

## **Metodologia para a aplicação da norma IEC 61850-9-2: aplicando SDN como reconfiguração de rede**

### **Methodology for the application of IEC 61850-9-2: applying SDN as network reconfiguration**

DOI:10.34117/bjdv8n8-212

Recebimento dos originais: 21/06/2022  
Aceitação para publicação: 29/07/2022

**Romulo Fabricio Corna**

Mestrado

Instituição: Lactec

Endereço: Rua Rio de Janeiro, 2000, Vila Guaíra, Curitiba, Paraná, CEP: 80630-180  
E-mail: romucorn@selinc.com

**Voldi Costa Zambenedetti**

Doutor

Instituição: Pontifícia Universidade Católica do Paraná (PUC-PR)

Endereço: R. Imac Conceição, 1155, Prado Velho, Curitiba - PR,  
CEP: 80215-901, Brasil

E-mail: voldi.zambenedetti@pucpr.br

**Edgard Jamhour**

Doutor

Instituição: Pontifícia Universidade Católica do Paraná (PUC-PR)

Endereço: R. Imac Conceição, 1155, Prado Velho, Curitiba - PR,  
CEP: 80215-901, Brasil

E-mail: edgard.jamhour@pucpr.br

## **RESUMO**

Tradicionalmente os relés de proteção recebem via cabos elétricos os sinais de tensão e corrente dos transformadores no Sistema Elétrico de Potência (SEP). A seção da norma IEC 61850-9-2 propõe uma alternativa para esse esquema, que seria utilizar um dispositivo eletrônico para digitalizar essas informações ainda no pátio da subestação, e enviá-las através de uma Local Area Network (LAN) por protocolo de comunicação Sampled Values (SV). Nesse contexto, todas as amostras e todas as informações recebidas pelos relés de proteção são obtidas através desta rede. A principal preocupação, nesse contexto, é justamente garantir que em qualquer perturbação do sistema elétrico, não haja indisponibilidade da comunicação, pois tal pode provocar o bloqueio das funções de proteção. O bloqueio das funções, por uma falha de comunicação, pode deixar o SEP desprotegido e consequentemente causar danos significativos ao sistema de energia elétrica. No relatório técnico IEC TR-61850-90-4, é possível encontrar soluções e ferramentas para garantir a disponibilidade dessa rede. Porém existe uma de sinais elétricos analógicos provenientes dos secundários de transformadores de corrente (TC) e de transformador de potencial (TP), conforme a Figura 1. alternativa, que é capaz de proporcionar a robustez da rede, essa alternativa é o Software Defined Network (SDN). Por essa razão, esse trabalho propôs o uso do SDN como alternativa as opções apresentadas pela IEC TR-61850-90-4, no gerenciamento e reconfiguração da rede.

Ethernet para garantir os requisitos e exigências da norma IEC 61850-9-2 de aplicação do protocolo SV, observando sua eficácia frente a falhas. Para a validação desta proposta, é proposto oito diferentes arquiteturas de comunicação, composto por quatro switches, um relé de proteção, um Stand- Alone Merging Units (SAMU) e um relógio preciso, compõem uma LAN, permitindo a comunicação de um barramento de processo. Nessa LAN são aplicadas falhas lógicas e físicas, e verificado se o SDN é capaz de restaurar a rede, sem que haja o bloqueio da função de proteção.

**Palavras-chave:** IEC 61850-9-2, sampled values, SDN, IEC TR- 61850-90-4.

## ABSTRACT

Traditionally, the protection relays receive via electric cables the voltage and current signals from the transformers in the Electric Power System (PES). The section of the IEC 61850-9-2 standard proposes an alternative to this scheme, which would be to use an electronic device to digitize this information while still in the substation building, and send it over a Local Area Network (LAN) by Sampled Values (SV) communication protocol. In this context, all samples and all information received by the protection relays are obtained through this network. The main concern, in this context, is precisely to ensure that in any disturbance of the electronic system, there is no unavailability of communication, because such a failure can cause the blocking of the protection functions. The blocking of functions, due to a communication failure, can leave the SEP unprotected and consequently cause significant damage to the electric power system. In the IEC TR-61850-90-4 technical report, it is possible to find solutions and tools to ensure the availability of this network. There is also a However, there is an alternative of analog electrical signals coming from the secondaries of current transformers (CT) and potential transformer (PT), as shown in Figure 1. There is an alternative, which is capable of providing the robustness of the network, This alternative is the Software Defined Network (SDN). For this reason, this work proposes the use of SDN as an alternative to the options presented by IEC TR-61850-90-4, in the management and reconfiguration of the Ethernet network to ensure the requirements of the IEC 61850-9-2 standard for the application of the SV protocol, observing its effectiveness against failures. For the validation of this proposal, eight different communication architectures are proposed, composed of four switches, a protection relay, a Stand Alone Merging Units (SAMU), and a precise relay, composing a LAN, allowing the communication of a process bus. On this LAN, physical and logical faults are applied, and it is verified if SDN is able to restore the network, without blocking the protection function.

**Keywords:** IEC 61850-9-2, sampled values, SDN, IEC TR- 61850-90-4.

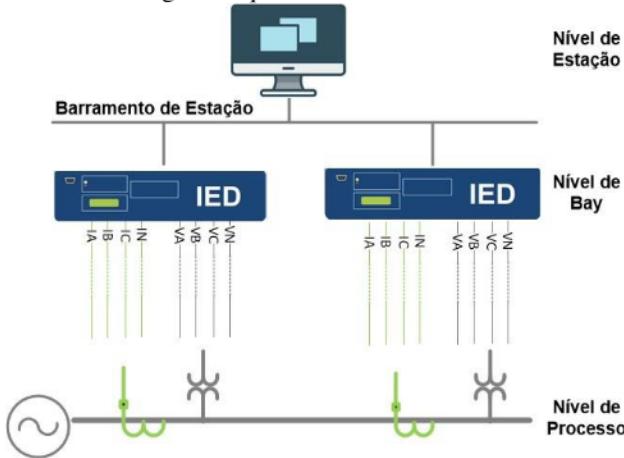
## 1 INTRODUÇÃO

### 1.1 CONTEXTO

Os relé de proteção que também podem ser chamados de *Intelligent Electronic Devices* (IED), pois possuem diversas funcionalidades dentre elas monitoramento, medição controle e funções de proteção o Sistema Elétrico de Potência (SEP). Esses equipamentos se comunicam através de diversos protocolos de comunicação para

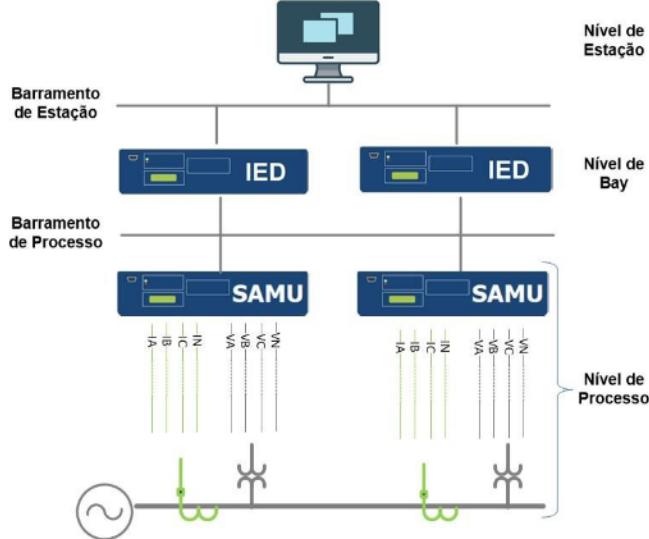
informar sobre a decisão de seus algoritmos [1]. Contudo, a forma tradicional pela qual o IED recebe informações do SEP, é através da aquisição de sinais elétrico analógicos provenientes dos secundários de transformadores de corrente (TC) e de transformador de potencial (TP), conforme a Figura 1.

Fig. 1. Arquitetura Convencional



A seção da norma IEC 61850-9-2 [2] propõe uma arquitetura, Figura 2, no qual a digitalização dos sinais ocorre próximo aos TP e ao TC, por um Stand-Alone Merging Units (SAMU), e enviando os sinais digitalizados via mensagens Sampled Values (SV) através do barramento de processo (BP) (rede Ethernet). Devido as funcionalidades de proteção, o IED reage com um ciclo de processamento para enviar comandos de abertura para disjuntores, isolando equipamentos do SEP e consequentemente minimizando os danos frente a alguma perturbação elétrica. Sendo que o BP necessita assegurar que o relé de proteção receba todas as mensagens SV, a fim de não desabilitar nenhuma proteção. O relatório técnico IEC TR 61850-90-4 [3], sugere soluções tecnológicas que possam garantir a aplicação do SV, mesmo frente a falhas na rede. Uma alternativa tecnológica, que não foi considerado pelo IEC TR 61850-90-4 [3] é o conceito do Software Defined Network (SDN).

Fig. 2. Arquitetura IEC 61850-9-2



## 1.2 OBJETIVOS

O objetivo deste trabalho é validar através de falhas no BP, se o SDN é capaz de garantir reconfiguração de rede e o sincronismo de tempo, para que o IED não desabilite as funções de proteção nem por perda de pacotes e nem por perda do sincronismo. Sendo que os objetivos específicos deste trabalho são:

- Propor um BP, montar em laboratório a rede Ethernet e aplicar falhas físicas e falhas lógicas.
- Monitorar no relé de proteção, através de registros oscilográficos, a perda de pacotes.
- Verificar a atuação do SDN quando ocorre falha no BP.
- Analisar os resultados, verificar possíveis bloqueios de funções de proteção ou perdas de sincronismo e propor a solução.

