

Case Study: Parallel Network Topologies Between Redundant OT Networks Implemented with Different Protocols

Lucas F. Dias¹, Otávio S. M. Gomes¹ Luiz L. G. Vermaas¹

¹Instituto de Engenharia de Sistemas e Tecnologias da Informação
Universidade Federal de Itajubá (UNIFEI)
Av. BPS 1303 – 37.500-903 – Itajubá – MG – Brazil

lucasfelipedias25, otavio.gomes, lenarth@unifei.edu.br

Resumo. *Este artigo apresenta um estudo de caso a respeito de arquiteturas de redes redundantes, e topologias de redes paralelas que as interconectam. Neste estudo são apresentados alguns padrões e recomendações da norma IEC 61850 referentes ao protocolo GOOSE, mecanismos de comunicação dos protocolos abordados, análises de arquiteturas de rede e resultados obtidos após testes, utilizando relés e switches convencionais e de tecnologia SDN. Por fim, são apresentadas algumas considerações a respeito das topologias abordadas e testadas durante o trabalho, destacando pontos de fragilidade das arquiteturas e possíveis melhorias a serem implementadas em estudos futuros.*

1. Introdução

Confiabilidade, alta disponibilidade, e alto desempenho são características essenciais de um Sistema de Automação de Subestações (SAS), para controle, proteção e supervisão nas fases de geração, transmissão e distribuição do Sistema Elétrico de Potência (SEP). As subestações (SE) funcionam como pontos de controle e transferência em um Sistema Elétrico, direcionando e controlando o fluxo energético, transformando os níveis de tensão, operando como pontos de entrega para consumidores.

Em sua segunda edição, publicada em 2009, a IEC 61850 definiu requisitos ainda mais rigorosos de desempenho, confiabilidade e disponibilidade das Redes de Comunicação de Subestações (SCN - *Substation Communication Networks*) e dos dispositivos eletrônicos inteligentes (*IED*), com base em novas tecnologias disponíveis. Com a revisão, foram especificados outros protocolos e padrões para implantação de redundâncias de rede nos SAS [Faustino Junior et al. 2018].

A transmutação do SEP rumo ao *Smart Grid*, guiada pelos padrões estabelecidos pela IEC 61580, referentes à infraestrutura de informação e comunicação automatizada, proporciona diversos desafios aos agentes responsáveis pelo desenvolvimento e manutenção do sistema elétrico [Lopes et al. 2012]. Esses desafios fazem com que o desenvolvimento de um sistema elétrico inteligente, no contexto brasileiro, seja desacelerado por características econômicas e geográficas.

Nesse cenário, onde novas tecnologias, em conformidade com a segunda edição da IEC 61850, são aplicadas em subestações que possuem infraestruturas de informação e proteção em acordo com a edição 1 da referida norma, podem surgir cenários como o que será abordado neste artigo, onde há necessidade de se desenvolver uma rede de comunicação redundante, segura e de alta disponibilidade interligando duas LANs projetadas em conformidade com as recomendações de diferentes edições da IEC 61850,

permitindo a troca de mensagens GOOSE utilizadas em esquemas de proteção, dada a necessidade de coordenação da proteção, e aproveitando a estrutura de rede existente entre as subestações.

No presente estudo, assumiremos uma das topologias em *ladder* com protocolo RSTP (*Rapid Spanning Tree Protocol* - Protocolo de árvore geradora rápida), e a outra rede com protocolo de redundância paralela, definido na IEC 62439-3 (*Parallel Redundancy Protocol* - Protocolo de Redundância Paralela), como recomenda a edição 2 da IEC 61850, conectadas em topologia e rede redundante para troca de mensagens ponto a ponto. O protocolo de comunicação *GOOSE* (*Generic Object Oriented Substation Events* - Eventos Genéricos de Subestação Orientados a Objetos), que será utilizado para testes de desempenho e qualidade do serviço, é definido pela IEC 61850 em sua primeira edição e reapresentado com a revisão da norma.

Este artigo apresenta a mecânica básica de operação das tecnologias e modelos de comunicação citados, introduz requisitos e padrões recomendados pela norma IEC 61850 no tráfego de mensagens GOOSE. Introduz conceitos sobre switches de tecnologia SDN (*Software Defined Networking*) aplicados ao cenário em foco, e apresenta a metodologia e os resultados dos testes realizados. O objetivo é avaliar o cumprimento das definições e recomendações apresentadas pelo relatório técnico "Diretrizes para Engenharia de Rede" (IEC 61850-90-4), para redes de automação de subestações baseadas em IEC 61850 [Yang et al. 2012], buscando realizar a análise de desempenho destas topologias de rede redundantes.

2. Conceitos Fundamentais

A seção a seguir apresenta conceitos, definições e exemplos de aplicação de protocolos, normas e tecnologias presentes neste artigo.

2.1. GOOSE: IEC 61850-8-1 Mapeamento específico de serviços de comunicação (SCSM)

A IEC 61850-8-1 compõe um conjunto de especificações que detalha a arquitetura de comunicação das concessionárias em camadas, e tem objetivo geral de fornecer instruções/especificações detalhadas sobre os mecanismos e regras necessárias para implementar os serviços, objetos e algoritmos especificados na IEC 61850-7-2, IEC 61850-7-3 e IEC 61850-7-4 enquanto faz uso da ISO 9506, MMS (*Manufacturing Message Specification* - Especificação de mensagens de fabricação), NTP (*Network Time Protocol* - Protocolo de Tempo de Rede) e outros protocolos de aplicação [61850 2011].

A IEC 61850-5 classifica as mensagens e sua classe de desempenho em sete tipos diferentes, entretanto no contexto deste trabalho, serão abordados os seguintes tipos: Tipo 1A (Trip), Tipo 1 (Mensagens rápidas), Tipo 2 (Mensagens de média velocidade) e Tipo 3 (Mensagens de baixa velocidade).

