TRÁFEGO DE MENSAGENS *GOOSE* EM REDUNDÂNCIA DE COMUNICAÇÃO EM SUBESTAÇÕES DE ENERGIA ELÉTRICA

WANDERLEY A. F. JUNIOR

Sistemas de Proteção e Controle, Transformadores e Serviços de Energia das Américas Ltda
Rua Comendador Araújo, 355, CEP 80420-000, TSEA Energia, Curitiba-PR
E-mail: wanderley.faustino@tseaenergia.com.br

ULISSES C. NETTO

PPGSE, DAELT, Universidade Tecnológica Federal do Paraná
Avenida Sete de Setembro, 3165, CEP 80230-901, UTFPR, Curitiba-PR
E-mail: ucnetto@utfpr.edu.br

Abstract— To minimize the impacts to the electrical power system, that some existing data communication network in an electrical substation could cause, the second edition of the IEC 61850 standard defined the use of active redundancy means for that network, for example, the Parallel Redundancy Protocol (PRP) defined by the IEC 62439 standard, which the main objective is increasing the reliability and continuity of the data communication network. For applications of the IEC 61850 standard to the protection systems, the latency of Generic Object Oriented Substation Events (GOOSE) messages is a pressing concern, because it may have deleterious influence on the time performance of those systems. In this research, the influence of the PRP on the behavior of the GOOSE messages during the occurrence of a disturbance in the communication network will be evaluated. Therefore, a laboratory apparatus was developed making possible the evaluation of a PRP network under different traffic conditions (basal and concurrent). The results of the PRP network were compared with a redundancy method that uses a hot-standby failover mechanism and show that the PRP doesn't degrade the behavior in the GOOSE messages timming while to the hot-standby failover was observed a pronounced transient component in those messages.

Keywords— Intelligent Electronic Device, IEC 61850, GOOSE Message, Parallel Redundancy Protocol, Communication Network, Substation Automation System, Electric Power System

Resumo— Para minorar os impactos ao sistema elétrico de potência, que a rede de comunicação de dados existente em uma subestação de energia poderia causar, a segunda edição do padrão IEC 61850 definiu a utilização de meios de redundância ativa para aquela rede como, por exemplo, o *Parallel Redundancy Protocol* (*PRP*) definido pela norma IEC 62439, cujo objetivo principal é aumentar a confiabilidade e continuidade da rede de comunicação de dados. Para aplicações do padrão IEC 61850 a sistemas de proteção a latência das mensagens *Generic Object Oriented Substation Events* (*GOOSE*) é uma preocupação premente, pois, pode ter influência deletéria sobre o desempenho no tempo daqueles sistemas. Nesta pesquisa será avaliada a influência do *PRP*, sobre o comportamento no tempo das mensagens *GOOSE* quando da ocorrência de um distúrbio na rede de comunicação. Para tanto, um aparato laboratorial foi desenvolvido tornando possível avaliar uma rede *PRP* em condições de tráfego distintas (basal e concorrente). Os resultados da rede *PRP* foram comparados com um método de redundância que utiliza um mecanismo *de hot-standby failover e* mostram que o *PRP* não degrada o comportamento no tempo das mensagens *GOOSE* enquanto para o *hot-standby failover* se observa um pronunciado componente transitório naquelas mensagens.

Palavras-chave— *Intelligent Electronic Device*, IEC 61850, Mensagem *GOOSE*, *Parallel Redundancy Protocol*, Redes de comunicação, Sistema de Automação de Subestações, Sistema Elétrico de Potência.

1 Introdução

Um Sistema de Automação de Subestações (SAS) possui vários equipamentos componentes como, por exemplo, relés de proteção digital, unidades de aquisição e controle, oscilógrafos, medidores multifunção, sistema de aquisição de dados e sistema de supervisão, os quais fornecem informações importantes para a análise e operação do Sistema Elétrico de Potência (SEP) (Araujo, Marcelo L.P.; Filho P., 2014).

Tais equipamentos podem ser interconectados pelo uso de padrões e protocolos de comunicação compondo uma rede de comunicação de dados para troca de informações entre os diversos elementos do SAS. Com tal interligação se busca uma operação e monitoramento do SEP que satisfaça demandas, postas por órgãos normativos ou outros, para a qualidade de produto, de serviço, redução de custos e confiabilidade, por exemplo.

