Comitê de Estudos B5 – Proteção e Automação

ANÁLISE DO MONITORAMENTO DE REDE NO CONTEXTO DA NORMA IEC 61850

P.S.P. JUNIOR*
CONPROVE
BRASIL
psjunior@conprove.com.br

R.C. BERNARDINO
CONPROVE
BRASIL
conprove@conprove.com.br

G.S. SALGE
CONPROVE
BRASIL
conprove@conprove.com.br

C.M. MARTINS
CONPROVE
BRASIL
conprove@conprove.com.br

G.E. LOURENÇO
CONPROVE
BRASIL
conprove@conprove.com.br

P.S. PEREIRA
CONPROVE
BRASIL
psp@conprove.com.br

Resumo *– Diversos aspectos de rede devem ser analisados para garantir a segurança, confiabilidade, velocidade e disponibilidade das informações que estão sendo transmitidas, alertando para possíveis falhas de comunicação ou invasões. Esses aspectos da rede estão relacionados à integridade da mensagem, configuração e segurança dos dados, sincronismo de tempo do sistema e estatísticas de temporização da mensagem, considerando o Intervalo entre Frames, TransferTime, Atraso de Propagação e Tempo de Processamento.*

Devido ao aumento da implantação de subestações digitais baseadas na norma IEC 61850, as vulnerabilidades de segurança cibernética também estão aumentando. Estas vulnerabilidades estão relacionadas tanto com o Process Bus como com o Station Bus, pelo que as mensagens Sampled Values, GOOSE ou MMS estão todas sujeitas a ataques cibernéticos.

Portanto, vale ressaltar que o desempenho da proteção dos sistemas de potência depende do desempenho da rede de comunicação. Desta forma, deve ser confiável e seguro.

Neste artigo, as razões para o monitoramento serão descritas e também discutido como implementá-lo para cada aspecto da rede. Os problemas de monitoramento que não podem ser verificados também serão analisados. Por fim, será discutido como o monitoramento da rede se comportará em relação às condições de teste, visto que nos testes de manutenção haverá duas streams de SV: uma simulada pela mala de testes e outra a partir de uma MU/SAMU, por exemplo.

Assim, este trabalho tem como objetivo realizar uma análise sobre a importância do monitoramento da rede no contexto da IEC 61850, destacando os requisitos de rede necessários para o monitoramento e discutindo suas implementações.

Palavras-chave: Monitoramento - IEC 61850 - Mala de Testes - Rede - Cibersegurança, - GOOSE - Sampled Values – PTP – MMS

1 INTRODUÇÃO

Os Sistemas de Proteção, Automação e Controle (PACS) estão evoluindo devido às constantes inovações proporcionadas com o advento da norma IEC 61850, cuja primeira edição foi lançada em 2003. Cada vez mais a implantação da norma IEC 61850 cresce em todo o mundo com o objetivo de implementar subestações totalmente digitais, onde o Process Bus destaca ainda mais o quão vital é o desempenho da rede de comunicação Ethernet no PACS.

Toda troca de dados recomendada pela norma é baseada em quatro protocolos de comunicação: Cliente/Servidor (MMS), GOOSE, Sampled Values (SV) e o Precision Time Protocol (PTP). Nesse contexto,

vários aspectos da rede devem ser analisados para garantir a confiabilidade, velocidade, disponibilidade e segurança das informações transmitidas.
A IEC 61850 padroniza a troca de informações entre IEDs (Intelligent Electronic Devices) de uma ou mais subestações, permitindo a implantação de SAS (Sistema de Automação de Subestações). A arquitetura da norma é baseada no modelo de dados orientado a objetos, abstraindo atributos e funções dos IEDs, chamados de Physical Devices. Cada Physical Device possui um conjunto de Logical Devices que são as diferentes funcionalidades implementadas pelo IED (Sistema, Controle, Proteção, entre outras). Cada Logical Device possui um conjunto de Logical Nodes que são os elementos funcionais do Logical Device. Exemplos de logical nodes de proteção: PDIS (proteção de distância), PTOC (proteção de sobrecorrente), PDIF (proteção diferencial), etc. Por fim, cada logical node possui um conjunto de Functional Constraints com seus Data Objects e Data Attributes.
Graças à estrutura de dados estabelecida pela IEC 61850, é possível implementar diferentes funções de aplicação (F1 e F2) distribuídas através de alocações de Logical Nodes (LN) em diferentes Physical Devices (PD), que irão trocar informações através de uma rede de comunicação onde LN são interligados por Logical Connections (LC) e PD são interligados por Physical Connections (PC), conforme o exemplo clássico demonstrado no item 8.4.2 da IEC 61850-5 Ed.2 que é mostrado na Figura 1 abaixo.