Os tipos 1 e 1A são definidos para mensagens no protocolo GOOSE que trafega mensagens comunicando sinais de proteção, variáveis digitais e analógicos de alta prioridade, sendo as mensagens de tipo 1 e 1A as mais prioritárias em uma SCN.

Já os tipos 2 e 3, são atribuídos a mensagens de comando, valores analógicos e digitais de média/baixa prioridade. Em geral, essas mensagens são mais densas que as

do tipo 1 e 1A, e são importantes para monitoramento e controle do sistema elétrico. A norma aponta o protocolo MMS para estas classes de mensagens.

Para mensagens do tipo 1 e 1A a norma padroniza o protocolo GOOSE e define os seguintes requisitos para serviços da camada 2 (Enlace de Dados) do modelo OSI (Open System Interconnection):

- É mandatório o uso de tags prioritárias - VLAN, para identificar e classificar a prioridade das mensagens GOOSE;
- É obrigatório o Controle de Colisão de Acesso Múltiplo (CSMA/CD);
- É opcional a implementação de redundância de link, através dos protocolos PRP, RSTP e HSR (*High-availability Seamless Redundancy* - Redundância contínua de alta disponibilidade);

De acordo com a IEC 61850-7-2, o modelo de serviço GOOSE fornece a possibilidade de uma distribuição rápida e confiável de valores de dados de entrada e saída em todo o sistema. Para garantir a confiabilidade, o modelo de transmissão é baseado em disparos por geração de eventos, a partir da aplicação local do servidor, e não há mecanismos de confirmação de recebimento como no protocolo MMS. O desempenho das mensagens é medido através do tempo de transferência, que é o tempo entre o envio e a recepção da mensagem, levando em consideração a camada de enlace (processamento das mensagens pela interface de rede do dispositivo), que é diferente do tempo de transmissão. Na prática, o tempo de processamento dos IEDs ocupa a maior parte do tempo de transferência, sendo o restante do tempo resultado da latência do canal de comunicação. Veja na Figura 1, como são definidos cada um dos intervalos de tempo.

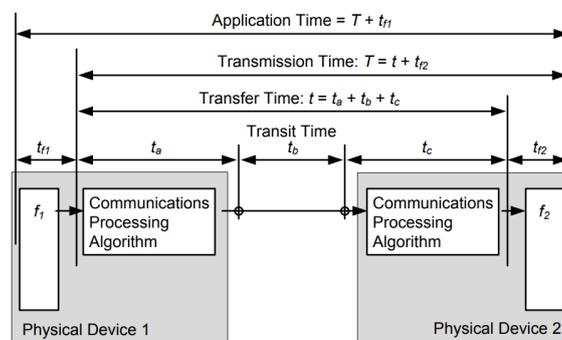


Figura 1. Tempos de transmissão e de transferência baseados na IEC 61850-5

2.2. Redes Redundantes

Neste artigo, as redes de comunicação redundantes, por escolha do autor, serão classificadas em dois tipos: Redes Paralelas e Redes de Cura (*Self-Healing Networks*), adaptando uma definição utilizada comumente em redes de TO (Tecnologia de Operação) com switches SDN [Yang and Smith 2019]. A escolha dessa terminologia objetiva simplificar o entendimento e a classificação das redes apresentadas neste trabalho.

2.2.1. Redes de Cura

São redes de comunicação em que as mensagens não são disponibilizadas de modo redundante aos dispositivos finais. Neste caso, a redundância pode existir até um dispositivo in-

intermediário, tipicamente um switch ou uma RedBox (*Redundancy Box*), e um mecanismo do tipo *Hot/Standby* ou *Failover* é responsável por gerenciar a redundância física de link e fazer o câmbio entre as portas de comunicação, se detectada uma falha no link principal. De acordo com a primeira edição da IEC 61850, o tempo de recuperação dessas redes deve ser de 10 a 100 ms [Khavnekar et al. 2015]. Dispositivos de redes definidas por software (SDN) podem conter *Failover* com tempo de resposta na ordem dos 100 μ s, tornando o uso destes vantajoso para o tempo de recomposição da rede em SAS [Kalra et al. 2020]. Para alcançar um tempo de resposta tão baixo é preciso uma abordagem de rede proativa [Meine 2019].

Deve-se ter cautela ao projetar a arquitetura de redes de cura com protocolos como o RSTP, dado os impactos diretos no desempenho da rede devido a latência da comunicação e ao cascateamento de dispositivos com tempo de reação diferente de zero [Dearien 2017].

2.2.2. Redes Paralelas

Este tipo de rede de comunicação é caracterizado pelo modelo de transmissão redundante de mensagens em vias paralelas até o dispositivo final, de ponto a ponto. Esses dispositivos gerenciam o aproveitamento dos pacotes de acordo com sua disponibilidade, descartando as mensagens redundantes quando a principal já houver sido recepcionada. O IED adota a primeira mensagem íntegra a chegar, e descarta a mensagem redundante que chega em sua outra porta de rede [Araujo et al. 2013].

Protocolos como o PRP e o HSR (*High-availability Seamless Redundancy*) são definidos na edição 2 da IEC-61850 para o desenvolvimento de redes redundantes paralelas em SAS. A grande vantagem desses protocolos é o tempo de recomposição zero em caso de falhas simples de link físico e lógico [Kirmann et al. 2007].

2.3. Protocolo PRP

O PRP aceita Nós de Conexão Única (SAN) diretamente conectado a uma das LANs, ou seja, é possível conectar um IED com apenas uma das portas de comunicação e o link ainda será útil, apesar de não haver redundância. Entretanto, outra maneira mais comum de se conectar um SAN à rede PRP é usando uma RedBox para fazer a interface com as LANs paralelas [Araujo et al. 2013].

