UNIVERSIDADE DE SÃO PAULO
ESCOLA DE ENGENHARIA DE SÃO CARLOS

FABIO ALVES FERNANDES

UM ESTUDO SOBRE O USO DA TOPOLOGIA ANEL EM REDES PROFINET COMO TÉCNICA DE IMPLEMENTAÇÃO DE REDUNDÂNCIA

SÃO CARLOS – SP
2015

FABIO ALVES FERNANDES

UM ESTUDO SOBRE O USO DA TOPOLOGIA ANEL EM REDES PROFINET COMO TÉCNICA DE IMPLEMENTAÇÃO DE REDUNDÂNCIA

Trabalho de Conclusão de Curso apresentado
à Escola de Engenharia de São Carlos, da
Universidade de São Paulo

Curso de Engenharia Elétrica com ênfase em
Sistemas de Energia e Automação

ORIENTADOR: Prof. Dr. Dennis Brandão

São Carlos
2015

Fernandes, Fabio Alves
F362u Um estudo sobre o uso da topologia anel em redes Profinet como técnica de implementação de redundância / Fabio Alves Fernandes; orientador Dennis Brandão. São Carlos, 2015.

Monografia (Graduação em Engenharia Elétrica com ênfase em Sistemas de Energia e Automação) -- Escola de Engenharia de São Carlos da Universidade de São Paulo, 2015.

1. Profinet. 2. Redundância. 3. Media Redundancy Protocol. 4. Topologia anel. 5. Redes de comunicação industrial. I. Título.

FOLHA DE APROVAÇÃO

Nome: Fabio Alves Fernandes

Título: "Um estudo sobre o uso da topologia anel em redes Profinet como técnica de implementação de redundância"

Trabalho de Conclusão de Curso defendido e aprovado em 10 / 11 / 2015,

com NOTA 10 (10 , 0 (dez)), **pela Comissão Julgadora:**

Prof. Associado Dennis Brandão - (Orientador - SEL/EESC/USP)

Mestre Guilherme Serpa Sestito - (Doutorando - SEL/EESC/USP)

Mestre André Luís Dias - (SEL/EESC/USP)

Coordenador da CoC-Engenharia Elétrica - EESC/USP:
Prof. Dr. José Carlos de Melo Vieira Júnior

Dedicatória

Para os meus pais, Nelson e Iranilda. Por todo o apoio, amor e educação que sempre me deram. Muito obrigado!

Agradecimentos

Agradeço primeiramente ao Prof. Dr. Dennis Brandão, por ter me recebido no laboratório de Automação Industrial e confiado em meu trabalho.

Ao Eng. Guilherme Serpa Sestito, que sem dúvida teve participação essencial para o desenvolvimento desta monografia. Muito obrigado por toda colaboração e ensino.

Ao Eng. André Luís Dias que mesmo distante, pode contribuir com importantes observações em todo o andamento do estudo.

A minha família, Nelson, Iranilda, Danielle e Fabiane por estarem ao meu lado em todos os momentos, me dando todo o apoio e amor necessário. A Aysline, pois com todo seu carinho sempre me ajudou a vencer os obstáculos.

“Pois dele, por ele e para ele são todas as coisas. A ele seja a glória para sempre! Amém.”
Romanos 11:36

Resumo

A disponibilidade de uma rede de comunicação industrial tem se tornado um tema cada vez mais importante, visto que a perda de comunicação entre dispositivos pode causar severas consequências. Assim é de extrema importância saber trabalhar com protocolos de redundância para assegurar a disponibilidade da rede. O presente trabalho propõe um estudo sobre o uso da topologia anel em redes Profinet como técnica de implementação de redundância. Assim é apresentado uma metodologia para analisar a redundância do anel e quantificar o tempo necessário para que a mesma se recupere de uma falha, chamado de tempo de recuperação. Por fim, esta monografia busca detectar possíveis fatores que possam influenciar de forma direta ou indireta este intervalo de recuperação. Os principais fundamentos teóricos para este trabalho são sobre redes de comunicação industrial, redes de computadores, e normatização. A presente monografia consiste em uma revisão bibliográfica sobre o assunto, seguido de testes em laboratório, apresentação e discussão dos resultados, através de tabelas e gráficos. Por fim, é apresentada a conclusão sobre o estudo e sugestões para trabalhos futuros na linha de pesquisa proposta.

Palavras-chave: Profinet, Redundância, *Media Redundancy Protocol*, Topologia anel, Redes de comunicação industrial.

Abstract

The availability of industrial communication network has become an increasingly important topic, since the loss of communication can cause severe consequences. So it is extremely important to know how to deal with redundancy protocols to assure the network availability. This paper purpose a study about the use of ring topology in Profinet network as technical implementation of redundancy. In addition, it is presented a methodology to analysis the network redundancy and quantify the time required for the network to recover from a failure. Lastly, it detects possible factors that can influence directly or indirectly the recovery time. The main theoretical foundations for this paper are industrial communication networks, computers networks and standardization. This monograph consists of a literature review of the subject, laboratory tests, presentation and discussion of results through tables and graphs. Ultimately, it is performed a conclusion about the study and proposed futures papers following the same method.

Palavras-chave: Profinet, *Redundancy*, *Media Redundancy Protocol*, *Ring topology*, *industrial communication networks*.

Lista de Figuras

Lista de Tabelas

Sumário

1. Introdução

As redes de comunicação industrial têm se tornado cada vez mais complexas ao longo das últimas duas décadas, assim como o número de sensores e atuadores tem crescido consideravelmente nas indústrias, indicando a tendência de um maior nível de automação industrial, isto é, menos humanos são envolvidos enquanto equipamentos de fábrica vão se tornando mais sofisticados.

A resposta da indústria para lidar com esse crescimento complexo começou na década de 1980 quando os sinais físicos de sensores e atuadores deram lugar a uma representação lógica. No começo da década de 1990 surgiram os chamados *fieldbuses,* como por exemplo, o protocolo de comunicação industrial Profibus [1]. Com o passar dos anos as redes de campo foram sendo aperfeiçoadas e evoluíram na velocidade e quantidade de transmissão de dados, na complexidade e quantidade de recursos implementados para facilitar a operação em campo.

Neste cenário, buscava-se uma rede capaz de interligar todos os níveis do sistema de automação industrial, isto é, uma única tecnologia capaz de controlar tanto o baixo nível (chão de fábrica) como também o alto nível (escritório). Foi então que surgiram soluções baseadas em Ethernet. Tais soluções apresentavam as seguintes vantagens: alta taxa de velocidade na comunicação, menores tempos de transmissão de dados, e a possibilidade de integrar todos os níveis e componentes da indústria em uma mesma infraestrutura [2].

Entretanto a Ethernet era considerada inapropriada para os ambientes industriais agressivos devido a sua baixa imunidade ao ruído, conectores inadequados e falta de determinismo [3]. Assim um elevado número de técnicas surgiram para adaptar a Ethernet para aplicações industriais. Com o passar dos anos a Ethernet foi sendo alterada e medidas foram tomadas para apropriar o seu uso em todos os níveis da indústria. Esse novo padrão foi denominado Ethernet de tempo real, ou RTE (Real Time Ethernet).

Dentre os protocolos de comunicação Real-Time Ethernet definidos pela IEC 61748-2 tem-se o Profinet, que é baseado na troca de mensagens entre um dispositivo de campo e um controlador. Este protocolo de comunicação tem alcançado uma importância destacada no mercado [3, 4].

O protocolo Profinet suporta diferentes topologias, entre elas a topologia em anel. Esta topologia apresenta a característica de através da adição de uma ligação física, inserir uma redundância na rede, aumentando assim a sua disponibilidade. Uma rede em

anel quando apresenta uma falha em uma de suas conexões tem a capacidade de encontrar um novo caminho para o fluxo de dados. O tempo necessário desde o momento em que ocorreu a falha no anel até que a comunicação entre controlador e uma estação remota seja restabelecida, é chamado tempo de Recuperação da rede.

1.1 Objetivo e contribuição do trabalho

Tendo em vista o contexto relatado, este trabalho irá estudar o comportamento de uma rede Profinet frente a variações em suas conexões, em especifico, a resposta de uma rede em anel quando ocorre uma falha em uma de suas ligações. Além de entender o funcionamento do anel, o objetivo deste estudo é definir uma técnica para medição do tempo de recuperação da rede e encontrar variáveis que possam influenciá-lo diretamente ou indiretamente.

Atingido estes objetivos, o presente trabalho fornecerá importantes informações para projetistas que desejarem aumentar a disponibilidade de sua rede de comunicação industrial, visto que através da inserção de uma redundância, a rede terá a capacidade de se recuperar de possíveis falhas. Além disso, o projetista terá ciência de importantes fatores que podem influenciar no tempo de recuperação de sua rede, tornando apto a tomar decisões importantes, como o valor de *watchdog* dos dispositivos, e o número de switches no anel.

Por fim, esta monografia possibilitará ao autor a aplicação e expansão de seus conhecimentos adquirido nas disciplinas de graduação correlatas, como SEL0406 Automação, SEL0430 Laboratório de Automação, SEL0432 Redes de Comunicação Industrial, SEL0431 Laboratório de Controle de Processos Industriais, SEL0378 Redes de Computadores.

1.2 Organização do trabalho

Este trabalho está organizado da seguinte maneira:

- ✓ Capítulo 2: Apresenta as características necessárias e suficientes para o embasamento teórico do protocolo Profinet.
- ✓ Capítulo 3: Detalha a metodologia utilizada em laboratório e exibe os resultados alcançados.
- ✓ Capítulo 4: Exibe as principais conclusões pertinentes ao trabalho.

2. Conceitos básicos do Profinet

Este capítulo tem por finalidade apresentar os principais conceitos teóricos referentes ao protocolo de comunicação Profinet. Deseja-se mostrar o embasamento teórico necessário para que seja desenvolvida a metodologia experimental.

2.1 Introdução ao Profinet

O Profinet é um protocolo Real Time Ethernet (RTE), definido pela Profibus International (PI), que foi desenvolvido para ser usado em redes de comunicação industrial, visando a conexão entre os dispositivos de campo e os controladores. O Profinet trouxe importantes benefícios para os sistemas de automação industrial, como por exemplo [5, 6]:

- ✓ Operações em alta velocidade;
- ✓ Estrutura simplificada de rede;
- ✓ Baixos custos;
- ✓ Cabeamento único;
- ✓ Rede de expansão simples;
- ✓ Integração com sistemas *fieldbus*

Além disso, o Profinet oferece uma importante e diferencial característica de unir todos os níveis do sistema de automação, ou seja, desde a supervisão no escritório até o controle de movimentos no chão de fábrica, tudo pode ser responsabilidade do Profinet [3].

2.2 Modelo Profinet

O Profinet é caracterizado por uma estação central que se comunica com dispositivos de campo espalhados pela rede. Cada estação é definida como segue:

- ✓ IO-Controller: Representa a estação central de inteligência, responsável por gerenciar e controlar todo o processo de transferência de dados. Além disso, o IO-Controller é o dispositivo que realiza toda configuração e parametrização associada aos dispositivos de campo. Ex.: Controlador Lógico Programável.
- ✓ IO-Device: Representa o dispositivo de campo, semelhante a uma unidade de entrada. Os dispositivos de campo trocam informações ciclicamente com IO-

Controller, recebendo-as e enviando posteriormente os dados de saída do processo. É sua responsabilidade também providenciar diagnósticos e alarmes para o IO-Controller. Ex.: Sensores, atuadores, módulos de entrada e saída.

- ✓ IO-Supervisor: Representa a estação de engenharia. Sua função é programar, configurar e realizar diagnósticos em toda rede. Ex.: Ferramenta de programação do CLP [3].

Uma rede Profinet deve possuir minimamente um IO-Controller e um IO-Device. Já o IO-Supervisor é geralmente integrado apenas temporariamente para comissionamentos e diagnósticos [7]. A Figura 1 apresenta cada um dos dispositivos citados em uma rede Ethernet.

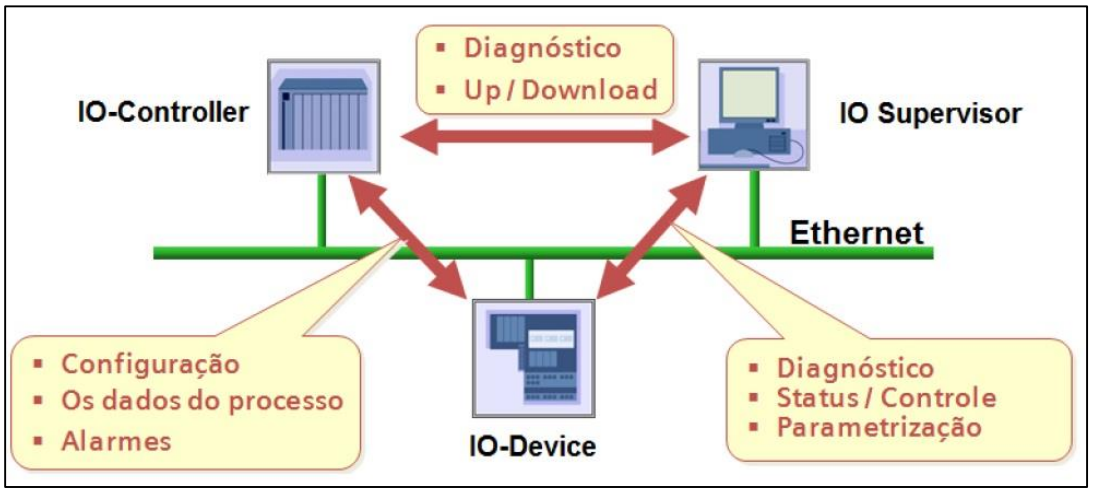


Figura 1: Modelo do Profinet

Fonte: [10]

Cada dispositivo da rede é definido por um arquivo XML chamado de GSD-file. Nesse arquivo está descrito o dispositivo de campo, bem como suas funcionalidades. A leitura deste arquivo pode ser realizada por alguma ferramenta de engenharia, como por exemplo, um software de CLP, tornando-se possível realizar a parametrização de cada dispositivo da rede Profinet. Todos estes dados são carregados no IO-Controller, a fim de que ele possa utilizar destas informações para configurar e organizar toda comunicação realizada entre os dispositivos [3].

2.3 Tipos de comunicação

O Profinet distingue três diferentes tipos de comunicação entre dois dispositivos, que são: *non real-time* (NRT), *real-time* (RT) e *isochronous real-time* (IRT). Cada um destes tipos apresentam características únicas que os diferem um dos outros. [3]

- ✓ Non real-time (NRT): Representa o canal TCP/IP, nele trafegam mensagens longas e lentas, responsáveis pela configuração e leitura dos parâmetros dos IO-Devices, além de ser responsável pela inicialização da *Application Relation*, que será explicada mais adiante [8].
- ✓ Real-time (RT): O canal RT apresenta tempos de ciclos menores que o NRT (na faixa dos milissegundos), além de possuir valores de *jitter* baixos. Esta maior velocidade na comunicação é devida ao fato de que o canal *real-time* acessa diretamente a camada Ethernet, onde está contido o MAC*,* pulando as pilhas UDP/IP. Este canal é utilizado para a troca de mensagens cíclicas e as mensagens de alarme acíclicas.
- ✓ *Isochronous real-time* (IRT): A comunicação IRT apresenta tempos de ciclo bem inferiores a comunicação RT, alcançando valores abaixo de 1 milissegundo, além de possuir *jitter* extremamente baixo, com valores na faixa de 1 microssegundo. Este tipo de comunicação é utilizado em aplicações em que a comunicação Real-time não é suficiente, como por exemplo, no controle de movimentos.

A Figura 2 apresenta a pilha de comunicação do protocolo Profinet segundo o modelo OSI.

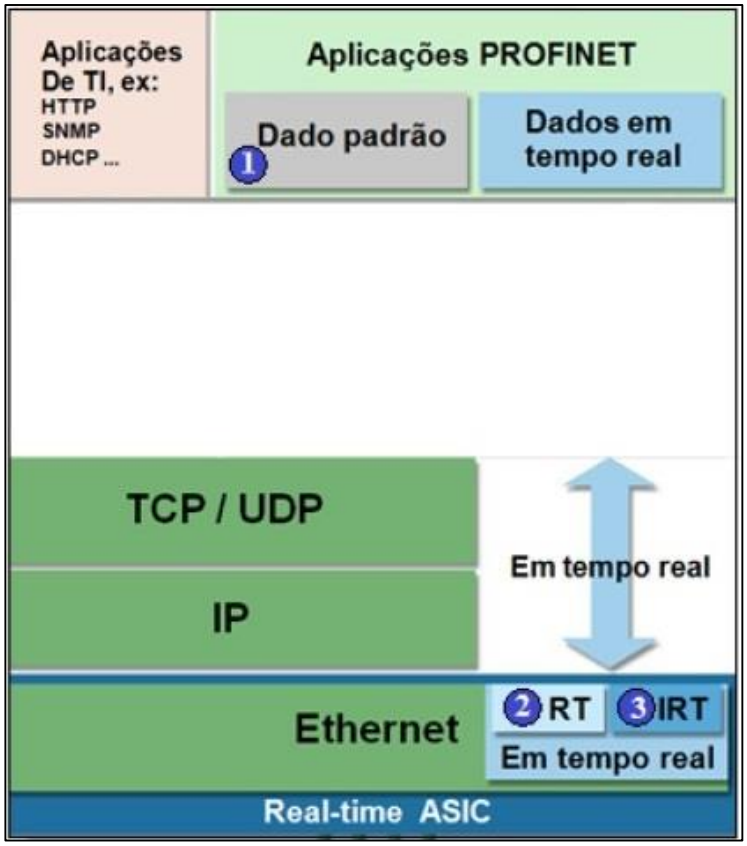


Figura 2: Pilha de comunicação do protocolo Profinet segundo o modelo OSI

Fonte: [9]

A Figura 3 apresenta diferentes aplicações para os três tipos de comunicação apresentados anteriormente.