## 1.3 JUSTIFICATIVA

A justificativa para o trabalho é aplicar o protocolo SV de forma segura, garantindo a estabilidade e o funcionamento do SEP, e utilizando para o barramento de processo, uma solução de gerenciamento de rede que não é citado como opção pelo IEC TR-61850-90-4 [3], no caso o SDN.

## 2 FUNDAMENTAÇÃO TEÓRICA

### 2.1 PROTOCOLOS DE COMUNICAÇÃO IEC 61850

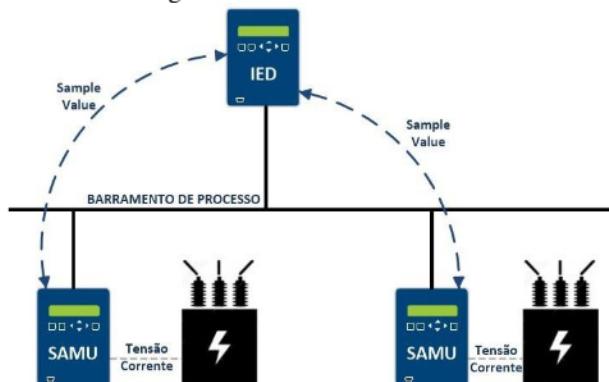
No esforço de propor e unificar os fabricantes ao redor de um mesmo protocolo, a indústria, através da Electric Power Research Institute (EPRI), começou a desenvolver a Utility Communications Architecture (UCA), em 1988. O resultado é um conjunto completo de normas que permite que dispositivos de monitoramento e controle, compatíveis com a UCA, interoperem com aplicativos de serviços públicos (não apenas supervisórios) em um ambiente multifornecedor. Com base na característica especificadas pelo protocolo UCA, que modela equipamentos e facilita sua integração e configuração, desenvolveu-se uma série de normas conhecida como IEC 61850, resultado do trabalho dos grupos do Comitê Técnico International Electrotechnical Commission (IEC) [1]. A série de normas apresenta pelo menos três protocolos de comunicação: Generic Object Oriented Substation Event (GOOSE), Manufacturing Message Specification (MMS) e SV.

Os dois primeiros estão difundidos e são utilizados pelas concessionárias de energia elétrica no Brasil e no Mundo. Contudo, o terceiro protocolo vem sendo aplicado com muitas limitações, por exigir uma complexa e eficiente rede Ethernet [1].

### 2.2 PROTOCOLO SAMPLED VALUE

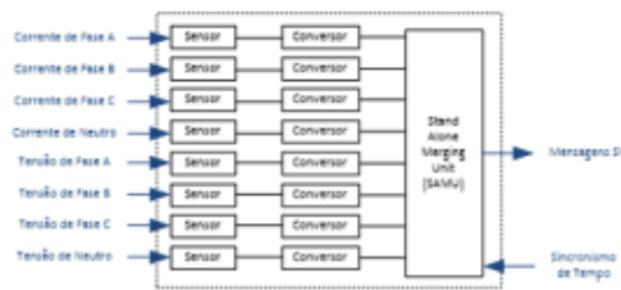
O protocolo SV é definido pela seção da norma IEC-61850- 9-2 [2], e tem como objetivo padronizar o envio de amostras instantâneas de valores analógicos com estampa de tempo, enviados pela rede Ethernet de um SAMU a um IED com funcionalidades de proteção e controle, conforme demonstrado na figura 3.

Fig. 3. Barramento de Processo



O SAMU é um hardware que realiza todo o processamento de dados necessários (amostragem, conversão analógica para digital, dimensionamento, formatação de mensagens, etc.) para produzir um fluxo de dados de saída coerente, de acordo com a IEC 61850-9-2 [2]. A figura 4 ilustra as partes que compõem um SAMU. As entradas do equipamento são valores analógicos de corrente e tensão. A saída são esses sinais amostrados e digitalizados no padrão da norma IEC 61850-9-2 [2]. De acordo com a seção da norma IEC 61850-7-4 [4], os SAMU devem disponibilizar alguns Logical Nodes (LN), tais como: o TCTR, que dispõe valores digitalizados de correntes; o LN TVTR, que dispõe os valores digitalizados das tensões; LLN0, que contém instância; e o MSVCB03, que controla a publicação das mensagens SV a uma taxa de 4800 amostras por segundo, para redes de 60Hz, e de 4000 amostras por segundo, para redes de 50Hz, segundo a norma IEC 61869-13

Fig. 4. SAMU



A transmissão de SV requer atenção especial com o desempenho da rede. Assim, a informação trocada deve ser baseada no mecanismo de publicação e assinatura, que consiste em o que publica escrever os valores em um buffer local no lado de envio, e o que assina ler os valores em um buffer do lado do que recebe. A estampa de tempo deve ser adicionada aos valores, para que o assinante possa conferir a sequência dos valores. O sistema de comunicação fica responsável em suprir o buffer local dos assinantes, enquanto o controle Sampled Values Control (SVC) é usado para controlar o procedimento de comunicação. A entrega de dados pode ser unicast ou multicast.

**Requisitos de sincronismo de tempo para aplicar SV:** Para a perfeita estampa de tempo das mensagens SV, a precisão do sincronismo de tempo deve ser inferior a 1 microsegundo. Por rede Ethernet somente o Precision Time Protocol (PTP) tem essa capacidade. Porém, se ocorrer uma falha física no BP, o sincronismo pode ser interrompido, comprometendo essa precisão. Por essa razão é necessário que a SAMU tenha a capacidade de manter a precisão de tempo por um determinado tempo, mesmo

sem a recepção do sincronismo. Essa capacidade é conhecida como holdover. O tempo máximo que o a SAMU deve ser capaz de manter o sincronismo de tempo é de 5 segundos, [3].

**Requisitos de reconfiguração de rede para SV:** Em um sistema elétrico de potência com 60 Hz, as 80 amostras por ciclo, especificada pela IEC 61850-9-2, se traduz em uma taxa de amostragem de 4,8 kHz. Com essa taxa cada mensagem SV é enviada pela SAMU a cada 208  $\mu$ s.

O fabricante do IED deve especificar e determinar quantos pacotes o IED tem capacidade de perder, sem desabilitar as funções de proteção. O IED interpola as amostras dos sinais de tensão e de corrente que recebe via protocolo, para poder reconstituir novamente a senoidal. O limite de perda de pacotes do IED utilizado nesse estudo de caso é de 3 pacotes, [6]. Por essa razão, a reconfiguração da rede deve ser menor ou igual a 624  $\mu$ s, para que não perca o quarto pacote desencadeando o bloqueio de proteção. O quarto pacote perdido ocorreria a 832  $\mu$ s, nesse momento espera-se que o IED inicie o bloqueio das proteções, deixando o SEP vulnerável nesse período.

### 2.3 PRECISION TIME PROTOCOL

O desempenho de redes Ethernet em tempo real depende de uma eficiente rede de sincronização de tempo. Por essa razão, a norma IEEE 1588 [7] define um padrão de sincronização por rede, conhecido como PTP. Sua utilização está em sincronizar relógios de sistemas de medição e controle, dependendo de uma fonte de tempo como o GPS. Esse padrão permite precisões melhores que 100 nanosegundos.

O protocolo tem características para aplicações no qual a redundância é requisitada. A fonte primária de tempo em um sistema que utilize PTP é um relógio chamado grandmaster, que geralmente inclui um receptor GPS, fornecendo um tempo comum para a rede. Existem também os relógios slave, que recebem o tempo do grandmaster e o convertem para outros protocolos de sincronismo como PPS e IRIG-B. O terceiro elemento no sistema do PTP é o relógio transparente (RT). As aplicações de RT são incluídas nos algoritmos dos switches gerenciáveis, que, por estarem no caminho entre o grandmaster e os slave, podem contribuir para o cálculo do atraso de tempo causado pelo deslocamento da informação. Por essa razão, os switches gerenciáveis que serão utilizados em uma rede Ethernet, a qual se espera ter uma boa precisão por PTP, deve ter essa aplicação prevista no seu algoritmo [7]. O PTP é organizado dentro de uma hierarquia Mestre e Escravo, com o relógio padrão no topo da hierarquia. PTP tem se

mostrado um método viável de fornecer tempo de sincronismo para SV, sendo que propagações de atrasos são compensados. Deste modo, esse protocolo apresenta benefícios sobre IRIG-B e sistemas de 1 PPS em transmissão dentro de subestações [8].

#### 2.4 GERENCIAMENTO DA REDE ETHERNET

Os requisitos que a norma IEC 61850 impõe, somando aos requisitos que os fabricantes também impõem para que uma função de proteção não seja desabilitada devido a uma falha na rede, são extremos. Por essa razão o relatório técnico IEC TR 61850-90-4, [3], sugere como opção a duplicação dos pacotes Ethernets da rede, utilizando os protocolos da norma IEC 62439-3 [9], Parallel Redundancy Protocol (PRP) ou o High-availability Seamless Redundancy (HSR) [10]. Contudo a duplicação da rede resolve a questão de uma falha física, uma vez que a solução prevê duas redes completamente separadas. Porém algumas desvantagens devem ser consideradas pela engenharia de rede, como as listadas a seguir:

-Esforço Computacional: Devido à duplicação de pacotes é inevitável um maior esforço computacional do IED, consumindo processamento e memória que poderiam ser utilizados para outros fins.

-MTBF: A diminuição do Mean Time Between Failures (MTBF), período médio entre falhas, pelo fato de ter mais equipamentos na subestação.

-Investimento: Como cada LAN é composta por muitos switches, a duplicação da rede implica na aquisição do dobro de switches.

-Conexão acidental: Na utilização do protocolo PRP existe uma impossibilidade técnica na conexão das redes, sendo que uma conexão acidental, já no período de operação, é capaz de trazer danos catastróficos para a rede Ethernet e a consequente interrupção dos dados.