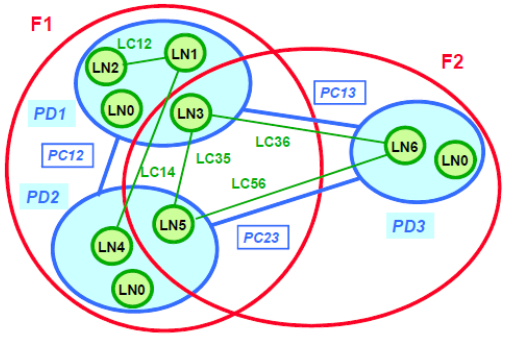

Figura 1 – Conceito de Funções Distribuídas de Acordo com a IEC 61850

A descrição detalhada deste exemplo demonstra que F1 é implementado em PD1 através de LN0, LN1, LN2 e LN3. LN1 e LN2 são conectados através de LC12. Da mesma forma, F1 é implementado em PD2 através de LN0, LN4 e LN5. PD1 e PD2 são conectados através de PC12. LN1 (PD1) e LN4 (PD2) são conectados através de LC14. LN3 (PD1) e LN5 (PD2) são conectados através de LC35.
Assim, este exemplo demonstra claramente que o desempenho da função a ser executada depende do desempenho da comunicação da rede. Portanto a rede de comunicação e sua disponibilidade fazem parte desta função. Assim, é de vital importância monitorar a rede para garantir o correto funcionamento do PACS.
A IEC 61850 desempenha um papel fundamental nos sistemas de proteção, automação e controle da rede elétrica. No entanto, à medida que a complexidade desse sistema aumenta, ele se torna mais vulnerável a ataques cibernéticos. Os ataques cibernéticos podem ocorrer não apenas de fonte externa, mas também interna, por exemplo: ex-funcionários insatisfeitos, fornecedores, equipe de manutenção terceirizada, funcionários que podem abrir mensagens de uma fonte não confiável em e-mail corporativo, etc.
Em 2020, devido ao cenário de pandemia do COVID-19, um aumento considerável no número de funcionários das concessionárias de energia estava trabalhando em casa e acessando a rede interna da subestação por meio de acesso remoto. Esta é uma das razões para abrir brechas de segurança para ameaças. Assim, os operadores do sistema elétrico de vários países estão examinando uma série de requisitos para incluir, em seus procedimentos de rede padrão, o monitoramento da rede IEC 61850.

2 CONSIDERAÇÕES A RESPEITO DA NORMA IEC 62351

A norma IEC 62351 foi elaborada pelo WG (Working Group) 15 do IEC TC (Technical Committee) 57, com o objetivo de tratar dos aspectos de segurança relacionados às séries de normas abrangidas pelo TC 57, incluindo a série IEC 61850.