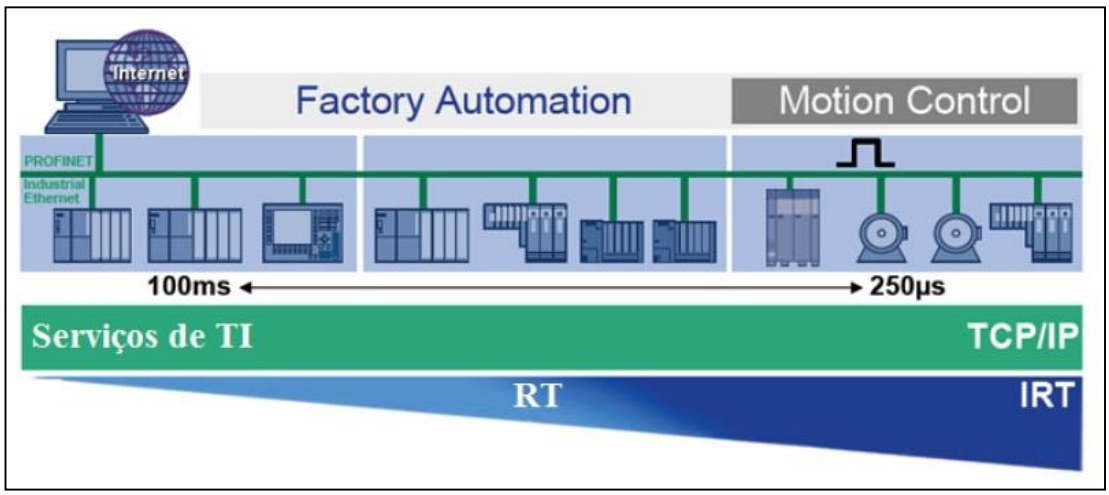


Figura 3: Os três modelos de comunicação

Fonte: [10]

2.4 Inicialização da rede

Na fase de inicialização de uma rede Profinet o IO-Controller deverá configurar todos os IO-Devices, tornando possível a comunicação entre eles [9]. Todo este processo de configuração ocorre da seguinte maneira: Primeiramente o IO-Controller deve receber informações sobre a configuração da rede enviada por uma ferramenta de engenharia (um software, por exemplo) bem como os arquivos GSD com informações relativas a cada dispositivo conectado à rede. Quando todos estes dados forem carregados, o IO-Controller irá checar e atribuir um endereço para cada um dos dispositivos que lhe foram apresentados [3].

O Profinet define três tipos de endereço para cada dispositivo da rede. O primeiro deles é o chamado MAC *address.* Este é um endereço único atribuído ao hardware do *device*, que não pode ser alterado. O quadro Ethernet demanda o MAC *address* do *device* que enviou a mensagem e do que vai recebê-la [10].

O segundo tipo de endereço é o chamado endereço IP. Este endereço é constituído de 32 bits, muitas vezes representado na forma decimal por quatro números separados por um ponto. Cada dispositivo da rede deve ter um endereço IP único.

O terceiro e último tipo de endereçamento utilizado pelo Profinet é através de um nome único, assim na fase de projeto da rede via software de configuração do CLP, deve ser definido um nome único para cada um dos dispositivos da rede.

Realizados todos os endereçamentos e configurações iniciais, a rede já está pronta para iniciar a troca de dados. Neste momento o IO-Controller irá criar o chamado Application *Relation* (AR) com cada um dos IO-Devices. Cada AR significa uma conexão lógica, necessária para que ocorra a troca de dados entre dois dispositivos. Dentro de uma AR define-se diferentes canais que irão diferenciar os tipos de comunicação existentes naquela AR. Estes canais são os chamados *Communication Relations* (CR) [9, 11]. Existem diferentes tipos de CRs, que são:

- ✓ IO Data CR: trafegam dados do processo, dados cíclicos trocados entre IO-Controller e IO-Device, sem que ocorra confirmação. Os intervalos de transmissão são definidos através de ferramentas de engenharia no momento de projeto da rede.
- ✓ Record Data CR: trafegam dados de configuração e outros dados acíclicos, como por exemplo, dados para definir parâmetros dos IO-Devices e ler mensagens de status.

- ✓ Alarm CR: trafegam dados de alarme em tempo real, que podem ser de dois tipos: definidos por sistema ou por usuário. É possível realizar a priorização de alarmes.

A Figura 4 apresenta uma AR estabelecida entre IO-Controller e IO-Device e também os três diferentes tipos de CRs existentes dentro de uma AR.

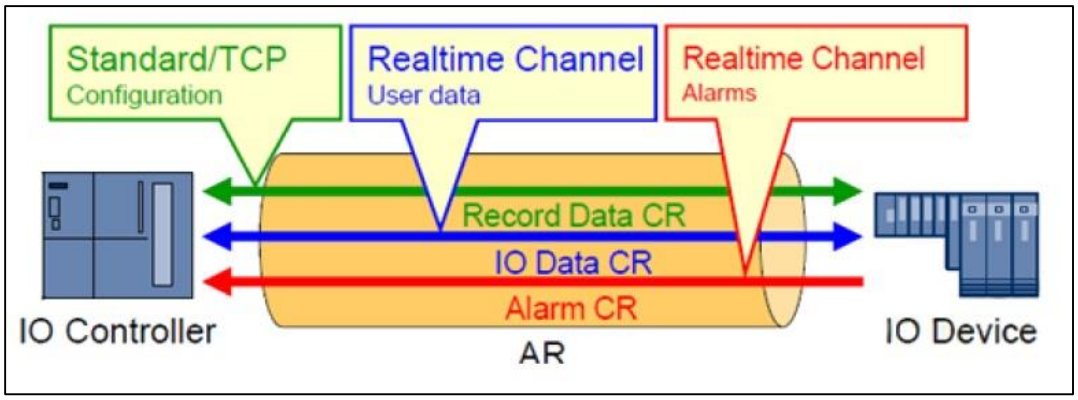


Figura 4: *Application Relation* entre IO-Controller e IO-Device
Fonte: [11]

Quando todos os IO-Devices são configurados e parametrizados pelo IO-Controller, a rede passa a trocar dados de forma cíclica entre seus módulos. [12]

2.5 Topologia

O Profinet permite diferentes opções no que diz respeito à topologia, isto é, no modo em que os equipamentos estão conectados. As topologias são:

- ✓ Linha: É a topologia mais conhecida no mundo da automação industrial em que todos os dispositivos estão conectados em série, como num barramento. Esta topologia apresenta como vantagem sua simplicidade e facilidade de instalação. Entretanto é extremamente vulnerável, pois se uma conexão falhar, todos os dispositivos seguintes a falha perderam sua comunicação. A Figura 5 apresenta a topologia em linha. Os dispositivos Profinet que possuem um switch interno facilitam o uso desta aplicação. Esta topologia é utilizada preferencialmente para conectar sistemas distantes.

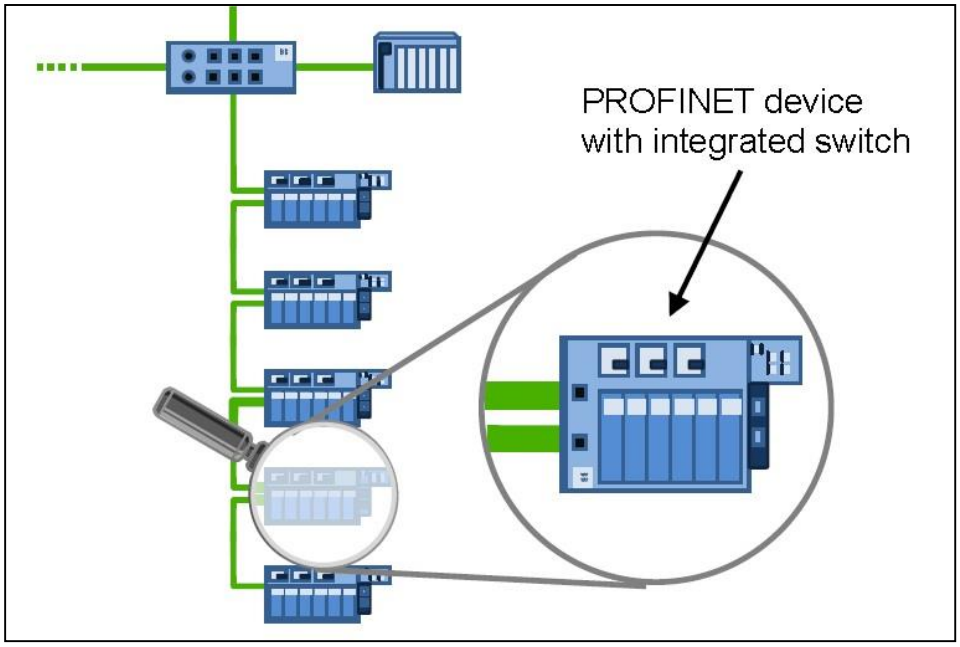


Figura 5: Topologia linha

Fonte [12]

- ✓ Estrela: Neste tipo de topologia existe um switch central que irá distribuir o sinal para cada elemento da rede. Para esta topologia se um único nó de comunicação falhar ou for removido, os outros nós irão continuar operando normalmente. Entretanto, se o switch central falhar, a comunicação de todos os dispositivos conectados será interrompida. A Figura 6 apresenta a topologia estrela. Esta topologia é utilizada em áreas com alta densidade de dispositivos e com extensões geométricas limitadas.

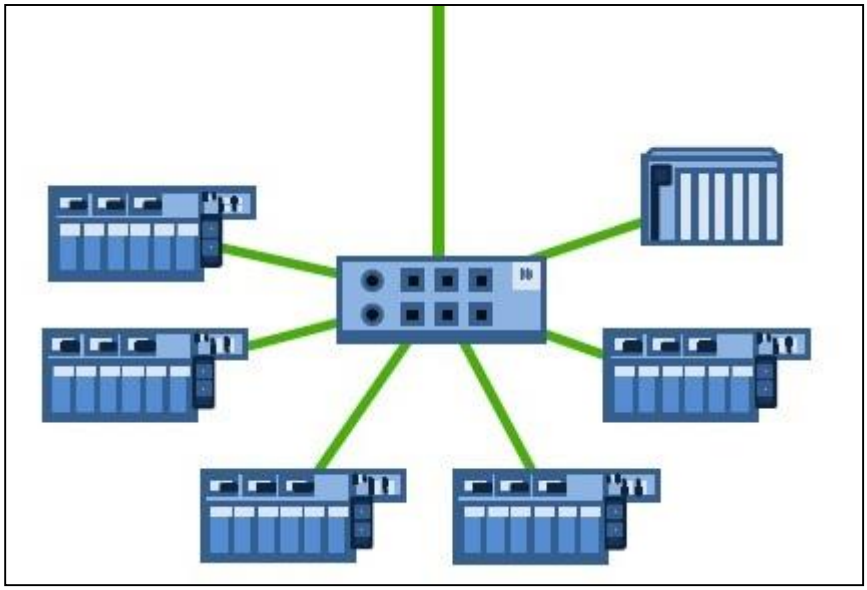


Figura 6: Topologia estrela

Fonte [12]

- ✓ Árvore: Esta topologia é a conexão entre várias topologias do tipo estrela. É utilizada quando um sistema complexo é dividido em subsistemas menores, por exemplo, uma planta de automação sendo dividida em diferentes ilhas de manufatura. A Figura 7 apresenta a topologia árvore.

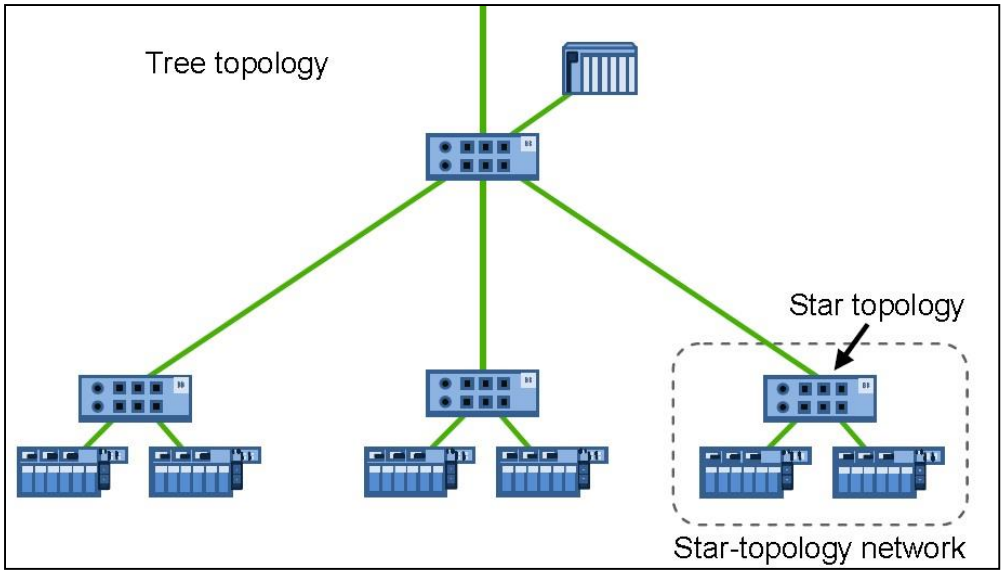


Figura 7: Topologia árvore

Fonte [12]

- ✓ Anel: É a conexão entre as duas extremidades da topologia tipo linha. Esta é uma topologia redundante, que protege a rede caso uma conexão for interrompida, isto é, caso o anel apresentar falha em uma de suas conexões, a rede passa a utilizar o caminho físico redundante como alternativa para que a comunicação permaneça como anteriormente. A Figura 8 apresenta uma rede em anel. As redes em anel serão estudadas com maior riqueza de detalhes no capítulo Redundância.

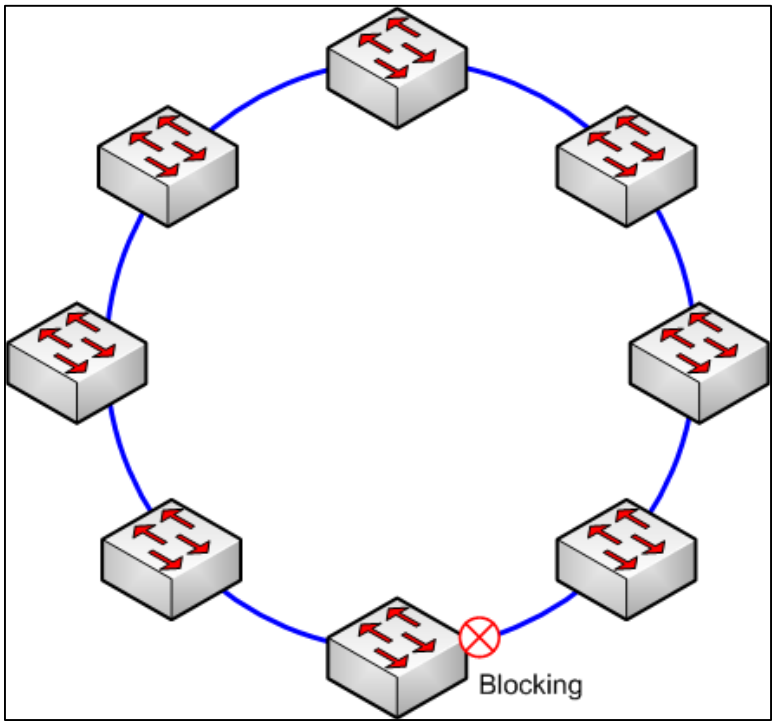


Figura 8: Topologia anel

2.6 Switch

O switch é um dispositivo que desempenha papel fundamental nas redes industriais. Além de conectar todos os dispositivos da rede, realizando a ponte entre o IO-Controller e os IO-Devices, os switches têm a capacidade de evitar colisões entre dados, devido ao fato de que eles são responsáveis pelo roteamento do tráfego na rede.

Os switches utilizados no Profinet são de 100Mbits/s e operam em full duplex [6]. Os dois principais tipos de switches são:

- ✓ *Cut-trought*: este é o modelo mais empregado no meio industrial. O switch *Cut-trought* realiza a checagem de apenas os 6 primeiros bytes da mensagem, que correspondem ao MAC *address* de destino. Assim o atraso entre a emissão e recepção é reduzido, tornando a comunicação praticamente sem atrasos. Em contrapartida, este switch não realiza a checagem de erros em todas as mensagens [8].
- ✓ *Store-and-forward*: Este modelo diferentemente do *Cut-trought* examina todos os dados antes de enviá-los, acrescentando um atraso maior na transmissão dos dados, porém aumentando a confiabilidade [6].

Os switches podem ainda estar integrados aos dispositivos ou mesmo independentes. A Figura 9 apresenta destacado em vermelho um switch integrado. [10]

Figura 9: Switch integrado ao dispositivo

Fonte: [10]

2.7 Classes de Conformidade

Os componentes do Profinet são divididos em três classes distintas chamadas de Classe de Conformidade. Cada uma dessas classes apresenta características e funcionalidades que a diferem das outras. Entretanto vale ressaltar que todas as três classes abrangem as funções básicas exigidas pelo protocolo Profinet. O objetivo da diferenciação de classes é o de facilitar o projeto das redes ao agrupar dispositivos de

características similares. As três classes que formam as Classe de Conformidade são: Classe de Conformidade A (CC-A), Classe de Conformidade B (CC-B) e a Classe de Conformidade (CC-C) [6,13]. Cada classe de comunicação contém todas as funções que a classe anterior a ela mais funções adicionais, como apresentado na Figura 10:

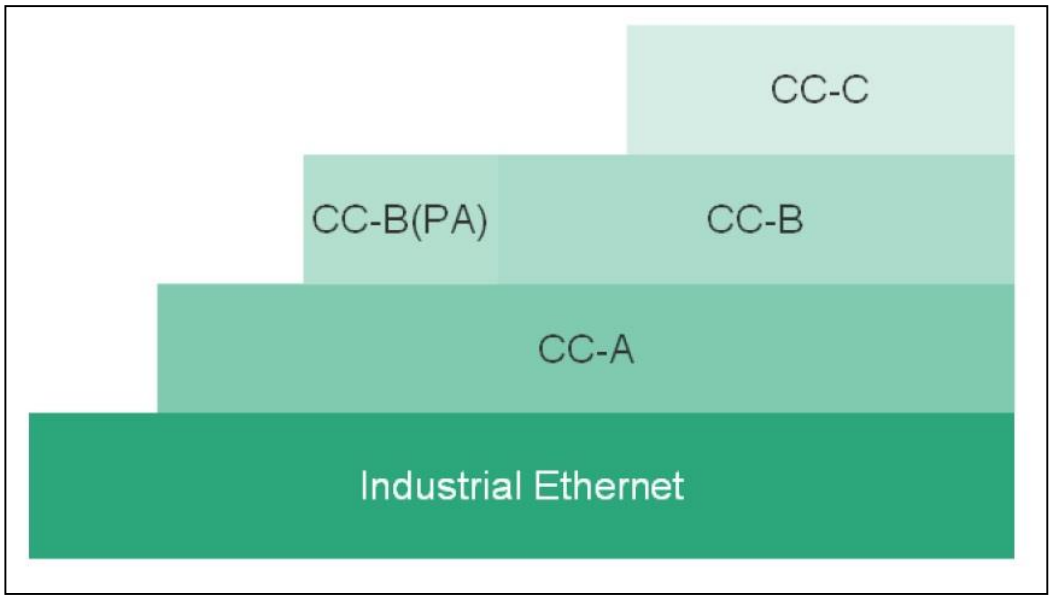


Figura 10: Hierarquia das Classe de Conformidade
Fonte [15]

Classe de Conformidade A: A mais básica das três classes. Utiliza a própria infraestrutura da rede Ethernet já existente, sem a necessidade de certificações [14]. A CC-A prove as funções básicas do Profinet com comunicação RT [15].