-Conexão das redes: Apesar do investimento e da duplicação das redes, é impossível conectá-las, uma possível conexão aumentaria o número de possíveis rotas para os pacotes [11].

Essas desvantagens abrem a oportunidade para que outras possibilidades de aplicação e reconfiguração da rede Ethernet, sejam estudadas e analisadas como a SDN.

A seguir é apresentado e explicado o funcionamento e os componentes do gerenciamento de rede através do SDN:

1) Software Defined Network: SDN é uma abordagem diferente do gerenciamento de rede que é encontrado nas redes tradicionais. Pois no caso das tradicionais, cada switch assume a função de encaminhar os dados e controlar o seu envio.

Com os switches SDN, eles ficam somente responsáveis pelo encaminhamento de dados, enquanto o controlador, que é um software instalado em um computador, estabelece e envia para os switches os circuitos lógicos, pré determinando inclusive os caminhos alternativos. Seu foco é a administração da rede, gerenciando o tráfego de dados e permitindo que a engenharia de rede decida como os pacotes serão encaminhados pela arquitetura, indiferentemente do tipo de rede Ethernet. Isso permite que o usuário do sistema tenha controle de cada frame no tráfego de rede, proporcionando um monitoramento de todas as aplicações. É possível configurar um fluxo para cada aplicação, separando logicamente o tráfego de alta prioridade com o de baixa prioridade, o que faz com que haja uma diminuição das diferenças de latência. Ademais, aumenta a eficiência das portas de alta velocidade, segregando tráfegos críticos como mensagens GOOSE e tráfegos apenas de monitoração, como um supervisório ou de configuração dos equipamentos, o que protege ambos os tráfegos. Na figura 5 observa-se um exemplo dessa segregação [12]

Fig. 5. Circuitos Lógicos

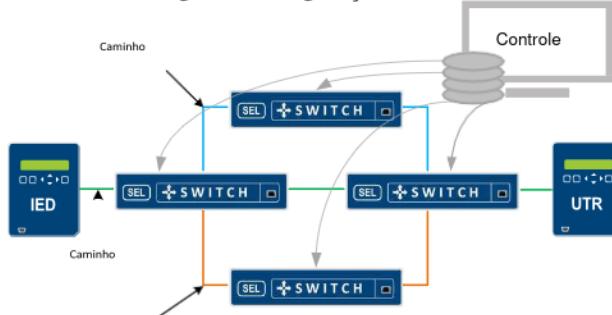


Ao invés de selecionar a topologia da rede como anel, ladder ou estrela, por meio do SDN é possível aperfeiçoar a rede para os equipamentos e aplicações disponíveis, projetando o melhor circuito possível para cada seção de comunicação e contemplando circuitos de redundância. O SDN está integrado com a norma IEEE 1588 (2008) [7], portanto, além de acrescenta o residence time nos pacotes e ajuda criando um caminho simétrico na ida e no retorno dos pacotes. A norma IEEE 1588 (2008) [7], não tem nenhum mecanismo de correção para assimetria da rede, o fato do SDN garantir essa simetria, favorece o PTP e consequentemente a precisão do sincronismo [12].

Protocolo OpenFlow 1.3: A abordagem do SDN permite a separação do plano de controle plano de dados da rede. Apesar de não ser uma proposta realmente nova, ganhou força apóis a criação do protocolo OpenFlow 1.3, com o qual é possível programar o encaminhamento dos pacotes através de um agente externo, além de poder controlar todos os nós da rede a partir de um único ponto [13]. O protocolo OpenFlow é a interface que conecta cada switch com o controlador, Figura 6. Através dessa interface, o controlador configura e gerencia o switch, recebendo eventos do switch e enviando pacotes para o switch. O protocolo OpenFlow permite os três tipos de mensagens a seguir [14]:

- Controller-to-switch: são mensagens de inicialização usadas para controlar e inspecionar o estado do switch.
- Asynchronous: são mensagens para provocar alterações no estado do switch;
- Symmetric: são mensagens que podem ser geradas pelo switch ou pelo controlador, e são enviadas sem solicitação.

Fig 6 Reconfiguração de Rede

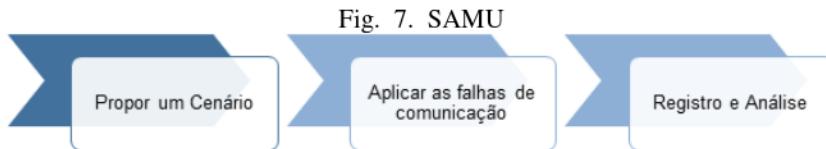


### 3 MATERIAIS E ME'TODOS

O estudo em questão tem como resultado a indicação do tempo de reconfiguração da rede em casos de falha física na rede SDN. Verificando se a rede SDN e' capaz de ser utilizada como opção para o barramento de processo. Nesse caso, com o intuito de tornar o estudo replicável, opta-se pela estruturação em três etapas.

#### 3.1 MÉTODO

O método deste trabalho consiste em montar em laboratório um barramento de processo e aplicar falhas na rede de comunicação. O método propõe aplicar as etapas da Figura 7, dez vezes para cada cenário de falha, com o intuito de verificar a repetibilidade dos tempos de possível escuridão da rede



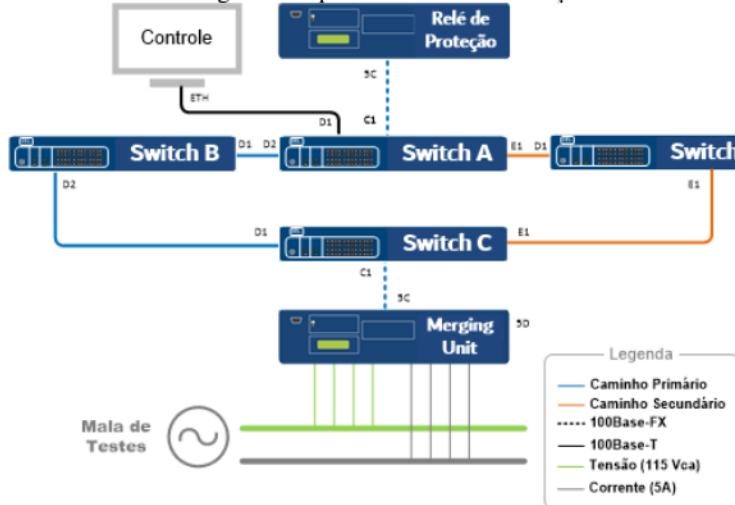
1) Etapa 1 - Propor um Cenário: A primeira etapa consiste na especificação de uma arquitetura para o barramento de processo. Ou seja, definir o caminho principal para as mensagens SV, e definir o caminho alternativo, com o qual a rede SDN irá alternar no momento da falha física na rede Ethernet.

2) Etapa 2 – Aplicar as falhas de comunicação: A segunda etapa consiste em aplicar falhas físicas ou falhas lógicas no barramento de processos, que provoquem interrupção da comunicação. No caso da falha física, ela deve ser proporcionada pela desconexão da fibra óptica ou do cabo UTP. No caso da falha lógica, ela é aplicada desabilitando uma porta do switch SDN, diretamente no controlador.

3) Etapa 3 – Registro e Análise: A terceira etapa consiste em efetuar o registro oscilográfico no relé de proteção. O registro grava valores analógicos e digitais amostrados durante 3 segundos. A taxa de amostragem do relé de proteção é de 8.000 hertz, isso quer dizer que é realizado um registro a cada 125 µs. Como as amostras das mensagens SV são enviados a uma amostragem de 4800 hertz, o IED consegue registrar todas as amostras.

4) Estabelecendo fluxos através de um controlador SDN: As seções anteriores explicaram o funcionamento e os objetivos de uma rede SDN, a intenção dessa seção é propor uma arquitetura e demonstrar como ela é configurada através de um controlador. Na Figura 8, temos uma arquitetura com quatro switches SDN, a linha azul representa o caminho principal enquanto a linha laranja representa o caminho alternativo.

Fig. 8. Arquitetura de Comunicação



Nas tabelas a seguir, está detalhado todos os fluxos e grupos que são utilizados para configurar um caminho entre A SAMU e o IED. Na configuração dos switches é necessário especificar pelo menos o MAC de origem e destino e o Ethertype da mensagem que será trafegada. É possível especificar mais informações das mensagens, mas nesse trabalho não foram utilizados filtros adicionais no estabelecimento dos fluxos. No fluxo define também a porta de ingresso e a porta de egresso. Como há duas opções de saída, a configuração para o switch SDN saber que deve comutar é utilizando um Grupo de Failover. Há duas formas do grupo de failover criado no switch detectar e comutar entre as portas. A primeira opção é a detecção por queda no link de comunicação. A segunda forma o switch passar a receber de novo as mensagens que ele estava enviando por um link de comunicação com outro switch. Essa recepção dos pacotes no sentido inverso, significa que o switch que está a frente, apresentou uma queda de link e está devolvendo os pacotes, pelo mesmo link. O switch que está recebendo de novo os pacotes, deve tomar uma ação, e a ação é comutar para o caminho alternativo.

No Switch C, é definido um fluxo com as informações de MAC de destino e de origem e do Ethertype, além das porta de ingresso e egresso. A porta de egresso é atribuída a um grupo de failover, para comutar entre elas em caso de falha de comunicação, as informações estão na tabela I. O grupo 1 é a saída do fluxo 1. O grupo 1 também tem alguns parâmetros, como o ingresso e o egresso, para determinar as opções de porta que o grupo pode selecionar para comutar.