A IEC 62351-6, cujo título é “Security for IEC 61850”, aborda questões de segurança dos protocolos de comunicação IEC 61850. As principais contribuições do IEC 62351-6 para a segurança dos protocolos GOOSE e SV são a inclusão de um campo extra na mensagem chamado “Authentication Value”, usado para verificar a integridade e métodos opcionais de criptografia. Este não é obrigatório devido a problemas de desempenho em caso de requisitos de tempo crítico como em GOOSE (Type 1A “Trip”, classe de desempenho P2/3) e Sampled Values, devido ao tempo de processamento adicional para criptografia e no caso de uma CPU com baixo poder de processamento. Assim, métodos de criptografia são recomendados sempre que não causem problemas.
A IEC 62351-7 descreve o monitoramento de segurança da infraestrutura de rede de comunicação do PACS, referindo-se a ela como Network and System Management (NSM). Esta parte do padrão define os objetos de dados necessários para esta função, denominados NSM Data Objects (NSM DOs), cujo objetivo é modelar informações de monitoramento de segurança. A Parte 7 da IEC 62351 também define a base de informações de gerenciamento de segurança cibernética (Management Information Base - MIBs), que abrange aspectos de monitoramento, como detecção de Out of Sequence e detecção de frames GOOSE e/ou SV duplicados.
A IEC 62351-14 especifica detalhes técnicos para a implementação de logs de segurança, baseados no Syslog. Esta é a principal forma para os centros de operação de segurança cibernética reagirem às informações de monitoramento e correlacionarem ainda mais as informações entre os sistemas.
O mecanismo de detecção no IEC 62351 pode ser disponibilizado em dois protocolos: SNMP (Simple Network Management Protocol) conforme definido na parte 7 e Syslog conforme definido na parte 14. Enquanto o SNMP é usado para monitoramento operacional, o Syslog é direcionado para o centro de operações de segurança.

3 SISTEMA DE MONITORAMENTO DE REDE E CIBERSEGURANÇA PARA O PACS

A rede PACS deve incorporar funções de monitoramento, considerando aspectos de cibersegurança, capazes de:

1) Detectar e apontar anomalias ou faltas de mensagens, como GOOSE ou SV, ou ainda mensagens imprevistas;
2) Detectar falta de sinal de sincronismo;
3) Verificar e apontar tempo de propagação anormal, ou seja, latência, e assimetria ou variação excessiva, ou seja, jitter, dos tempos de propagação das mensagens;
4) Ser implementado de forma independente de dispositivos de proteção ou dispositivos de teleproteção local;
5) Ter recursos para armazenar registros de eventos de anomalias detectadas.

Além disso, a rede PACS deve incorporar mecanismos que ofereçam segurança cibernética para garantir os seguintes tópicos:

1) Confidencialidade: limitar o acesso aos dados apenas a usuários autorizados;
2) Integridade: garantir que não haja modificações não autorizadas nos dados das mensagens ou roubo de informações;
3) Disponibilidade: para garantir acesso autorizado a dados ou serviços;
4) Autenticidade: para garantir que os dados sejam provenientes de uma fonte legítima.

Portanto, o sistema de monitoramento será capaz de registrar quaisquer problemas de hardware/software, além dos aspectos de ataques cibernéticos.
Para garantir que todas essas funcionalidades citadas nos tópicos acima sejam contempladas pelo sistema de monitoramento, alguns aspectos da rede devem ser analisados. Uma delas está relacionada à integridade das mensagens, ou seja, se não há perda de pacotes ou pacotes corrompidos. Além disso, a configuração e segurança dos dados, ou seja, verificar se todas as mensagens contidas no arquivo SCL da subestação estão presentes na rede e se há alguma mensagem em execução não prevista e relacionada à estrutura do quadro comparando campos como endereços MAC de origem e de destino, VLAN ID e tag de prioridade.
Outro aspecto da rede a ser considerado está relacionado ao sincronismo de tempo do sistema, através da checagem do tráfego de mensagens PTP.
Por fim, devem ser verificadas as estatísticas de tempo da mensagem na rede, considerando o Intervalo entre Frames, Transfer Time, Atraso de Propagação e Tempo de Processamento.