A reestruturação do setor elétrico acompanhada com o desenvolvimento da tecnologia tem proporcionado uma melhora nas instalações de supervisão, controle e proteção de uma subestação, devido à integração de novas filosofias, funções, dispositivos numéricos de proteção, sistemas de telecomunicações e computação (Miranda, 2009).

Naquele contexto, a indústria da energia elétrica utilizou e concebeu várias tecnologias que aprimoraram o SAS, como, por exemplo, o desenvolvimento

de *IEDs* (*Intelligent Eletronic Devices*) e a Norma IEC 61850, a qual foi proposta para ser um padrão internacional de comunicação e permitir a interoperabilidade entre os *IEDs* de diferentes fabricantes.

Para (Chemin Netto, 2012), a rede de comunicação representa um elemento de extrema importância ao SEP, portanto, a confiabilidade e o desempenho de um sistema de proteção da subestação dependem da rede de comunicação. No entanto, algumas anomalias, como exemplo, defeito em softwares, uso abusivo de recursos da rede, falha em equipamentos, erros em configurações e ataques, podem comprometer seu funcionamento adequado (Zarpelão, 2010).

Um dos pontos que vem sendo levantados e discutido é o desempenho das funções do SAS diante de um problema de comunicação, ou seja, caso ocorra um rompimento de fibra óptica ou um defeito no próprio *switch ethernet* como um *IED* irá se comportar (Igarashi, 2016)? Diante desta situação, se faz necessário um estudo das métricas que podem ser aplicadas na verificação de desempenho visando à confiabilidade de uma rede principal e de redundância ou em *PRP* durante o tráfego de mensagens *GOOSE*.

Segundo a Norma IEC 61850 (IEC, 2002), uma subestação deve continuar operando, mesmo que haja um componente do SAS em falha, ou seja, uma falha em qualquer componente não pode resultar em uma perda de funções não detectadas via sistema supervisório e nem ocasionar perdas múltiplas de componentes, consequentemente impactando no fornecimento de energia elétrica.

2 Revisão da Literatura

2.1 Norma IEC 61850

Diante da necessidade de uma rede de comunicação agregada, robusta e independente de protocolos ou estruturas subjacentes, em 1994, grupos especialistas como, por exemplo, *WG10 (Power system IED communication and associated data models), WG11 (Communication standards for substations: Communications within and between unit and station levels) e WG12 (Communication standards for substations: Communication within and between process and unit levels)* do comitê técnico *TC57* (*Power systems management and associated information Exchange) do IEC (International Electrotechnical Commission*), iniciaram o desenvolvimento do padrão internacional IEC 61850, redes de comunicação e sistemas em subestações (Miranda, 2009).

Segundo (Khavnekar, Wagh and More, 2015), com a primeira edição publicada da Norma IEC 61850 foi padronizado um sistema global para o SAS, apesar disso não havia uma especificação na redundância de rede. Essa questão foi corrigida na segunda edição da Norma IEC 61850, publicada a partir de 2009.

A segunda edição, na parte 8-1: *Specific communication service mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3*, propõe aumentar o nível de consistência da comunicação especificando a redundância de rede, para diminuir o tempo de recuperação pós falta para valores próximos de zero, a partir do uso do *PRP* e do *HSR* (*High-availability Seamless Redundancy*). Visto que, na primeira edição da norma, o tempo de recuperação da rede está entre 10 – 100ms em topologias lógicas como o turbo *ring*, *RSTP* e o *MRP* (*Media Redundancy Protocol*) (IEC, 2011; Khavnekar, Wagh and More, 2015).

Na Tabela 1, é apresentada uma análise comparativa entre a primeira e a segunda edição da Norma IEC 61850. Segundo (Khavnekar, Wagh and More, 2015), a segunda edição da norma fornece uma redundância contínua de rede, a qual minora a indisponibilidade da rede de comunicação de dados e seus impactos sobre o sistema de proteção. Outro tema observado pelo autor é a utilização de topologias lógicas na segunda edição da norma, por exemplo, o *PRP* e o *HSR* que podem proporcionar um tempo de recuperação da rede igual a zero milissegundo. Além disso, esta edição a norma não está aplicada apenas á subestação, mas também à usinas hidrelétricas e a recursos de energia distribuída.

