidades que atendam a alguns modos de análise. No modo de validação do SCL, o objetivo principal é comparar todo o arquivo SCL e verificar se há qualquer informação não compatível com a norma IEC 61850, como o comprimento dos campos nos frames, recomendação do range de endereços MAC de destino, melhores práticas de configuração como um endereço MAC de destino por stream GOOSE ou SV, e outros. No modo sniffer, o objetivo principal é examinar a rede e averiguar se há tráfego não previsto pelo arquivo SCL, isto é, frames GOOSE ou SV não incluídos na "White List", conhecidos como "órfãos", e confirmar que todo o tráfego esperado está presente na rede. Com este último, uma verificação completa campo-a-campo deve ser realizada para comparar o frame que está trafegando na rede com aquele respectivo descrito no arquivo SCL. O objetivo disto é encontrar diferenças de configuração como Application ID e Configuration Revision. No modo de supervisão, o objetivo principal é verificar a rede em busca de erros. Diversos eventos de supervisão podem ser configurados dependendo de qual protocolo será supervisionado. No caso da supervisão GOOSE, alguns exemplos de eventos:

- Time Allowed to Live (TTL) está expirado: este evento ocorre se a mensagem GOOSE não estiver presente na rede por um tempo igual ou maior que o máximo permitido, de acordo com a definição da norma referente ao campo TTL;
- Frames fora de ordem: este evento ocorre se o sequence number ou state number estiver fora da sequência definida na norma;
- Pacotes mal-formados: este evento ocorre se o formato do frame GOOSE não está em conformidade com as definições da norma;
- Frames nunca vistos: este evento ocorre se o frame GOOSE não está presente na rede por um tempo suficiente para concluir que ele nunca foi visto;
- Eventos de quality dos dados: estes eventos ocorrem se os bits Validity forem diferentes de "good" ou ainda se o bit Test alterar seu valor;
- Eventos de quality do timestamp: estes eventos ocorrem se o byte "Time Quality" do campo timestamp alterou qualquer um dos bits, ou ainda se o bit "Clock not Synchronized" estiver true;
- Evento de transfer time: este evento ocorre se o transfer time GOOSE é maior que o esperado.

No caso do PTP, alguns exemplos de eventos:

- Perda de sincronismo: este evento ocorre se o escravo perde as mensagens do mestre;
- Escorregamento de clock: este evento ocorre se o clock do escravo está escorregando mais que o esperado em relação ao clock do mestre;
- Alteração da acurácia do grandmaster: este evento ocorre se a acurácia do clock do mestre foi alterada;

- Estabelecimento da sincronização: este evento ocorre quando o escravo sincroniza seu clock com o do mestre numa acurácia definida;
- Alteração do ID do grandmaster: este evento ocorre se foi detectada uma alteração no ID do mestre, indicando que outro grandmaster assumiu como fonte de sincronismo PTP;
- Atualização do valor do current UTC offset do grandmaster: este evento ocorre quando é detectado que houve alteração no valor do current UTC offset do mestre. A flag de UTC offset valid deve ser verificada pelo sistema de monitoramento para indicar se a alteração do UTC offset do mestre foi válida.

No caso do SV, alguns exemplos de eventos:

- Timeout expirado: este evento ocorre se os frames SV de uma MU não estiverem presentes na rede por um determinado tempo;
- Frames fora de ordem: este evento ocorre se o sample counter está fora da sequência definida pela norma;
- Pacotes mal-formatados: este evento ocorre se o formato do frame SV não está em conformidade com as definições da norma;
- Frames nunca vistos: este evento ocorre se o frame SV não está trafegando na rede por um tempo suficiente para concluir que ele nunca foi visto;
- Eventos de quality das amostras: este evento ocorre se os bits Validity forem diferentes de “good” ou ainda se bit Test alterar seu valor;
- Escorregamento de clock: este evento ocorre se o clock da MU está escorregando mais que o esperado;
- Evento de tempo de digitalização + transfer time: este evento ocorre se o tempo alocado pela MU para processar e publicar o frame SV somado à latência da rede é maior que o esperado;
- Alteração da flag de sincronismo: este evento ocorre se o campo da flag de sincronismo foi alterado, indicando alguma mudança no tipo de sincronismo da rede.