TABLE I SWITCH C

<b>Fluxo 1</b>		<b>Grupo 1</b>	
<b>MAC Destino</b>	010CCD040001	<b>Ingresso</b>	Fluxo 1
<b>MAC Origem</b>	0030A71DAA8A	<b>Egresso</b>	D1 ou E1
<b>EtherType</b>	SV	Ação	Comut. Ráp.
<b>Ingresso</b>	C1	-	-
<b>Egresso</b>	Grupo 1	-	-
<b>Descrição</b>	Caminho Princ.	-	-

No Switch B, é definido um fluxo com porta D1 de ingresso e porta de egresso para um grupo de failover. Como o switch B só tem um caminho através da porta D1, o grupo failover, no caso de uma falha na porta D1, devolve a informação pelo mesmo caminho de ingresso, a porta D2, as informações estão na tabela II.

TABLE II SWITCH B

<b>Fluxo 1</b>		<b>Grupo 1</b>	
<b>MAC Destino</b>	010CCD040001	<b>Ingresso</b>	D2
<b>MAC Origem</b>	0030A71DAA8A	<b>Egresso</b>	D1 ou D2
<b>EtherType</b>	SV	Ação	Comut. Ráp.
<b>Ingresso</b>	D2	-	-
<b>Egresso</b>	Grupo 1	-	-
<b>Descrição</b>	Caminho Princ.	-	-

No Switch D, é definido um fluxo com porta E1 de ingresso e porta de egresso para um grupo de failover. Como o switch D só tem um caminho através da porta D1, o grupo failover, no caso de uma falha na porta D1, devolve a informação pelo mesmo caminho de ingresso, a porta E1, as informações estão na tabela III.

TABLE III SWITCH D

<b>Fluxo 1</b>		<b>Grupo 1</b>	
<b>MAC Destino</b>	010CCD040001	<b>Ingresso</b>	D2 ou E1
<b>MAC Origem</b>	0030A71DAA8A	<b>Ação</b>	Comut. Ráp.
<b>EtherType</b>	SV	-	-
<b>Ingresso</b>	E1	-	-
<b>Egresso</b>	Grupo 1	-	-
<b>Descrição</b>	Caminho Altern.	-	-

No Switch A como tem duas portas de ingresso, utiliza-se um grupo de failover para escolher as opções de ingresso, e a porta de egresso será sempre a porta C1, as informações estão na tabela IV.

TABLE IV SWITCH A

Fluxo 1		Grupo 1	
<b>MAC Destino</b>	010CCD040001	<b>Ingresso</b>	D2 ou E1
<b>MAC Origem</b>	0030A71DAA8 A	<b>Egresso</b>	C1
<b>EtherType</b>	SV	<b>Ação</b>	Comut. Ráp.
<b>Ingresso</b>	Grupo 1	-	-
<b>Egresso</b>	Grupo 1	-	-
<b>Descrição</b>	Caminho Princ.	-	-

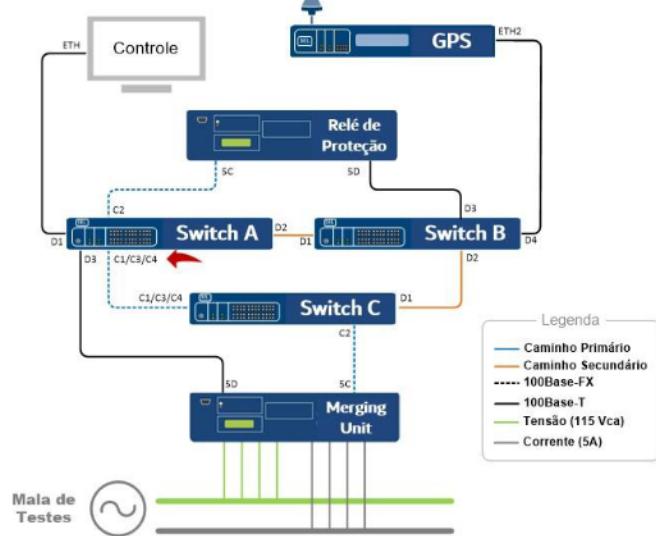
## 4 ESTUDO DE CASO

Para o estudo de caso, é proposto oito arquiteturas de comunicação, montadas e os testes realizados em laboratório. Sendo o resultado apresentado para cada cenário. Do cenário 1 ao cenário 4 serão aplicados falhas físicas, com a perda do link da porta Ethernet. Do cenário 5 ao 6 serão realizados falhas lógicas, desabilitando as portas dos switches por software, não provocando dessa forma a perda de link. Nos cenários 1, 2, 3 e 7 o caminho principal será de 100Base-FX, enquanto que nos demais cenários, o caminho principal será 100Base-T. O objetivo é aplicar uma falha no caminho principal, e verificar se haverá perda de pacotes para o IED e o bloqueio da função de proteção.

### 4.1 ARQUITETURA DE COMUNICAÇÃO DO CENÁRIO 1

Na Figura 9 temos a arquitetura, composta por uma rede em anel de três switches SDN. A aplicação da falha física proposta foi executada desconectando a porta C1 do switch A, repetindo esse teste cinco vezes, e outras cinco vezes desconectando a porta C1 do switch C. Ao todo foram realizados dez testes de desconexão do caminho principal. O mesmo teste foi realizado, estabelecendo o caminho principal pela porta C3 dos switches A e B, e uma vez mais estabelecendo como caminho principal a porta C4, dos switches A e B. Essa repetição do processo, com portas diferentes tem o objetivo de assegurar que outras portas do mesmo switch não apresentariam comportamento diferente.

Fig. 9. Arquitetura do Cenário 1

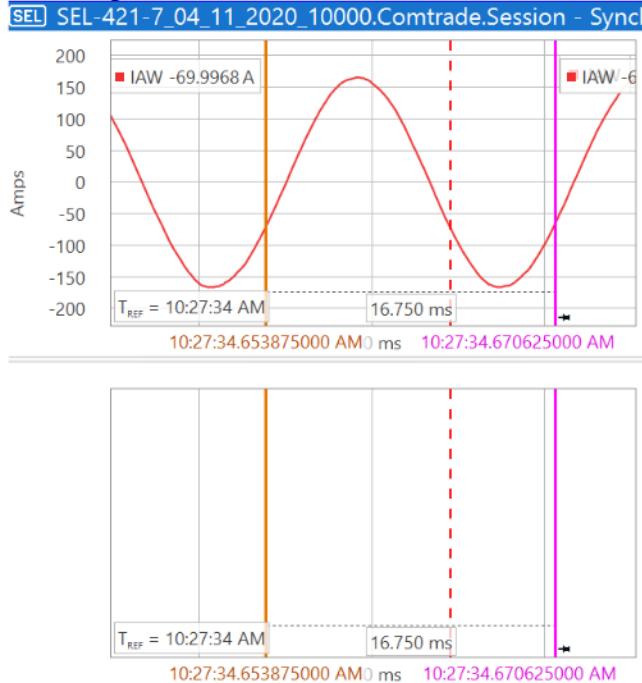


1) Mensagens Capturadas do Cenário 1. Todos os 30 testes apresentam tempos de restauração inferiores a 100 us, conforme apresentado na Tabela V. Com o intuito de comprovar a captura de todos os pacotes, foi selecionado o primeiro teste, na Figura 10. Com o resultado obtido é possível constatar que não houve a perda de nenhum pacote. A comutação realizada pelos switches SDN do caminho principal para o caminho secundário é inferior a 100 ps. Pelo fato de que cada mensagem SV é enviada a cada 208  $\mu$ s, não foi possível observar a perda de nenhum pacote em todos os testes realizados. A variável SVBLK permaneceu no estado zero. Com isso é possível concluir que em nenhum momento ocorreu bloqueio por perda de pacotes SV e as funções de proteção não foram desabilitadas.

TABLE V  
TEMPO DE RESTAURAÇÃO DO CENÁRIO 1

Teste C1/C3/C4	Tempo de Restauração
1	$\leq 100\mu s$
2	$\leq 100\mu s$
3	$\leq 100\mu s$
4	$\leq 100\mu s$
5	$\leq 100\mu s$
6	$\leq 100\mu s$
7	$\leq 100\mu s$
8	$\leq 100\mu s$
9	$\leq 100\mu s$
10	$\leq 100\mu s$

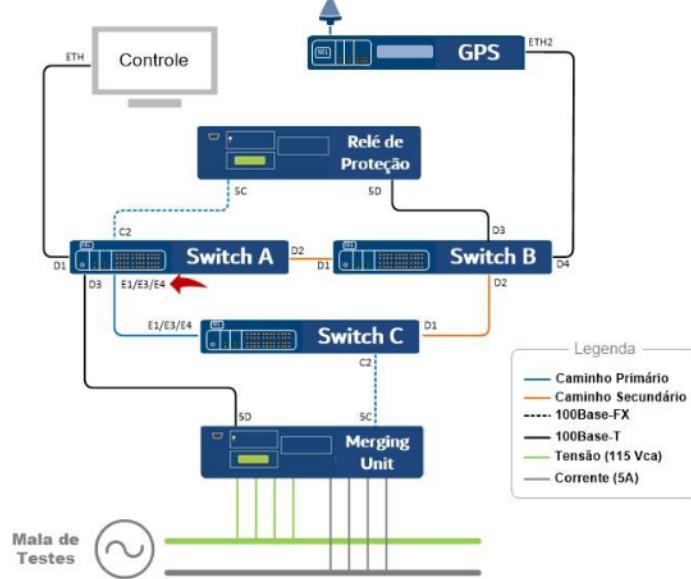
Fig. 10. Estado das Variáveis no Cenário 1



#### 4.2 ARQUITETURA DE COMUNICAÇÃO DO CENÁRIO 2

O cenário 2, Figura 11, mantém toda a estrutura do cenário 1, as diferenças estão no meio físico. A aplicação da falha física proposta foi executada desconectando a porta El do switch A, repetindo esse teste cinco vezes, e outras cinco vezes desconectando a porta El do switch C. Ao todo foram realizados dez testes de desconexão do caminho principal. O mesmo teste foi realizado, estabelecendo o caminho principal pela porta E3 dos switches A e B, e uma vez mais estabelecendo como caminho principal a porta C4, dos switches A e B. Essa repetição do processo, com portas diferentes tem o objetivo de assegurar que outras portas do mesmo switch não apresentariam comportamento diferente.