Tabela 1. Análise comparativa da Norma IEC 61850 edição I e II. Fonte: (Khavnekar, Wagh and More, 2015).

Parâmetro	**IEC 61850 – Edição I**	**IEC 61850 – Edição II**
Modelos de Dispositivos	Subestação	Subestação, usinas hidrelétricas e recursos de energia distribuída
Redundância	Não	Sim (usando *PRP* e *HSR*)
Tempo de Recuperação	10-100ms (protocolo de redundância e anel)	0ms (*PRP* e *HSR*)
Probabilidade de falha	Ocasional	Raramente
Comunicação com outra estação	Não	Sim
Tempo de Sincronização	*SNTP*	Protocolo de tempo de precisão (*PTP*-IEEE 1588/2008)
Mecanismo de segurança	Não definido	Definido
Perda de frame	Sim	Não
Custo de Instalação	Baixo	Alta
Confiabilidade de comunicação	Moderada	Alta

2.2 Redundância de comunicação

A redundância é um dos principais pontos em um sistema de automação de uma subestação, onde não são apenas contemplados os dispositivos de proteção, mas também os sistemas de comunicação (Antonova, Frisk and Tournier, 2011).

A topologia de rede deve estar adequada para garantir a transferência dos dados em qualquer situação, sendo assim, gera a necessidade de uma rede com redundância (Araujo, 2014). De fato, para adquirir uma confiabilidade e disponibilidade segura do sistema, precisa-se evitar qualquer interrupção na transmissão de dados, mesmo ocorrendo uma falha em algum dispositivo da rede de comunicação (Antonova, Frisk and Tournier, 2011).

Embora a conexão de uma rede *Ethernet LAN* para um sistema de automação de subestações tenha facilidade em aspectos quanto à manutenção e expansão, sua arquitetura deve atender aos requisitos, utilizados como indicadores de qualidade (Bellora Junior, 2005; TAN, Jian-Cheng; LUAN, 2011).

A Latência é uma função da natureza dos protocolos envolvidos na rede de comunicação, pois indica o atraso apresentados pela rede e também pelos seus equipamentos, desde o início da comunicação até o recebimento da resposta. Neste caso são considerados os tempos de propagação, transmissão e fila. Enquanto, a probabilidade de perda consiste no levantamento quantitativo de pacotes perdidos em uma transmissão ou fluxo de dados (TAN, Jian-Cheng; LUAN, 2011).

Além disso, outros aspectos, como, por exemplo, a taxa média onde os pacotes podem ser servidos pela rede, tempo máximo e mínimo de envio e chegada dos pacotes de mensagens *GOOSE* também devem ser analisados.

De fato, toda análise de verificação de desempenho de rede conforme métricas são de extrema importância, pois a topologia projetada deve garantir a transmissão de dados, principalmente os pontos relacionados à proteção, respeitando os tempos de atuação definidos pela Norma IEC 61850 em qualquer circunstância (Araujo, Marcelo L.P.; Filho P., 2014).

3 Desenvolvimento do aparato experimental

3.1 Metodologia aplicada

Esta pesquisa foi realizada em um modelo físico reduzido de uma rede de comunicação de dados, de uma subestação de energia elétrica, exemplificada para fins de proteção de sistemas elétricos caracterizada em laboratório. Essa rede de comunicação foi composta por dois *switches ethernet*, relógio *GPS (Global Positioning System)* para sincronização de tempo via *NTP* (*Network Time Protocol*), *IEDs* de mesmo fabricante, uma estação para geração de pacotes *ethernet* na rede, uma estação de trabalho para configuração da rede de comunicação de dados e resgate de informações de interesse.

O tráfego de mensagens via Norma IEC 61850 foi implementado através de um *looping* de mensagens *GOOSE* (*round trip test*) entre dois *IEDs*. Todo o monitoramento do tempo de transmissão de mensagens foi realizado através da média de cada ciclo do *round trip test* nas topologias de rede simples, em *PRP* e modo *Failover*, sem considerar a existência de um fluxo de dados concorrente. Com o intuito de verificar o desempenho das redes em modo *Failover* e *PRP* e a influência que elas podem sofrer sob a ocupação de banda da rede de comunicação de dados, foram gerados pacotes *ethernet* através de um gerador de tráfego de rede, Ostinato 0.8, e monitorado o tempo de transmissão das Mensagens *GOOSE* nessa condição operativa.