Classe de Conformidade B: Contém todas as características da CC-A além de utilizar o protocolo TCP/IP pra integrar a segurança dos dados. Esta classe permite a reposição de dispositivos da rede sem a necessidade de uma ferramenta de engenharia [14]. O sistema de redundância, tão importante para os processos de automação, é contido em uma versão estendida do CC-B, chamada de CC-B (PA) [15].

Classe de Conformidade C: Contém todas as funcionalidades da CC-B, além de possuir alta precisão e determinismo na transmissão de dados, sendo indicada para aplicações como sincronismo de motores [12]. Esta classe é a que apresenta melhor performance entre as três CC e é a base para a comunicação IRT [13, 15].

A Figura 11 apresenta um resumo das principais características de cada classe.

	CC-A	CC-B	CC-C
Funções Básicas	• Profinet com comunicação RT • Entradas e saídas cíclicas • Parâmentros • Alarmes • Informação da topologia (LLDP)	• Profinet com comunicação RT • Entradas e saídas cíclicas • Parâmentros • Alarmes • Informação da topologia (LLDP) • Diagnóstico da rede via IP (SNMP) • Informação da topologia com LLDP-MIB • Redundância	• Profinet com comunicação RT • Entradas e saídas cíclicas • Parâmentros • Alarmes • Informação da topologia (LLDP) • Diagnóstico da rede via IP (SNMP) • Informação da topologia com LLDP-MIB • Redundância • Sincronização de Hardware

Figura 11: Resumo das principais características de cada CC

Fonte: Adaptado de [15]

Uma grande vantagem do Profinet é a capacidade de combinar as *Classe de Conformidade*. Todas as três classes podem ser integradas dentro de um sistema como apresentado na Figura 12 [15].

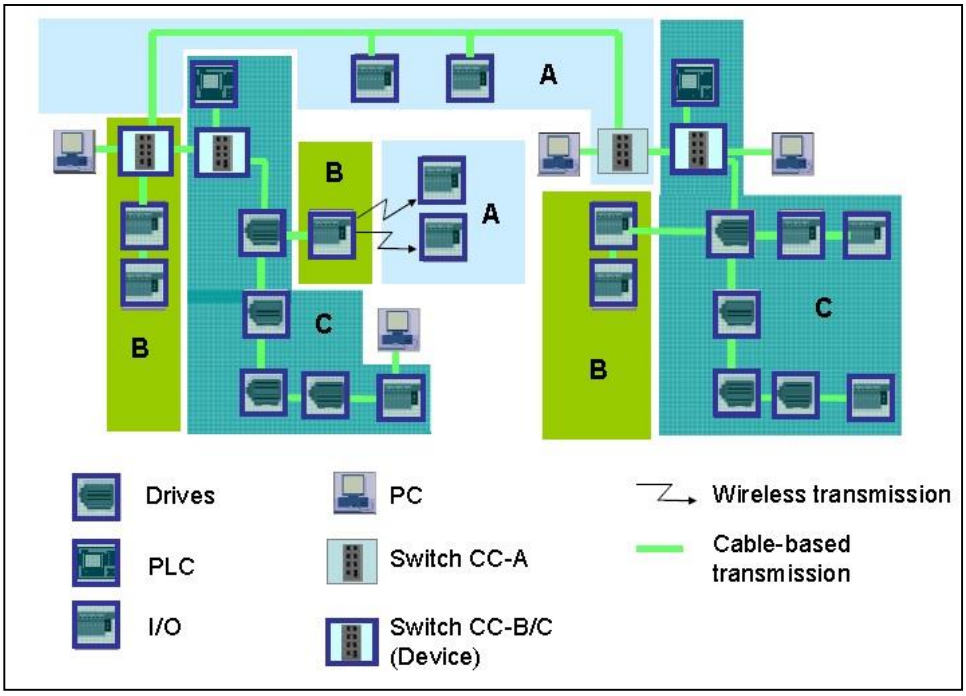


Figura 12: Sistema com diferentes *Classe de Conformidade*

Fonte: [15]

Em particular nas comunicações *real-time* (RT) e *isochronous real-time* (IRT) existe uma classificação que diz respeito ao grau de determinismo:

- ✓ RT_Class 1: utilizada em sistemas de automação que requerem ciclo de tempo cerca de 10ms e *jitter* na ordem de poucos milissegundos. Representa comunicação RT.
- ✓ RT_Class 2: utilizada em aplicações que exigem tempo de ciclo menores do que 10ms.
- ✓ RT_Class 3: são usados quando as aplicações requerem um tempo de cerca de 250µs até 4ms e com baixíssimo *jitter*, na ordem de 1µs. É importante salientar que RT_Class 3 requer uma topologia de rede robusta, bem como switches especiais. Mais detalhes sobre a comunicação IRT nas referências [8, 16].

2.8 Aspectos de temporização

Duas importantes variáveis temporais em redes Profinet são o tempo de ciclo e o valor de *watchdog*. Ambos podem ser definidos no momento de projeto e a escolha de seus valores é de extrema importância para o desempenho da rede.

O tempo de ciclo se refere às taxas de atualização que são enviados pacotes de um dispositivo para a rede. Ele é definido em cima de outras duas variáveis chamadas de *sendclock* e *Reduction Ratio*. O *sendclock* é o intervalo de tempo comum em um tempo de ciclo e o *Reduction Ratio* irá indicar a quantidade de intervalos de *sendclock* o dispositivo deverá esperar para enviar seus dados ciclicamente [17].

Já o valor de *watchdog* corresponde ao tempo utilizado para controlar o recebimento correto de dados. Segundo [18] o tempo de *watchdog* de um dispositivo pode ser calculado pela Equação 1:

$$Watchdog = WatchdogFactor\ x\ Tempo\ de\ ciclo \quad (1)$$

Em que o *WatchdogFactor* é definido como sendo o número de mensagens consecutivas não recebida pelo dispositivo. Assim se o tempo de ciclo for de 10 milissegundos e um dispositivo tolerar ficar sem receber até 10 mensagens consecutivas, o valor do tempo de *watchdog* será de 100 milissegundos.

A troca de dados no Profinet é baseada em um repetitivo ciclo como descrito na IEC61158-5-10 e ilustrado na Figura 13. A mensagem de sincronização indica o início do ciclo, que então é seguido de 4 fases que são:

- ✓ VERMELHA: Durante esta fase apenas mensagens da RT_Class 3 são enviadas. Outros tipos de tráfegos, por exemplo, TCP/IP, são bloqueados dentro dos *switches buffers*. Neste momento todos os dispositivos sabem quando e em qual porta física eles estão autorizados para se comunicar.
- ✓ LARANJA: Nesta fase apenas mensagem do tipo RT_Class 2 são enviadas, entretanto nesta fase não está definido qual porta física que o dispositivo irá trocar dados, portanto é usado roteamento com base nos endereços MAC dos dispositivos.
- ✓ VERDE: Nesta fase são enviados mensagens do tipo RT_Classe 2, RT_Classe 1 e todos os restantes frames Non Real-Time (NRT), como frames TCP/IP e UDP/IP. Os frames são transmitidos e roteados de acordo

com a prioridade Ethernet. As mensagens do tipo NRT enviam grande quantidade de dados, ocupando no mínimo 40% da largura de banda.

- ✓ AMARELA: Esta é uma fase de transição utilizada para o mesmo tipo de tráfego que ocorre na fase VERDE. Apenas os frames que podem ser completamente enviados nessa fase são enviados [16,19].

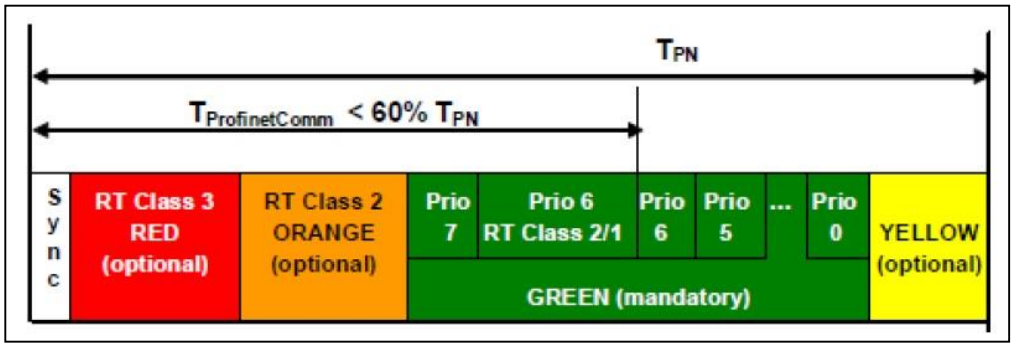


Figura 13: Fases do ciclo de comunicação do Profinet

Fonte [19]

2.9 Redundância

Um importante requisito no mundo de automação industrial é a disponibilidade do sistema de controle, o que infere diretamente na disponibilidade da comunicação da rede. Dentre as diversas possibilidades para elevar a disponibilidade de comunicação de uma rede de automação industrial, a mais simples delas é através da introdução da redundância. Assim na IEC 62439 foram propostos quatro diferentes protocolos como solução para redundância: [20]

- ✓ *Media Redundancy Protocol* (MRP)
- ✓ *Parallel Redundancy Protocol* (PRP)
- ✓ *Cross-network Redundancy Protocol* (CRP)
- ✓ *Beacon Redundancy Protocol* (BRP)

Neste trabalho será estudado o MRP que é baseado em topologias do tipo anel. O MRP é o sucessor do HiPER Ring Protocol (criado pela Hirschmann e Siemens em 1999, foi o primeiro protocolo de redundância de topologia anel para redes baseadas em Ethernet) e foi proposto em 2005, para então ser padronizado pela IEC 62439. Diferentemente do seu antecessor que apresentava um tempo de recuperação de 500 milissegundos, buscava-se um protocolo simples, fácil de implementar em redes já

existentes e capaz de recuperar a rede em um tempo de no máximo 200 milissegundos caso ocorresse uma ruptura no anel [20, 21].

O *Media Redundancy Protocol* é baseado na segunda camada do modelo OSI, apresentada na Figura 14 [20]. Além disso, vale ressaltar que o MRP é aplicado na *Conformance Classe* B do protocolo Profinet. Caso seja necessário aplicação de redundância em redes do tipo CC-C um protocolo mais avançado, chamado de *Media Redundancy for Planned Duplication* (MRPD), deve ser aplicado [21].

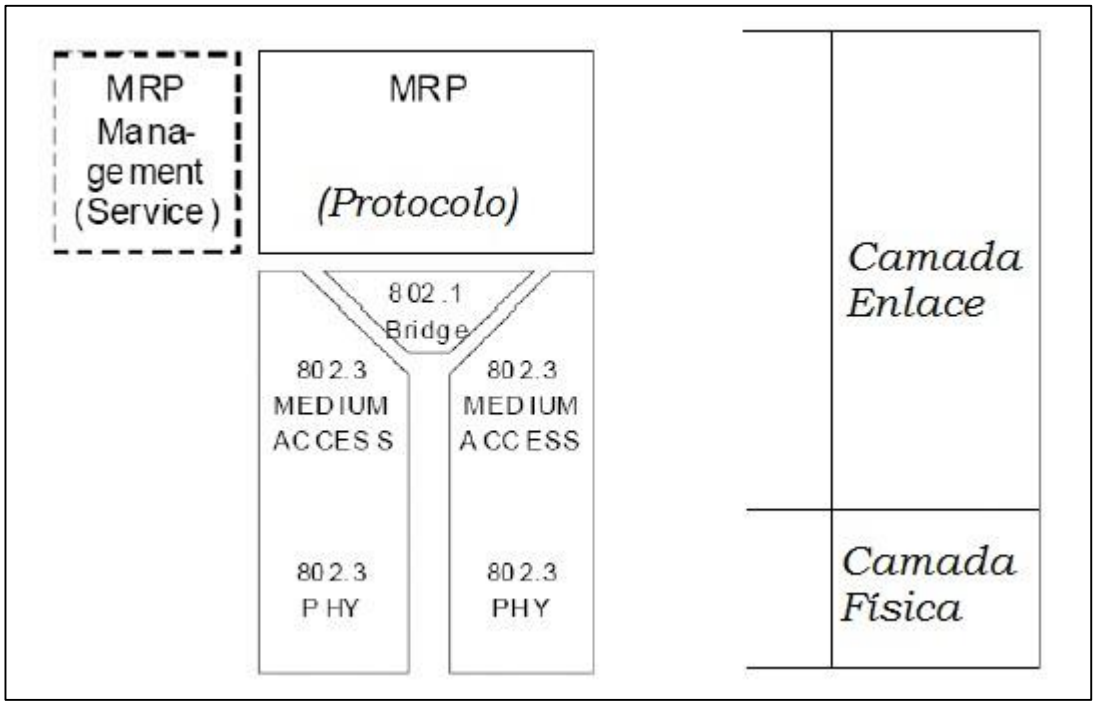


Figura 14: MRP no modelo OSI

Fonte: [21]

A Figura 15 mostra um anel com um único domínio MRP. Uma rede Profinet pode conter diferentes domínios, desde que os mesmos não se sobreponham. Um domínio da rede deve conter um swtich que realize o papel de *Media Redundancy Manager* (MRM) e um ou mais switches que realizem o papel de *Media Redundancy Clients* (MRCs). Cada um dos switches contém duas portas conectadas ao anel, que são chamadas de *ring ports*. As *ring ports* são definidas no momento de configuração da rede, entretanto em alguns dispositivos já existem portas especificas para exercerem esta função [21].

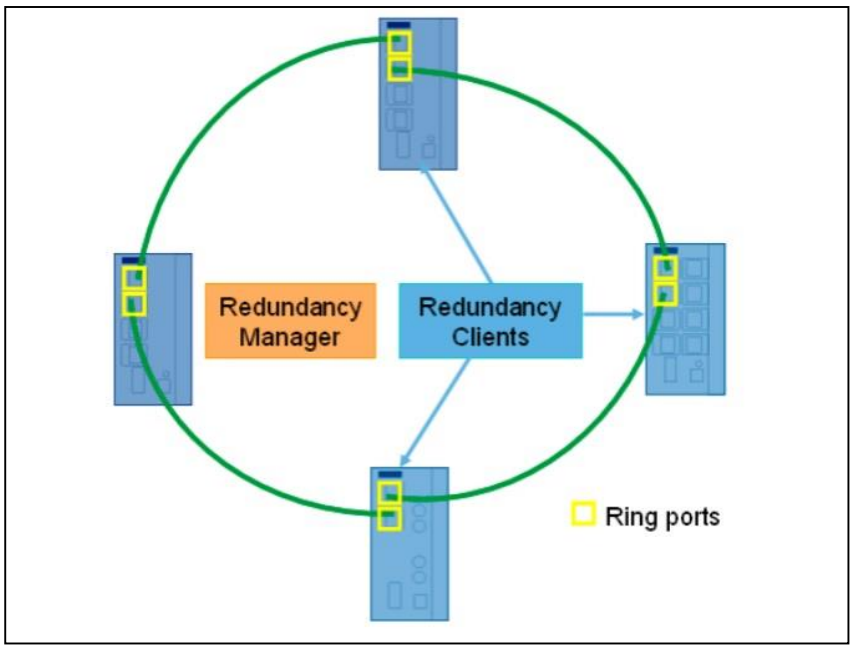


Figura 15: Ring Ports

As portas conectadas ao anel podem apresentar três diferentes status, que são:

- ✓ *Disable*: Porta desabilitada, bloqueia todo o tráfego de dados.
- ✓ *Blocked*: Porta bloqueada, bloqueia todo o tráfego de dados exceto os frames de controle MRP e outros como os frames LLDP (*Link Layer Protocol*)
- ✓ *Forwarding*: Porta liberada, permite a passagem de todos os tipos de frames.

Portanto observa-se na Figura 16 que todas as portas apresentam o status *Forwarding*, exceto a porta do MRM conectada ao MRC_3, cujo status é *Blocked*. A rede nesta situação é chamada de Anel Fechado.