2.4. Protocolo RSTP

O protocolo RSTP é um algoritmo distribuído, definido pela IEEE 802.1Q-2014. O algoritmo é gerenciado por switches de camada 2 e IEDs com essa mesma característica, que controlam os caminhos ativos de uma rede Ethernet com o objetivo de eliminar loops e permitir redundâncias em *standby* (espera) [Dearien 2017].

RSTP é um protocolo *on-the-wire* que transporta BPDUs (*Bridge Protocol Data Units* - Unidades de dados do protocolo ponte) entre portas fisicamente conectadas em uma rede. As decisões são controladas pelo algoritmo **RSTA** (*Rapid Spanning Tree Algorithm*). O RSTA recebe informações das portas dos switches via BPDUs e as usa para tomar decisões com base no estado atual da rede. Cada IED executa seus processos e

concorda com a topologia da rede lógica atual ou propõe mudanças para outros dispositivos, enviando informações via BPDUs. Assim que todos os IEDs entram em acordo sobre a topologia da rede, as portas são habilitadas (*designated* - designadas) ou desabilitadas (*alternate* - alternadas) para controlar o fluxo de tráfego na rede, eliminando loops e gerenciando vias redundantes em standby. Este processo de tomada de decisão leva tempo e envolve muitas trocas de BPDUs antes da conclusão, por este motivo o tempo de processamento real depende de fatores como a latência do canal, topologia da rede e o número de dispositivos conectados. Desabilitar logicamente links na rede para remover loops físicos resulta em uma árvore de abrangência (*spanning tree*), equilibrada e centrada ao redor de um dispositivo chamado nó raiz (*root*). Pode haver somente um nó raiz em qualquer rede determinada [SEL].

Adicionando peso e prioridade aos nós e caminhos, é possível determinar a topologia a ser acordada pelo algoritmo e assim controlar a arquitetura da rede. O tempo de recomposição da rede após uma falha é diretamente influenciado pela topologia física e lógica da rede. A Figura 2 apresenta os registros do RSTP durante uma falha da porta ativa e a migração para a porta alternativa. O tempo de recomposição medido no experimento foi de 62 ms.

330	12/07/2023	03:25:21.943	VB012		Deasserted
329	12/07/2023	03:25:21.951	LT02		Asserted
328	12/07/2023	03:25:21.960	PortA	RSTP Role Disabled	
327	12/07/2023	03:25:21.961	PortA	RSTP State Discarding	
326	12/07/2023	03:25:22.001	PortB	RSTP Role Rootport	
325	12/07/2023	03:25:22.002	PortB	RSTP State Learning	
324	12/07/2023	03:25:22.022	PortB	RSTP State Forwarding	
323	12/07/2023	03:25:22.985	VB012		Asserted
322	12/07/2023	03:25:22.993	LT02		Deasserted

Figura 2. Registros sequenciais da falha de link principal do RSTP

2.5. Topologias

Neste estudo a topologia Ladder foi adotada na rede RSTP, como veremos mais adiante, devido a capacidade de expansão e minimização dos danos a rede em casos de falha de link. Para além das topologias de rede e dos protocolos adotados, a tecnologia de redes definidas por software será aplicada neste estudo com a finalidade de aumentar a segurança e a confiabilidade da rede a partir de regras de restrição estabelecidas, e do uso de portas com a tecnologia *Fast Failover*. Veja a seguir um breve resumo sobre esta tecnologia [Dearien 2017].

2.6. SDN - Software Defined Networking

Um SDN de TO (tecnologia de operação) difere de um SDN de tecnologia da informação (TI) pelo uso de entradas de fluxo projetadas proativamente para os caminhos primário e de failover. Através do *OpenFlow* o controlador configura os switches SDN que operam em um esquema de ação de correspondência, para controlar como os quadros Ethernet serão encaminhados. Assim que os quadros ingressam no switch, eles são comparados com um conjunto de regras predefinidas. As correspondências podem estar em qualquer lugar da Camada 1 a Camada 4 do modelo OSI. Dependendo de qual regra corresponde ao quadro Ethernet, ele é descartado ou encaminhado para as portas de destino [Kalra et al. 2020].

No cenário adotado, será abordada a tecnologia SDN para prover maior segurança e controle das redes desenvolvidas. Também será fundamental a tecnologia de Failover

que os switches SDN do fabricante dispõe, devido ao tempo de recomposição já citado introdutoriamente.

3. Cenário Proposto

Com objetivo de estudar e investigar, a partir de análises e testes de conformidade, topologias de rede redundantes capazes de conectar subestações com protocolos de redundância não compatíveis, desenvolveu-se uma aplicação contendo duas redes de comunicação de subestações, em acordo com diferentes versões da IEC 61850. Uma delas utiliza o protocolo RSTP para gerenciamento de uma rede de cura e seus loops, e outra possui o protocolo PRP com redes paralelas.

Ambos os protocolos podem coexistir em uma mesma rede, pois atuam com diferentes princípios de redundância. Frequentemente eles são combinados em sistemas secundários digitais, devido às características singulares de cada um. Nesta combinação, o PRP provém uma recuperação de mensagens sem solavancos (*bumpless*) ao dispositivo final, em caso de falhas na rede. Por sua vez, o RSTP gerencia links redundantes entre LANs, e prevenindo a existência de loops [Adilson Kotryk and Ferrari 2023].

A seguir, são apresentadas as arquiteturas das LANs RSTP e PRP projetadas e implementadas fisicamente para os testes:

3.1. LAN RSTP

Adotou-se uma topologia ladder para construir a rede da subestação 1, de modo que o tempo de recomposição fosse o menor possível, e que a expansão da rede fosse possível sem haver grandes impactos no desempenho, e que um único switch (*root*) consiga alcançar toda a rede. Veja a figura 3.

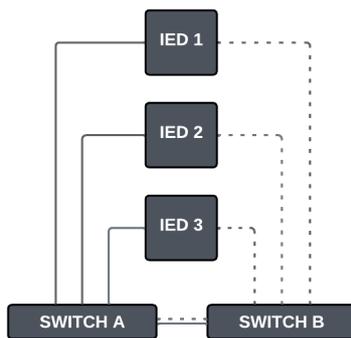


Figura 3. Topologia RSTP adotada no estudo

3.2. LAN PRP

A topologia de rede adotada na LAN com protocolo PRP, é apresentada na Figura 4 e corresponde a uma arquitetura de rede tradicional, onde dois switches representam duas LANs, paralelas, distribuindo os dados entre os dispositivos finais de forma independente. A seguinte topologia foi adotada:

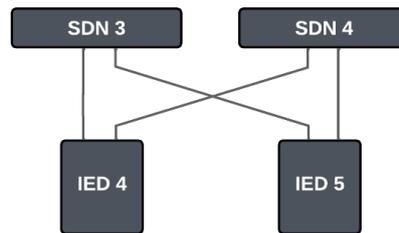


Figura 4. Topologia PRP adotada no estudo

3.3. Integração das LANs

À partir das redes apresentadas, este estudo contempla análises de viabilidade e testes de desempenho de candidatas topologias de redes paralelas que interliguem as LANs de forma que os requisitos de tempo de recomposição e integridade do tráfego de mensagens GOOSE sejam degradados minimamente. A meta era encontrar a topologia de rede mais veloz, confiável e disponível para a conexão entre as redes, baseando-se no conceito de redes paralelas que permitem alcançar tempo de recomposição nulo e alto desempenho. A latência de comunicação da WAN será desprezada neste estudo, pois essa métrica varia de acordo com a topologia, protocolos e meio físico, e pode-se conhecer este valor através de medições e cálculos referentes ao canal de comunicação, e desprezando as características e o comportamento da WAN, os testes se tornam mais simples.

Em ambas as topologias, o objetivo é garantir alta disponibilidade e desempenho para o link entre as redes locais. A topologia 1 é apresentada com o objetivo de fomentar estudos e conclusões a respeito das limitações que os switches tradicionais possuem ao gerenciar redes paralelas de forma passiva, diante de uma incompatibilidade de protocolos. Em contraponto, a topologia 2 traz a implementação da tecnologia SDN, garantindo maior segurança, melhor desempenho e maior controle das redes.

3.4. Topologia 1

As topologias mais óbvias, quando se quer desenvolver uma rede paralela, provavelmente guardam semelhança com a que é apresentada na Figura 3, onde uma LAN possui 2 switches gerenciáveis na entrada que são conectados a outros 2 da outra rede, em paralelo, de modo que não seja formado um loop, devido à topologia e às características dos IEDs da rede PRP (Figura 4). O algoritmo da rede RSTP vai se limitar ao laço da LAN de origem, extinguindo os loops locais. Entretanto, essa topologia não trata da duplicidade de pacotes nos dispositivos finais. Logo, as redes enviarão os pacotes simultaneamente, de modo que os dispositivos receberão as mensagens contendo ecos (cópias da mensagem original sem incremento do números de sequência).

O uso de redes sem restrições nesta aplicação causa problemas do tipo:

- Invalidez na qualidade das mensagens GOOSE por mensagens fora de sequência (*Out Of Sequence*);
- Fragilidades de segurança devido ao tráfego sem restrições;
- Menor disponibilidade da rede em decorrência de restrições dos ecos, aplicadas na origem em vez de tratá-los na recepção.

Para ilustrar melhor um dos problemas citados, propõe-se o seguinte experimento mental: Imagine que o IED 1 envia um GOOSE ao IED 5. Esta mensagem irá trafegar pelos IEDs da LAN RSTP, e isso implica que a mensagem será recebida pelos 2 switches da entrada.

Estes irão designar o tráfego aos switches de entrada da rede 2, que farão as mensagens chegarem aos IEDs finais por 2 vias, pois é essa a mecânica do PRP.

Entretanto, sem o trailer do protocolo nestas mensagens, pois foram geradas a partir de um IED sem PRP, não é possível descartar a mensagem repetida, gerando a recepção de mensagens fora de sequência, como mostra a Figura 5.

Esta sinalização pode ser utilizada para determinar a qualidade do link GOOSE estabelecido, invalidando as mensagens recebidas. Vale destacar que o mesmo problema ocorre nos IEDs da LAN RSTP, pois os dois switches receberão as mensagens e encaminharão aos IEDs.

GOOSE Transmit Status						
MultiCastAddr	Ptag:Vlan	AppID	StNum	SqNum	TTL	Code
01-0C-CD-01-00-05	4:5	5	2	10066	936	
Data Set: _PRPCFG/LLN0\$G0\$PP_Resp_GOOSEMessage						
Data Set: _PRPCFG/LLN0\$DTS_PPTeste_Resp						
GOOSE Receive Status						
MultiCastAddr	Ptag:Vlan	AppID	StNum	SqNum	TTL	Code
01-0C-CD-01-00-01	4:1	1	1	10146	2000	OUT OF SEQUENC
Data Set: _RSTPCFG/LLN0\$DS_GOOSETest						
01-0C-CD-01-00-02	4:2	2	1	10137	2000	OUT OF SEQUENC
Data Set: _RSTPCFG/LLN0\$DS_GOOSE_Test						
01-0C-CD-01-00-03	4:3	3	2	10071	2000	OUT OF SEQUENC
Data Set: _RSTPCFG/LLN0\$GO\$MSG_GOOSE_Test						
01-0C-CD-01-00-04	4:4	4	2	10066	2000	
Data Set: _PRPCFG/LLN0\$G0\$PP_GOOSEMessage						
Data Set: _PRPCFG/LLN0\$TestePP_Digitais						

IEC 61850 Mode/Behavior On
IEC 61850 Simulation Mode Off

Figura 5. Out Of Sequence

Estratégias de segregação baseadas em VLANs, são incapazes de operar dinamicamente em uma rede, logo a solução mais adequada é a homogeneização dos protocolos. Esta porém, exige um investimento considerável para troca ou upgrade dos IEDs da rede RSTP que comunicam com IEDs da rede PRP, adicionando o protocolo PRP.

Seria esta a solução ideal, mas ela não é aplicável em diversos cenários, sem contar que apesar de solucionar o problema das trocas de mensagens, a rede com switches gerenciáveis ainda será vulnerável à falhas de comunicação de dispositivos que podem inundar a rede com mensagens densas disparadas continuamente, como em ataques cibernéticos de *flooding* (Inundação) por exemplo, entre outros fenômenos que podem causar indisponibilidade da rede pelo mesmo princípio.

Outra forma de lidar com este problema local primário, é fazendo a troca dos switches de entrada das redes por switches SDN. E a partir das regras e restrições gerenciadas pelo controlador, estabelecer as regras de controle de tráfego, e fazer uso das ferramentas de monitoramento e recomposição de links, disponíveis em switches de TO com esta tecnologia.

3.5. Topologia 2

A segunda topologia proposta conta com a tecnologia SDN, aplicada para a restrição do tráfego redundante, quando necessário, e definição dos caminhos da rede de forma proativa, com o objetivo de minimizar o impacto no tempo de recomposição da rede 2. Para este experimento os switches tradicionais deram lugar a switches SDN, dispostos em uma arquitetura equivalente à rede 1, sendo um par de switches SDN na entrada de cada LAN. Assim, é preciso construir os fluxos de mensagens através dos switches de modo centralizado, no controlador de cada LAN. A Figura 6 mostra o rack montado para realização dos testes de desempenho e recomposição abordados neste trabalho.

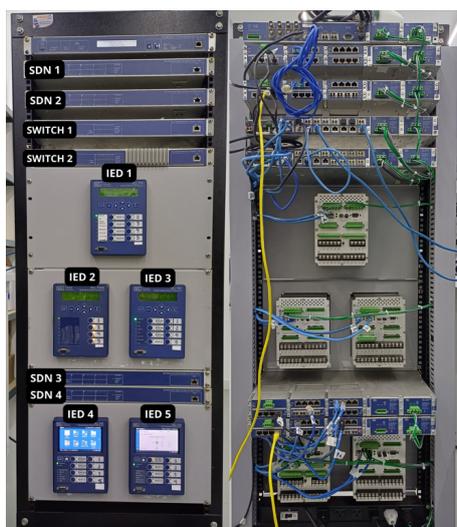


Figura 6. Rack montado para a realização dos testes

Com os switches SDN é possível definir regras de restrição que tornam a rede mais segura e confiável, além de possuir o Fast FailOver, com tempo de reposta menor que o tempo mínimo do protocolo RSTP. Permitindo melhor desempenho na recomposição de rede em casos de falha nas vias que conectam as redes.

Como apontado anteriormente, os dispositivos finais são incapazes de tratar redundâncias que não operam em seus protocolos nativos, e por este motivo foram definidos conjuntos de restrições de fluxo no controlador SDN, na tentativa de garantir a qualidade das mensagens GOOSE utilizando as regras e correspondências de camada 1 a 4 do modelo OSI. A Tabela 1 apresenta um exemplo de configuração das regras de camada 1 e 2:

Tabela 1. Regras e restrições de fluxo aplicadas a uma das portas do SDN A1

Objeto	Restrição
EtherType	GOOSE
MAC de destino	01-0C-CD-01-00-05
VLAN	0x005
Porta/Grupo de ingresso	C1
Porta/Grupo de egresso	Failover: C2 D1

Há restrições quanto à porta de ingresso, destino MAC Multicast da mensagem,

VLAN e EtherType. Além disso, o egresso pode ser definido para um grupo que contém o mecanismo de Failover, possibilitando o redirecionamento de tráfego a uma porta secundária se a primária apresentar falha de link. A ferramenta para comissionamento dos SDN do fabricante, permite a visualização dos fluxos, dos links físicos e lógicos desenvolvidos, e dos caminhos redundantes.

Ao iniciar os testes, esta topologia se mostrou deficiente, uma vez que os switches não trocam informações via *OpenFlow* sobre o estado de suas portas e sobre as restrições contidas nelas. Cada switch SDN toma conta de suas portas e controla suas restrições de tráfego. Apesar do controle ser centralizado e comissionado em um só dispositivo, as regras ficam embarcadas em cada switch e não há troca de informações em *OpenFlow* entre eles durante a operação. Mesmo assim, prosseguiu-se com os testes de desempenho para que as evidências levantadas sirvam de base para o estudo e desenvolvimento de novas arquiteturas e tecnologias passíveis de uso na solução de problemas como este.

4. Metodologia e Testes

Antes de testar e avaliar o desempenho da topologia proposta para interligar as LANs, foram realizados experimentos isolados em cada rede, com tráfego denso de mensagens menos prioritárias que o GOOSE, simulando uma condição de regime permanente de uma rede em operação, e também de uma rede totalmente disponível.

4.1. Testes de Conformidade em Redes Isoladas

Para medir o desempenho das mensagens GOOSE e estimar o tempo de recomposição baseado no atraso das mensagens durante uma falha na rede, uma lógica simples de *ping-pong* foi implementada nos IEDs, de modo a criar um loop de mensagens GOOSE. Essa metodologia também é chamada de RTT (*Round Trip Test* - Teste de ida e volta), possibilitando o monitoramento do canal de comunicação a partir da coleta de dados em escala e dos registros sequencias dos IEDs. A Figura 7 apresenta a lógica implementada para o disparo inicial e dos ecos das mensagens GOOSE.

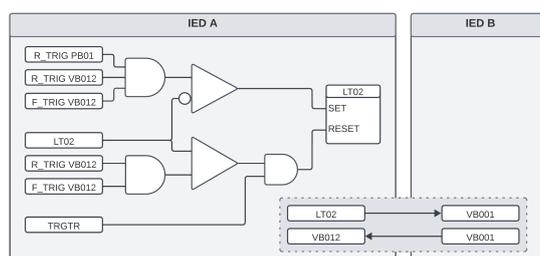


Figura 7. Lógica Ping-Pong desenvolvida entre IEDs

O disparo e a interrupção do ping-pong, foi realizado pelo agente ao pressionar botões no painel frontal do IED. As variáveis virtuais VB (*Virtual Bits*) apresentadas na lógica tem seu valor atribuído na recepção do GOOSE, e a variação de estado destas foi utilizado como disparo para os ecos da lógica. Para não associar erros de sincronismo de tempo entre dispositivos aos resultados do teste, optou-se por registrar as variáveis em um único IED. Sendo assim, os tempos registrados no SOE (*Sequencie of Events*) correspondem à soma do tempo de ida e volta das mensagens. Portanto, guardada a

simetria do canal de comunicação, o tempo de transmissão pode ser determinado como metade do tempo registrado, descontando-se o tempo de um ciclo do IED ($T = r/2 - \text{CIED}$).

O SER dos IEDs registra até 1024 linhas, logo fez-se uso desta quantidade de registros para cada teste realizado, preocupando-se apenas com o fato de que o evento estudado (falha de link) deve estar contido dentro do intervalo experimental. Sendo assim, disparou-se o teste de RTT e gerou-se a falha na rede removendo um dos cabos da porta de rede do IED e devolvendo-o na sequência. Por fim, o teste foi interrompido. A Figura 8 exibe um exemplo do sequencial de eventos de um dos IEDs utilizado nos testes.

#	DATE	TIME	ELEMENT	STATE
28	12/06/2023	09:21:21.882	TESTE1	PICKUP
27	12/06/2023	09:21:21.886	LT01	Asserted
26	12/06/2023	09:21:21.818	VB011	Asserted
25	12/06/2023	09:21:21.827	LT01	Deasserted
24	12/06/2023	09:21:21.839	VB011	Deasserted
23	12/06/2023	09:21:21.847	LT01	Asserted
22	12/06/2023	09:21:21.860	VB011	Asserted
21	12/06/2023	09:21:21.868	LT01	Deasserted
20	12/06/2023	09:21:21.881	TESTE1	DROPOUT
19	12/06/2023	09:21:21.881	VB011	Deasserted
18	12/06/2023	09:21:21.889	LT01	Asserted
17	12/06/2023	09:21:21.982	VB011	Asserted
16	12/06/2023	09:21:21.910	LT01	Deasserted
15	12/06/2023	09:21:21.922	VB011	Deasserted
14	12/06/2023	09:21:21.931	LT01	Asserted
13	12/06/2023	09:21:21.943	VB011	Asserted
12	12/06/2023	09:21:21.952	LT01	Deasserted
11	12/06/2023	09:21:21.964	VB011	Deasserted
10	12/06/2023	09:21:21.972	LT01	Asserted
9	12/06/2023	09:21:21.985	VB011	Asserted
8	12/06/2023	09:21:21.993	LT01	Deasserted
7	12/06/2023	09:21:22.006	VB011	Deasserted
6	12/06/2023	09:21:22.014	LT01	Asserted
5	12/06/2023	09:21:22.023	RESET	PICKUP
4	12/06/2023	09:21:22.027	RESET	DROPOUT
3	12/06/2023	09:21:22.027	LT01	Deasserted
2	12/06/2023	09:21:22.027	VB011	Asserted
1	12/06/2023	09:21:22.039	VB011	Deasserted

Figura 8. Sequencial de eventos de um teste rápido contendo o início e o fim do ping-pong

Inicialmente o desempenho e o tempo de recomposição, das redes RSTP e PRP, foi testado sem que houvesse outro tipo de tráfego concorrente na LAN. Deste modo, o teste ping-pong resultou nas estatísticas exibidas na Tabela 2. Onde a coluna dois apresenta o tempo máximo entre mensagens, que ocorre durante a recomposição da rede, e a coluna três contém o tempo médio entre mensagens trocadas durante todo o teste.

Tabela 2. Dados experimentais referentes ao desempenho das mensagens GO-OSE nas redes vazias - tempo em milisegundos

Rede	Δt Máximo	Δt Médio
PRP	4,5	4,168
RSTP	4,5	4,168
Recomp. PRP	6,5	5,210
Recomp. RSTP	517	5,906

Note que, como o tempo médio de ciclo dos IEDs é de 4 ms e a latência do canal é muito semelhante entre as redes, devido às características de meio físico, o tempo médio entre mensagens nas redes RSTP e PRP é praticamente o mesmo. Isso ocorre pois o tempo de transferência está contido quase que por completo no tempo de ciclo do IED.

A Figura 9 apresenta uma amostra do resultado dos testes realizados com a rede totalmente disponível. A LAN RSTP apresentou o comportamento inesperado no teste de queda e recomposição do link da porta designada (conectada ao root). Note que há um tempo máximo registrado para recomposição da rede de aproximadamente 500 ms. O tempo para a convergência do algoritmo RSTA medido durante os experimentos foi

menor que 70 ms, como consta na Figura 2, entretanto há um atraso até que o GOOSE volte a ser recebido pelo assinante, e retomar o ping-pong. Como a lógica desenvolvida depende da borda de subida ou da borda de descida das variáveis para gerar eventos, a hipótese para o atraso das mensagens GOOSE na retomada do link RSTP decai sobre a lógica do ping-pong e o modelo de transmissão das mensagens GOOSE. Como este fenômeno não ocorreu para quedas de links fora da rede RSTP, uma boa hipótese é que há alguma condição que atrasa o disparo do evento.

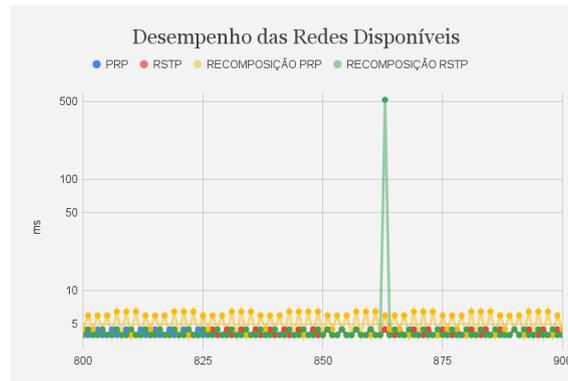


Figura 9. Amostra de dados resultantes dos experimentos de RTT com a rede disponível

A resposta vem quando se olha para o mecanismo de transmissão do GOOSE. Na configuração da transmissão das mensagens, o Tempo Máximo entre mensagens foi definido como 1000 ms. Logo, se as retransmissões do GOOSE geradas após o evento, forem perdidas por alguma indisponibilidade da rede, haverá uma nova transmissão após este período (T_0). Como o tempo de recomposição do RSTP nos relés de proteção pode ser de até 150 ms, como aponta o fabricante [SEL], há um atraso significativo na recomposição que gera uma janela de perdas de mensagens GOOSE. Assim, a mensagem será recebida somente após o tempo máximo definido. Somando o tempo de ciclo do IED e considerando que o tempo foi dividido ao meio (ida e volta), pois somente um IED faz o registro das mensagens, tem-se um valor bem próximo ao medido na recomposição do RSTP experimentada. Da experimentação obteve-se o tempo de aproximado de 500 ms na retomada do ping-pong. Estudos futuros podem ser realizados no intuito de validar esta hipótese.

Buscando simular uma condição mais próxima da condição de operação de uma rede em uma SE, um script em Python [*dados omitidos para revisão duplo-cega*] foi utilizado em um computador auxiliar, com sistema operacional Linux, para injetar tráfego na rede, a fim de gerar uma sobrecarga controlada. A Figura 10 apresenta o fluxo de dados capturado através do software Wireshark, injetado para simular a rede sobrecarregada em pouco mais de 80 Mbps (Megabits por segundo), sendo as portas ethernet dos IEDs de no máximo 100 Mbps.

Refazendo os testes de desempenho e de recomposição, com a rede ocupada por tráfego menos prioritário que o GOOSE, os seguintes resultados foram obtidos:

A Figura 11 apresenta, graficamente, o comportamento das mensagens em uma amostra de tamanho 100, contendo os piores casos. Novamente, o tempo de recomposição da rede RSTP apresenta o tempo máximo entre mensagens de aproximadamente 500 ms, pelo mesmo motivo já explicado anteriormente.

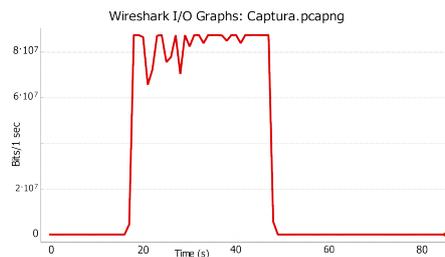


Figura 10. Volume de dados injetados para os testes com rede operacional

Tabela 3. Dados experimentais referentes ao desempenho das mensagens GO-OSE nas redes sobrecarregadas - tempo em mili-segundos

Rede	Δt Máximo	Δt Médio
PRP	6,5	4,953
RSTP	8,5	5,214
Recomp. PRP	6,5	5,210
Recomp. RSTP	519	5,975

4.2. Desempenho e Disponibilidade da Rede Integradora

Sabendo das limitações encontradas no desenvolvimento das regras aplicáveis ao SDN na topologia 2, uma terceira topologia foi utilizada para prosseguir com os estudos. Nesta há um link simples interligando as redes PRP e RSTP. Considerando isso, os mesmos testes e ferramentas foram utilizados para medir o tempo máximo e médio de troca de mensagens, permitindo avaliar o desempenho da rede. Nos testes efetuados com a rede disponível, os resultados obtidos se encontram na Tabela 4. Dois testes foram realizados, disparando o ping-pong a partir de cada uma das redes.

Tabela 4. LAN integradora sem adição de tráfego - tempo em mili-segundos

Rede	Δt Máximo	Δt Médio
PRP - RSTP	6,5	4,17844
RSTP - PRP	4,5	4,16793

O tempo máximo divergiu entre os experimentos devido a algum evento intermitente do canal de comunicação, consideram-se os atrasos no processamento do IED. Mas o tempo medido ainda é adequado, pois se desconsiderarmos o ciclo do IED (4 ms) o tempo de transferência da mensagem ainda é menor que 3 ms.

Os testes realizados com tráfego denso na rede (80% da banda), resultaram nos dados apresentados na Tabela 5.

Os testes realizados com tráfego denso na rede apresentaram desempenho diferente dos testes com a rede ociosa, pois há sobrecarga na rede RSTP e os switches não gerenciáveis não estão comissionados para restringir este tráfego desconhecido.

Para além da disponibilidade mensurada com os testes, é preciso analisar a confiabilidade e integridade das mensagens através das estatísticas e relatórios do GOOSE. Os IEDs da topologia 2 respondem ao comando GOOSE com um relatório das transmissões e recepções de mensagens, onde o item *CODE* consta como *Out Of Sequence* em men-

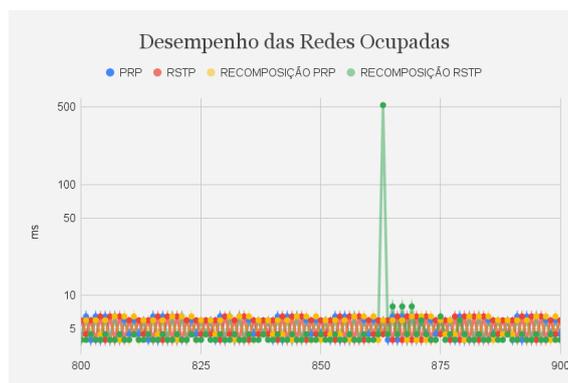


Figura 11. Amostra de dados resultantes dos experimentos de RTT com a rede sobrecarregada

Tabela 5. LAN integradora com adição de tráfego - tempo em mili-segundos

Rede	Δt Máximo	Δt Médio
PRP - RSTP	10,5	4,75429
RSTP - PRP	10,5	5,26044

sagens originárias da rede interligada, como mostrado na Figura 5, e isso indica que há perda ou replicação de pacotes na rede. Portanto, após os testes com a topologia 2 fica evidente que, apesar de os tempos médios estarem em acordo com as determinações da norma IEC 61850, em todos os casos testados, os requisitos de qualidade do serviço (QoS) não são cumpridos, pois há falha de sequência nas mensagens transmitidas entre as redes, e isso pode gerar, por exemplo, falhas na atuação de esquemas de proteção coordenada.

5. Conclusão

Após a realização dos testes e análise dos resultados obtidos, conclui-se que ambas as topologias propostas são insuficientes para atingir os objetivos estabelecidos no início do estudo. As restrições de rede necessárias para tratar a redundância de mensagens o mais próximo possível do dispositivo final não são cabíveis com a tecnologia e as topologias utilizadas neste experimento.

Novas topologias podem ser avaliadas a partir dos testes realizados neste estudo de caso, com uso de RedBox para tratar redundâncias do PRP na estrada da rede RSTP, por exemplo, e com tráfegos de igual ou maior prioridade, como o SV (*Sampled Values*), concorrendo com o GOOSE na rede. Entretanto, com os resultados obtidos neste trabalho, a proposição ideal de aplicação do PRP em todos os dispositivos finais, juntamente com o uso de switches SDN como porta de entrada de cada LAN, se apresenta como a solução mais adequada para atuais projetos de engenharia de redes de comunicação em um SAS.

Finalmente conclui-se que o estudo de topologias de rede é importante para compreender os problemas de disponibilidade e qualidade de mensagens em comunicações ponto a ponto de alta velocidade, sendo necessário a compreensão clara dos mecanismos de transmissão dos protocolos utilizados e das diretrizes da norma IEC 61850 em aplicações nos SAS. Pois assim como a estrutura de proteção deve ser rápida, segura e confiável, com a digitalização das subestações a rede de TO e os sistemas de automação devem assim ser também confiáveis, seguros e ágeis.

Referências

- 61850, I. (2011). Part 8-1: Specific communication service mapping (scsm) - mappings to mms (iso 9506-1 and iso 9506-2) and to iso/iec 8802-3 - 2nd ed. In *IEC 61850-8-1, Communication networks and systems for power utility automation*, Geneva, Switzerland.
- Adilson Kotryk, Eduardo Goncalves, R. A. M. S. P. L. and Ferrari, V. (2023). Complete monitoring solution to improve reliability and performance of digital secondary systems. In *Protection, Automation Control World Conference*.
- Araujo, J., Lázaro, J., Astarloa, A., Zuloaga, A., and Moreira, N. (2013). Duplicate and circulating frames discard methods for prp and hsr (iec62439-3). In *IECON 2013 - 39th Annual Conference of the IEEE Industrial Electronics Society*, pages 4451–4456.
- Dearien, J. (2017). *Escolhendo a Melhor Topologia de Rede de Comunicação para Aplicações com IEC 61850*.
- Faustino Junior, W. A. et al. (2018). Tráfego de mensagem goose em redundância de comunicação em subestações de energia elétrica. Master's thesis, Universidade Tecnológica Federal do Paraná.
- Kalra, A., Dolezilek, D., Mathew, J. M., Raju, R., Meine, R., and Pawar, D. (2020). Using software-defined networking to build modern, secure iec 61850-based substation automation systems. In *15th International Conference on Developments in Power System Protection (DPSP 2020)*, pages 1–6. IET.
- Khavnekar, A., Wagh, S., and More, A. (2015). Comparative analysis of iec 61850 edition-i and ii standards for substation automation. In *2015 IEEE International Conference on Computational Intelligence and Computing Research (ICIC)*, pages 1–6. IEEE.
- Kirrmann, H., Hansson, M., and Muri, P. (2007). Iec 62439 prp: Bumpless recovery for highly available, hard real-time industrial networks. In *2007 IEEE Conference on Emerging Technologies and Factory Automation (EFTA 2007)*, pages 1396–1399. IEEE.
- Lopes, Y., Franco, R. H. F., Molano, D. A., dos Santos, M. A., Calhau, F. G., Bastos, C. A. M., Martins, J. S., and Fernandes, N. C. (2012). Smart grid e iec 61850: Novos desafios em redes e telecomunicações para o sistema elétrico. *XXX Simpósio Brasileiro de Telecomunicações*.
- Meine, R. (2019). A practical guide to designing and deploying ot sdn networks. In *proceedings of the Power and Energy Automation Conference, Spokane, WA*.
- SEL, S. E. L. *SEL-751 Feeder Protection Relay - Instruction Manual - Date Code: 20230607*.
- Yang, Q. and Smith, R. (2019). Improve protection communications network reliability through software-defined process bus. In *Power and Energy Automation Conference*, page 4.
- Yang, S.-H., Yang, H.-S., Ahn, Y.-H., and Kim, Y.-H. (2012). Performance analysis of iec 61850 based substation. In *2012 14th International Conference on Advanced Communication Technology (ICACT)*, pages 854–858.