Alguns requisitos podem não estar previstos no sistema de monitoramento e essa é uma questão importante a ser abordada. Além disso, deve-se avaliar como o sistema de monitoramento se comportará em uma configuração de Teste/Simulação quando houver duas streams SV: a simulada de uma mala de testes e a real de uma Merging Unit.
Essas verificações permitirão aumentar a confiabilidade, a segurança e, consequentemente, a disponibilidade da rede, alertando sobre possíveis falhas de comunicação (causadas por um bug no adaptador de rede do IED, por exemplo) ou invasões. As verificações vão gerar logs de eventos que podem ser armazenados e consultados, possibilitando rastrear o problema e localizar sua origem. Além disso, logs de eventos podem ser usados em relatórios para facilitar a compreensão da falha. Na prática, o monitoramento de rede pode ser realizado por meio de uma porta Trunk no Switch ou através de espelhamento de porta.
Considerando os frames GOOSE que carregam como dado um comando de Trip, se essas mensagens não forem entregues à SCU (Switchgear Control Unit) para que o disjuntor atue, o sistema de proteção fica comprometido, afetando severamente a operação da subestação. Antes que essa situação aconteça, o sistema de monitoramento deve detectar essa anomalia e alertar o supervisório através de um alarme, indicando que não existe um frame GOOSE que deveria estar trafegando na rede e registrar esse evento como um log para ser analisado pelo usuário. Uma forma do sistema de monitoramento implementar esta função é analisar todas as instâncias dos IEDs (dispositivos publicadores e assinantes), através de arquivo SCD (ou mesmo arquivos ICD), verificando se todas as mensagens GOOSE estão trafegando na rede da subestação. Para isso, podem ser utilizados alguns filtros como Destination MAC Address, GOOSE Control Block Reference e Application ID da estrutura do frame GOOSE.
Outra situação de dano que pode ocorrer é um invasor conseguir publicar frames GOOSE maliciosos na rede com duas finalidades: abrir ou fechar um disjuntor causando sérios problemas ou causando uma sobrecarga na rede para atrasar os frames GOOSE legítimos. Neste caso, o sistema de monitoramento deve detectar esta anomalia, ou seja, frames GOOSE esperados de acordo com o arquivo SCD, porém com tempos de retransmissão muito diferentes do que está configurado ou com Sequence Number (SqNum) errado antes ou depois do esperado (fora de ordem). Para desenvolver essa funcionalidade, o sistema de monitoramento pode analisar os tempos de recebimento dos frames e verificar se a diferença de tempo entre eles está correta. Também é possível verificar se SqNum está correto. A Figura 2 exemplifica esse caso: os campos destacados em vermelho demonstram o que deve ser verificado pelo sistema de monitoramento.

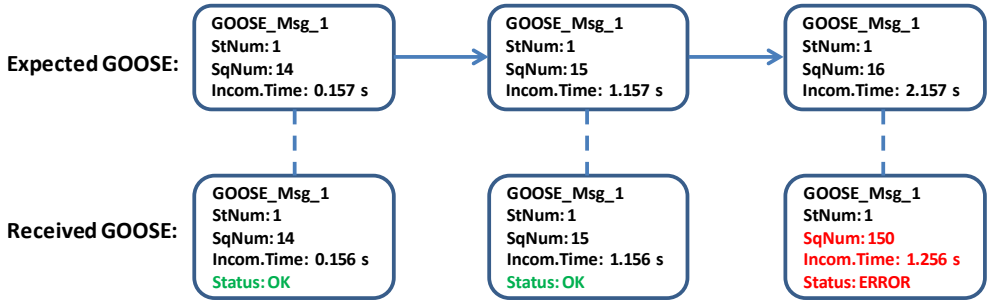

Figura 2 - Sistema de Monitoramento Analisando Tempos de Retransmissão GOOSE e Frames Fora de Ordem

Um ponto cego para o sistema de monitoramento no caso descrito acima é se o invasor for capaz de publicar frames GOOSE maliciosos no tempo de retransmissão correto e na sequência correta.
O sincronismo de tempo PTP (Precision Time Protocol) é um aspecto bastante importante para o sistema de monitoramento verificar, ou seja, deve ser capaz de verificar se mensagens GM (Grand-Master) estão trafegando na rede Ethernet. É uma ameaça a perda de sincronismo, tendo em vista que as MUs ou SAMUs do Nível de Processo dependem dele para funcionar adequadamente; caso contrário, o sistema de proteção pode ser comprometido, porque as merging units não irão amostrar na taxa correta. Uma forma de analisar se as mensagens do GM estão trafegando é verificar se existem duas principais: Announce e Sync.
O Best Master Clock Algorithm (BMCA) é usado para escolher o melhor nó da rede para se tornar o GM. Este algoritmo é dinâmico e funciona da seguinte forma: enquanto nenhuma Announce é recebida por um intervalo de tempo definido, todos os nós (que implementam o BMCA) tornam-se mestres e enviam suas próprias mensagens Announce. Todos os nós recebem esta mensagem e verificam suas informações de quality do clock (campos de class, priorities e qualities). Se um nó concluir que o Announce recebido contém