Fig. 11. Arquitetura do Cenário 2



1) Mensagens Capturadas: Todos os 30 testes apresentam tempos de restauração inferiores a 100 ps, conforme apresentado na Tabela VI. Com o intuito de comprovar a captura de todos os pacotes, foi selecionado o primeiro teste, na Figura 12. Com o resultado obtido é possível constatar que não houve a perda de nenhum pacote. A comutação realizada pelos switches SDN do caminho principal para o caminho secundário é inferior a 100 us. Pelo fato de que cada mensagem SV é enviado a cada 208 ps, não foi possível observar a perda de nenhum pacote em todos os testes realizados. A Variável SVBLK permaneceu no estado zero. Com isso possível concluir que em nenhum momento ocorreu bloqueio por perda de pacotes SV e as funções de proteção não foram desabilitadas.

Fig. 12. Estado das Variáveis no Cenário 2

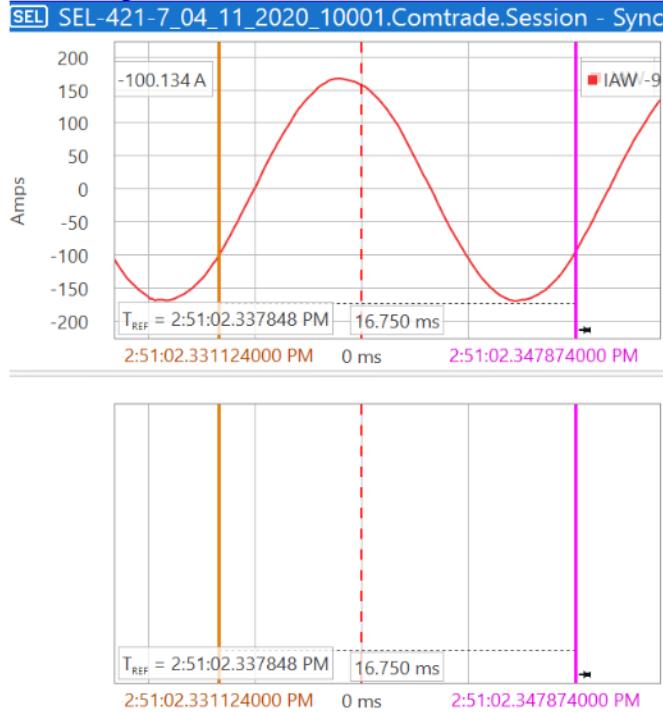


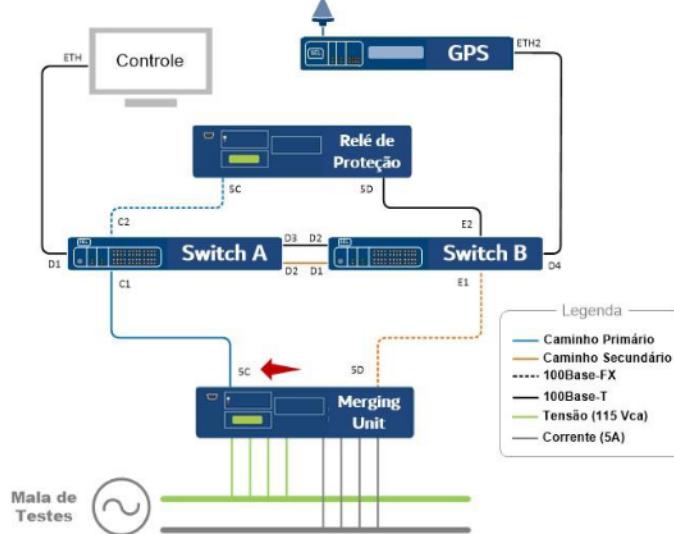
TABLE VI TEMPO DE RESTAURAÇÃO DO CENÁRIO

Teste E1/E3/E4	Tempo de Restauração
1	$\leq 100\mu\text{s}$
2	$\leq 100\mu\text{s}$
3	$\leq 100\mu\text{s}$
4	$\leq 100\mu\text{s}$
5	$\leq 100\mu\text{s}$
6	$\leq 100\mu\text{s}$
7	$\leq 100\mu\text{s}$
8	$\leq 100\mu\text{s}$
9	$\leq 100\mu\text{s}$
10	$\leq 100\mu\text{s}$

#### 4.3 ARQUITETURA DE COMUNICAÇÃO DO CENÁRIO 3

O arquitetura é apresentado na Figura 13, a falha física não é mais aplicada entre os switches SDN, mas sim nas conexões com a SAMU. O teste de falha física é realizado através da desconexão da fibra óptica da SAMU, porta SC. Para assegurar a constância dos tempos a teste é repetido igualmente dez vezes.

Fig. 13. Arquitetura do Cenário 3



1) Mensagens Capturadas do Cenário 3: Todos os tempos dos 10 testes realizados estão apresentados na Tabela VII. Com o intuito de expor a captura dos pacotes e demonstrar como é realizado a análise, o teste com menor tempo de captura foi selecionado. Na Figura 14, é possível observar o tempo 1,750 ms que o IED deixou de receber as mensagens SV. Na Figura 15, do lado esquerdo esta registrado o tempo de 75us que corresponde a perda do quarto pacote, enquanto do lado direito esta destacado mais 2 ms que corresponde ao ciclo de processamento do IED. O equipamento processa a informação e alterna o estado da variável SVBK1 para 1, =desencadeando o bloqueio da função de proteção por 1 ciclo de processamento. O IED não publica as mensagens SV ao mesmo nas duas portas, o equipamento espera a percepção da queda do link e chaveia a publicação para a outra porta. Esse tempo de comutação é conhecido como tempo de failover do IED. Sendo assim, mesmo que o SDN trabalhe rápido, nesse teste há uma soma do tempo que o próprio IED leva para detectar a queda no link da porta.

TABLE VII  
TEMPO DE RESTAURAÇÃO DO CENÁRIO 3

Teste SAMU 5C	Tempo de Restauração
1	$\leq 3250\mu s$
2	$\leq 6250\mu s$
3	$\leq 5500\mu s$
4	$\leq 5250\mu s$
5	$\leq 2000\mu s$
6	$\leq 6750\mu s$
7	$\leq 5000\mu s$
8	$\leq 1750\mu s$
9	$\leq 4125\mu s$
10	$\leq 3875\mu s$

Fig. 14. Corrente na Falha do Cenário 3

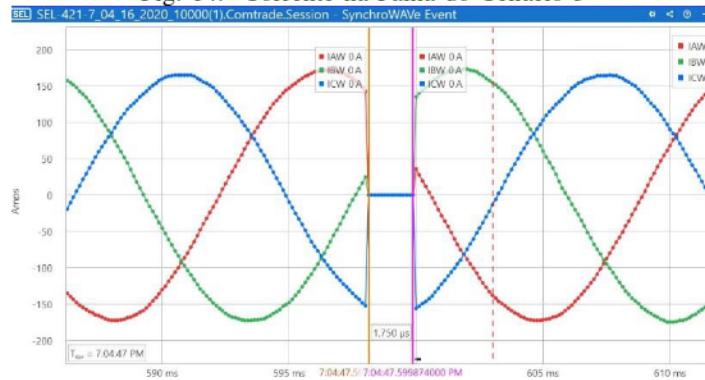
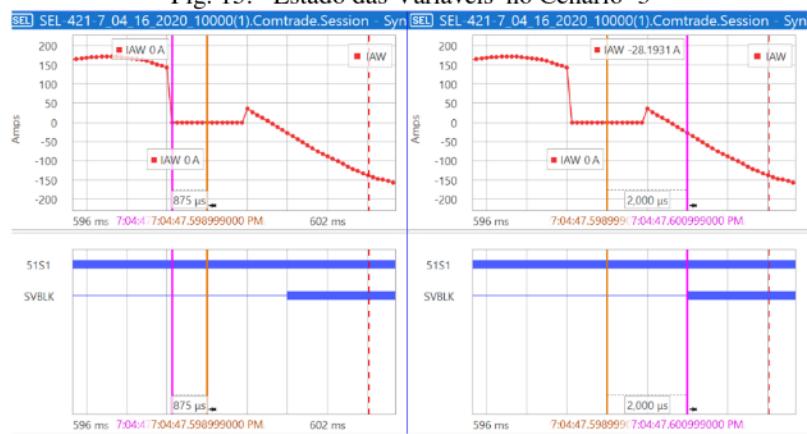


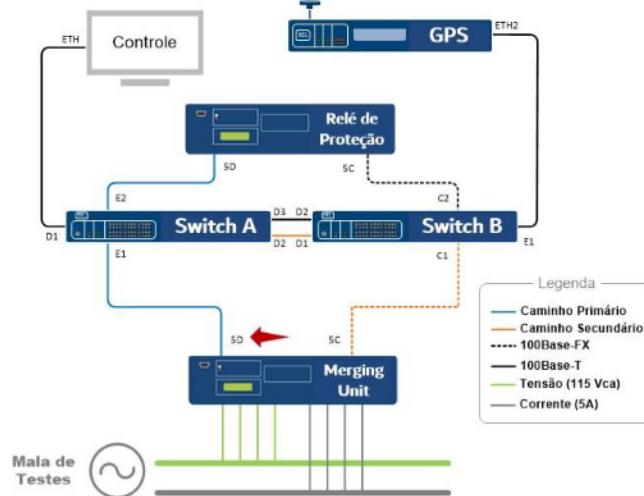
Fig. 15. Estado das Variaveis no Cenário 3



#### 4.4 ARQUITETURA DE COMUNICAÇÃO DO CENÁRIO 4

O arquitetura é apresentado na Figura 16, a falha física é aplicada através da desconexão da porta elétrica RJ45 da SAMU, porta 5D. A falha física é aplicada entre os switches SDN e a SAMU.