A largura de banda pode ser configurada no momento de gerar os pacotes *ethernet*, ou seja, quanto maior o pacote a ser gerado, mais carregado ficava a rede de comunicação, dessa forma, foi utilizada a largura máxima do pacote *ethernet*. Para o índice de vazão, durante todo o ensaio, a taxa de vazão de pacotes gerados pelo Ostinato 0.8 também foi máxima, onde foi atingida quase a capacidade total da porta dos *switches ethernet*.

Para o desenvolvimento do ensaio foi definido que 1000 (mil) pacotes seriam enviados para carregamento da rede a cada segundo, em um *looping* gradativo, ocupando 99% da banda de comunicação da rede. Este procedimento foi realizado aproximadamente 1000 (mil) vezes e o resultado deste ensaio foi extraído do relatório sequencial de eventos dos *IEDs*.

Após a realização dos testes mencionados, os dados de desempenho do *round trip test* foram coletados e utilizados para traçar a um gráfico de desempenho das mensagens *GOOSE* no tempo para cada topologia e condição de ensaio mencionada. Como o número de 1000 (mil) mensagens é muito extenso e dificultaria a visualização, foram coletadas apenas 30 (trinta) mensagens, visto que, o comportamento do gráfico permaneceu uniforme desde o primeiro ciclo.

3.2 Teste de looping de mensagens GOOSE sem redundância de comunicação

Para primeira etapa de realização dos ensaios, foi considerada uma rede de comunicação sem redundância, havendo tráfego de mensagens *GOOSE* em um único caminho da rede, conforme Figura 1. Para esta topologia, uma rede caracterizada sem redundância, a média de tempo entre o envio e o recebimento da mensagem *GOOSE* do relé 1 para o relé 2, foi de 4,75 ms, estando dentro dos padrões permitidos pela Norma IEC 61850.

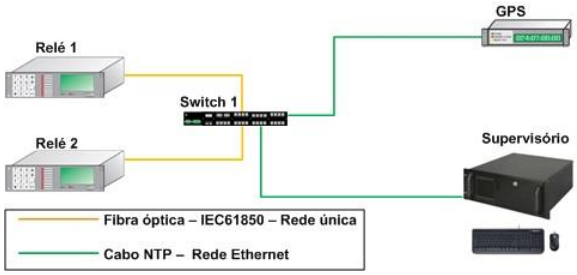

Figura 1. Arquitetura de rede simples – sem redundância

O menor tempo de um ciclo completo entre o envio e recebimento de Mensagens *GOOSE* foi 4,25 ms, enquanto o maior tempo deste ciclo foi de 5,25 ms. Entretanto, quando este único caminho da rede está em falha, o tráfego das mensagens *GOOSE* é interrompido, como pode ser observado, a partir do vigésimo oitavo ciclo do *round trip test*, apresentado no Gráfico 1. Ou seja, funções como de proteção e intertravamentos nos sistemas de automação que dependem do tráfego das mensagens *GOOSE* são afetados, podendo comprometer e até perder a confiabilidade de um sistema de proteção e controle da subestação.

Contudo, além de uma falha de um caminho da rede, outro aspecto que pode comprometer um sistema sem redundância é a falha do *switch*, responsável pela interconexão entre os *IEDs*.

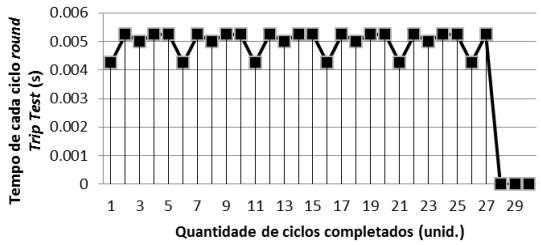

Gráfico 1. Desempenho do *Looping* de mensagens *GOOSE* sem tráfego de rede

Para esta mesma topologia foi repetido o ensaio do *round trip test*, considerando um segundo computador existente na rede de comunicação, com o objetivo de gerar os pacotes *ethernet*, caracterizando tráfego concorrente, durante a troca de mensagens *GOOSE* entre o relé 1 e o relé 2.

Para este caso, a falha de comunicação também afetou o sistema de proteção, apresentando o mesmo comportamento do teste de looping mensagens *GOOSE* sem tráfego de pacotes *ethernet* na rede.