informação de quality superior à sua, deixa de enviar a Announce e torna-se Escravo; mas se um nó concluir que o Announce recebido é pior em seu quality, o nó permanece como Mestre e continua enviando a Announce. Assim, na rede só pode haver um nó como Mestre, recebendo o nome de Grand-Master.
É importante considerar que o sistema de monitoramento deve ser um escravo PTP, para sincronizar com o GM e estar na mesma base de tempo de todos os dispositivos da subestação. Assim, o sistema de monitoramento também pode analisar se há perda de sincronismo de tempo, verificando se o jitter do clock do escravo está aumentando em relação ao clock do mestre. Esta situação pode indicar duas possibilidades: Link Ethernet perdido ou, se o link estiver saudável, pode ter ocorrido algum problema de hardware com o Transparent Clock ou mesmo com a calibração de clock do GM e o BMCA ainda não conseguiu escolher outro GM.
Ainda sobre a questão do sincronismo de tempo com PTP, existe a possibilidade de um invasor se passar pelo GM e derrubar o sincronismo da subestação. Este ataque pode ser realizado de duas formas: o invasor pode forçar o envio de mensagens do GM com o mesmo Clock Identity do GM atual ou com Clock Identity diferente. O primeiro caso é um ponto cego para os sistemas de monitoramento, pois não há como diferenciar as mensagens GM reais das mensagens GM falsas, pois o Clock Identity é o mesmo em ambas. O segundo caso pode ser verificado pelo sistema de monitoramento através de uma “Lista Branca”, ou seja, uma lista com todos os Clock Identities possíveis dos nós GM da rede da subestação. Como o Clock Identity da ameaça é diferente do GM atual, o sistema de monitoramento deve verificar que ele não está na “Lista Branca” e tomar alguma ação como sinalizar por um alarme.
Uma função importante que o sistema de monitoramento deve implementar está relacionada à análise estatística dos frames SV e GOOSE.
No caso dos Sampled Values, o objetivo é verificar o atraso de propagação, tempo de processamento e tempo entre frames. O primeiro é o tempo que uma mensagem leva para sair da porta Ethernet de um dispositivo e entrar na porta Ethernet de outro dispositivo, ou seja, o tempo de latência da rede. É importante que o sistema de monitoramento verifique o atraso de propagação e analise se há sobrecarga na rede.
O tempo de processamento é o tempo que uma MU/SAMU leva para amostrar os sinais que vêm dos transformadores de instrumentos, encapsulá-los no frame padrão e publicá-los, mais o tempo de latência da rede. Assim, os usuários podem analisar se está ocorrendo escorregamento em relação ao tempo normal de processamento. Além disso, o número de erros de frames SV na rede e a flag de sincronismo podem ser verificados.
O tempo entre os frames indica se a MU/SAMU está amostrando corretamente de acordo com o que foi configurado. Essa funcionalidade pode ser implementada pelo sistema de monitoramento apenas marcando o tempo de recebimento do frame no controlador Ethernet e obtendo a diferença entre eles.
A Figura 3 exemplifica essas análises estatísticas de frames SV.