Fig. 16. Arquitetura do Cenário 4



1) Mensagens Capturadas do Cenário 4 Todos os tempos dos 10 testes realizados estão apresentados na Tabela VIII. Com o intuito de expor a captura dos pacotes e demonstrar como é realizado a análise, o teste com menor tempo de captura foi selecionado. Na Figura 17, é possível observar o tempo 6,625 ms que o IED deixou de receber as mensagens SV. Na Figura 18, do lado esquerdo et registrado o tempo de 875ps que corresponde a perda do quarto pacote, enquanto que do lado direito esta destacado mais 2 ms que corresponde ao ciclo de processamento do IED. O equipamento processa a informação e alterna o estado da variável SVBKL para 1, desencadeando o bloqueio da função de proteção por 1 ciclo de processamento. O IED não publica as mensagens SV ao mesmo nas duas portas, o equipamento espera a percepção da queda do link e chaveia a publicação para a outra porta. Esse tempo de comutação é conhecido como tempo de failover do IED. Sendo assim, mesmo que o SDN trabalhe rápido, nesse teste há uma soma do tempo que o próprio IED leva para detectar a queda no link da porta.

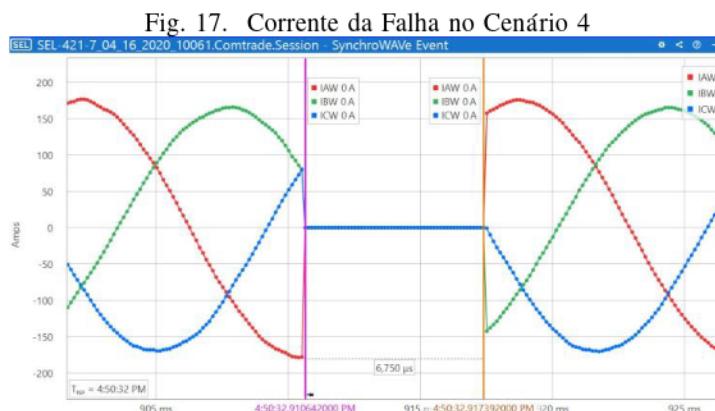


Fig. 18. Estado das Variáveis no Cenário 4

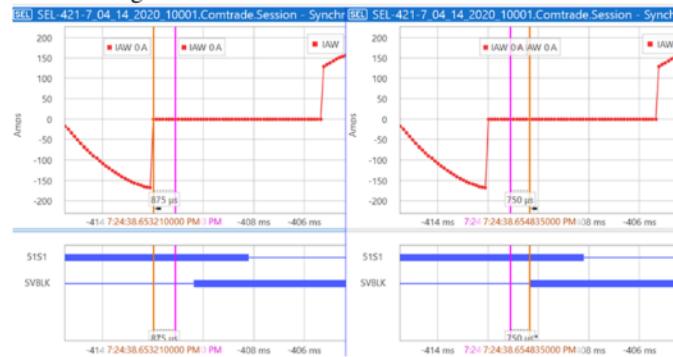


TABLE VIII  
TEMPO DE RESTAURAÇÃO DO CENÁRIO 4

Teste SAMU 5D	Tempo de Restauração
1	$\leq 11750\mu s$
2	$\leq 8000\mu s$
3	$\leq 6525\mu s$
4	$\leq 10250\mu s$
5	$\leq 10750\mu s$
6	$\leq 7000\mu s$
7	$\leq 10000\mu s$
8	$\leq 6000\mu s$
9	$\leq 11500\mu s$
10	$\leq 10750\mu s$

#### 4.5 ARQUITETURA DE COMUNICAÇÃO DO CENÁRIO 5

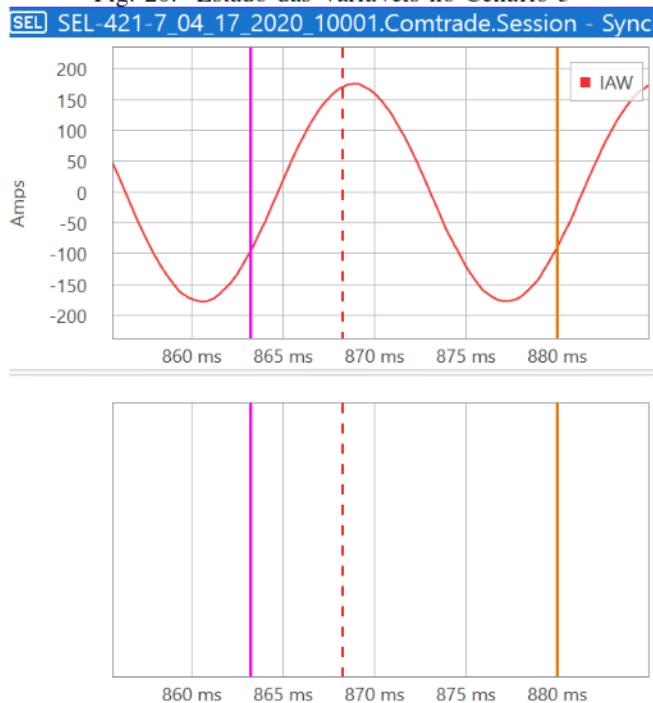
A arquitetura da Figura 19 é composta por uma rede em anel de quatro switches SDN. A aplicação da falha lógica proposta foi executada desabilitando via software a porta D1 do C, repetindo esse teste dez vezes no link principal estabelecido pelo controlador. A repetição do teste tem o objetivo de assegurar que os tempos são constantes.

1) Mensagens Capturadas do Cenário 5: Todos os 10 testes apresentam tempos de restauração inferiores a 100 ps, conforme apresentado na Tabela IX. Com o intuito de comprovar a captura de todos os pacotes, foi selecionado o primeiro teste, na Figura 20. Com o resultado obtido e possível constatar que não houve a perda de nenhum pacote. A comutação realizada pelos switches SDN do caminho principal para o caminho secundário é inferior a 100 us. Pelo fato de que cada mensagem SV é enviado a cada 208 us, não foi possível observar a perda de nenhum em todos os testes realizados. A variável SVBLK permaneceu no estado zero. Com isso é possível concluir que em nenhum momento ocorreu bloqueio por perda de pacotes SV e as funções de proteção não foram desabilitadas.

TABLE IX  
TEMPO DE RESTAURAÇÃO DO CENÁRIO 5

Teste SWC DI	Tempo de Restauração
1	$\leq 100\mu s$
2	$\leq 100\mu s$
3	$\leq 100\mu s$
4	$\leq 100\mu s$
5	$\leq 100\mu s$
6	$\leq 100\mu s$
7	$\leq 100\mu s$
8	$\leq 100\mu s$
9	$\leq 100\mu s$
10	$\leq 100\mu s$

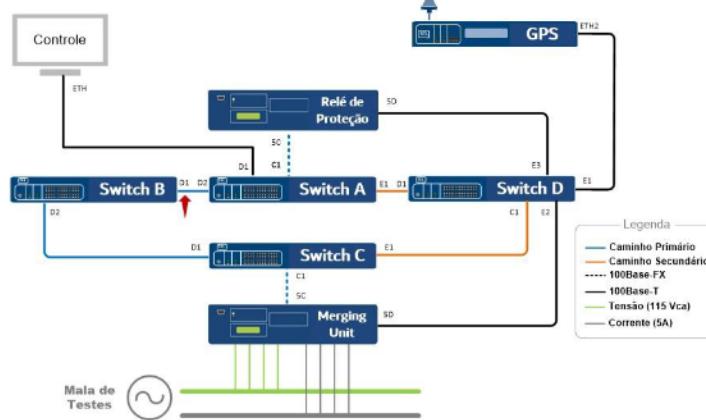
Fig. 20. Estado das Variáveis no Cenário 5



#### 4.6 ARQUITETURA DE COMUNICAÇÃO DO CENÁRIO 6

O cenário 6, Figura 21, mantém toda a estrutura do cenário 5, contudo a falha lógica foi aplicado em um switch diferente. O intuito seria avaliar o desempenho em um segundo hardware. A aplicação da falha lógica proposta foi executada desabilitando a porta D1 do switch B, repetindo esse teste dez vezes.