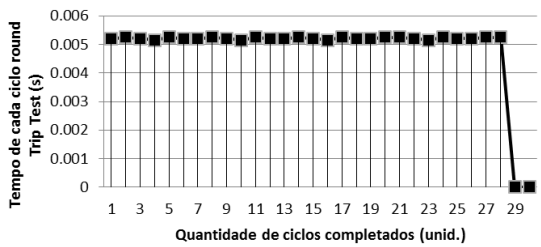

Gráfico 2. Desempenho do *Looping* de mensagens *GOOSE* com tráfego de rede

Após a finalização destes ensaios, foi constatado que independente da existência de tráfego de pacotes concorrentes na rede, a falta de um caminho alternativo nessa poderá comprometer o funcionamento normal e seguro do sistema elétrico de potência, visto que, o sistema de proteção e automação se torna vulnerável após uma falha de *hardware* de um *switch* ou através de uma falha de comunicação dos equipamentos.

Além disso, comparando o Gráfico 1 e o Gráfico 2, foi possível observar que após a injeção de pacotes *ethernet* na rede, cada ciclo de envio e recebimento de mensagens *GOOSE* teve um atraso de 0,45ms. Esse atraso é relativamente pequeno, visto que, temos apenas 2 *IEDs* na rede, contudo, em uma rede com vários *IEDs*, próximo a realidade de uma subestação de energia elétrica, esse atraso tende a aumentar, podendo influenciar de uma forma mais acentuada em uma rede de comunicação.

3.3 Teste de looping de mensagens GOOSE em rede principal e redundante

Para a realização da segunda etapa dos ensaios, foi considerada uma rede em topologia principal e redundante, para a qual os *switches ethernet* estão interligados e as portas dos relés estão operando em modo *hot stand-by*, ou seja, uma porta do relé está ativa em operação e a outra estará em *stand-by*, havendo tráfego de mensagens *GOOSE* em um único caminho da rede, conforme a Figura 2.

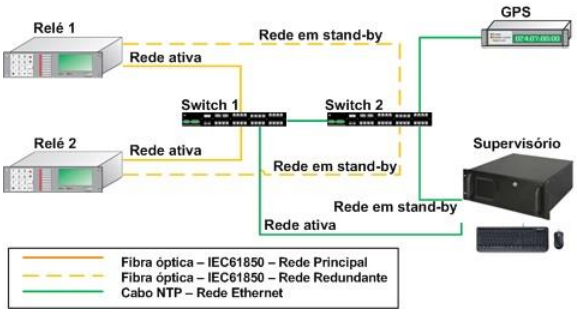

Figura 2. Arquitetura de rede em *hot stand-by*

Entretanto, quando há uma falha na rede principal, a rede que está em *stand-by* tornava-se ativa, não impactando em perdas de mensagens *GOOSE* no sistema de rede de comunicação da subestação.

Essa topologia de rede de comunicação apresentada é comumente aplicada em vários projetos de clientes transmissores e distribuidores de energia, por este motivo, o desenvolvimento do aparato experimental torna-se motivacional para ser objeto de pesquisa.

Com base no Gráfico 3, uma rede caracterizada como principal e redundante, teve o menor tempo de um ciclo completo entre o envio e recebimento de Mensagens *GOOSE* de 4,15 ms, enquanto o maior tempo deste ciclo foi de 4,2 ms. Em relação ao tempo médio entre o envio e o recebimento da mensagem *GOOSE* do relé 1 para o relé 2, foi de 4,17 ms.

Durante os testes de chaveamento de rede de comunicação, ou seja, quando a rede principal estava em falha e a rede redundante tornou-se ativa, o tempo do ciclo de envio e o recebimento da mensagem *GOOSE* foi de 4,65 ms, pode ser observado no sétimo ciclo do *round trip test*, apresentado no Gráfico 3. De fato, houve um aumento de aproximadamente de 0,5 ms no ciclo do *round trip test* durante transição da rede principal para a rede redundante.

Apesar dessa diferença de tempo, comparado aos testes quando não há o chaveamento de redes, o valor coletado do ciclo (4,65 ms) está dentro dos padrões permitidos pela Norma IEC 61850 em sua parte 5 para a classe P1.