Em todos esses eventos abordados acima, um registro de arquivo PCAP deve ser realizado para disponibilizar o tráfego de rede considerando as etapas de pré-trigger e pós-trigger. Desta forma, o sistema de monitoramento irá atuar como um “oscilógrafo de rede” ou “registrador digital de rede”.

No modo de estatística, deverá ser realizada uma análise dos frames GOOSE e SV de forma a implementar uma verificação específica e objetiva com dados estatísticos destes tráfegos de rede. Esta análise abrange todos os campos do frame, incluindo dados e quality.

No caso do GOOSE, a análise estatística deve verificar o tempo de recebimento dos pacotes, e alguns contadores como: pacotes recebidos, alterações de state number, alterações perdidas de state e sequence numbers e pacotes duplicados. Além disso, deve ser avaliado se ocorreu expiração de TTL e um contador indicando quantas vezes isto ocorreu. Com relação à análise de transfer time, o sistema de monitoramento deve calcular os valores máximo, médio e mínimo encontrados durante o processamento. Também, um contador deve indicar o número de vezes que o transfer time foi maior que o valor determinado por norma.

No caso do SV, a análise estatística deve verificar o tempo de recebimento dos pacotes e os contadores: pacotes recebidos e sample counter perdidos. Além disso, deve verificar a quantidade de frames fora de sequência e duplicados. Também, o sistema de monitoramento deve avaliar o tempo de recebimento do frame com sample counter zero, o escorregamento de clock da MU atual e acumulado desde o início do processamento. Se determinados frames SV não estiverem trafegando na rede por um determinado tempo e o número de vezes que isto ocorreu, também devem ser avaliados pelo sistema de monitoramento. Com relação à análise dos tempos de digitalização + transfer time, o sistema de monitoramento deve calcular os valores máximo, médio e mínimo encontrados durante o processamento. Os valores máximo, médio e mínimo do intervalo entre frames SV também devem ser calculados.

É importante salientar que em condições de teste/simulação, ou seja, quando houver duas streams GOOSE ou SV trafegando na rede como a mesma identificação, mas uma publicada de um dispositivo real e outra de um dispositivo de teste, o sistema de monitoramento deve considerar dois diferentes filtros, que implica na configuração de duas diferentes mensagens: uma com o bit de simulação false e outra com o bit de simulação true.

### 3.0 ESTUDOS DE CASO

Neste tópico, alguns casos de problemas de rede em subestações digitais serão discutidos, como também a forma que o sistema de monitoramento pode detectar e identificar estes problemas para auxiliar na solução.

O primeiro caso está relacionado a erros de frames SV duplicados devido a um problema de RedBox (Redundancy Box). Este fato ocorreu numa subestação com 13 MUs e, por volta, de 168 streams GOOSE inseridas na arquitetura de rede.

Os frames SV estavam sendo publicados na taxa de amostragem preferida da IEC 61869-9, a 4800 amostras/segundo e 2 ASDUs. O problema de duplicação de frames acontecia cada segundo nos mesmos sample counters, e na saída da RedBox, isto é, os frames estavam sendo publicados na ordem correta pela MU. Este erro pôde ser detectado pelo sistema de monitoramento como um evento de “fora de sequência” no modo de supervisão, evidenciando que o sample counter atual não é o incremento de uma unidade do anterior, como demonstrado na Figura 3.

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		Sample Count: 3332 (3333)
6	✖	14/11/2022 07:24:03.694470	CE-67NET 01	ETH1	SV	Out of sequence		Sample Count: 3332 (3333)
5	✖	14/11/2022 07:24:02.694460	CE-67NET 01	ETH1	SV	Out of sequence		Sample Count: 3332 (3333)
4	✖	14/11/2022 07:24:01.694470	CE-67NET 01	ETH1	SV	Out of sequence		Sample Count: 3332 (3333)
3	✖	14/11/2022 07:24:00.694460	CE-67NET 01	ETH1	SV	Out of sequence		Sample Count: 3332 (3333)
2	✖	14/11/2022 07:23:59.694460	CE-67NET 01	ETH1	SV	Out of sequence		Sample Count: 3332 (3333)
1	✖	14/11/2022 07:23:58.694470	CE-67NET 01	ETH1	SV	Out of sequence		Sample Count: 3332 (3333)

Date:	14/11/2022 07:23:58.694470	Device:	CE-67NET 01
Classification:	Critical	Interface:	ETH1
Category:	SV	Network Traffic:	Download PCAP
Event:	Out of sequence Sample Count Received = 3332 Previous Sample Count = 3333	Origin:	
		Destination MAC:	01:0C:CD:04:24:23

Figura 3 - Evento de Supervisão SV "Fora de Sequência"

Os frames duplicados estavam relacionados aos sample counters 3332 e 3333 nos frames 2716 e 2717, como mostra o arquivo PCAP na Figura 4.