Fig. 21. Arquitetura do Cenário 6

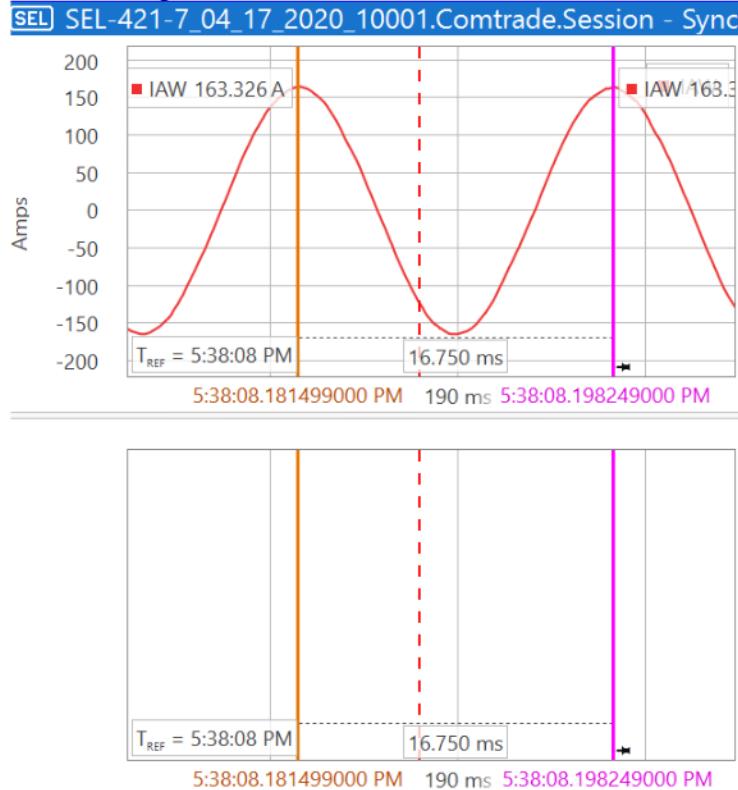


1) Mensagens Capturadas do Cenário 6: Todos os 10 testes apresentam tempos de restauração inferiores a 100 us, conforme apresentado na Tabela X. Com o intuito de comprovar a captura de todos os pacotes, foi selecionado o primeiro teste, na Figura 22. Com o resultado obtido é possível constatar que não houve a perda de nenhum pacote. A comutação realizada pelos switches SDN do caminho principal para o caminho secundário é inferior a 100 us. Pelo fato de que cada mensagem SV é enviado a cada 208 us, não foi possível observar a perda de nenhum pacote em todos os testes realizados. A variável SVBLK permaneceu no estado zero. Com isso é possível concluir que em nenhum momento ocorreu bloqueio por perda de pacotes SV e as funções de proteção não foram desabilitadas.

TABLE X  
TEMPO DE RESTAURAÇÃO DO CENÁRIO 6

Teste SWB D1	Tempo de Restauração
1	$\leq 100\mu s$
2	$\leq 100\mu s$
3	$\leq 100\mu s$
4	$\leq 100\mu s$
5	$\leq 100\mu s$
6	$\leq 100\mu s$
7	$\leq 100\mu s$
8	$\leq 100\mu s$
9	$\leq 100\mu s$
10	$\leq 100\mu s$

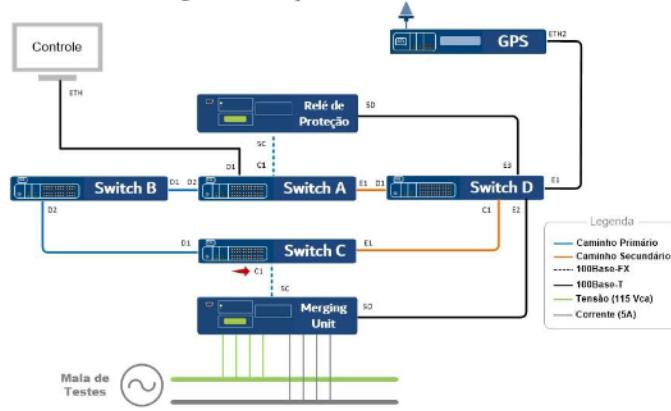
Fig. 22. Estado das Variáveis no Cenário 6



#### 4.7 ARQUITETURA DE COMUNICAÇÃO DO CENÁRIO 7

A arquitetura na Figura 23, possui 4 switches SDN e a conexão da SAMU em dois switches diferentes. O teste de falha lógica é aplicado desabilitando a porta C1 do switch que conecta à porta em fibra óptica 5C da SAMU.

Fig. 23. Arquitetura do Cenário 7



1) Mensagens Capturadas do Cenário 7: Todos os tempostos dos 10 testes realizados estão apresentados na Tabela XI. Com o intuito de expor a captura dos pacotes e demonstrar como é realizado a análise, o teste com menor tempo de captura foi

selecionado. Na Figura 24, é possível observar o tempo 5,250 ms que o IED deixou de receber as mensagens SV.

TABLE XI  
TEMPO DE RESTAURAÇÃO DO CENÁRIO 7

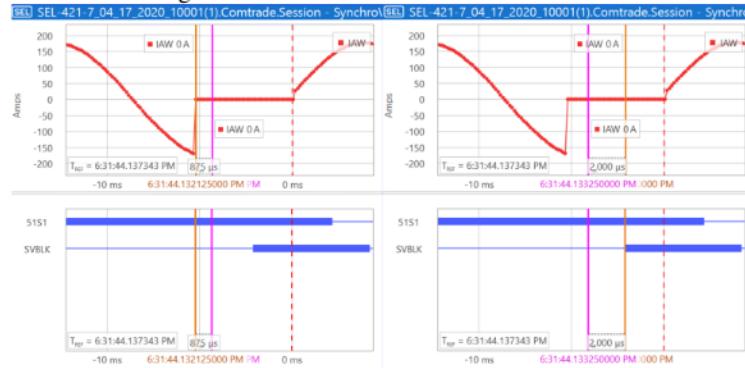
Teste SWD E2	Tempo de Restauração
1	$\leq 5250\mu s$
2	$\leq 6375\mu s$
3	$\leq 5250\mu s$
4	$\leq 6125\mu s$
5	$\leq 5250\mu s$
6	$\leq 5750\mu s$
7	$\leq 5250\mu s$
8	$\leq 6000\mu s$
9	$\leq 5750\mu s$
10	$\leq 5500\mu s$

Fig. 24. Estado das Variáveis no Cenário 7



Na Figura 25, do lado esquerdo está registrado o tempo de 875μs que corresponde a perda do quarto pacote, enquanto do lado direito está destacado mais 2 ms que corresponde ao ciclo de processamento do IED. O equipamento processa a informação e alterna o estado da variável SVBKL para 1, desencadeando o bloqueio da função de proteção por 1 ciclo de processamento. O IED não publica as mensagens SV 20 mesmo nas duas portas, o equipamento espera a percepção da queda do link e chaveia a publicação para a outra porta. Esse tempo de comutação é conhecido como tempo de failover do IED Sendo assim, mesmo que o SDN trabalhe rápido, nesse teste há uma soma do tempo que o próprio IED leva para detectar a queda no link da porta.

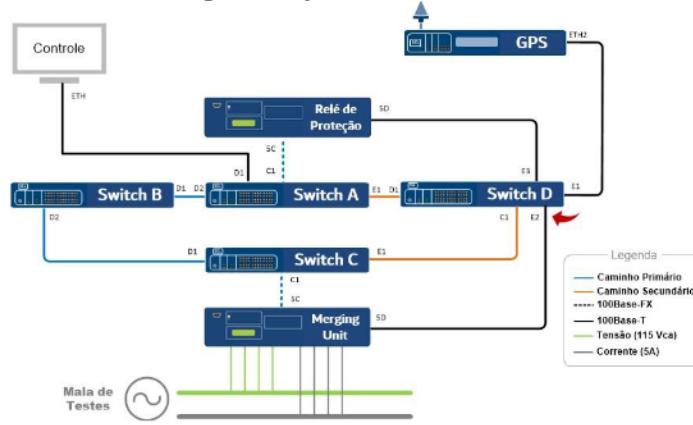
Fig. 25. Corrente da Falha no Cenário 7



#### 4.8 ARQUITETURA DE COMUNICAÇÃO DO CENÁRIO 8

A arquitetura na Figura 26, mantém toda a estrutura do cenário 7, contudo a falha lógica foi aplicada na porta E2 do switch D que conecta à porta elétrica 5D da SAMU

Fig. 26. Arquitetura do Cenário 8



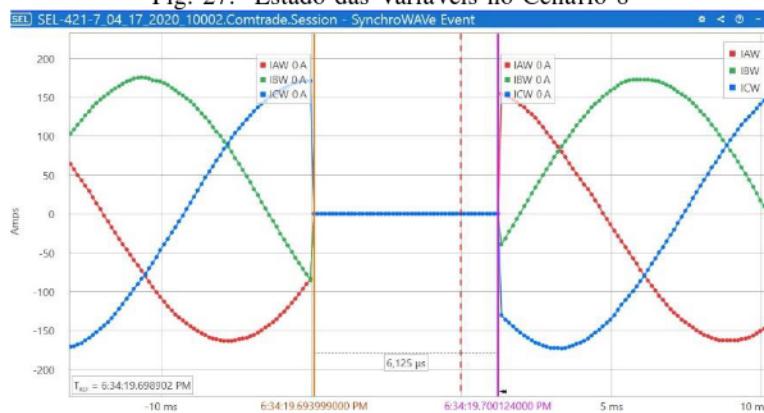
1) Mensagens Capturadas: Todos os tempos dos 10 testes realizados estão apresentados na Tabela XII. Com o intuito de expor a captura dos pacotes e demonstrar como é realizado a análise, o teste com menor tempo de captura foi selecionado.

Na Figura 27, é possível observar o tempo 6,125 ms que o IED deixou de receber as mensagens SV.