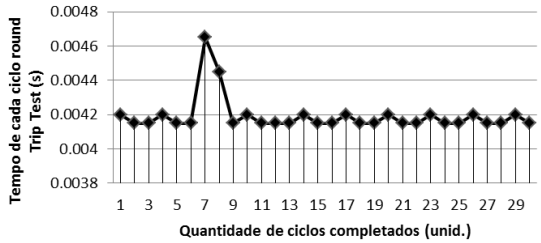

Gráfico 3. Desempenho do *Looping* de mensagens *GOOSE* sem tráfego de rede

Para essa mesma topologia foi repetido o ensaio do *round trip test*, contudo um segundo computador foi inserido na rede para gerar os pacotes *ethernet* durante a troca de mensagens *GOOSE* entre o relé 1 e o relé 2.

Com base no Gráfico 4, uma rede caracterizada como principal e redundante, teve o menor tempo de um ciclo completo entre o envio e recebimento de Mensagens *GOOSE* de 5,15 ms, enquanto o maior tempo deste ciclo foi de 5,25 ms. Em relação ao tempo médio entre o envio e o recebimento da mensagem *GOOSE* do relé 1 para o relé 2, foi de 5,2 ms.

Durante os testes de chaveamento de rede de comunicação, ou seja, quando a rede principal estava em falha e a rede redundante tornou-se ativa, o tempo do ciclo de envio e o recebimento da mensagem *GOOSE* foi de 5,5 ms, pode ser observado no décimo quarto ciclo do *round trip test*, apresentado no Gráfico 4. Houve um aumento de aproximadamente de 0,3 ms no ciclo do *round trip test* durante transição da rede principal para a rede redundante.

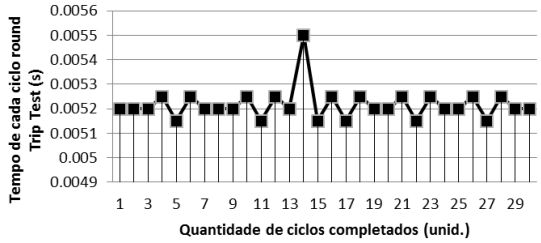

Gráfico 4. Desempenho do *Looping* de mensagens *GOOSE* com tráfego de rede

Após a realização destes ensaios, foi constatado que para as duas situações (testes com tráfego de rede e testes sem tráfego de rede), houve um pequeno atraso durante a comutação da rede principal para a rede em *stand-by*.

O incremento de tempo verificado no momento da comutação entre a rede principal e a redundante deve ser destacado, pois, pode causar um problema de coordenação do sistema de proteção, como, por exemplo, partir indevidamente a função de falha do disjuntor, pois a atuação de uma proteção pode ocorrer em aproximadamente 3ms. De fato, o somatório de atrasos impostos pela rede e pelos equipamentos utilizados na comunicação, está abaixo dos 10 ms e também não ocorreu perda pacotes de dados na rede para os dois ensaios.

Contudo, vale ressaltar que, esse tempo de transferência está muito acima da topologia em *PRP* proposta na segunda edição da Norma IEC 61850, no qual as duas redes operam instantaneamente. Por fim, com a inclusão de outros *IEDs* na rede de topologia principal e redundante, pode se observar que, a latência de envio e recebimento de mensagens *GOOSE* seria influenciada e se tornaria maior gradativamente.

3.4 Teste de looping de mensagens GOOSE em rede PRP

Para realização deste ensaio, foi considerada uma rede em topologia *PRP*, onde os *switches ethernet* não estão interligados, portanto, são duas redes distintas (Rede A e Rede B) e as duas portas dos relés estão ativas, havendo tráfego de mensagens *GOOSE* em ambos os caminhos da rede conforme Figura 3. Para esta topologia o tempo de recuperação pós falta é igual a 0 ms.