<p>Frame 2716: 209 bytes on wire (1672 bits), 209 bytes captured on interface 0</p> <p>Ethernet II, Src: IEC61850 Sampled Values, Dst: IEC61850 Sampled Values</p> <p>APPID: 0x5aca Length: 195</p> <p>Reserved 1: 0x0000 (0) Reserved 2: 0x0000 (0)</p> <p>savPdu noASDU: 2 seqASDU: 2 items</p> <p>ASDU svID: [redacted] smpCnt: 3332 confRev: 180001 smpSynch: global (2) PhsMeas1: [redacted] gmIdentity: [redacted]</p> <p>ASDU svID: [redacted] smpCnt: 3333 confRev: 180001 smpSynch: global (2) PhsMeas1: [redacted] gmIdentity: [redacted]</p>	<p>Frame 2717: 209 bytes on wire (1672 bits), 209 bytes captured on interface 0</p> <p>Ethernet II, Src: IEC61850 Sampled Values, Dst: IEC61850 Sampled Values</p> <p>APPID: 0x5aca Length: 195</p> <p>Reserved 1: 0x0000 (0) Reserved 2: 0x0000 (0)</p> <p>savPdu noASDU: 2 seqASDU: 2 items</p> <p>ASDU svID: [redacted] smpCnt: 3332 confRev: 180001 smpSynch: global (2) PhsMeas1: [redacted] gmIdentity: [redacted]</p> <p>ASDU svID: [redacted] smpCnt: 3333 confRev: 180001 smpSynch: global (2) PhsMeas1: [redacted] gmIdentity: [redacted]</p>
---	---

Figura 4 - Arquivo PCAP com Frames SV Duplicados

O sistema de monitoramento também pôde detectar estes frames SV duplicados no modo estatística, verificando que o contador de frames duplicados foi incrementado, como mostrado na Figura 5.

Origin	General	Comparison SCL x Network	Orphan	Statistic	Supervision	Recording																																																
<p>System</p> <p>GO/SV: All</p> <p>IED</p> <ul style="list-style-type: none"> <li>GOOSE</li> <li>SV</li> <li>LD SV</li> </ul>				<p>Control Block</p> <p>Package Information</p> <p>Statistics</p> <table border="1"> <tr><td>Initial Time</td><td>16/11/2022 18:20:08</td></tr> <tr><td>Duration</td><td>8,00 s</td></tr> <tr><td>Final time</td><td>16/11/2022 18:20:16</td></tr> <tr><td>Receive time</td><td>16/11/2022 18:20:16</td></tr> <tr><td>Packages</td><td>21477</td></tr> <tr><td>Samples seen</td><td>42954</td></tr> <tr><td>Samples missed</td><td>0</td></tr> <tr><td>Samples duplicate</td><td>9</td></tr> <tr><td>Samples Out of Sequence</td><td>0</td></tr> <tr><td>Sampling rate</td><td>4800</td></tr> <tr><td>Last packet SmpCnt=0</td><td>16/11/2022 18:20:16</td></tr> <tr><td>Clock drift (Current)</td><td>-2,45 µs</td></tr> <tr><td>Clock drift (since start)</td><td>-1,16 µs</td></tr> <tr><td>Timed Out</td><td>No</td></tr> <tr><td>Timed Out count</td><td>0</td></tr> <tr><td>Packet Interval:</td><td></td></tr> <tr><td>  Minimum</td><td>22,78 µs</td></tr> <tr><td>  Average</td><td>416,49 µs</td></tr> <tr><td>  Maximum</td><td>431,52 µs</td></tr> <tr><td>Processing Time (PT):</td><td></td></tr> <tr><td>  Minimum</td><td>285,95 µs</td></tr> <tr><td>  Average</td><td>287,21 µs</td></tr> <tr><td>  Maximum</td><td>288,52 µs</td></tr> <tr><td>No. of PT Greater than Max Config.</td><td>0</td></tr> </table>			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
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																																																					

Figura 5 - Frames Duplicados no Modo Estatística SV

Ainda analisando esta mesma subestação digital, foi verificado um erro de compatibilidade com os requisitos da norma relacionados ao range de endereços MAC de destino. Na IEC 61850-9-2 Ed. 2, Anexo B, é possível verificar a recomendação de endereçamento MAC multicast, de acordo com cada protocolo, como mostrado na Tabela 4 retirada da norma.