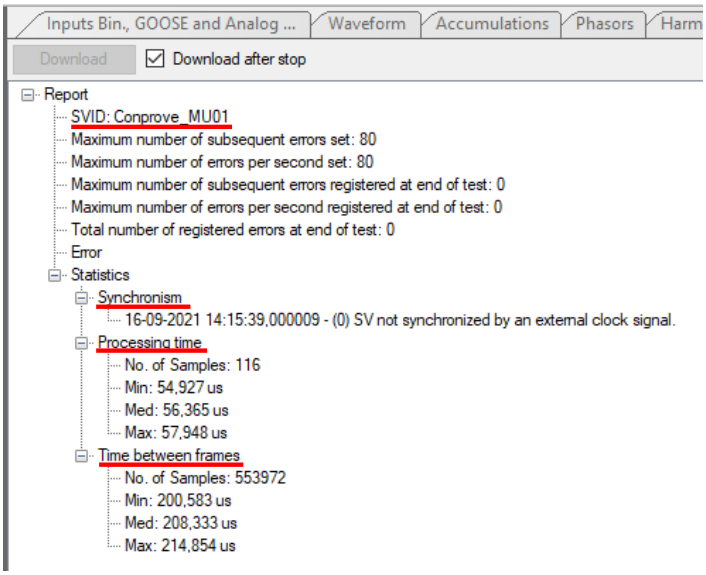

Figura 3 - Exemplo de Análises Estatísticas de Frames SV

No caso do GOOSE, o objetivo é calcular o Transfer Time e verificar se ele ficou dentro dos limites definidos pela IEC 61850-5 de acordo com as classes de performance definidas na IEC 61850-8-1.
Com base no item 11.1.1.4 da IEC 61850-5 Ed.2, o Transfer Time é definido como o tempo completo de transmissão do frame incluindo o processamento do publicador e do assinante. Em detalhes, é a soma de três tempos: ta, tb e tc, onde:
- ta é o tempo contado desde o momento em que o publicador coloca o frame no topo de sua pilha de transmissão (codificação) até o momento em que ele é enviado para a rede;
- tb é o tempo de latência da rede;
- tc é o tempo contado a partir do instante em que o frame entra no assinante até que o frame seja extraído da pilha de recebimento.
Retirada da IEC 61850-5 Ed.1, a Figura 4 ilustra o conceito de Transfer Time.

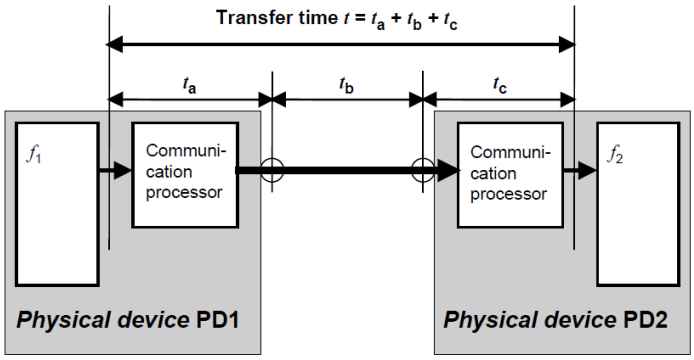

Figura 4 - O Conceito de Transfer Time

Para sistemas de proteção, a classe de Transfer Time para aplicações de Trip é “TT6” e o tempo deve ser menor que 3ms. Retirada da IEC 61850-5 Ed.2, a Tabela 1 mostra as classes para o Transfer Time.

Tabela 1 - Classes para o Transfer Time

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

Com base nisso, é muito importante que o sistema de monitoramento detecte e reporte qualquer tempo maior que 3ms, considerando as mensagens GOOSE de Trip.
Uma importante funcionalidade de monitoramento das mensagens GOOSE devido ao seu tempo de retransmissão está relacionada ao campo Time Allowed to Live. Esta informação pode ser usada para alertar se houve algum problema de perda de Link.
A IEC 61850 definiu dois Logical Nodes com Data Objects específicos para monitoramento de mensagens GOOSE e SV. Os LNs LGOS e LSVS definidos pela IEC 61850-7-4 Ed.2.1 nos itens 6.3.5 e 6.3.6, respectivamente, podem ser analisados pelo sistema de monitoramento como cliente de um IED como servidor através do protocolo de comunicação MMS.
O LGOS possui Data Objects específicos para fins de monitoramento GOOSE, pois eles definem as informações de status da assinatura. A Tabela 2, retirada da norma, mostra esses Data Objects em detalhes.

Tabela 2 - Logical Node LGOS e 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

O LSVS possui Data Objects específicos para fins de diagnóstico e monitoramento de Sampled Values, pois eles definem as informações de status da assinatura. A Tabela 3, retirada da norma, mostra esses Data Objects em detalhes.