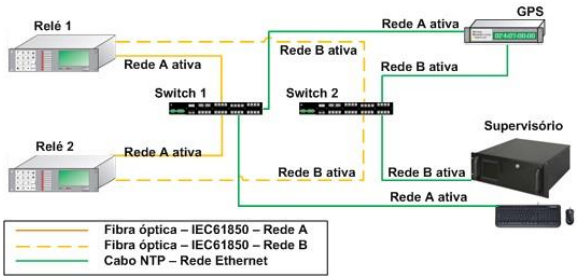

Figura 3. Arquitetura de rede em *PRP*

Com base no Gráfico 5, uma rede caracterizada como *PRP*, teve o menor tempo de um ciclo completo entre o envio e recebimento de Mensagens *GOOSE* de 4,1 ms, enquanto o maior tempo deste ciclo foi de 4,2 ms. Em relação ao tempo médio entre o envio e o recebimento da mensagem *GOOSE* do relé 1 para o relé 2, foi de 4,15 ms. Diante disso, foi constatado que o tempo mínimo e máximo foi praticamente igual.

Durante o ensaio, quando a rede A estava em falha, a rede B estava operando normalmente, o tempo de envio e recebimento foi de 4,16 ms, ou seja, o valor coletado não teve nenhuma variação, diferen-

temente o que havia acontecido com as demais topologias de rede.

Dessa forma, todos os valores coletados estão dentro dos padrões permitidos pela Norma IEC 61850. Ou seja, funções como de proteção e intertravamentos nos sistemas de automação que dependem do tráfego das mensagens *GOOSE* não são afetados, pois não há tempo de recuperação ou chaveamento de rede, diferentemente ao que foi apresentado para a rede de *hot stand-by*.

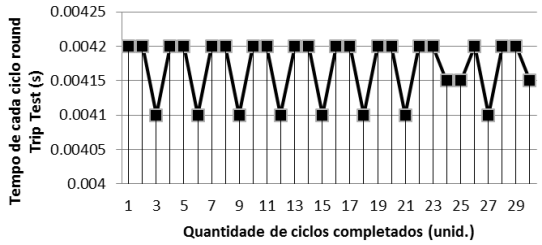

Gráfico 5. Desempenho do *Looping* de mensagens *GOOSE* sem tráfego de rede

Para a mesma topologia, os testes foram repetidos com tráfego de pacotes *ethernet* na rede.

Com base no Gráfico 6, uma rede caracterizada em *PRP*, teve o menor tempo de um ciclo completo entre o envio e recebimento de Mensagens *GOOSE* de 5,2 ms, enquanto o maior tempo deste ciclo foi de 5,25 ms. Em relação ao tempo médio entre o envio e o recebimento da mensagem *GOOSE* do relé 1 para o relé 2, foi de 5,23 ms.

Durante o ensaio, quando a rede A ficou em falha, a rede B estava operando normalmente, não houve nenhuma variação, diferentemente o que havia acontecido com as demais topologias de rede.

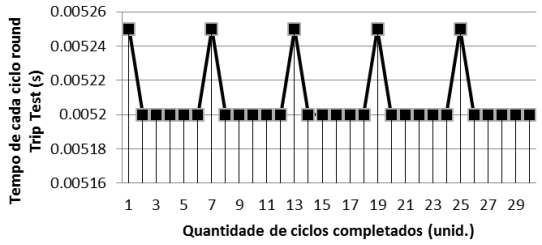

Gráfico 6. Magnetização em função do campo aplicado

Após a realização destes ensaios, foi constatado que para as duas situações (testes com tráfego de rede e testes sem tráfego de rede), não há tempo de recuperação quando um caminho de rede inicie uma falha, sendo assim, estando de acordo com a proposta da segunda edição da Norma IEC 61850.

Esta é uma solução melhor quando se via a maior disponibilidade e confiabilidade dos sistemas de proteção, pois além de não haver perdas de pacotes na rede, o *PRP* não possui duas redes distintas para trafegar informações diferentes, e sim redundantes. O que o *PRP* faz é verificar nas duas portas a mensagem que chegou primeiro e descartar a mensagem que chegar mais atrasada. O tratamento das mensagens é feito pela aplicação em uma mesma fila, posteriormente à seleção do pacote que será usado.

Dessa forma, o *PRP* não terá tempo de latência para comutação de redes e todo o sistema de proteção poderá atuar normalmente sem comprometer o sistema elétrico em caso da falha de um caminho de rede.

3.5 Comentários finais

Ao término desses ensaios no aparato experimental foi possível contribuir de forma significativa com a avaliação do comportamento das mensagens *GOOSE* durante o tráfego na rede principal e redundante e de topologia em *PRP*. Durante o fluxo das 1000 (mil) mensagens *GOOSE* na rede, para o índice de qualidade, probabilidade de perda, não houve a perda pacotes de dados na rede. Apesar de que, o esquema de retransmissão das mensagens garante a confiabilidade da instalação, já que, por mais que um pacote seja perdido em seguida outro é enviado.