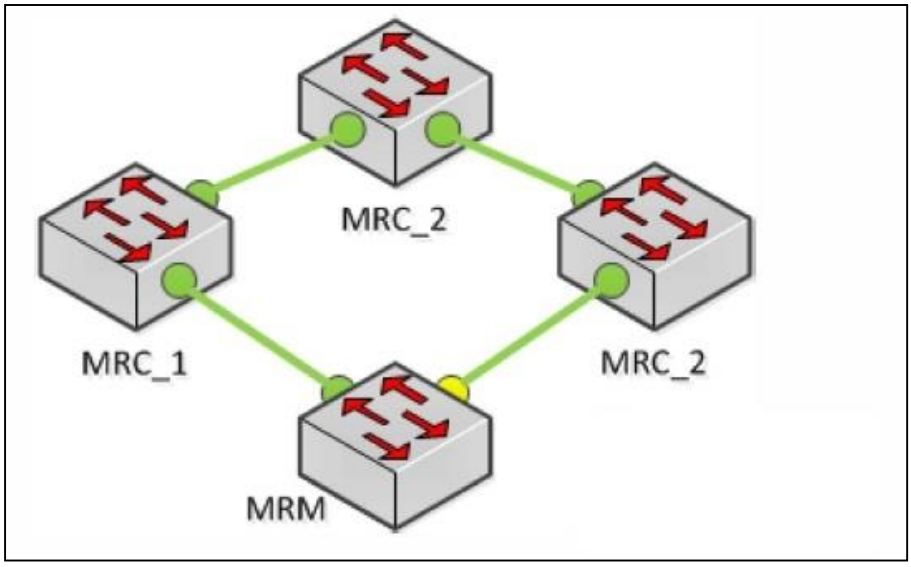


Figura 16: Anel Fechado

Fonte: [20]

No caso em que uma conexão entre os switches falhar, é de responsabilidade do MRM mudar o status da porta *Blocked* para *Forwarding*, e então lidar com a falha. As portas ao lado da ruptura também sofrem uma alteração de status, tornando-se portas do tipo *Disable,* como apresentado na Figura 17. Neste instante a rede é chamada de Anel Aberto e esta transição recebe o nome de *swicht-over* [21].

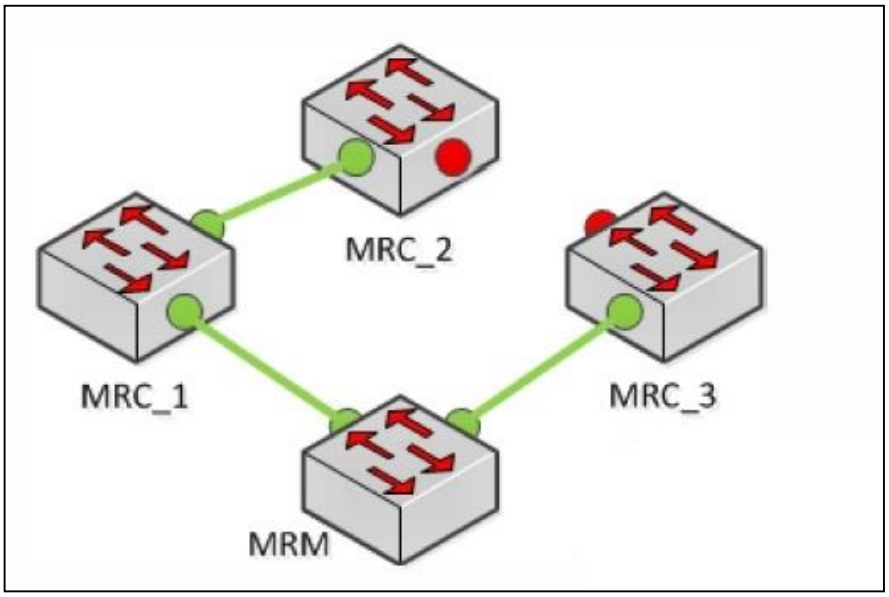


Figura 17: Anel Aberto

Fonte: [20]

O processo para detecção de falha na rede MRP ocorre da seguinte maneira: Enquanto a rede está trabalhando no modo anel fechado, o MRM irá enviar constantemente os chamados *test frames*. Estes são um tipo de frame de controle enviado para todos os MRCs da rede. Os *test frames* são enviados pelo MRM em ambas as portas (*Forwarding* e *Blocked*) a cada tempo pré-definido, chamado de *TSTdefault* (indicado ser 20 milissegundos). O tempo para que o MRM receba de volta os frames de controle é medido e definido como *TestTimer*. Se os *test frames* não retornarem depois de passado o *TestTimer*, o MRM incrementa um contador interno (*TestCounter*). Se o contador alcançar certo valor pré-determinado, definido como *TSTNRmax* (tipicamente 3 ou 5), MRM declara uma falha na rede. No caso dos frames retornarem a tempo o *TestCounter* é zerado novamente [20, 21].

Portanto, de acordo com [20], o tempo para detecção de falha no anel é de:

$$T_{detecção} = TST_{default}\, x\, TSTNR_{máx} \quad (2)$$

Por fim, o tempo de recuperação de uma rede em anel é o tempo gasto para que a rede detecte a falha, e que o MRM mande mensagens do tipo *TopologyChange* para todos os MRCs, para que então a rede se adapte e volte a trocar dados como anteriormente. De acordo com IEC 62439, o tempo limite para uma rede MRP se recuperar é de 200 milissegundos. Este valor inclui estimações pessimistas, pois na prática este tempo deve apresentar uma desempenho bem melhor.

Para a configuração do anel deve-se levar em consideração os seguintes itens:

- ✓ MRP é suportado para uma topologia anel com até 50 dispositivos;
- ✓ O anel deve ser composto de apenas dispositivos que suportem o MRP;
- ✓ Os dispositivos devem ser ligados aos outros através de suas *ring ports*;
- ✓ Todos os dispositivos dentro do anel devem ser membros do mesmo domínio de redundância.

2.10 Indicadores de desempenho

Para especificar o desempenho da rede Profinet a norma IEC 61784-2 define nove indicadores de desempenho. Os indicadores de desempenho que são aplicáveis ao Profinet são:

- *Delivery time:* intervalo de tempo que um dado leva desde o momento que é enviado por um dispositivo até o momento que é recebido por outro dispositivo.
- *Number of RTE end-stations:* Número máximo de dispositivos que um protocolo RTE suporta. Não consideram-se as switches neste cálculo.
- *Time synchronization accuracy:* Máximo desvio entre quaisquer dois clocks de dispositivos.
- *Throughput RTE:* Total de dados RTE em bytes em um ponto da rede por segundos.
- *Non-RTE bandwidth:* Porcentagem da largura de banda que pode ser utilizada pela comunicação non-RTE em um ponto da rede.
- *Redundancy recovery time:* tempo máximo do período da falha até tornar-se totalmente operacional.
- *Basic network topology:*A topologia de rede que um protocolo RTE suporta deve ser uma ou a combinação das topologias: estrela, anel ou barramento
- *Nunber of switches between RTE end-stations:* Número de switches entre dois dispositivos que tenham uma AR [18, 22].

Os indicadores de desempenho apresentados não são independentes um do outro. A Figura 18 ilustra mostra as relações entre cada um dos indicadores.

INDICADORES DE DESEMPENHO		Indicador Influente							
		Delivery Time	*Number of RTE end-stations*	*Basic network topology*	*Number of switches between RTE end-stations*	*Throughput RTE*	*Non-RTE bandwidth*	Time synchronization accuracy	Redundancy recovery time
Indicador dependente	*Delivery Time*		Não	Não	Sim	Não	Não	Sim	Sim
	Number of RTE end-stations	Não		Sim	Sim	Não	Não	Sim	Sim
	Basic network topology	Não	Não		Não	Não	Não	Sim	Sim
	Number of switches between RTE end-stations	Sim	Sim	Sim		Não	Não	Sim	Sim
	Throughput RTE	Sim	Sim	Sim	Sim		Sim	Sim	Sim
	Non-RTE bandwidth	Não	Não	Não	Não	Sim		Sim	Sim
	Time synchronization accuracy	Não	Não	Não	Sim	Não	Não		Não
	Redundancy recovery time	Não	Não	Sim	Sim	Não	Não	Não	

Figura 18: Relação entre os indicadores de desempenho de uma rede Profinet

Fonte: Adaptado de [10]

Identifica-se na Figura 18 que um dos indicadores de desempenho é o *Redundancy Recovery Time*, isto é, o tempo de Recuperação da rede que será estudado

neste trabalho. Além disso, observa-se que este indicador apresenta duas dependências que são: a topologia básica da rede e o número de switches entre duas estações.

3. Estudo do caso

O objetivo deste capítulo é verificar na prática alguns aspectos referentes à teoria apresentada. Dada uma rede em anel, deseja-se estudar o comportamento da rede quando o anel é rompido, encontrar os tempos de restabelecimento da comunicação, aqui chamado de tempo de recuperação, e analisar a influência que o *watchdog* e que o número de switches exercem nesses tempos. Para isso, foram realizados ensaios no Laboratório de Automação Industrial (LAI) a fim de obter resultados reais.

Desta forma, será apresentada a metodologia adotada, discriminando os equipamentos necessários para criar a rede, a topologia definida para realização das coletas, as práticas de coletas e análise dos dados para obtenção dos resultados. As análises pertinentes ao trabalho serão devidamente discutidas.

3.1 Descrição da rede

A rede estudada é composta pelos itens descritos pela Tabela 1.

Tabela 1: Descrição dos componentes da rede Profinet

Quantidade	Equipamento	Função
1	CPU S7 – 1200	IO Controller
1	Remota ET 200-S	IO Device
3	Switch Scalance X208	Switch
1	TAP EDS 2100	TAP Ethernet Industrial
1	Software TIA Portal	IO Supervisor

Os switches são próprios para aplicações de Ethernet Industrial do tipo gerenciável. Estes possuem oito portas elétricas RJ45 e suportam o protocolo MRP, utilizado em redes com topologia em anel.

A Figura 19 apresenta as conexões realizadas em laboratório entre os equipamentos descritos pela Tabela 1 para obter a topologia em anel. É importante salientar que neste estudo do caso o anel é formado único e exclusivamente pelos switches.

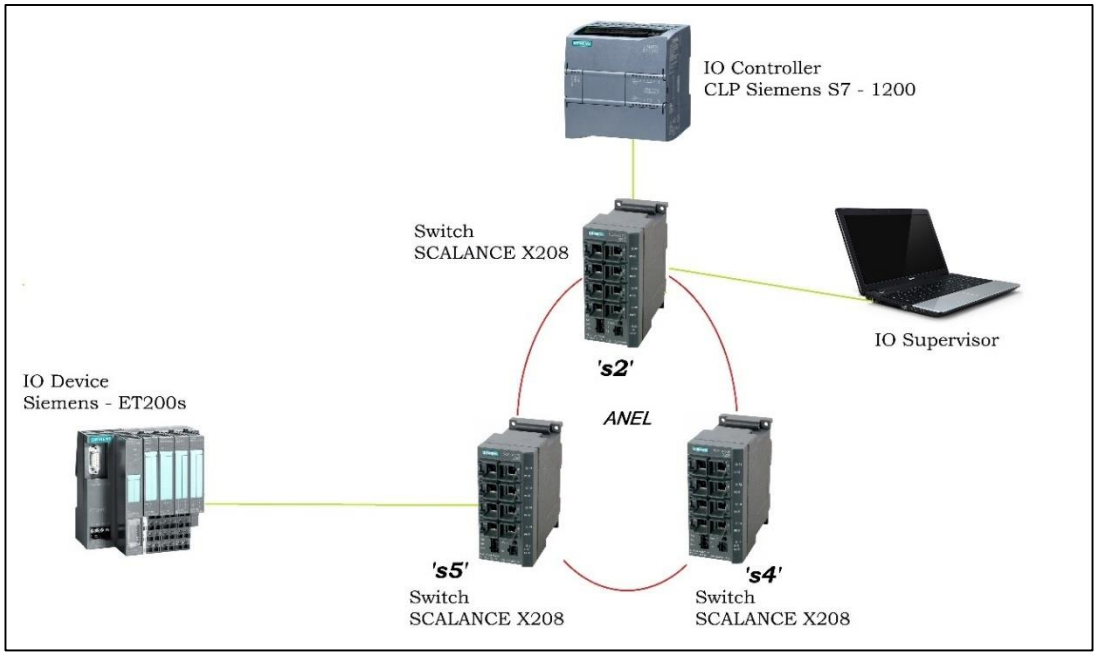


Figura 19: Topologia da rede

Como próxima etapa, dá-se o processo de configuração da rede e atribuição dos endereços (IP e nome) de todos os elementos no software TIA Portal V12 da Siemens. A Figura 20 apresenta os endereços MAC, IP e o nome de cada equipamento na rede.

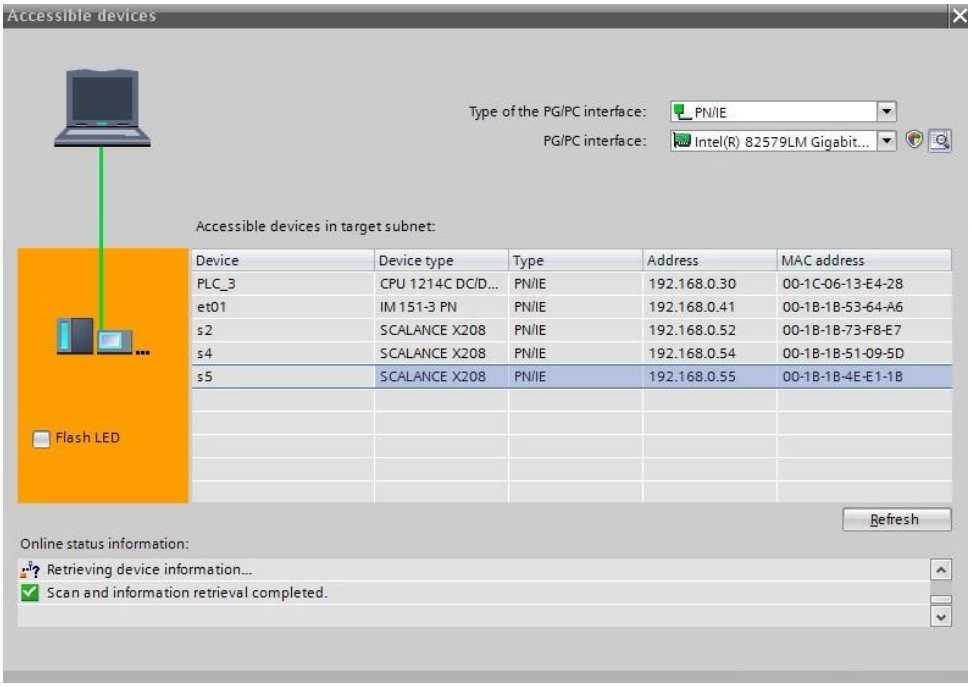


Figura 20: Endereçamento e nomes dos equipamentos da rede

Em relação ao anel criado entre os switches SCALANCE X208, foi definido como o *Media Redundancy Manager* (MRM) o switch de nome ‘s2’, e os switches ‘s4’ e ‘s5’ como os *Media Redundancy Clients* (MRCs). Além disso, para todos os switches foram definidas as portas 1 e 2 como as *ringports*. Todas as portas conectadas ao anel apresentam o status *Forwarding*, exceto a porta do switch s2, que se conecta ao switch s5, cujo status é *Blocked*. Neste instante a rede apresenta o status de Anel Fechado.

A captura de dados através de uma porta espelhada no switch é um possível método para a leitura dos pacotes que trafegam na rede. Este método consiste na duplicação ativa do pacote, isto é, o switch copia e direciona o tráfego da porta desejada para uma porta livre, denominada “espelho”. Esta forma de captura é uma estratégia simples e que apresenta um baixo custo, entretanto possui uma resolução de tempo na casa dos microssegundos, por sua vez, não é indicado para análises onde precisa-se ter precisão elevada de tempo, como é o caso do *jitter*.

Uma segunda maneira para a realização da captura de dados é através do TAP de Ethernet Industrial, modelo EDS2100 do fabricante Kunbus. Este é um dispositivo praticamente transparente para a rede que copia e direciona todos os pacotes de comunicação sem interferir no desempenho da comunicação, pois insere um tempo de atraso na ordem de 1 nanosegundo. Além disso, o modelo citado adiciona ao quadro transmitido 20 bytes que são relacionados a estampa de tempo, chegando assim, a precisão de nanossegundos.

Portanto sendo o TAP um equipamento de maior confiabilidade e melhor desempenho quando comparado a técnica da porta espelhada, optou-se pelo seu uso na coleta dos dados. Sua ligação na rede é realizada conforme a Figura 21, mais detalhes sobre essa ligação serão expostos mais adiante.

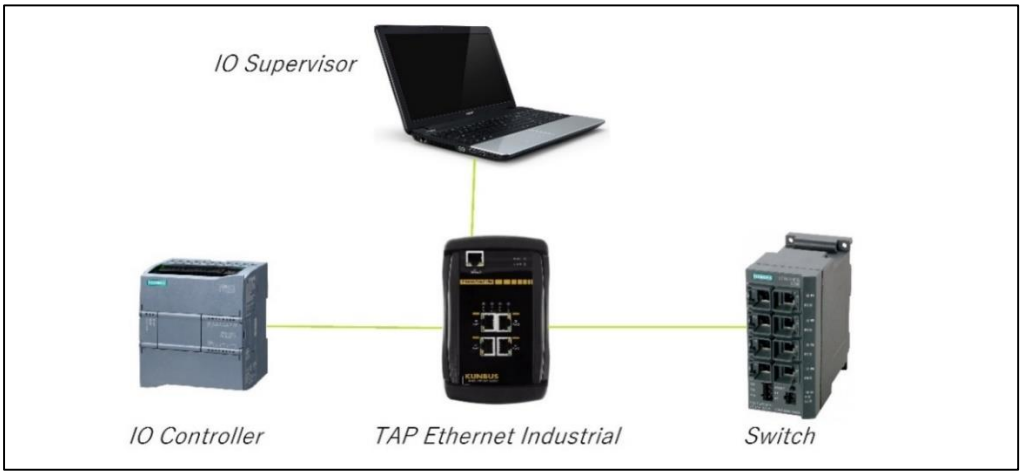


Figura 21: Ligações do TAP de Ethernet Industrial

A leitura e análise dos dados capturados foram realizadas via o software Wireshark. Este é um software livre que apresenta toda a comunicação que está sendo transmitida na rede de forma detalhada.

3.2 Metodologia e Resultados

3.2.1 Funcionamento da rede em anel

Com o objetivo inicial de estudar o comportamento da rede quando uma das ligações do anel é rompida, o TAP de Ethernet Industrial foi colocado entre o IO-Controller e o switch, conforme a Figura 22.

Tendo em vista que a comunicação Profinet é porta a porta, optou-se pela inserção do TAP no link ao qual pertence o IO-Controller, pois toda comunicação é direcionada ao controlador. Assim, é possível verificar todo o tráfego de dados existente. Se o TAP fosse inserido em outro link, a comunicação seria vista de forma parcial, ou seja, somente seria observada a comunicação dos dispositivos pertencentes a esse link e não da rede inteira.