Tabela 4 - Recomendação de Endereçamento Multicast

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

No arquivo SCL desta subestação, os endereços MAC de destino estavam fora do range recomendado pela norma, como mostrado na Figura 6, composta pelo arquivo SCL e registro PCAP.

```
<SMV IdInst="SV" cbName= >
  <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">SACA</P>
  </Address>

```

```
> Frame 2717: 209 bytes on wire (1672 bits), 209 bytes captured (1672 bits) on interface
> Ethernet II, Src: , 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:

```

Figura 6 - SCL: Verificação de Compatibilidade com a IEC 61850

O sistema de monitoramento pôde detectar esta incompatibilidade com a norma através do modo de validação SCL.

O segundo exemplo conta com quatro diferentes fabricantes de IEDs, e com streams GOOSE e SV sendo publicadas. Problemas relacionados a frames GOOSE duplicados e perda de sincronismo da MU foram detectados pelo sistema de monitoramento, tanto no modo de supervisão quanto no modo de estatística.

No modo de supervisão, foram verificados frames GOOSE duplicados como evento de "fora de sequência", como mostrado na Figura 7.

The screenshot shows the 'Supervision' mode interface. At the top, there are tabs for 'Origin', 'General', 'Comparison SCL x Network', 'Orphan', 'Statistic', 'Supervision', and 'Recording'. The 'Event List' tab is active, displaying a table with columns: N°, C., Date, Device, Interface, Category, Event, IED, and Details. A single event is listed with N° 1, Classification 'Critical', Date '01/12/2022 10:07:59.978470', Device 'CE-67NET 01', Interface 'ETH1', Category 'GOOSE', and Event 'Out of sequence'. Below the table, the 'Details' section shows: 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: , Destination MAC: .

Figura 7 - Frame GOOSE Duplicado no Modo de Supervisão

O sistema de monitoramento também pôde verificar perda de sincronismo da MU no modo de estatística, como mostrado na Figura 8.

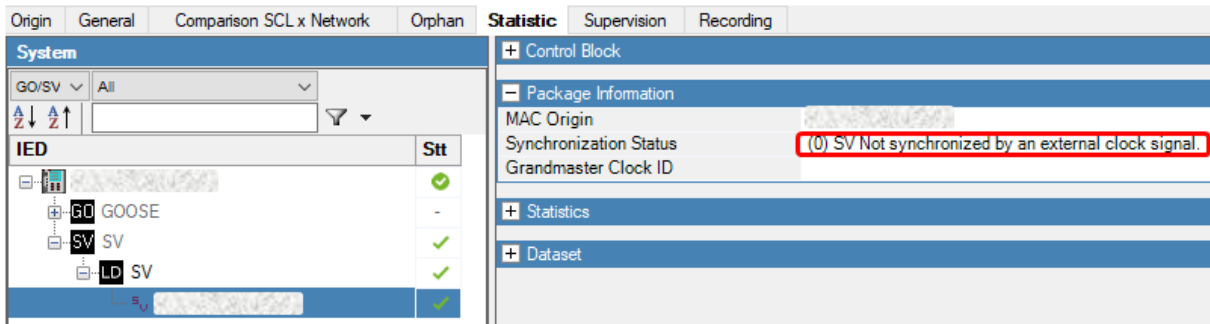


Figura 8 - Detecção de Perda de Sincronismo da UM

O terceiro exemplo conta com problemas de incompatibilidade dos arquivos SCL entre os IEDs, de forma que ocorreram erros de processamento na importação destes arquivos em um IED quando exportados por outro IED do mesmo fabricante. Estes erros ocorreram devido a diferenças entre os frames que estavam trafegando na rede e os respectivos frames descritos nos arquivos SCL. O sistema de monitoramento pôde detectar esta questão através do modo sniffer, identificando as diferenças entre os campos dos frames, como mostrado na Figura 9.