Além disso, o tempo de latência foi menor que o tempo limitado pela primeira edição da Norma IEC 61850, sendo possível constatar que na topologia *PRP* não há tempo de latência para comutação de rede.

4 Conclusão

Em relação aos resultados, destaca-se:

• A rede de comunicação em *hot stand-by failover* apresentou um tempo médio no envio e recebimento das mensagens *GOOSE* igual a 4,17 ms sem tráfego concorrente e de 5,2 ms considerando tráfego concorrente. Quando a falha na rede foi criada houve um incremento de 0,5 ms no tempo das mensagens *GOOSE* subsequentes. Ressalta-se que quanto maior o ajuste de tempo para comutação *hot stand-by failover* ou maior a quantidade de *IEDs* na rede, maior será o número das mensagens *GOOSE* com tempo aumentado.

• A rede *PRP* apresentou um tempo médio no envio e recebimento das mensagens *GOOSE* igual a 4,15 ms sem tráfego concorrente e de 5,23 ms considerando tráfego concorrente. Neste mecanismo não há incremento de tempo no envio e recebimento das mensagens *GOOSE* tão pouco a perda de pacotes quando a falha na rede ocorre.

Conclui-se, portanto, que para fins da proteção do sistema elétrico de potência não apenas o caráter de redundância e disponibilidade da rede é importante, mas, além disso, é fundamental caracterizar no tempo a influência desses mecanismos sobre o funcionamento temporal (tempo de *trip* e coordenação) das funções de proteção aplicadas a um dado empreendimento.

Agradecimentos

Os autores agradecem a Toshiba América do Sul Ltda. pela infraestrutura que proporcionou o desenvolvimento deste trabalho.

Referências Bibliográficas

Antonova, G., Frisk, L. and Tournier, J. C. 2011, 'Communication redundancy for substation automation', *2011 64th Annual Conference for Protective Relay Engineers*, pp. 344–355.

Araujo, Marcelo L.P.; Filho P., C. 2014, 'Projeto de Redes de Comunicação Redundantes Aplicadas em Sistemas de Automação Baseados na IEC 61850', *XX Congresso Brasileiro de Automática*, pp. 1–8.

Araujo, M. L. P. 2014, 'Proposta de Proteção de Sobrecorrente no Âmbito Industrial através de Comunicação de IEDs baseados na Norma IEC 61850', Dissertação de Mestrado, UFMG, Belo Horizonte-MG.

Bellora Junior, J. C. 2005, 'Medição de Tráfego Baseada na Decomposição Temporal de Fluxos', Dissertação de Mestrado, UFRJ, Rio de Janeiro-RJ.

Chemin Netto, U. 2012, 'Determinação de um Parâmetro para Monitoramento do Desempenho de Mensagens GOOSE do Padrão IEC 61850 Utilizadas em Subestações de Energia Elétrica', Tese de Doutorado, USP, São Carlos-SP.

IEC 2002, *IEC-61850, Part 3: General requirements*. Geneva, Switzerland.

IEC 2011, *IEC-61850, 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.* Geneva, Switzerland.

Igarashi, G. 2016, 'Contribuições para a implementação de um barramento de processo segundo a Norma IEC 61850-9', Tese de Doutorado, USP, São Paulo-SP.

Khavnekar, A., Wagh, S. and More, A. 2015, 'Comparative Analysis of IEC 61850 Edition-I and II Standars for Substation Automation', *IEEE International Conference on Computational Intelligence and Computing research*, pp. 1–6.

Miranda, J. C. 2009, 'IEC-61850 : Interoperabilidade e Intercambialidade entre Equipamentos de Supervisão , Controle e Proteção Através das Redes de Comunicação de Dados', Dissertação de Mestrado, USP, São Carlos-SP.

TAN, Jian-Cheng; LUAN, W. 2011, 'IEC 61850 Based Substation Automation System Architecture Design', *IEEE Power and Energy Society General Meeting*, pp. 1–6.

Zarpelão, B. B. 2010, 'Detecção de Anomalias em Redes de Computadores', Tese de Doutorado, UNICAMP, Campinas-SP.