Tabela 3 - Logical Node LSVS e 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

O aspecto final que vale a pena abordar é o comportamento em cenários de Teste/Simulação, ou seja, como o sistema de monitoramento deve agir quando há dois frames SV trafegando: um simulado e outro real. Neste caso, uma mala de testes vai publicar SV com o bit de simulação setado ao mesmo tempo em que uma MU/SAMU vai publicar frames SV reais, ou seja, com o bit de simulação resetado. Assim, o sistema de

monitoramento deve ser capaz de assinar os frames SV publicados e verificar o campo Simulation Bit que é o bit mais significativo do byte mais significativo do campo Reserved 1, conforme mostra a Figura 5, retirada de uma captura do Wirekshark.

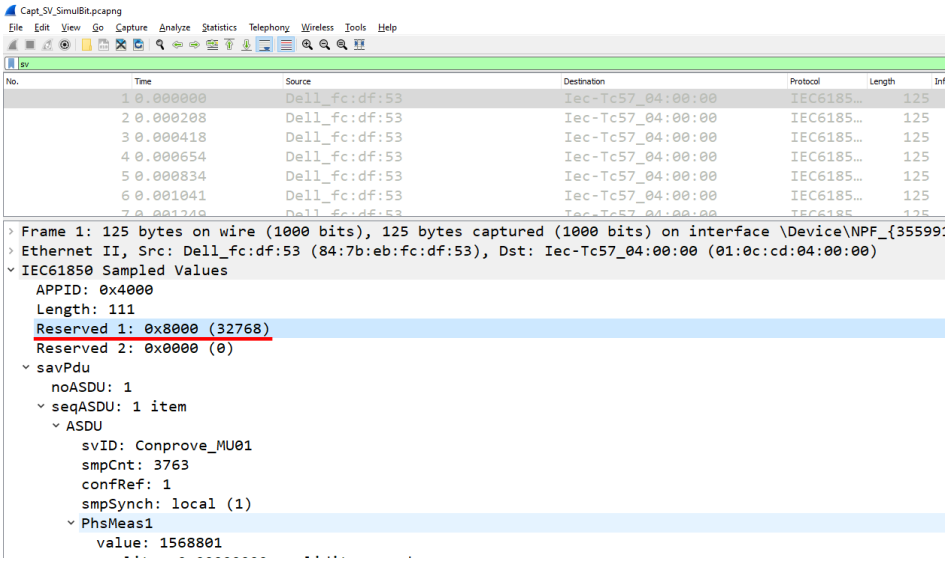

Figura 5 - Simulation Bit no Frame SV

Caso o sistema de monitoramento não tenha sido notificado de que a subestação está em manutenção, ele deve relatar a inconsistência dos dados e salvar essas informações em um log.

4 CONCLUSÕES

Através deste trabalho, foi possível avaliar os requisitos para o monitoramento da rede e avaliar as metodologias de identificação de falhas. Aspectos não previstos pelo monitoramento de rede também foram abordados, como seus pontos cegos caso um invasor seja capaz de publicar frames GOOSE maliciosos no tempo de retransmissão correto e sequência correta, ou se um invasor for capaz de enviar mensagens GM com o mesmo Clock Identity do GM atual.

A implantação de uma subestação digital pode ser mais confiável com a implantação do sistema de monitoramento, pois qualquer evento de falha será alarmado e registrado para que seja possível rastrear suas causas, otimizando assim o PACS.

Desta forma, espera-se que este trabalho contribua para possibilitar o bom funcionamento das redes de comunicação. Como esta é a única forma de garantir o tráfego seguro e confiável de informações, o PACS será executado de forma satisfatória, tornando a dependência da performance da comunicação inquestionável.

5 REFERÊNCIAS BIBLIOGRÁFICAS

[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] Norma 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] Norma IEC 62351-6 – “Power systems management and associated information exchange – Data and communications security – Part 6: Security for IEC 61850.
[6] Norma 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.
[7] Norma IEC 62351-14 ED1 – “Power systems management and associated information exchange – Data and communications security – Part 14: Cyber security event logging.
[8] Network and System Management using IEC 62351-7 in IEC 61850 Substations: Design and Implementation – Chantale Robillard – Concordia University, 2018.
[9] 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).
[10] Introduction to PTP Basics – NetTimeLogic, GMBH.
[11] Norma IEC IEC 61850 – Communication networks and systems in substations – Part 5: Communication requirements for functions and device models, Ed. 1 - 2003.
[12] Norma 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.
[13] Norma 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.