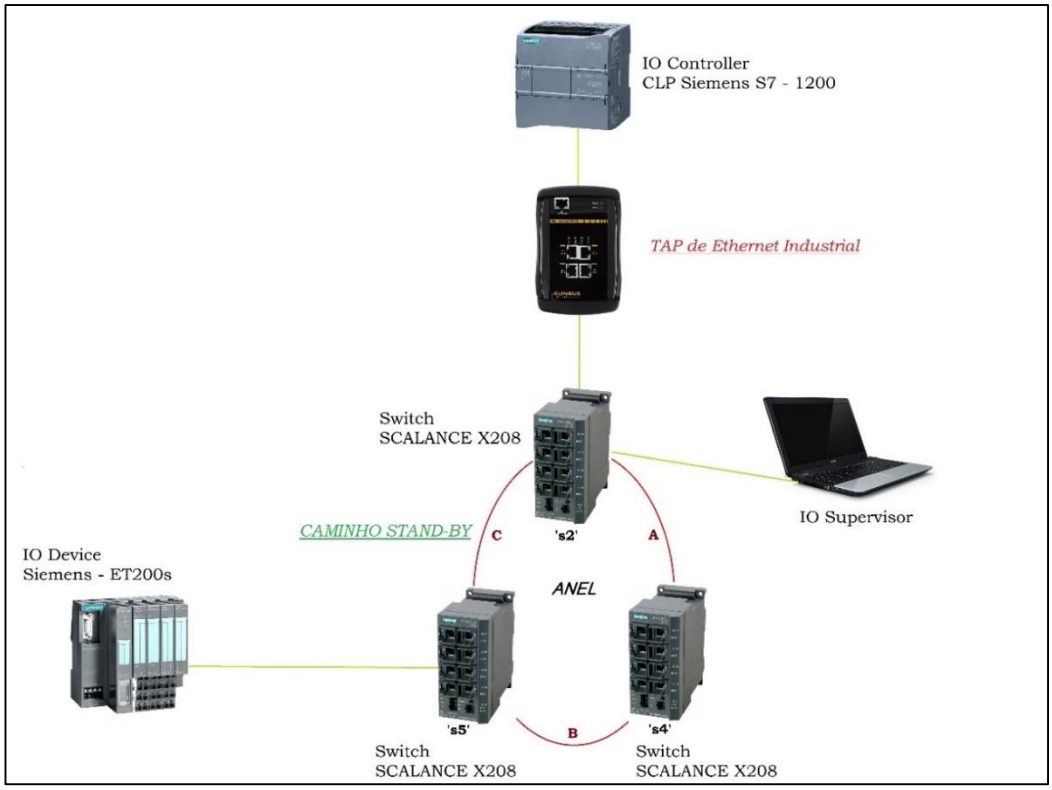


Figura 22: Topologia da rede com a inserção do TAP

A metodologia aqui aplicada consiste em retirar manualmente o cabo B realizando uma ruptura no anel entre os switches. A partir deste instante a rede é chamada de Anel Aberto. Após alguns segundos, o cabo B é reconectado a sua posição original, e a rede volta a ser um Anel Fechado. Em ambos os momentos a topologia da rede é alterada, tornando-se possível analisar o seu comportamento nestes instantes. No total foram realizadas 10 amostras para obter resultados reais.

Com o TAP na posição apresentada acima é possível através do software Wireshark verificar toda comunicação que o controlador realiza com o restante da rede. O gráfico apresentado na Figura 23, mostra no eixo da abscissa a unidade chamada de "*tick interval*" que representa a resolução do tempo decorrido, e no eixo das ordenadas a unidade "*packet/tick*" que representa a quantidade de pacotes que trafegaram na rede por unidade de tempo. No gráfico apresentado abaixo foi definido 100 milissegundos para a variável "*tick interval*". Assim pode-se ver a quantidade de pacotes trocados entre IO-Controller e outros equipamentos da rede versus o tempo. Para melhor entendimento o gráfico foi divido em três etapas como indicado abaixo.

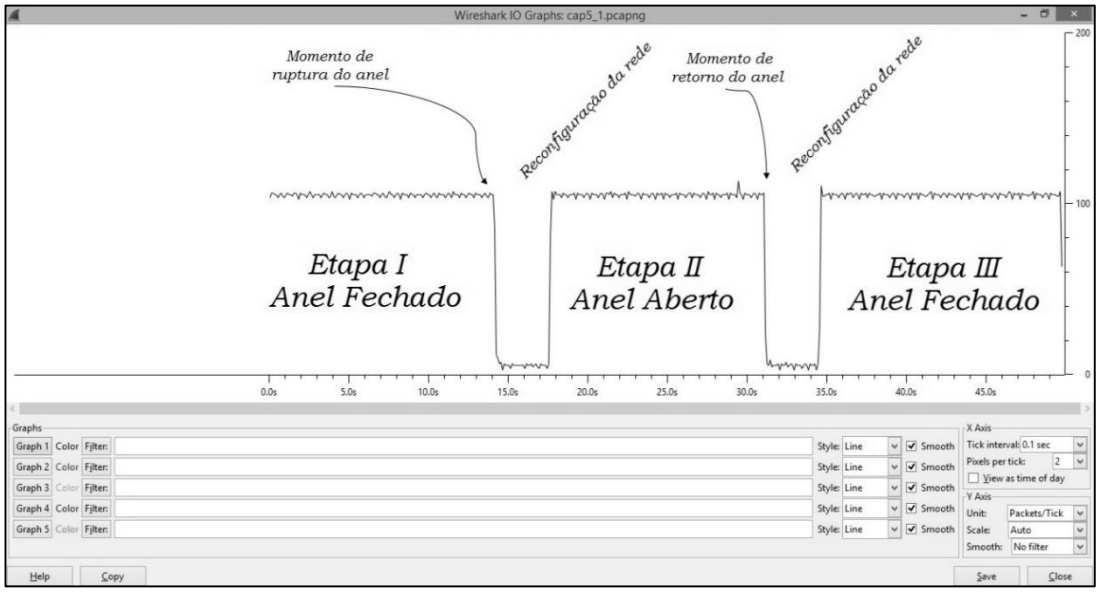


Figura 23: Quantidade de pacotes trocados entre IO-Controller e o restante da rede

A etapa I corresponde ao momento inicial de troca de dados da rede. Neste instante o anel está fechado e o fluxo de informação ocorre conforme indicam as setas na Figura 24, isto é, não trafegam dados PNIO pelo caminho *stand-by*. A etapa número II

representa os instantes após o rompimento e reconfiguração do anel. Neste período o anel está aberto e o fluxo de dados é representado pelas setas na Figura 25. É possível notar que estando o anel aberto, a rede passa a utilizar o caminho *stand-by* como meio para tráfego de dados PNIO. Por fim, a etapa III refere-se ao momento em que o anel é restabelecido e a rede é novamente configurada, a partir deste instante o anel está fechado e a rede deixa de utilizar o cabo *stand-by*. O tráfego de dados retorna ao caminho original conforme a Figura 24.

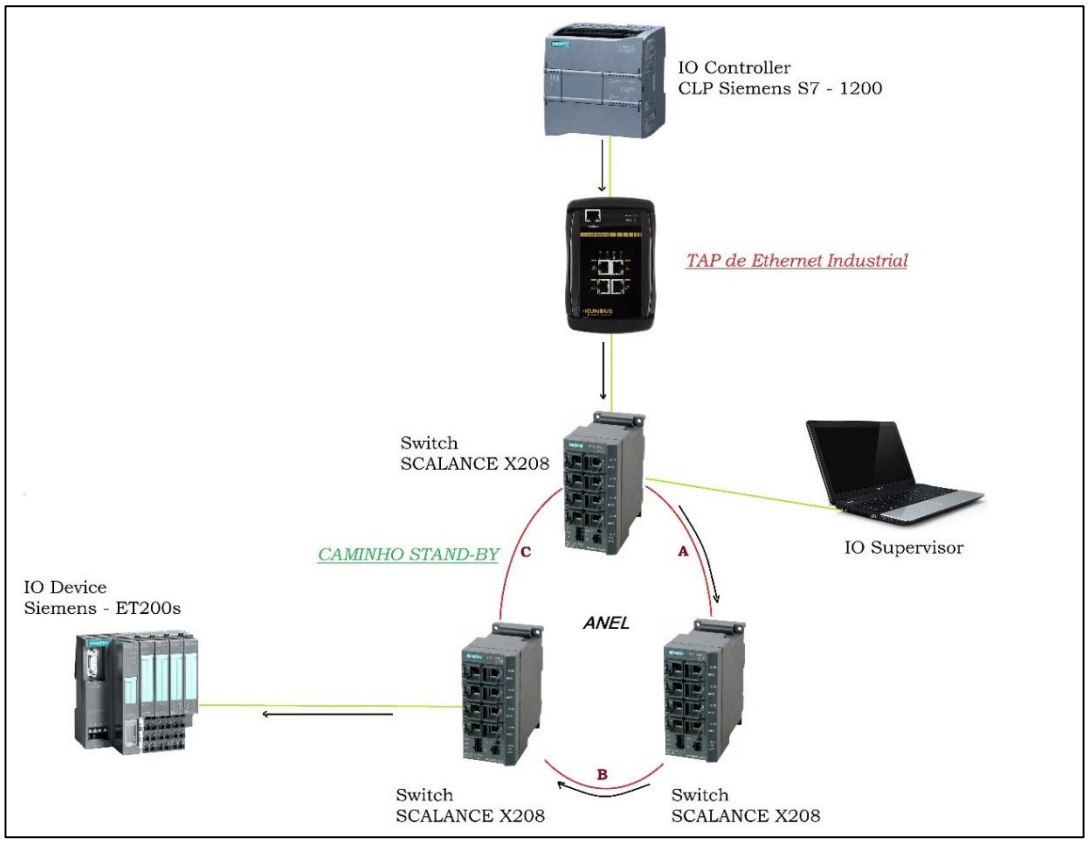


Figura 24: Caminho pelo qual os dados trafegam no anel fechado

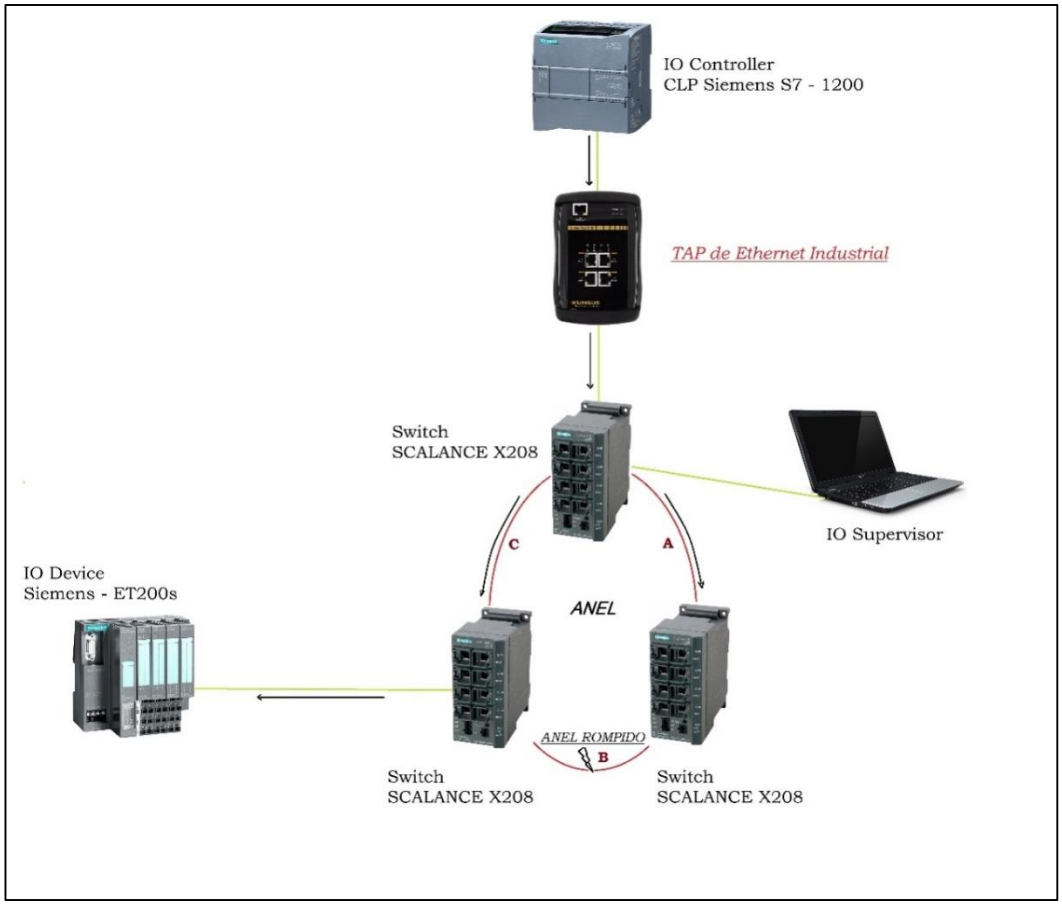


Figura 25: Caminho alternativo pelo qual os dados trafegam no anel aberto

Outra análise pode ser realizada em relação ao gráfico apresentado na Figura 23, se for definido a unidade "*bytes/tick*" para o eixo das ordenadas. Esta unidade representa a quantidade de *bytes* que trafegam na rede em determinado instante de tempo. Na Figura 26 foi definido para o eixo das abscissas o valor de "*tick interval*" de 100 milissegundos e para o eixo das ordenadas a unidade "*bytes/tick*". Pode-se notar um pico de na quantidade de *bytes* nos momentos finais de reconfiguração da rede. Este elevado número de *bytes* ocorre devido ao processo de inicialização do IO-Device.

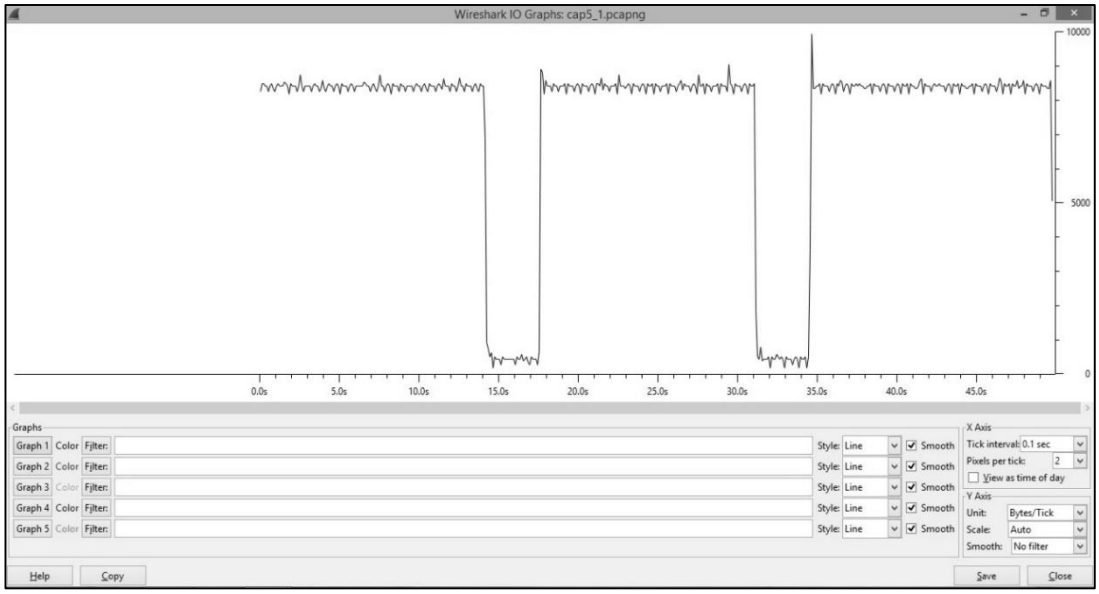


Figura 26: Quantidade de *bytes* trocados entre IO-Controller e o restante da rede

Ainda com relação a Figura 23 percebe-se claramente dois intervalos de tempo em que o número de pacotes que estão trafegando na rede sofrem uma brusca queda. A primeira queda, por volta de 14 segundos, se refere ao instante em que o cabo B foi desconectado e a segunda, por volta de 31 segundos, ao instante em que o mesmo foi reconectado. Ambas as quedas representam o tempo necessário de reconfiguração da rede devido à mudança de topologia. Neste intervalo o controlador deve encontrar um novo caminho para se comunicar com o IO-Device. A rede levou 3 segundos para realizar esta configuração e retornar com a comunicação neste experimento. Além disso, observa-se que após a rede reconfigurada, a comunicação volta a ocorrer na mesma quantidade que anteriormente. Vale lembrar que a volta do tráfego após o restabelecimento do anel é um parâmetro importante para diagnosticar problemas na rede. O volume de dados precisa, necessariamente, ser o mesmo do volume antes da queda. Caso contrário, atribui-se essa diferença a ausência de dispositivos trocando dados.

É importante salientar que nos momentos de ruptura e retorno do anel ainda existe comunicação na rede, como pode ser visto na Figura 23 e Figura 26. Porém esta comunicação não é entre IO-Controller e IO-Device, mas sim se refere à troca de dados entre IO-Controller e os switches.

A Figura 27 apresenta em detalhes a troca de dados capturada com auxílio do TAP. Em específico, o momento apresentado é o instante da primeira queda de

comunicação, referente a ruptura do cabo e consequente mudança de topologia. Para melhor entendimento a figura foi dividida em 6 etapas, que são explicadas a seguir:

- ✓ Etapa 1: IO-Controller e IO-Device trocam mensagens normalmente. Este é o instante antes da ruptura do anel.
- ✓ Etapa 2: Após seis mensagens enviadas sem resposta do IO-Controller (Siemens) para o IO-Device (ABB), o controlador envia a primeira mensagem de alarme (PNIO-AL) para a remota.
- ✓ Etapa 3: O controlador que antes apenas trocava dados com o IO-Device, passa a enviar mensagens para os switches na busca de encontrar qual é a ligação do anel que foi rompida.
- ✓ Etapa 4: O primeiro switch a responder é justamente o *s4* (-5d), com uma mensagem de alarme do tipo *'port data change notification',* indicando ao controlador a necessidade de mudança da porta responsável pela troca de dados.
- ✓ Etapa 5: Com a confirmação da mensagem pelo controlador, a swtich *s4* já é capaz de enviar uma mensagem do tipo PNIO.
- ✓ Etapa 6: A mesma troca de mensagens e mudança de portas de dados ocorre para os outros switches (*s2* e *s5*). A partir deste instante, o controlador passa trocar dados com os switches, isto porque, o IO-Device perdeu sua conexão com a rede devido ao erro ocorrido.