Defined	Found
Control Block	Control Block
Control Block	Control Block
MAC Destination	MAC Destination
AppID 10242	AppID 9984
GOOSE ID	GOOSE ID
Dataset	Dataset
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

Figura 9 - Comparação SCL x Frames Trafegando na Rede

#### 4.0 CONCLUSÕES

Este trabalho realizou um estudo detalhado do monitoramento de rede no contexto de subestações digitais, discutindo os requisitos necessários para a implementação de um sistema de monitoramento completo, que abrange todo o ciclo de vida da subestação digital: etapas de testes de comissionamento como FAT e SAT, e testes de manutenção.

Foram abordados estudos de casos em subestações digitais com um sistema de monitoramento completo, desenvolvido em hardware e software, que implementa diversas funcionalidades, sendo capaz de realizar análises de arquivos SCL, sniffer de rede, supervisão e estatística de protocolos GOOSE, SV e PTP. Foram discutidos diversos problemas de rede e a forma que o sistema de monitoramento pôde detectar e identificar tais erros para auxiliar na solução.

Somente quando a rede de comunicação estiver operando adequadamente para garantir um tráfego seguro e confiável de dados, o PACS será implementado satisfatoriamente, tornando inquestionável a confiança no desempenho da comunicação.

#### 5.0 BIBLIOGRAFIA

[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.

## DADOS BIOGRÁFICOS



Paulo Sergio Pereira Junior é o diretor da empresa CONPROVE, uma empresa de alta tecnologia com foco em pesquisa e desenvolvimento de instrumentos elétricos de teste. Graduou-se em Engenharia Elétrica em 2004 pela Universidade Federal de Uberlândia, UFU. Também se formou em Administração de Empresas em 2006 pela UFU, e concluiu MBA pela Fundação Getúlio Vargas, FGV, como especialista em Gestão de Projetos. Paulo tem mais de quinze anos de experiência em Desenvolvimento e Aplicação em Projetos de Software e Hardware para Proteção, Automação e Controle de Sistemas de Potência na CONPROVE.

### (2) PAULO SERGIO PEREIRA

Paulo é engenheiro Eletricista, Graduado em 1975, pela ESCOLA FEDERAL DE ENGENHARIA DE ITAJUBÁ (EFEI). Mestre em Ciências, em 1977 também pela UNIFEI e PhD, em 1980, pela UNIVERSITY OF MANCHESTER INSTITUTE OF SCIENCE AND TECHNOLOGY (UMIST), em Manchester, Inglaterra. Atualmente é diretor da CONPROVE ENGENHARIA. Possui mais de 30 anos de experiência em Pesquisa e Desenvolvimento de Instrumentos de Testes de Relés.

### (3) CRISTIANO MOREIRA MARTINS

Cristiano Moreira Martins é Engenheiro Eletricista formado pela Universidade Federal de Uberlândia em 2004. Desde 2005 trabalha na Conprove com foco em pesquisa e desenvolvimento de novos produtos voltados para o setor de energia elétrica.

### (4) RODOLFO CABRAL BERNARDINO

Engenheiro Eletrônico, graduado pela Universidade Federal de Uberlândia (UFU). Trabalha com pesquisas e desenvolvimento, com sistemas de controle, desenvolvimento de hardware e em sistemas de proteção com IEC 61850. Possui experiência em trabalhos de desenvolvimento e pesquisa na CONPROVE. Engenheiro e Instrutor de treinamento da CONPROVE em cursos de IEC 61850.

### (5) GUSTAVO ESPINHA LOURENÇO

Gustavo Espinha Lourenço é Engenheiro Eletricista formado pela Universidade Federal de Uberlândia em 1998 e desde então trabalha na Conprove com foco em pesquisa e desenvolvimento de novos produtos voltados para o setor de energia elétrica.

### (6) GUSTAVO SILVA SALGE

Possui graduação em Engenharia Elétrica pela Universidade Federal de Uberlândia (UFU), concluído em 2008. Atualmente é Engenheiro de Pesquisa e Desenvolvimento da empresa Conprove, atuando principalmente nos seguintes temas: Proteção de Sistemas Elétricos de Potência e Transitório Eletromagnéticos em Sistemas Elétricos de Potência.