TABLE XII  
TEMPO DE RESTAURAÇÃO DO CENÁRIO 8

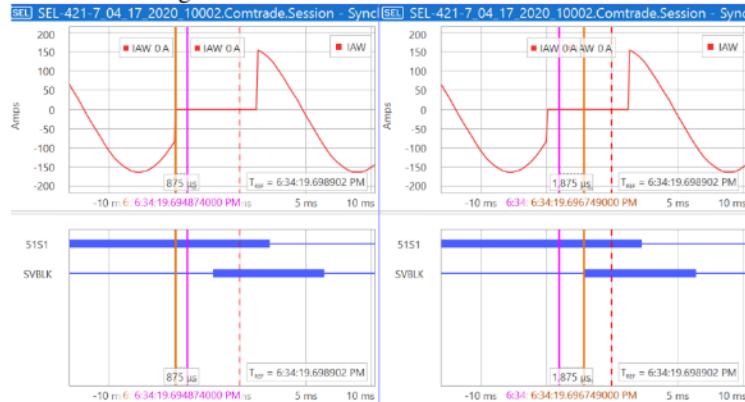
Teste SWC C1	Tempo de Restauração
1	$\leq 6125\mu s$
2	$\leq 6500\mu s$
3	$\leq 6125\mu s$
4	$\leq 6250\mu s$
5	$\leq 6500\mu s$
6	$\leq 6375\mu s$
7	$\leq 6250\mu s$
8	$\leq 6500\mu s$
9	$\leq 6125\mu s$
10	$\leq 6375\mu s$

Fig. 27. Estado das Variáveis no Cenário 8



Na Figura 28, do lado esquerdo está registrado o tempo de  $875\mu s$  que corresponde a perda do quarto pacote, enquanto que do lado direito está destacado mais 2 ms que corresponde ao ciclo de processamento do IED. O equipamento processa a informação e alterna o estado da variável SVBKL para 1, desencadeando o bloqueio da função de proteção por 1 ciclo de processamento. O IED não publica as mensagens SV ao mesmo nas duas portas, o equipamento espera a percepção da queda do link e chaveia a publicação para a outra porta. Esse tempo de comutação é conhecido como tempo de failover do IED Sendo assim, mesmo que o SDN trabalhe rápido, nesse teste há uma soma do tempo que o próprio IED leva para detectar a queda no link da porta.

Fig. 28. Corrente da Falha no Cenário 8



## 5 ANALISE DOS RESULTADOS

Nas Tabelas XIII e XIV são exibidos os dados resultantes dos oito cenários 10s quais foram aplicados o método Na falha aplicada entre os switches tanto para falha física quanto para falha lógica, a perda de pacotes não é suficiente para desabilitar as funções de proteção. Quando os pacotes do fluxo principal deixam de entregar os pacotes ao destino, o switch SDN comuta para o fluxo alternativo, e a comunicação é restabelecida, esse comportamento é possível ver nos cenários 1, 2, 5 e 6. Contudo, quando a falha ocorre na comunicação com a SAMU o tempo é maior. O equipamento necessita perceber a falha no link, para então iniciar o envio dos dados pela outra por O tempo que acaba proporcionando o atraso da recomposição e consequentemente desabilitando as funções nos relés de proteção. Comparando os meios físicos, quando as falhas foram físicas, cenários 2 e 3, é possível constatar que há uma grande diferença. Contudo, nas falhas lógicas, cenários 7 e 8, diferença foi pequena.

Com relação ao sincronismo de tempo, em nenhum dos cenários o tempo superou o tempo de 5 segundos. Por essa razão a proteção e a SAMU não tiveram o sincronismo de tempo afetado pelas falhas físicas aplicadas.

TABLE XIII  
RESULTADOS DOS CENÁRIOS 1 AO 4

Cenários	1	2	3	4
Local da Falha	Entre SWs	Entre SWs	SWeSAMU	SWeSAMU
T min	$\leq 100\mu s$	$\leq 100\mu s$	$1750\mu s$	$6525\mu s$
T max	$\leq 100\mu s$	$\leq 100\mu s$	$6750\mu s$	$11750\mu s$
T med	$\leq 100\mu s$	$\leq 100\mu s$	$4375\mu s$	$9252\mu s$
Tipo da Falha	Física	Física	Física	Física
Conexão	F.O.	F.O.	F.O.	UTP
Bloq. da Prot.?	Não	Não	Sim	Sim

TABLE XIV  
RESULTADOS DOS CENÁRIOS 5 AO 8

Cenários	5	6	7	8
Local da Falha	Entre SWs	Entre SWs	SWeSAMU	SWeSAMU
T min	$\leq 100\mu s$	$\leq 100\mu s$	$5250\mu s$	$6125\mu s$
T max	$\leq 100\mu s$	$\leq 100\mu s$	$6375\mu s$	$6375\mu s$
T med	$\leq 100\mu s$	$\leq 100\mu s$	$5650\mu s$	$6312\mu s$
Tipo da Falha	Lógica	Lógica	Lógica	Lógica
Conexão	UTP	UTP	F.O.	UTP
Bloq. da Prot.?	Não	Não	Sim	Sim

## 6 CONCLUSÕES E TRABALHOS FUTUROS

A contribuição de trabalho está em analisar o bloqueio de funções de proteção em IEDs, durante as falhas físicas no barramento de processo. Ao longo deste trabalho foram apresentadas e analisadas falhas em oito diferentes arquiteturas de comunicação, que podem ser aplicadas a barramento de processos. A solução com SDN se mostrou eficiente e rápida, a ponto de não desabilitar a função de proteção quando o tempo de recomposição dependia somente dela. As recomposições sempre foram abaixo de 100 ps. Porém houve bloqueios de funções por um período, mas como apresentado a razão é o tempo de failover da porta do IED. O tempo de failover do IED, é especificado na norma IEEE 802.3 (2015) [15], sendo que ela estabelece um tempo mínimo para a identificação da falha do link. Esse tempo de detecção do link contrasta com os tempos de bloqueio das funções de proteção, uma vez que as funções de proteção são bloqueadas com falhas superiores a 624 ps, e os tempos de detecção de perda do link do IED está acima dos 2 ms. Por essa razão uma possível revisão da norma IEEE 802.3 (2015) [15] poderia ser proposta, para aplicações como a SAMU. Para resolver essa questão há três possibilidades. A primeira seria utilizar um SAMU com porta simples e conectar duas SAMU a rede SDN, dessa forma a publicação nunca seria interrompida. A segunda possibilidade é o cliente final operar com a possibilidade da proteção ficar indisponível por alguns milissegundos, utilizando porta em fibra óptica. A terceira possibilidade é a SAMU disponibilizar PRP. A vantagem de utilizar o PRP com o SDN estaria no fato de ser necessário uma única estrutura de barramento de processo, ou seja, uma única LAN, e não duas estruturas independentes como o PRP, sem SDN, estabelece.

### 6.1 TRABALHOS FUTURO

Com aprofundamento e pesquisa, tendo como base este trabalho, sugere-se ramificações que podem ser objeto de estudo para trabalhos futuros:

- Verificar falhas lógicas na comunicação dos switches.
- Analisar os tempos com conexões em 1000Base-SX
- Verificar a aplicação da Rede SDN, para envio e recepção de mensagens em sistemas de Teleproteção.
- Verificar o comportamento das mensagens SV, quando o PTP utiliza o BMCA para comutar o relógio GPS.

## REFERÊNCIAS

- [1]G. Clarke, D. Reynders, and E. Wright, Practical modern SCADA protocols: DNP3, 60870.5 and related system. Newnes, 2004.
- [2] IEC 61850-9-2, communication networks and systems for power utility automation-Part 9-2: Specific communication service mapping (SCSM) -Sampled values over ISO/IEC 8802-3, Std., 2011.
- [3]T. IEC, "61550-90-4:2013, communication networks and systems for power utility automation-part 90-4: Network engineering guidelines," International Electrotechnical Commission, 2013.
- [4] IEC 61850-7-4, communication networks and systems for power utility automation - Part 7-4: Basic communication structure Compatible logical node classes and data object clarerer, Std., 2010.
- [5] IEC 61869-13, instrument Transformers - Part 13 Standalone Marging Unit, Std., 2021.
- [6]S. E. Laboratories, SEL-421-7 Protection Automation, and Control System With Sampled Valuer, Schweitzer Engineering Laboratories.
- [7] leee standard for a precision clock synchronization protocol for networked measurement and control systems," IEEE Std 1588-2019 (Revizion ofIEEE Std 1588-2008), pp. 1-499, 2020.
- [8]D M. Ingram, D. A. Campbell, and P. Schaub, "Use of ieee 1588-2008 for a sampled value process bus in transmission substations," in 2011 IEEE International Instrumentation and Measurement Technology Conference. IEEE, 2011, pp. 1-6.
- [9] IEC 62439-3, INDUSTRIAL COMMUNICATION NETWORKS - HIGH AVAILABILITY AUTOMATION NETWORKS - PART 3: PARALLEL REDUNDANCY PROTOCOL (PRP) AND HIGH-AVAILABILITY SEAM
- [10]I. Araujo, J Lazaro, A. Astarlea, A Zuloaga, and A. Garcia, "Prp and har LESS REDUNDANCY (HSR), Std., 2016 version 1 (ec 62439-2), improvements and a prototype implemen tation," in IECON 2013-39th Annual Conference of the IEEE Industrial Electronics Society IEEE, 2013, pp. 4410-4415.
- [11]G GPC, R. F. CORNA, M. G. DA SILVEIRA, and W.OLIVEIRA, Solucionande problemas de automação com redes sdn Lacunas de configuração das mensagens goose, xxv saptee seminario nacional de produção e transmitilo de energia elétrica 10 13 de novembro de 2019 belo horizonte-mg" Gelberger, N. Yemini, and R. Giladi, Performance analysis of software-defined networking (sdn)," in 2013 IEEE 21st International Sympozion on Modelling. Anabis and Simulation of Computer and Telecommumcation Stems IFFF 2013 pm 389-393

- [12]A. Gelberger, N. Yemini, and R. Giladi, "Performance analysis of software-defined networking (sdn)," in 2013 IEEE 21st International Symposium on Modelling, Analysis and Simulation of Computer and Telecommunication Systems. IEEE, 2013, pp. 389-393.
- [13]N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "Openflow: enabling innovation in campus networks," ACM SIGCOMM Computer Communication Review, vol. 38, no. 2, pp. 69-74, 2008.
- [14]A. Nygren, B. Pfaff, B. Lantz, B. Heller, C. Barker, C. Beckmann, D. Cohn, D. Malek, D. Talayco, D. Erickson et al, "Openflow switch specification version 1.5. 1," Open Networking Foundation, Tech. Rep, 2015
- [15] IEEE standard for ethernet," IEEE Std 802.3-2015 (Revision of IEEE Std 802.3-2012), pp. 1-4017, 2016.