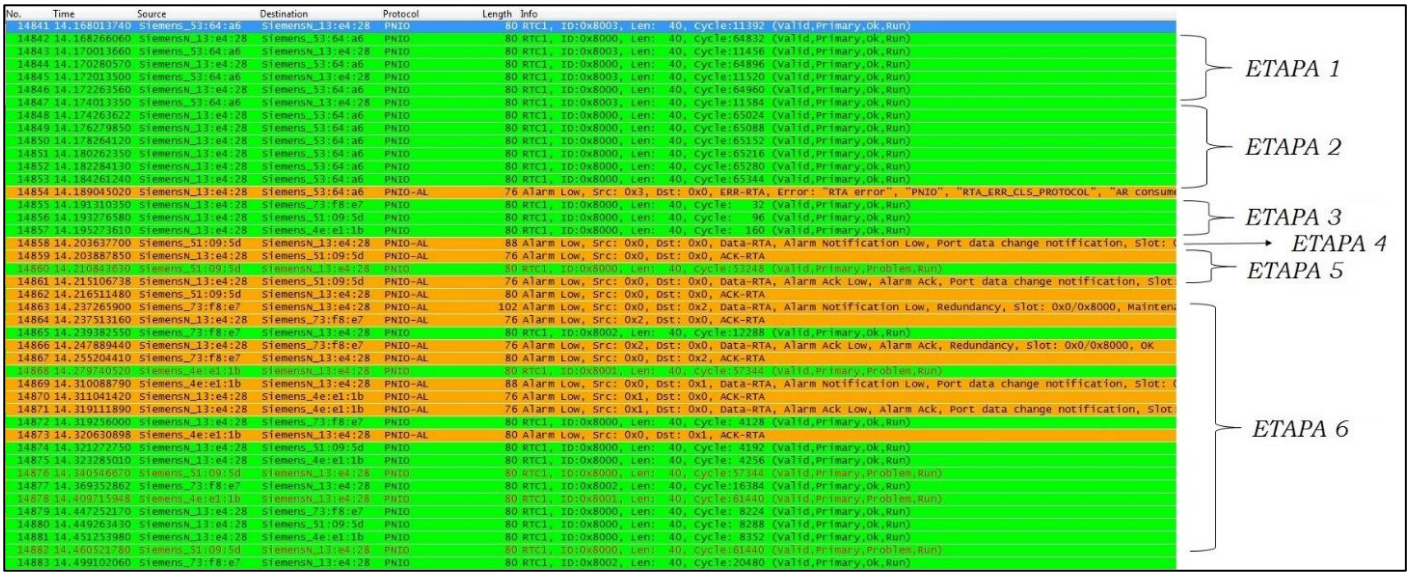
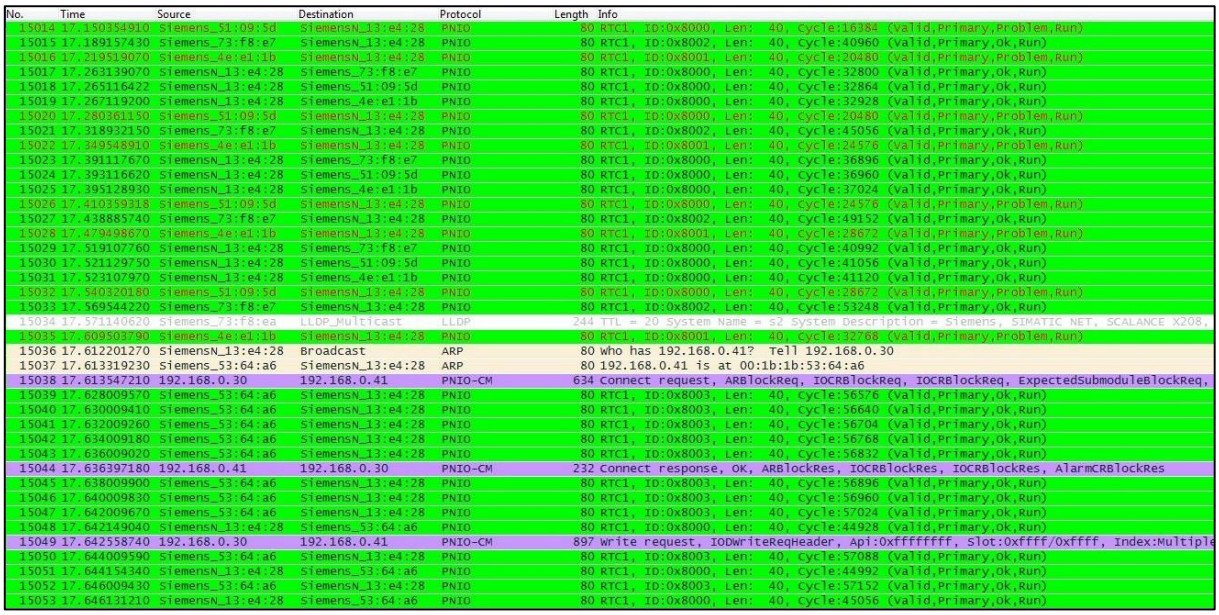


Figura 27: Pacotes transferidos entre IO-Controller e restante da rede no momento de ruptura do anel

A Figura 28 nos mostra a troca de dados no instante de retorno da conexão do IO-Device para a rede, justamente depois dos aproximados três segundos, apresentado na Figura 23. Nela estão destacadas mensagens do tipo ‘PNIO-CM’, pedindo permissão para conexão entre IO-Device e IO-Controller. Após permissões concedidas, inicia-se a troca de dados entre controlador e remota como definido inicialmente. Vale ressaltar que neste instante a rede se apresenta como um anel aberto.



No.	Time	Source	Destination	Protocol	Length	Info
15014	17.150354910	Siemens_51:09:5d	SiemensN_13:e4:28	PNIO	80	RTC1, ID:0x8000, Len: 40, Cycle:16384 (Valid,Primary,Problem,Run)
15015	17.189157430	Siemens_73:f8:e7	SiemensN_13:e4:28	PNIO	80	RTC1, ID:0x8002, Len: 40, Cycle:40960 (Valid,Primary,Ok,Run)
15016	17.219519070	Siemens_4e:e1:1b	SiemensN_13:e4:28	PNIO	80	RTC1, ID:0x8001, Len: 40, Cycle:20480 (Valid,Primary,Problem,Run)
15017	17.263139070	SiemensN_13:e4:28	Siemens_73:f8:e7	PNIO	80	RTC1, ID:0x8000, Len: 40, Cycle:32800 (Valid,Primary,Ok,Run)
15018	17.265116422	SiemensN_13:e4:28	Siemens_51:09:5d	PNIO	80	RTC1, ID:0x8000, Len: 40, Cycle:32864 (Valid,Primary,Ok,Run)
15019	17.267119200	SiemensN_13:e4:28	Siemens_4e:e1:1b	PNIO	80	RTC1, ID:0x8000, Len: 40, Cycle:32928 (Valid,Primary,Ok,Run)
15020	17.280361150	Siemens_51:09:5d	SiemensN_13:e4:28	PNIO	80	RTC1, ID:0x8000, Len: 40, Cycle:20480 (Valid,Primary,Problem,Run)
15021	17.318932150	Siemens_73:f8:e7	SiemensN_13:e4:28	PNIO	80	RTC1, ID:0x8002, Len: 40, Cycle:45056 (Valid,Primary,Ok,Run)
15022	17.349548910	Siemens_4e:e1:1b	SiemensN_13:e4:28	PNIO	80	RTC1, ID:0x8001, Len: 40, Cycle:24576 (Valid,Primary,Problem,Run)
15023	17.391117670	SiemensN_13:e4:28	Siemens_73:f8:e7	PNIO	80	RTC1, ID:0x8000, Len: 40, Cycle:36896 (Valid,Primary,Ok,Run)
15024	17.393116620	SiemensN_13:e4:28	Siemens_51:09:5d	PNIO	80	RTC1, ID:0x8000, Len: 40, Cycle:36960 (Valid,Primary,Ok,Run)
15025	17.395128930	SiemensN_13:e4:28	Siemens_4e:e1:1b	PNIO	80	RTC1, ID:0x8000, Len: 40, Cycle:37024 (Valid,Primary,Ok,Run)
15026	17.410359318	Siemens_51:09:5d	SiemensN_13:e4:28	PNIO	80	RTC1, ID:0x8000, Len: 40, Cycle:24576 (Valid,Primary,Problem,Run)
15027	17.438885740	Siemens_73:f8:e7	SiemensN_13:e4:28	PNIO	80	RTC1, ID:0x8002, Len: 40, Cycle:49152 (Valid,Primary,Ok,Run)
15028	17.479498670	Siemens_4e:e1:1b	SiemensN_13:e4:28	PNIO	80	RTC1, ID:0x8001, Len: 40, Cycle:28672 (Valid,Primary,Problem,Run)
15029	17.519107760	SiemensN_13:e4:28	Siemens_73:f8:e7	PNIO	80	RTC1, ID:0x8000, Len: 40, Cycle:40992 (Valid,Primary,Ok,Run)
15030	17.521129750	SiemensN_13:e4:28	Siemens_51:09:5d	PNIO	80	RTC1, ID:0x8000, Len: 40, Cycle:41056 (Valid,Primary,Ok,Run)
15031	17.523107970	SiemensN_13:e4:28	Siemens_4e:e1:1b	PNIO	80	RTC1, ID:0x8000, Len: 40, Cycle:41120 (Valid,Primary,Ok,Run)
15032	17.540320180	Siemens_51:09:5d	SiemensN_13:e4:28	PNIO	80	RTC1, ID:0x8000, Len: 40, Cycle:28672 (Valid,Primary,Problem,Run)
15033	17.569544220	Siemens_73:f8:e7	SiemensN_13:e4:28	PNIO	80	RTC1, ID:0x8002, Len: 40, Cycle:53248 (Valid,Primary,Ok,Run)
15034	17.571140620	Siemens_73:f8:ea	LLDP_Multicast	LLDP	244	TTL = 20 System Name = s2 System Description = Siemens, SIMATIC NET, SCALANCE X208,
15035	17.609503790	Siemens_4e:e1:1b	SiemensN_13:e4:28	PNIO	80	RTC1, ID:0x8001, Len: 40, Cycle:32768 (Valid,Primary,Problem,Run)
15036	17.612201270	SiemensN_13:e4:28	Broadcast	ARP	80	Who has 192.168.0.41? Tell 192.168.0.30
15037	17.613319230	Siemens_53:64:a6	SiemensN_13:e4:28	ARP	80	192.168.0.41 is at 00:1b:1b:53:64:a6
15038	17.613547210	192.168.0.30	192.168.0.41	PNIO-CM	634	Connect request, ARBlockReq, IOCRBlockReq, IOCRBlockReq, ExpectedSubmoduleBlockReq,
15039	17.628009570	Siemens_53:64:a6	SiemensN_13:e4:28	PNIO	80	RTC1, ID:0x8003, Len: 40, Cycle:56576 (Valid,Primary,Ok,Run)
15040	17.630009410	Siemens_53:64:a6	SiemensN_13:e4:28	PNIO	80	RTC1, ID:0x8003, Len: 40, Cycle:56640 (Valid,Primary,Ok,Run)
15041	17.632009260	Siemens_53:64:a6	SiemensN_13:e4:28	PNIO	80	RTC1, ID:0x8003, Len: 40, Cycle:56704 (Valid,Primary,Ok,Run)
15042	17.634009180	Siemens_53:64:a6	SiemensN_13:e4:28	PNIO	80	RTC1, ID:0x8003, Len: 40, Cycle:56768 (Valid,Primary,Ok,Run)
15043	17.636009020	Siemens_53:64:a6	SiemensN_13:e4:28	PNIO	80	RTC1, ID:0x8003, Len: 40, Cycle:56832 (Valid,Primary,Ok,Run)
15044	17.636397180	192.168.0.41	192.168.0.30	PNIO-CM	232	Connect response, OK, ARBlockRes, IOCRBlockRes, IOCRBlockRes, AlarmCRBlockRes
15045	17.638009900	Siemens_53:64:a6	SiemensN_13:e4:28	PNIO	80	RTC1, ID:0x8003, Len: 40, Cycle:56896 (Valid,Primary,Ok,Run)
15046	17.640009830	Siemens_53:64:a6	SiemensN_13:e4:28	PNIO	80	RTC1, ID:0x8003, Len: 40, Cycle:56960 (Valid,Primary,Ok,Run)
15047	17.642009670	Siemens_53:64:a6	SiemensN_13:e4:28	PNIO	80	RTC1, ID:0x8003, Len: 40, Cycle:57024 (Valid,Primary,Ok,Run)
15048	17.642149040	SiemensN_13:e4:28	Siemens_53:64:a6	PNIO	80	RTC1, ID:0x8000, Len: 40, Cycle:44928 (Valid,Primary,Ok,Run)
15049	17.642558740	192.168.0.30	192.168.0.41	PNIO-CM	897	Write request, IODWriteReqHeader, Api:0xffffffff, Slot:0xffff/0xffff, Index:Multiple
15050	17.644009590	Siemens_53:64:a6	SiemensN_13:e4:28	PNIO	80	RTC1, ID:0x8003, Len: 40, Cycle:57088 (Valid,Primary,Ok,Run)
15051	17.644154340	SiemensN_13:e4:28	Siemens_53:64:a6	PNIO	80	RTC1, ID:0x8000, Len: 40, Cycle:44992 (Valid,Primary,Ok,Run)
15052	17.646009430	Siemens_53:64:a6	SiemensN_13:e4:28	PNIO	80	RTC1, ID:0x8003, Len: 40, Cycle:57152 (Valid,Primary,Ok,Run)
15053	17.646131210	SiemensN_13:e4:28	Siemens_53:64:a6	PNIO	80	RTC1, ID:0x8000, Len: 40, Cycle:45056 (Valid,Primary,Ok,Run)

Figura 28: Pacotes transferidos entre IO-Controller e restante da rede no momento de retorno do anel

Uma análise similar pode ser realizada para o momento de reconexão do cabo B. Porém com a diferença que a rede deixa de ser um Anel Aberto e passa a ser um Anel Fechado.

Com objetivo de analisar o comportamento do caminho *stand-by,* o TAP foi colocado na posição, que é apresentada pela Figura 29.

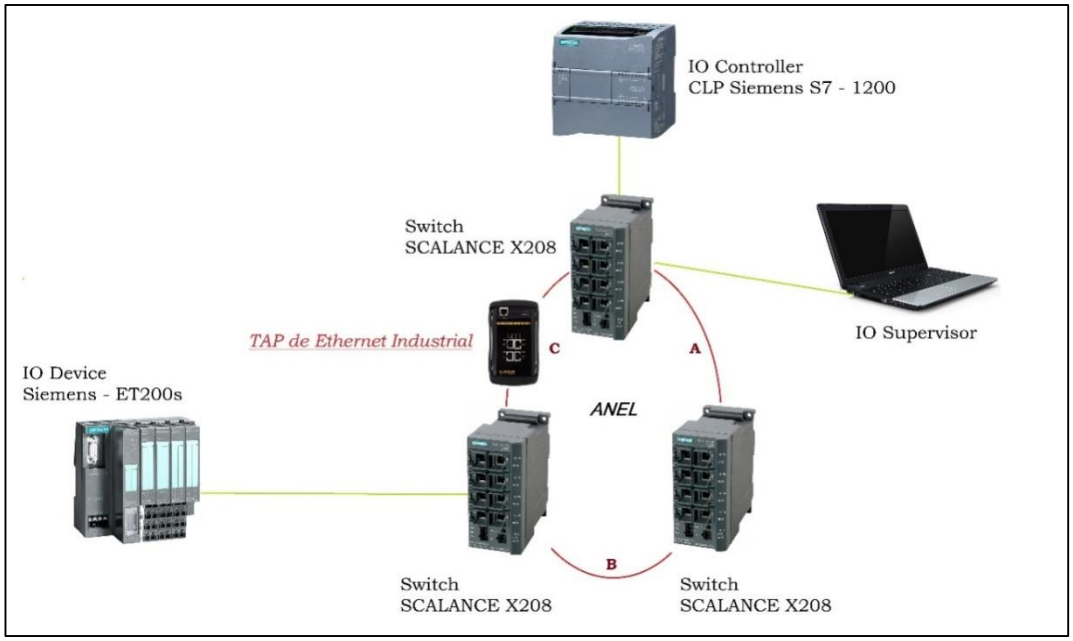


Figura 29: Posição do TAP para análise do caminho *stand-by*

Através do software Wireshark é possível ver o gráfico apresentado na Figura 30, que relaciona as variáveis '*tick interval*', definida com o valor de 100 milissegundos, e o *packet/tick*. Como esperado, neste gráfico nota-se que inicialmente não ocorre troca de dados do tipo PNIO pelo caminho *stand-by*. Entretanto quando o cabo B é rompido, por volta dos 14 segundos, a rede passa a utilizar um novo caminho, através do cabo C, para comunicação entre IO-Controller e IO-Device. Apenas quando o cabo B é restabelecido, a rede deixa de utilizar o caminho *stand-by* e passa a se comportar novamente como uma rede em Anel Fechado, ou seja, não existe mais tráfego de dados pelo cabo C.

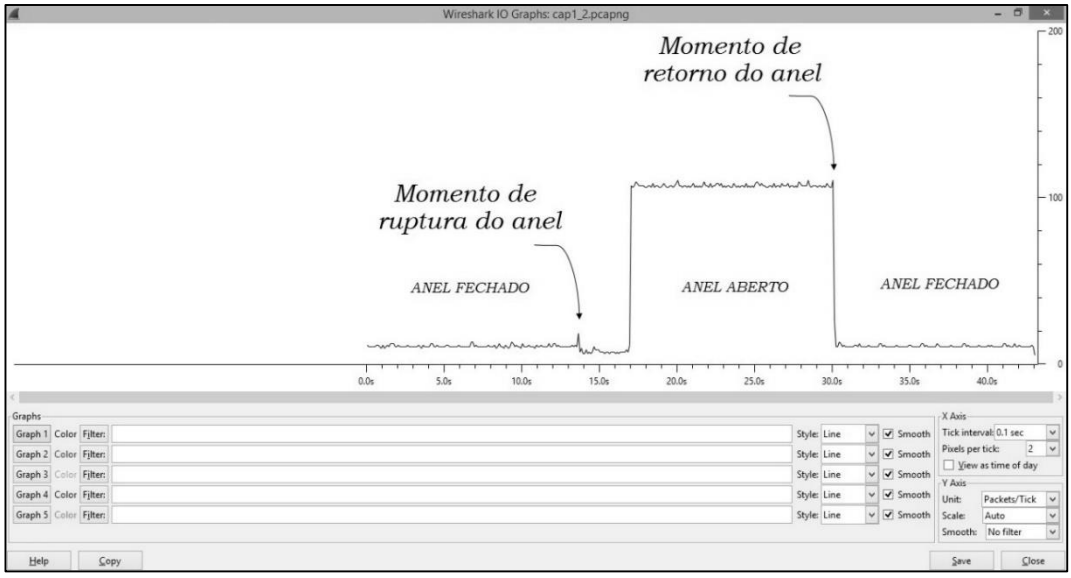


Figura 30: Número de pacotes por unidade de tempo que trafegam no caminho *stand-by*

Vale ressaltar, que embora o caminho *stand-by* apresente momentos em que por ele não ocorre nenhuma comunicação do tipo PNIO, não significa que ele está totalmente inativo. É possível notar que enquanto o anel entre os switches apresenta-se integro, trafegam pelo cabo C, mensagens do tipo PNIO-MRP, responsáveis pela verificação do estado do anel. Estas mensagens são controladas pelo *Media Redundancy Manager* (MRM).

3.2.2 Medição dos tempos de recuperação

Como apresentado nos capítulos anteriores o anel estava funcionando corretamente, isto é, ao abrir uma de suas ligações o MRM passava a utilizar o caminho *stand-by* como alternativa de comunicação entre IO-Controller e IO-Device. Entretanto o tempo de recuperação estava completamente fora do padrão. Enquanto a norma IEC 62439 estabelece tempo máximo de recuperação da rede em 200 milissegundos, a rede apresentada acima levava 3 segundos para se recuperar de uma mudança na topologia. Esta diferença se deve ao fato de que a *Application Relations* (AR) entre IO-Controller e IO-Device estava sendo desfeita, o que obrigava a rede a estabelecer uma nova AR.

O principal responsável por este acontecimento é o tempo de *Watchdog,* definido até então com o valor de 6 milissegundos. Uma AR é supervisionada pelo tempo de *watchdog*, isto significa que se o consumidor da AR não receber nenhum dado cíclico (*IO*

Data CR) durante um intervalo de tempo pré-definido (chamado de tempo de *watchdog*) a AR é desfeita, e deve ser reconstruída. O tempo necessário para reestabelecimento da AR é muito maior do que o tempo de recuperação da rede em anel.

Portanto, se o objetivo deste capítulo é medir os tempos de recuperação da rede é necessário que a AR entre IO-Controller e IO-Device não seja anulada. Para isso é preciso estabelecer um tempo de *watchdog* maior. Nesta etapa do trabalho o *watchdog* foi definido com o valor de 60 milissegundos.

Através da mesma metodologia apresentada no item 3.2.1, foram realizadas 7 coletas de dados em laboratório. Neste momento do trabalho deseja-se coletar apenas a comunicação entre IO-Controller e IO-Device. Assim o TAP de Ethernet Industrial foi posicionado entre a remota e o switch, conforme a Figura 31.

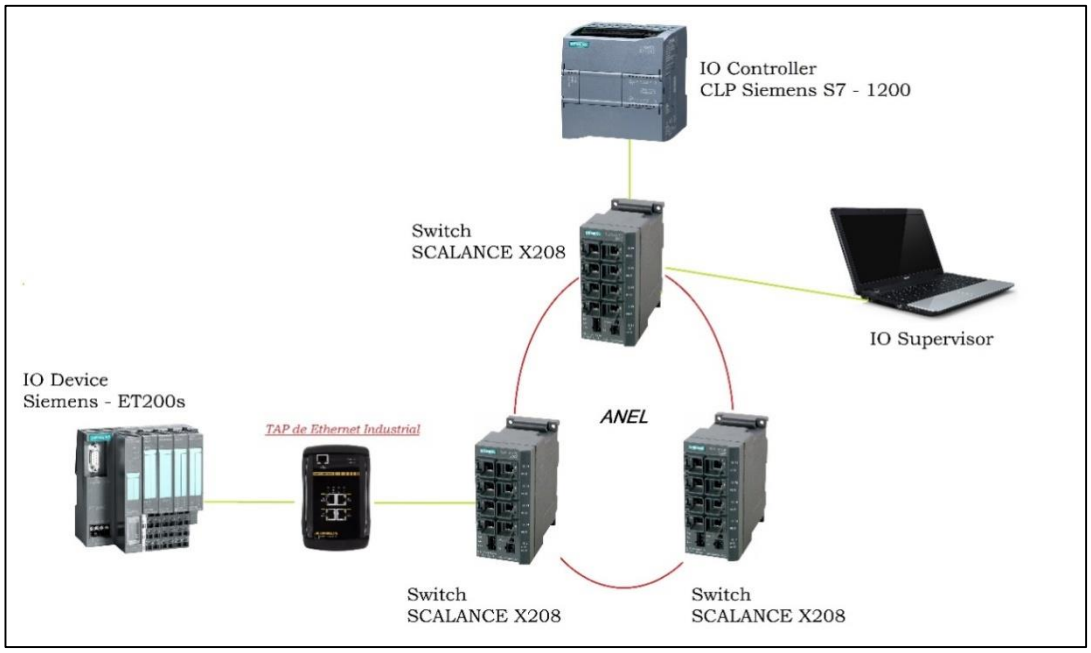


Figura 31: Posição do TAP para medição dos tempos de recuperação

Define-se aqui o Tempo de Recuperação (TR) de uma rede em anel como o tempo necessário para que a comunicação entre IO-Controller e IO-Device seja reestabelecida na rede caso ocorra o rompimento do anel. Já o tempo necessário para restabelecimento da comunicação entre IO-Controller e IO-Device caso o anel for reconectado é definido aqui como o Tempo de Recuperação de Retorno da rede (TRR).

Na Figura 32 pode-se ver a troca de dados entre o controlador e a remota, observa-se que no instante 6 segundos há uma queda na comunicação dada pelo TR e no instante 16 segundos há outra queda dada pelo TRR. Assim, é possível notar que em

ambos os momentos acima definidos IO-Controller e IO-Device perdem sua comunicação devido as ações de rompimento e reconexão do anel.

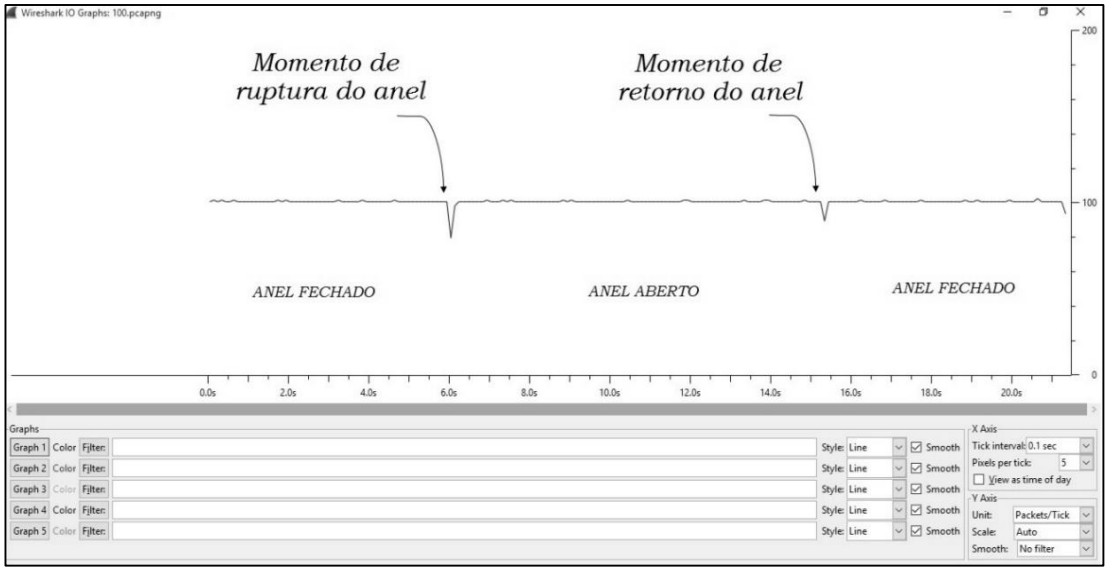


Figura 32: Análise do tráfego de dados da rede em anel

Se for definido o valor de 1 milissegundo para a unidade "*tickinterval*" percebemos claramente que nos instantes de ruptura e restabelecimento do anel a quantidade de pacotes por unidade de tempo coletados pelo TAP cai pela metade. Isto ocorre devido ao fato de que apenas o IO-Device enviará dados para o IO-Controller, não obtendo resposta. Na Figura 33 é possível ver o momento do rompimento do anel e na Figura 34 o momento de retorno. Em ambos os casos pode-se confirmar a perda da comunicação, além de notar o fato de que o tempo de Recuperação de Retorno é menor que o tempo de Recuperação.

Figura 33: Tempo de Recuperação do anel

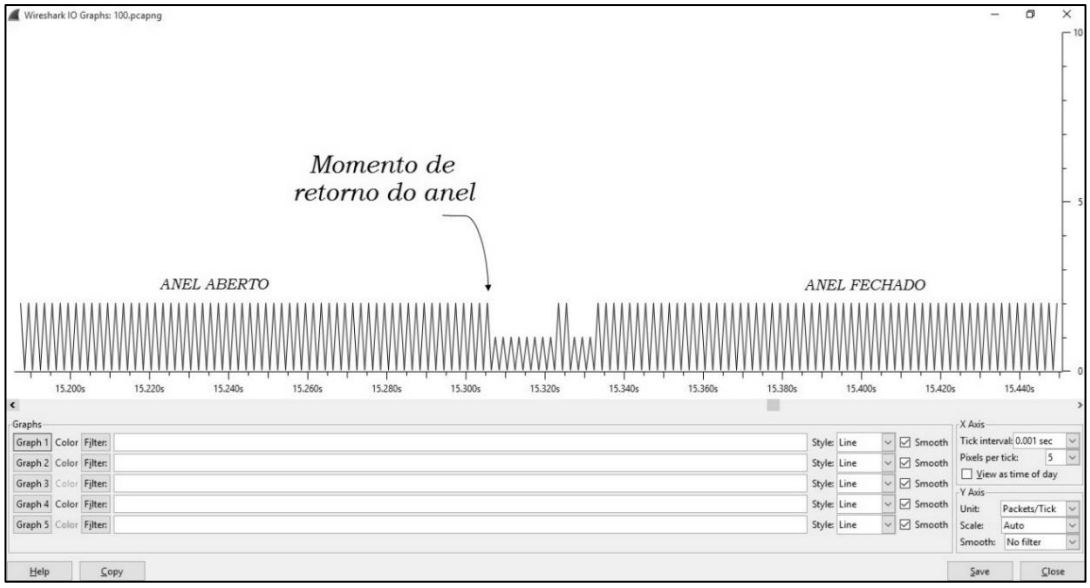


Figura 34: Tempo de Recuperação de Retorno do anel

Através do software Wireshark é possível medir ambos os tempos aqui estudados. A Tabela 2 a seguir apresenta o tempo de Recuperação e o tempo de Recuperação de Retorno do anel em cada uma das 7 capturas realizadas.

Tabela 2: Tempos de recuperação da rede

Coleta	TR [ms]	TRR [ms]
1	51,99	18,02
2	55,99	26,00
3	58,01	24,01
4	59,99	24,02
5	47,98	28,02
6	59,98	18,02
7	50,01	24,01
Média	54,85	23,16

Portanto define-se o tempo de recuperação da rede estudada sendo 54,85 milissegundos e o tempo de recuperação de retorno sendo 23,16 milissegundos.

3.2.3 A Influência do *Watchdog* nos Tempos de Recuperação

Com o conhecimento dos tempos de recuperação da rede iniciou-se o estudo da influência do *watchdog* nos períodos de reconfiguração da rede. A mesma metodologia apresentada no item 3.2.1 foi utilizada e o TAP foi posicionado conforme Figura 31. Determinou-se três diferentes valores de *watchdog* para a remota ET200s que estão apresentado na Tabela 3. Para cada valor de *watchdog* foram realizadas 7 amostras.

Tabela 3: Valores de *watchdog* definidos para o IO-Device

Coleta	*Watchdog* [ms]
1	60
2	40
3	6

Inicialmente foi configurado o valor de 60 milissegundos como o *watchdog* do IO-Device. A Figura 35 apresenta o tráfego de comunicação coletado pelo TAP. Nota-se que sendo o valor de *watchdog* maior do que o tempo de Recuperação, não ocorre uma queda brusca de comunicação entre IO-Controller e IO-Device no momento da ruptura do anel. Análise similar pode-se ser realizada em relação ao tempo de Recuperação de Retorno.

Este rápido tempo de recuperação da rede se deve ao fato de que a *Application Relation* (AR) entre IO-Controller e IO-Device não foi cancelada. Isso porque a remota não ficou mais de 60 milissegundos sem receber dados PNIO, pelo contrário a rede levou apenas cerca de 54 milissegundos para se recuperar no momento de ruptura e cerca de 23 milissegundos no momento de retorno do anel.

Assim a rede é estabilizada rapidamente e embora a comunicação flua por outro caminho, ela retorna nos mesmos patamares que anteriormente.

Figura 35: Tráfego de dados entre IO-Controller e IO-Device com watchdog de 60ms

Posteriormente foi configurado na remota um valor de *watchdog* de 40 milissegundos, isto é, menor que o tempo de Recuperação da rede (de 54,85 ms), porém maior do que o tempo de Recuperação de Retorno (de 23,16 ms). A Figura 36 apresenta a troca de dados da rede acima especificada.

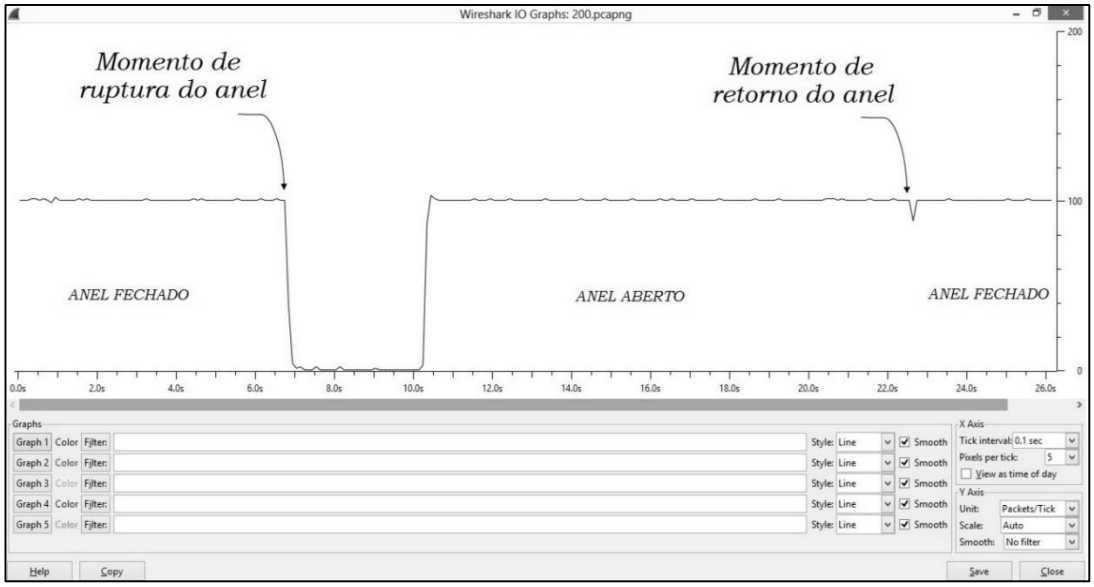


Figura 36: Tráfego de dados entre IO-Controller e IO-Device com watchdog de 40ms

Pode-se notar que no momento em que o anel é rompido a rede tem uma queda muito maior do que os 54 milissegundos, antes definido como tempo de Recuperação. A Tabela 4 indica o tempo em que a rede levou para se auto configurar após o rompimento do anel em cada uma das 7 coletas realizadas.

Tabela 4: Tempo de recuperação da rede para *watchdog* de 40ms

Captura	**TR [s]**
1	3,52
2	3,51
3	3,50
4	3,53
5	3,53
6	3,52
7	3,51
Média	**3,52**

Este tempo na casa dos segundos nos indica que sendo o *watchdog* menor que o tempo de Recuperação a rede leva um tempo 65 vezes maior para se recuperar. Isto se deve ao fato de que quando o anel é rompido a remota ficou mais de 40 milissegundos sem receber dados do tipo PNIO, com isso a AR entre IO-Device e IO-Controller é desfeita, sendo necessário realizar uma outra AR para que a comunicação possa voltar a

ocorrer normalmente. O tempo necessário para criar-se outra AR é muito elevado, no caso estudado a rede levou em média 3,52 segundos para realizar uma nova conexão.

Já no momento de retorno do anel, observa-se que sendo o tempo de Recuperação de Retorno menor que o tempo de *watchdog* a rede é capaz de se recuperar rapidamente. Neste caso a remota não ficou mais de 40 milissegundos sem receber dados PNIO, assim a rede se recuperou antes que a AR fosse cancelada. Portanto neste caso a rede levou em média os 23,16 milissegundos, assim definidos no item 3.2.2.

Por fim, foi configurado um tempo de *watchdog* de 6 milissegundos para o IO-Device. Neste caso, tem-se um valor de *watchdog* menor do que o tempo de Recuperação e do tempo de Recuperação de Retorno do anel. Na Figura 37 pode-se observar o tráfego de dados entre IO-Controller e IO-Device.

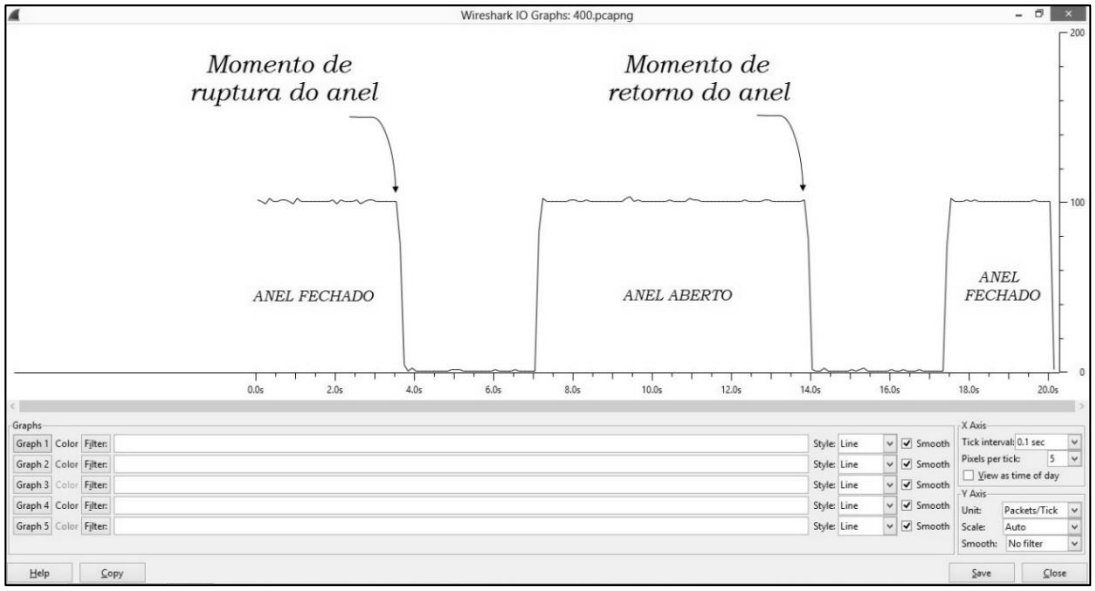


Figura 37: Tráfego de dados entre IO-Controller e IO-Device com watchdog de 6ms

Na figura acima verifica-se que a rede apresentou dois grandes intervalos sem comunicação, referentes aos momentos de ruptura e retorno do anel. A Tabela 5 indica para as sete capturas realizadas o intervalo de tempo sem comunicações referentes ao momento de ruptura do anel, e ao momento de retorno do mesmo. Notou-se que o tempo de Recuperação foi 64 vezes maior e o tempo de Recuperação de Retorno foi 150 vezes maior que anteriormente.

Tabela 5: Tempos de recuperação da rede para *watchdog* de 6ms

Captura	TR [s]	TRR [s]
1	3,46	3,47
2	3,46	3,47
3	3,46	3,46
4	3,47	3,48
5	3,47	3,47
6	3,46	3,47
7	3,47	3,47
Média	**3,46**	**3,47**

Estes grandes intervalos sem comunicação se deve ao fato de que tanto no momento de ruptura do anel, quanto no momento de retorno do mesmo a remota ficou mais de 6 milissegundos sem receber dados PNIO e portanto a AR entre IO-Device e IO-Controller foi cancelada, sendo necessário estabelecer uma nova conexão. Devido estas perdas de conexão a rede levou um tempo muito maior para se recuperar do que os definidos anteriormente.

3.2.4 A Influência do Número de Switches nos Tempos de Recuperação

Como última etapa do trabalho buscou-se estudar a influência da quantidade de switches do anel nos tempos de Recuperação da rede. Assim foram utilizados os mesmos equipamentos apresentados na Tabela 1, com a ressalva de que neste momento o anel é formado por apenas dois switches. A Figura 38 apresenta as conexões realizadas entre os equipamentos para obter a topologia desejada. É importante salientar que o anel é formado único e exclusivamente pelos switches e que o *watchdog* definido para o IO-Device é de 60 milissegundos.

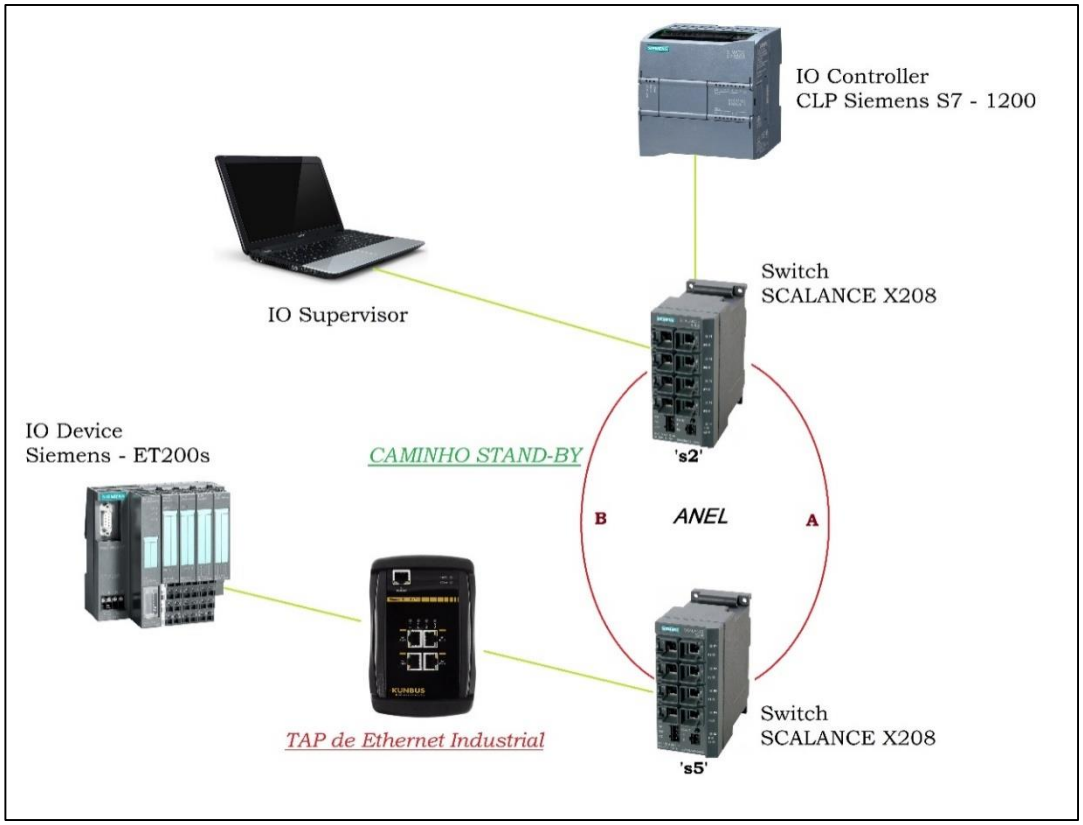


Figura 38: Topologia da rede com 2 switches

Posteriormente foram atribuídos os endereços (IP e nome) de todos os dispositivos da rede via o software TIA Portal V12 da Siemens. A Figura 39 apresenta os endereços MAC, IP e nome de cada equipamento da rede.

Accessible devices in target subnet:

Device	Device type	Type	Address	MAC address
et01	IM 151-3 PN	PN/IE	192.168.0.41	00-1B-1B-53-64-A6
s2	SCALANCE X-200	PN/IE	192.168.0.52	00-1B-1B-73-F8-E7
s5	SCALANCE X208	PN/IE	192.168.0.55	00-1B-1B-4E-E1-1B
PLCKIT5	CPU 1214C DC/D...	PN/IE	192.168.0.151	00-1C-06-13-E4-99
▶ Device				

Figura 39: Dispositivos da rede

Na configuração do anel criado entre os switches SCALANCE X208 foi definido como o *Media Redundancy Manager* (MRM) o switch de nome ‘s2’, e os switch ‘s5’ como

o *Media Redundancy Client* (MRC). Além disso, para ambos os switches foram definidas as portas 1 e 2 como as *ringports*. Neste instante a rede apresenta o status de Anel Fechado.

A metodologia aqui realizada para medição do tempo de Recuperação é similar a realizada no capítulo 3.2.1. Entretanto para que ocorra a ruptura no anel, o cabo A é retirado manualmente e após alguns segundos, o cabo A é reconectado a sua posição original. Em ambos os momentos ocorre a mudança de topologia, e quedas de comunicação entre IO-Controller e IO-Device.

Através do software Wireshark é possível medir o tempo de Recuperação da rede. A Tabela 6 apresenta qual o valor deste tempo em cada uma das 7 capturas realizadas.

Tabela 6: Tempo de recuperação do anel formado com dois switches

Coleta	TR [ms]
1	26,00
2	20,00
3	22,00
4	31,98
5	24,00
6	21,98
7	20,00
Média	23,71

Portanto definimos o tempo de Recuperação desta rede com o valor de 23,71 milissegundos. É possível observar que o tempo de Recuperação do anel com 2 switches caiu consideravelmente quando comparado com o tempo de Recuperação do anel formado por 3 switches isto é, quanto maior o número de switches presentes no anel, maior o tempo de Recuperação da rede. O gráfico apresentado na Figura 40 mostra ambos os tempos encontrados para cada situação. Em relação ao momento de retorno do anel, não ocorreu nenhuma queda de comunicação entre IO-Controller e IO-Device, isto é, o tempo de Recuperação de Retorno da rede para este caso é zero.

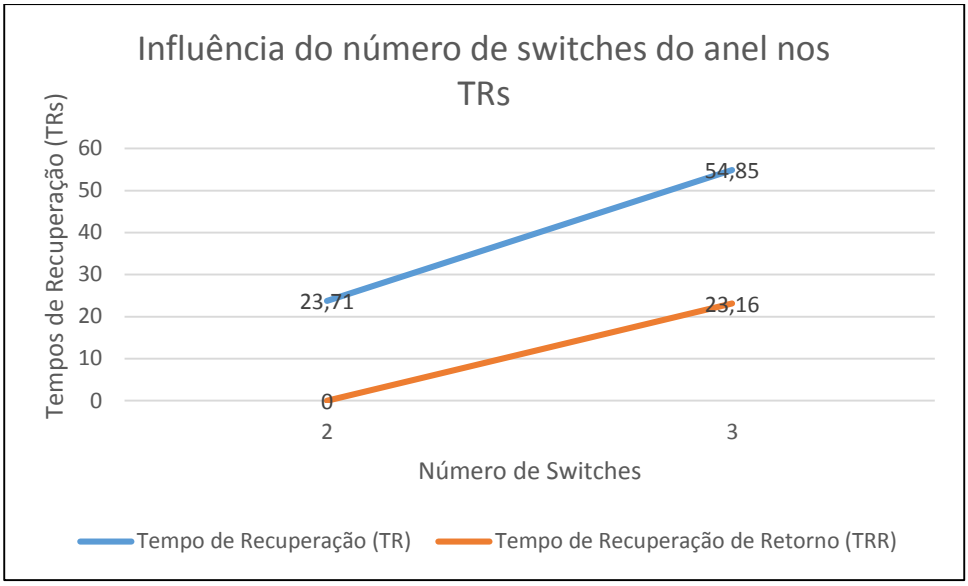


Figura 40: Relação entre switches e TR

4. Conclusões

Pode-se observar inicialmente o comportamento de uma rede em anel frente a mudanças em sua topologia. Sem dúvida, o protocolo MRP é uma importante técnica para se aumentar a disponibilidade de uma rede de automação industrial, além de ser uma estratégia simples e de fácil aplicação.

Através deste trabalho foi possível encontrar uma metodologia para se quantificar os tempos de recuperação de uma rede Profinet em anel, isto é, o tempo de Recuperação e o tempo de Recuperação de Retorno.

Posteriormente notou-se que o tempo de *watchdog* definido para o IO-Device exerce influência sobre os tempos de recuperação da rede. A relação entre o tempo de Recuperação de uma rede em anel formada por 3 switches com o valor de *watchdog* esta apresentada na Tabela 7.

Tabela 7: Influência do *watchdog* na recuperação da rede em anel formada por 3 switches

SE	TEMPO MÉDIO NECESSÁRIO PARA RESTABELECER A COMUNICAÇÃO	Unidade	Tempo em relação ao definido pela IEC 62439
TR > *Watchdog*	3,50	Segundos	17,5 vezes maior
TR < *Watchdog*	54,85	Milissegundos	3,6 vezes menor
TRR > *Watchdog*	3,46	Segundos	17,3 vezes maior
TRR < *Watchdog*	23,16	Milissegundos	8,6 vezes menor

Além disso, foi possível notar que o tempo de configuração de uma nova *Application Relation* (AR) é muito longo. Vale ressaltar que neste trabalho foi necessário reconfigurar apenas um dispositivo, e o tempo gasto para isso foi de aproximadamente 3 segundos. Em redes reais, o número de dispositivos que podem perder sua AR pode ser elevado, causando consequentemente tempos sem comunicação elevados também. Assim embora o MRP ofereça tempos de recuperação relativamente baixos, no máximo de 200 milissegundos, de nada adiantará se o *watchdog* dos dispositivos da rede forem menores do que ele. Pois como visto na Tabela 7, sendo o *watchdog* menor que os tempos de recuperação, a técnica de redundância não mais se enquadrará naquilo definido pela IEC 62439.

Por fim, pode-se perceber que a quantidade de switches presentes no anel também exerce influência sobre o tempo de recuperação da rede. Assim quanto maior for o número de switches, maior será o tempo de recuperação, pois maior será a quantidade de switches que devem ter suas *ring ports* reconfiguradas. É importante ainda entender a tendência da curva apresentada na Figura 40. Para este entendimento torna-se necessário realizar novas medições com anéis formados com quatro, cinco ou mais switches. Neste trabalho não foram realizadas estas medições devido ao fato de que o laboratório conter apenas 3 switches que suportam o MRP.

Identifica-se para futuros projetos de redes em anel o quão importante é relacionar variáveis como tempo de ciclo, tempo de *watchdog* e quantidade de switches presentes no anel, devido ao fato de que elas influenciam de forma direta ou indireta o tempo de Recuperação da rede. Assim deve-se encontrar um ponto ótimo de trabalho entre estas variáveis.

Por fim, este trabalho complementa o curso de graduação em Engenharia Elétrica com Ênfase em Sistemas de Energia e Automação, contribuindo com o enriquecimento e aprofundamento dos conhecimentos em comunicação industrial, protocolos de comunicação, Profinet, e em todas as disciplinas referentes ao Certificado de Estudos Especiais em Automação.

Referências Bibliográficas

[1] KJELLSON, J.; VALLESTAD, A. E.; STEIGMANN, R.; DZUNG, D. *Integration of a Wireless I/O Interface for PROFIBUS and PROFINET for factory automation.* IEEE Transactions on Industrial Electronics, Vol. 56, No 10, Outubro 2009.

[2] FERRARI, P.; FLAMMINI, A.; VITTURI, S. *Performance analysis of PROFINET networks.* Elsevier Computer Standards & Interfaces 28, pp. 369-685, 2005.

[3] KLEINES, H.; DETERT, S.; DROCHNER, M.; SUXDORF, F. *Performance Aspects of PROFINET*. IEEE Transactions on Nuclear Science, Vol. 55, No 1, 2008.

[4] FERRARI, P.; FLAMMINI, A.; RINALDI, S.; GADERER, G. *Evaluation of clock synchronizations accuracy of coexistent Real-Time Ethernet protocols*. International IEEE Symposium on Precision Clock, 2008.

[5] SAHIN, V.; OZCELIK, I.; BALTA, M.; ISKEFIYELI, M. *Topology Discovery of Profinet Networks using Wireshark*. IEEE, 2013.

[6] MARCOS, L. B. **Metodologia para análise de desempenho do protocolo Profinet aplicado a redes de comunicação industrial**. 2013. Trabalho de Conclusão de Concurso – Escola de Engenharia de São Carlos, Universidade de São Paulo, São Carlos. 2013.

[7] PROFINET System Description, Technology and Application. Profibus International. 2011.

[8] DIAS, A. L.; SESTITO G. S.; TURCATO, A. C.; SOUZA, P.H.; BRANDÃO, D. *Um estudo sobre a tecnologia Profinet.* ISA Sertãozinho, 2013.

[9] DUERKOP, L.; TRSEK, H.; JASPERNEITE, J.; WISNIEWSKI, L. *Towards Autoconfiguration of Industrial Automation System: A Case Study Using PROFINET IO.* International Conference on Emerging Technologies & Factory Automation, 17, 2012. New York: IEEE, 2012.

[10] SESTITO, G. S. **Uma proposta metodológica para a previsão do Throughput durante a inicialização de redes Profinet através de Redes Neurais Artificiais**. 2014. Dissertação (Mestrado) - Escola de Engenharia de São Carlos, Universidade de São Paulo, São Carlos. 2014.

[11] AKERBERG, J.; BJORKMAN, M. *Introducing Security Modules in PROFINET IO*. Emerging Technologies & Factory Automation, 2009, Mallorca. IEEE, 2009a, p. 1-8.

[12] PROFINET, Design Guideline. Profibus International, versão 1.04, novembro 2010.

[13] FONTANELLI, D.; MACII, D.; RINALDI, S.; FERRARI, P.; FLAMMINI, A. *Performance Analysis of a Clock State Estimator for PROFINET IO IRT Syncronization*.

[14] SESTITO, G. S. **Uso de Ethernet em automação industrial**. 2011. Trabalho de Conclusão de Concurso - Escola de Engenharia de São Carlos, Universidade de São Paulo, São Carlos. 2011.

[15] PROFINET IO Conformance Classes, Guideline for PROFINET IO. Profibus International, Versão 1.1. 2011.

[16] FERRARI, P.; FLAMMINI, A.; RINALDI, S.; SISINNI, E. *On the Seamless Interconnection of IEEE 1588 – Based Devices Using a PROFINET IO Infrastructure.* IEEE Transactions on Industrial Informatics, Vol. 6, No 3, 2010.

[17] DIAS, A. L. **Análise de desempenho de redes de comunicação industrial em acionamentos de motores elétricos trifásicos**. 2014. Dissertação (Mestrado) - