VALIDAÇÃO DO PROTOCOLO RSTP EM SISTEMAS DE AUTOMAÇÃO DE SUBESTAÇÃO PARA APLICAÇÃO COM GOOSE

Marcelo Antonio C. de Sant'Anna[1], Oberdan Rocha Pinheiro[2]

[1]Instituição/Empresa SENAI CIMATEC, E-mail: marcelo_acs@hotmail.com;

[2]Instituição/Empresa SENAI CIMATEC, E-mail: oberdan.pinheiro@fieb.org.br;

VALIDATION OF THE RSTP PROTOCOL IN SUBSTATION AUTOMATION SYSTEMS FOR GOOSE APPLICATION

Resumo: *Os Sistemas de Automação de Subestações Industriais já estão se tornando comuns e amplamente utilizados. Com o advento desta modalidade, as redes Ethernet precisaram se adaptar aos níveis de exigência requeridos por estes sistemas. Os equipamentos de automação tornaram-se mais robustos e as topologias redundantes mais presentes. O protocolo RSTP surgiu para garantir a ausência de loops nestas topologias e reduzir os tempos de convergência e reestruturação da rede ativa em caso de falhas. Este artigo traz a análise sobre o desempenho do protocolo RSTP em uma rede Ethernet implementada em um projeto de digitalização de uma subestação, bem como a observação do tempo de recomposição para aplicação protocolo GOOSE.*

Palavras-Chaves: RSTP; Subestação Automatizada; Ethernet; GOOSE

Abstract: *Industrial Substation Automation Systems are already becoming common and widely used. With the advent of this modality the Ethernet networks had to adapt to the levels of exigency required by these systems. Automation equipment has become more robust and redundant topologies are more present. The RSTP protocol was introduced to guarantee the absence of loops in these topologies and reduce the convergence and restructuring times of the active network in case of failures. This paper presents analysis of the performance of the RSTP protocol in an Ethernet network implemented in a project of a digital substation, as well as the observation of the recomposition time for the GOOSE protocol application.*

Keywords: RSTP; Automated Substation; Ethernet; GOOSE

1. INTRODUÇÃO

Os sistemas de automação (SA) industrial atingiram níveis de importância que exigem rápida recuperação em caso de falha de cabos e equipamentos, além de uma comunicação robusta. No que diz respeito a automação de sistemas elétricos, as redes Ethernet se apresentam como uma das principais soluções, tendo equipamentos fundamentais como relés, com endereço MAC e IP, ligados a redes com switches e roteadores. [1] A partir do momento em que setores vitais para a segurança no fornecimento de energia elétrica, como o de proteção, passaram a integrar o sistema de automação, as atenções voltaram para o desenvolvimento dos SAs de modo que estes acompanhassem os níveis de exigência de confiabilidade e disponibilidade.

Uma das preocupações mais comuns é com a disponibilidade do equipamento, no qual os dispositivos de redes, switches, roteadores, etc. necessitam de taxas de disponibilidades equivalentes a um relé de proteção (99,9945%), evitando a adição de um ponto vulnerável. [1] Outra forma muito utilizada para aumentar a disponibilidade do sistema é implementar redundâncias, ou seja, algumas partes do sistema de automação são duplicadas de forma que, caso ocorra alguma falha de equipamento ou de link, a parte redundante assuma as tarefas, restaurando a comunicação em curtos períodos de tempo. [2]

A redundância de caminhos entre switches demanda a implementação de protocolos de redundância de rede que têm como objetivo definir a topologia em situações de estabilidade e redefini-la em caso de falhas, evitando a presença de loops (laços lógicos). Em aplicações Ethernet o protocolo RSTP (*Rapid Spanning Tree Protocol* – IEEE *Standard* 802.1Q) é uma das alternativas padronizada pela IEEE para possibilitar a arquitetura de redes locais com enlaces redundantes, focando também na redução no tempo de reestabelecimento após falhas. [3] Neste estudo, além de analisar o comportamento do RSTP em uma rede de subestação diante de contingências, será observado o tempo de reestabelecimento das mensagens GOOSE (*Generic Object Oriented Substation Events*) após a falha de algum ponto da rede.

1. OBJETIVOS

1.1. Objetivo Geral

Apresentar a arquitetura da rede de automação de uma subestação com o protocolo RSTP implementado e discutir a performance da definição e reestruturação da topologia e da troca de dados.

1.2. Objetivos Específicos

Apresentar os resultados do protocolo RSTP obtidos nas simulações de operação e contingências da rede de automação feitas no Teste de Aceitação de Fábrica (TAF) do projeto de digitalização de uma subestação. Analisando a definição e reestruturação dos degraus de switches em relação a presença de loops, além de mensurar o tempo de recomposição da mensagem GOOSE após uma contingência.

2. METODOLOGIA

O desenvolvimento do trabalho se baseou nas definições do IEEE em relação ao protocolo RSTP e nas informações de artigos sobre a norma IEC 61850, assim como nos artigos relacionados ao tema e a automação de subestações. Organizando as informações teóricas para estruturar a base do trabalho, descreve-se as características do sistema de automação da subestação de uma determinada empresa, os principais dispositivos pertencentes e a estrutura da rede.

Por fim, de posse dos dados referente ao Teste de Aceitação de Fábrica realizado pelo fabricante no projeto de digitalização da subestação, no qual foram simuladas contingências na rede, perda de links, analisou-se os dados para validação do protocolo RSTP em uma arquitetura em camadas (*ladder*). Adicionalmente, por se tratar de uma aplicação de rede para norma IEC 61850, se observou o tempo de recomposição da mesma, no qual foi medido o tempo em que a mensagem GOOSE é reestabelecida após a abertura de algum ponto da rede. Analisando e discutindo o protocolo baseado na reestruturação dos degraus de switches e nas recomendações de performance definidos na norma IEC-61850.

3. REDES *ETHERNET* EM SUBESTAÇÕES

As redes *Ethernet* passaram a ganhar espaço em diversos ambientes da automação. Não diferente disto, começou a ser utilizada na comunicação entre dispositivos da subestação para diferentes aplicações. Cada uma destas aplicações requer que a mesma atenda requisitos variados, chegando a atingir níveis rígidos de tempo de transferência inferior a 3 milissegundos para sistemas de controle baseados máquina-a-máquina de alta velocidade em IEC 61850. [4]

A norma IEC 61850 surgiu para padronizar a comunicação nas subestações de forma que dispositivos de diferentes fabricantes pudessem interagir. Dentre os diversos protocolos especificados pela norma, o protocolo GOOSE foi criado para comunicação de dados de alta prioridade e tempos de transferência críticos. Mensagens de proteção, intertravamento e controle,

devido a importância das mesmas, devem ser trafegadas utilizando o protocolo GOOSE. Em função disto, a IEC 61850-90-4 define recomendações de tráfego em redes Ethernet baseado na aplicação do sistema. A Tabela 2 apresenta as recomendações referente ao protocolo GOOSE, aplicação na qual o sistema do estudo de caso faz uso. A classe de tempo P1 se refere a aplicações no nível de distribuição da subestação e a P2 e P3 são utilizadas a nível de transmissão. [5]

Tabela 1. Mensagens GOOSE e as classes de desempenho. [5]

Tipo da Função	Mensagem	Protocolo	Tempo de transf. Recomendado	Largura de Banda	Prioridade	Aplicação
1A – Trip	GOOSE	L2, Multicast	3 (P2/P3) a 10 (P1) ms	Baixa	Alta	Proteção
1B – Outros	GOOSE	L2, Multicast	20 (P2/P3) a 100 (P1) ms	Baixa	Média Alta	Proteção

Adicionalmente, a interrupção da chegada de mensagens no receptor, ou um atraso na entrega superior a 18 milissegundos é caracterizado como uma falha (tipo 1A). Sendo assim, os projetos de redes *Ethernet* tem de criar dispositivos para atender os requisitos em condição normal de operação, bem como o mínimo tempo de recuperação caso haja uma falha de switch ou link. A linha inicial básica para atender estes critérios é utilizar equipamentos de alta confiabilidade e instalações que visem reduzir ao mínimo as chances de falhas. [5]

Quando o sistema não alcança níveis desejados de desempenho, alternativas como a implementação de redes redundantes também são utilizadas. Para escolha da topologia normalmente se leva em consideração o tamanho da rede. Com isso, caso a rede seja muito pequena (com 5 switches ou menos) utiliza-se a topologia em anel. Para redes maiores (com 6 switches ou mais), para aplicações de proteção de alta velocidade, a topologia em camadas (*ladder*) é a mais apropriada. [4] A Figura 1 apresenta as duas topologias descritas.

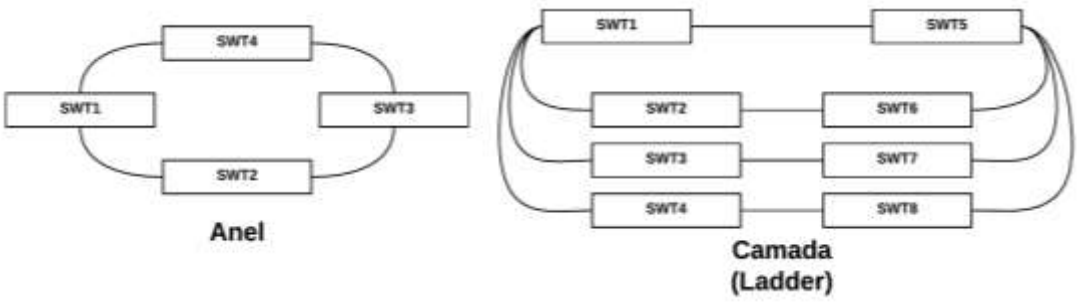

Figura 1. Esquema de topologia em anel e camadas (ladder).

Uma topologia pequena em anel contém poucos switches, fazendo com que os tempos de troca de mensagens entre quaisquer um destes permaneça com valores próximos, devido aos poucos saltos. Os tempos de definição e recuperação do protocolo de redundância (RSTP) são melhores nesta condição de topologia menor, essencial para aplicações de proteção. Em contrapartida, caso haja uma falha em um link ou dispositivo todos os outros switches da rede são afetados, potencializando o defeito. [4]

Já em redes amplas, a topologia em camadas (*ladder*) mostrou-se a mais resiliente e mais rápida para comunicação de mensagens críticas e para implementação do protocolo de redundância (RSTP). Esta topologia permite a adição de novas camadas de switches (degraus) sem afetar os existentes, já que a root e a backup root estão na base da “escada”. Os fatores de destaque para aplicações críticas são: Os diferentes caminhos ofertados potencializam a confiabilidade da rede; e o trafego das mensagens são isolados por degrau, ou seja, caso haja algum defeito em um dos níveis os outros não são afetados, aumentando a integridade da rede. [4]

4. RAPID SPANNING TREE PROTOCOL (RSTP)

Desenvolvido pela IEEE Standard, o protocolo RSTP é uma versão aprimorada do *Spanning Tree Protocol* (STP – IEEE Standard 802.1d), cuja principal evolução foi a redução no tempo de recuperação da comunicação após algum evento. O objetivo principal continua sendo solucionar os loops no tráfico e evitar loops acidentais, através de uma ideia principal, no qual alguns links são forçados para o modo *hot standby*, reduzindo a topologia da rede. [3] [6]

O gerenciamento da topologia ativa da rede é feito a partir da definição da prioridade relativa de cada switch e das suas portas, assim como definir o custo do “caminho” associado a cada porta (*path cost*). Baseados nestas premissas são desenvolvidos conceitos a respeito do protocolo. Inicialmente, se determina o switch principal da rede, também conhecido como *Root Bridge*, a partir do Bridge ID, número de identificação determinado administrador da rede. A *bridge* que tiver o menor número de identificação é considerada a *root* da topologia, fazendo com que as demais bridges da rede troquem mensagens com informações de configuração com aquela. Nesta etapa ocorre o cálculo do melhor caminho entre as *bridges* e a *Root Bridge* baseado no custo envolvido em cada link (*path cost*). As funções das portas dos switches são definidas a partir destas informações envolvendo o caminho com menor custo até a *Root Bridge*. [6]

Os pacotes referentes a comunicação entre as *bridges* são denominados de BPDU (*Bridge Protocol Data Unit*), sendo responsáveis pelo transporte de informações de controle que orientam as ações das mesmas. Estas mensagens são trocadas por todas as portas a cada tempo definido (*hello time*). O processo de tomada de decisão da topologia envolve muitas trocas de BPDUs.

Após caracterização dos switches, com a *Root Bridge* estabelecida, os papéis e os estados das portas de cada um destes dispositivos da rede são definidos, por meio dos BPDUs, para o correto funcionamento do protocolo RSTP. Os estados das portas podem ser *Forwarding* (Encaminhamento), significando que a porta envia e recebe frames regulares da rede e BPDUs, *Discarding* (Descarte), significando que a porta recebe BPDUs mas os frames regulares da rede são descartados, e *Learning* (Aprendizagem), significando que a porta está aprendendo informações dos pacotes BPDUs. Em relação aos papéis das portas, os mesmos são caracterizados da seguinte forma [3] [6] [7]:

- Porta *Root*: Porta com menor *path cost* até a *Root Bridge*;
- Porta *Designated*: Porta que disponibiliza informação da *Root Bridge* para o segmento associado;
- Porta *Alternated*: Porta de melhor opção para comunicação com a *Root Bridge* caso a porta *Root* atual falhe, deixando o link ativo apenas para troca de BPDUs;
- Porta *Backup*: Porta com ligação redundante para a mesma *bridge*, contudo não oferece uma conexão alternativa para a *Root Bridge*;
- Porta *Edge*: Porta conectada a uma estação final (*host*).

Ao final do processo, com as portas e as bridges com o seu papel definido, juntamente com o estado de cada porta, o protocolo RSTP define a topologia ativa da rede (spanning tree). Caso seja adicionado ou removido um componente da rede, a transição de learning para fowarding é atrasada, e as portas podem ser definidas como discarding temporariamente a fim de garantir a ausência de caminhos duplicados. Além da ausência de loops, a rápida transição para estado forwarding dos segmentos ativos é um dos objetivos do protocolo para evitar/reduzir mensagens perdidas.

5. ESTUDO DE CASO

As informações referentes a planta industrial e aos resultados das simulações em ambiente laboratorial foram fornecidas ao autor desse artigo para fins acadêmicos. O nome da empresa e outras informações que relacione a estrutura real foram omitidas.

O sistema elétrico industrial da Unidade 1 é formado por um conjunto de subestações principais SE-Alfa, SE-Beta, SE-Charlie e os consumidores, sendo que a SE-Alfa é a mais importante do sistema. Desta subestação partem alimentadores de 69kV ou 13,8kV para as demais subestações da própria instituição e outras SEs das empresas da região. O projeto em questão consistia em atender dois escopos que se interligavam, o da implantação do novo esquema de rejeição de cargas automático e o de digitalização com os relés inteligentes (IEDs) conectados através de uma rede Ethernet, definindo a norma IEC 61850 como padrão.

O estudo apresentado neste artigo tem como objetivo analisar a solução para recomposição dos degraus de switches que constituem a rede

IEC 61850 de digitalização para os IEDs de controle e proteção fornecida pelo fabricante, através de testes laboratoriais utilizando uma quantidade representativa de equipamentos capazes de emular a rede real. Adicionalmente, foram utilizados analisadores de protocolos, sequenciadores de eventos e ferramentas para mensurar o desempenho da rede com o protocolo RSTP.

A rede utilizada para análise é composta por switches *Ethernet* de nível 2 e IEDs que atendem o tempo de transferência de 3 milissegundos, definido na IEC 61850. A taxa de transferência dos links adotadas para comunicação entre IEDs é de 100 Mbps. Já que a arquitetura das redes que compõem as subestações é bastante similar, os testes para validação da arquitetura em camada e do protocolo RSTP foram realizados na rede relacionada a SE-Alfa, conforme Figura 2. Também, ilustra-se na mesma as configurações do protocolo RSTP e a sua rede ativa resultante.

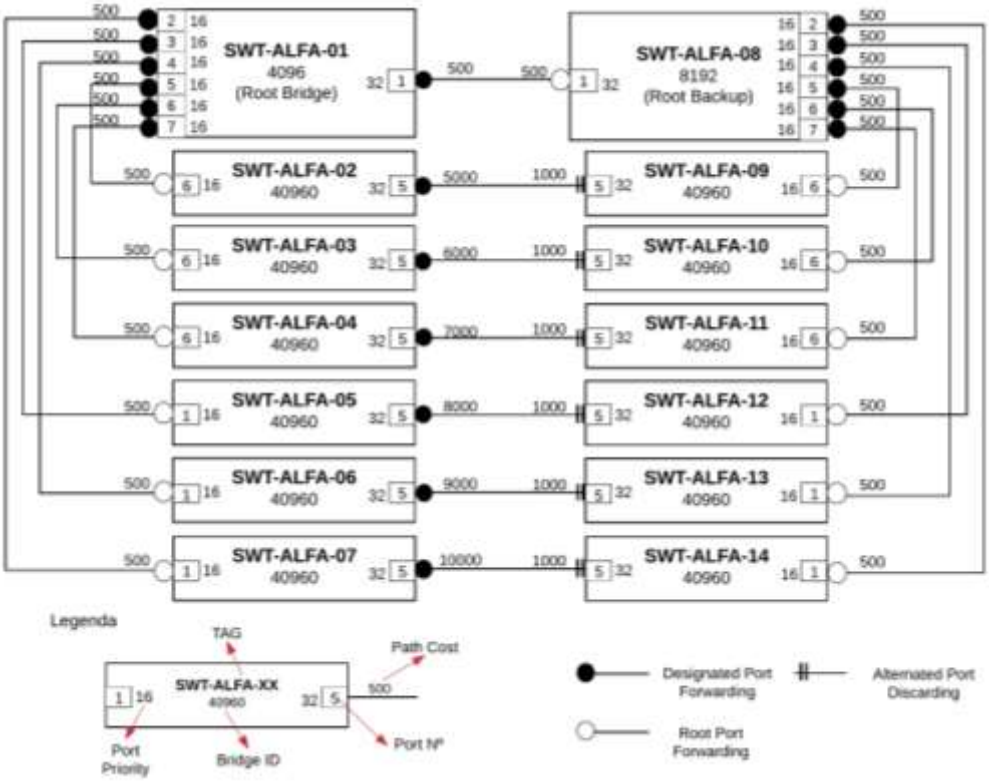

Figura 2. Configuração do RSTP na rede da SE-Alfa.

5.1. Teste 1: Falha no link entre os switches SWT-ALFA-02 e SWT-ALFA-09

A falha no link entre os switches SWT-ALFA-02 e SWT-ALFA-09 não resulta em nenhuma modificação na topologia ativa da rede já que o link em questão estava inativo, ou seja, descartando dados convencionais, transmitindo apenas de controle (Alternate Discarding). O comportamento do protocolo para

o evento ocorrido foi coerente com os dados implementados, atuando dentro da normalidade.

5.2. Teste 2: Falha no link entre os switches SWT-ALFA-01 e SWT-ALFA-08

A falha no link entre os switches SWT-ALFA-01 (Root bridge) e SWT-ALFA-08 (Root bridge backup) proporciona mudanças consideráveis na topologia da rede devido a importância dos mesmos no algoritmo RSTP. O SWT-ALFA-08, na topologia ativa, atua como o elo de comunicação dos demais switches do lado direito com a Root bridge localizada no lado esquerdo. O algoritmo do protocolo, baseado nos paths cost e Bridge ID definidos, responde a mudança conforme esperado. A Figura 3 ilustra o resultado da reconvergência.

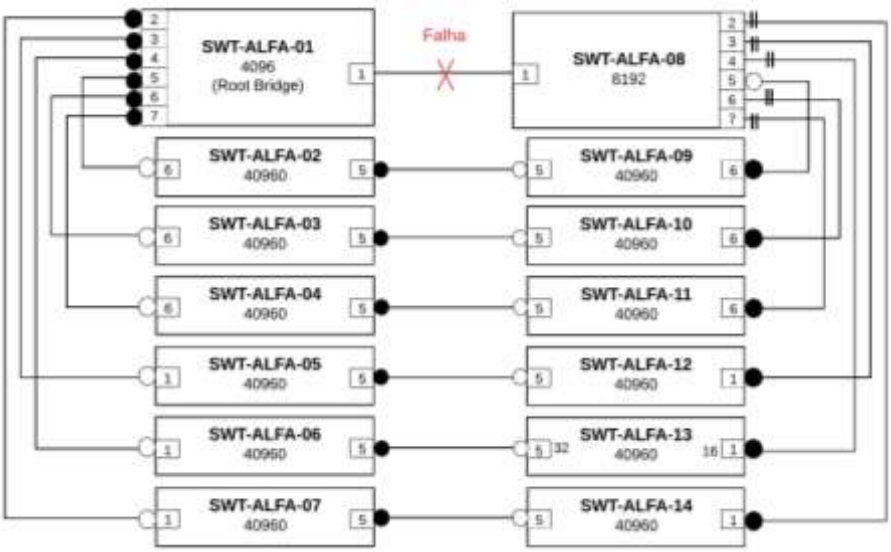

Figura 3. Reconvergência da rede após falha do Teste 2.

5.3. Teste 3: Falha no link entre os switches SWT-ALFA-01 e SWT-ALFA-02

Ao ocorrer uma falha no link entre o SWT-ALFA-01 e SWT-ALFA-02 há uma perda de comunicação com a *Root bridge*, fazendo com que esta comunicação tente ser reestabelecida através da porta restante. Como resultado da simulação, o algoritmo do RSTP altera o papel da porta que conecta o SWT-ALFA-02 ao SWT-ALFA-09 para *Root port*, caracterizando este link como o novo caminho até a *Root bridge*. Após a reconvergência o sistema estabiliza e os demais switches não sofrem alterações.

5.4. Teste 4: Falha no link entre os switches SWT-ALFA-08 e SWT-ALFA-09

Assim como o teste realizado no item 4.3, a falha no link entre os switches SWT-ALFA-08 e SWT-ALFA-09 compromete a conexão do segundo com a Root bridge. O único link remanescente ligado ao SWT-ALFA-09 é o do SWT-ALFA-02, implicando na ativação do mesmo por parte do algoritmo do protocolo. A porta do SWT-ALFA-09 conectada a este link passa a ser uma Root port e as demais portas e links permanecem sem alterações e estáveis.

5.5. Tempo de Recomposição da Aplicação

Além da performance do protocolo RSTP no que diz respeito a definição e reestruturação da topologia ativa, evitando a presença de loops, foram realizadas medições do tempo em que a mensagem GOOSE (aplicação da rede) é reestabelecida após abertura de algum ponto da rede. Os testes foram feitos utilizando dois IEDs fazendo ping-pong na rede, ou seja, um deles publica a mensagens GOOSE e outro as subscreve, reenviado elas para o IED publicador inicial, conforme demonstrado na Figura 4.

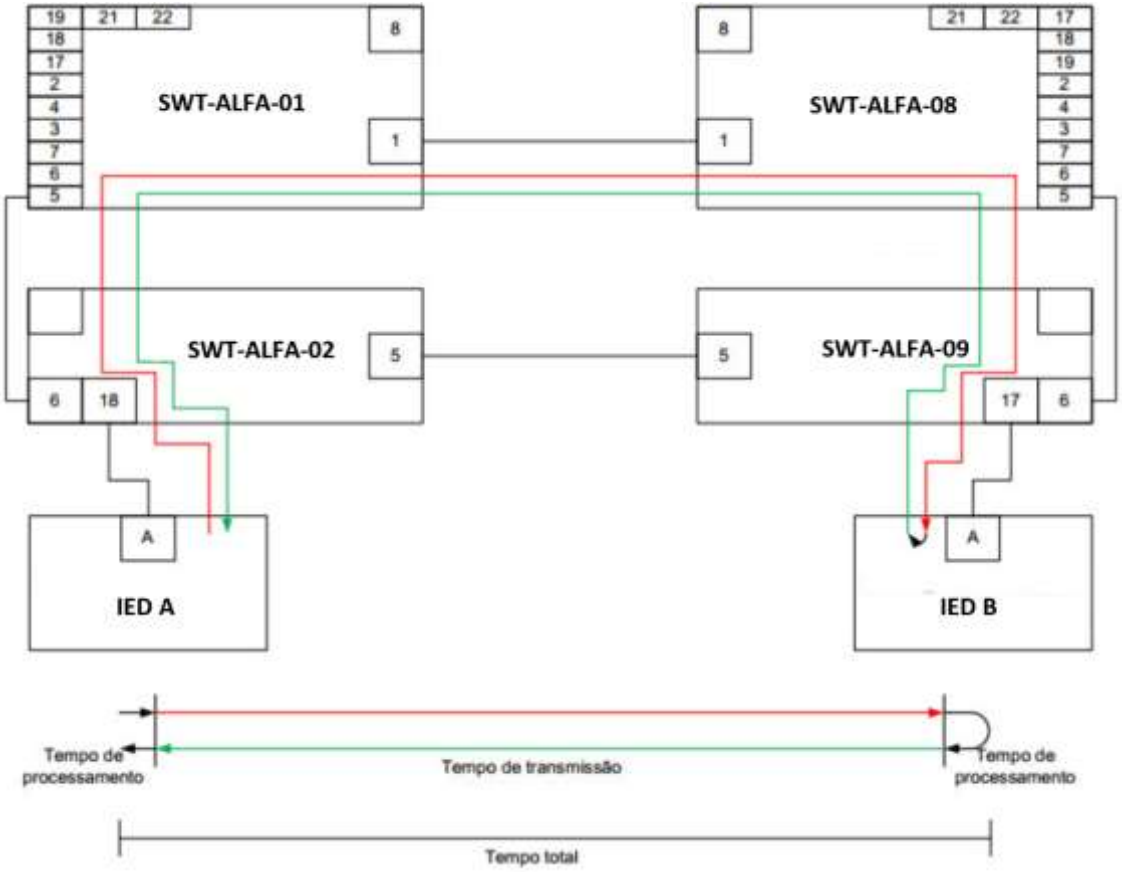

Figura 4. Configuração do RSTP na rede da SE-Alfa.

O tempo de recomposição é medido entre o instante que o IED parar de subscrever as mensagens e o momento de retorno. O cálculo do tempo de recomposição foi realizado utilizando o sequencial de eventos do IED publicador inicial. Os mesmos defeitos realizados nos testes dos itens 4.1 ao 4.4 foram refeitos para medição do tempo e os resultados estão demonstrados na Tabela 2.

Tabela 2. Tempo de recomposição da mensagem GOOSE

Teste	Tempo do ping-pong		Tempo de Recomposição	Mensagens Perdidas
Teste 1	Mínimo	00:00:00.016	0ms (zero)	Nenhuma
	Máximo	00:00:00.017		
	Média	00:00:00.017		
Teste 2	Mínimo	00:00:00.024	50ms	2
	Máximo	00:00:00.075		
	Média	00:00:00.025		
Teste 3	Mínimo	00:00:00.024	799ms	32
	Máximo	00:00:00.825		
	Média	00:00:00.026		
Teste 4	Mínimo	00:00:00.013	362ms	14
	Máximo	00:00:00.387		
	Média	00:00:00.025		

Para cada teste foram gerados 1000 eventos com intervalos de 16ms para o Teste 1 e de 20ms para os demais, dos quais foram medidos os tempos mínimo, máximo e médio do ping-pong. Os dados do tempo de recomposição são definidos através da diferença entre o tempo máximo e o tempo médio, sendo exibidos na Tabela 1.

Como já descrito no item 4.1, a falha do Teste 1 ocorre em um link que estava logicamente desabilitado, sem provocar assim alterações na estrutura da rede por parte do RSTP. Portanto, o tempo de recomposição deste teste é zero, além de não comprometer com a perda de pacotes. Em contrapartida, os demais testes afetam links ativos da rede, fundamental para troca de mensagens entre os IEDs, fazendo com que exista um tempo de recomposição proveniente da reestruturação da rede. O teste com pior tempo foi o Teste 3 (799ms), seguido pelo Teste 4 (362ms) e por fim o Teste 2 (50ms), adicionalmente, todos eles apresentaram perda de pacotes.

Os testes foram repetidos algumas vezes para comprovar a repetitividade dos dados. Os resultados apresentados foram satisfatórios e em conformidade com os ajustes implementados do protocolo RSTP, sem apresentar nenhuma anormalidade. A topologia em camadas com o RSTP se mostrou satisfatória no que diz respeito a ausência de loops e na integridade

dos demais degraus que não ocorreram a falha. Em relação ao tempo de recomposição da mensagem GOOSE, em caso de falhas que envolvam links de switches com a *Root bridge e root backup* o impacto é grande, fazendo com que os tempos de escuridão sejam elevados (acima dos 18 ms), considerando ainda que há perda de pacotes durante estas falhas.

6. CONCLUSÃO

O RSTP apresenta uma alternativa adequada para implementação em redes *Ethernet* com caminhos redundantes, visando atender as aplicações que exigem elevada disponibilidade. A configuração deste protocolo permite a flexibilidade na definição da topologia ativa da rede e prever como a mesma se reestruturará após uma falha. A implementação do RSTP em topologia de camadas (ladder) incrementa a confiabilidade graças a redundância e a ausência de loops. Além do que, mudanças envolvendo cabeamento ou em algum dispositivo, os switches se adaptam automaticamente e em casos de defeitos em uma das camadas as outras não são afetadas.

Contudo, problemas envolvendo os switches root e root backup acarretam em períodos de escuridão durante a reconfiguração da rede que podem prejudicar a comunicação caso ocorra algum evento no sistema de potência. Em aplicações GOOSE tipo 1A, que trafegam dados críticos, as recomendações de tráfego da norma são bastante rígidas, envolvendo até mesmo o tempo de escuridão inferior à 18 ms nas classes P2/P3. [5] Na rede apresentada no estudo de caso, durantes os testes de falha, os tempos de restabelecimento das mensagens trocadas entre os IEDs excederam muito aos recomendados para aplicações GOOSE.

A probabilidade de falhas envolvendo o switch root e root backup podem ser mitigados através da escolha de dispositivos robustos, com disponibilidade elevada, medida com o tempo médio entre falhas (MTBF) em anos. Outra alternativa de mitigação pode ser através do gerenciamento da topologia ativa, realizando outros testes com o intuito de encontrar uma que aumente significativamente o desempenho da rede, consequentemente reduzindo os tempos de escuridão [4].

7. REFERÊNCIAS

[1] SCHWEITZER ENGINEERING LABORATORIES (SEL). Arquiteturas e redundâncias em redes Ethernet. **O Setor Elétrico,** São Paulo, v. 51, n. 4, p.56-61, abr. 2010. Disponível em: <http://www.osetoreletrico.com.br/wp-content/uploads/2010/04/Ed51_fasc_subestacoes_cap4.pdf>. Acesso em: 02 set. 2017.

[2] WISNIEWSKI, Lukasz et al. A survey of ethernet redundancy methods for real-time ethernet networks and its possible improvements. **IFAC Proceedings Volumes**, v. 42, n. 3, p. 163-170, 2009.

[3] INSTITUTE OF ELETRICAL AND ELECTRONICS ENGINEERS. **STD. 802.1D**: Media Access Control (MAC) Bridges. Nova Iorque, 2004. Pp

[4] JASON DEARIEN. Schweitzer Engineering Laboratories (SEL). **Escolhendo a Melhor Topologia de Rede de Comunicação para Aplicações com IEC 61850.** 2017. Disponível em: <https://selinc.com/api/download/120806/?lang=pt>. Acesso em: 23 out. 2017.

[5] SCHWEITZER ENGINEERING LABORATORIES (SEL). ***Entendendo e validando redes Ethernet para aplicações de proteção, automação e controle de missões críticas.***

[6] INSTITUTE OF ELETRICAL AND ELECTRONICS ENGINEERS. **STD. 802.1Q**: Bridges and Bridged Networks. Nova Iorque, 2014. Pp

[7] CISCO. **Compreendendo o protocolo de abrangência de árvore rápida (802.1w).** Disponível em: <https://www.cisco.com/c/pt_br/support/docs/lan-switching/spanning-tree-protocol/24062-146.html>. Acesso em: 23 out. 2017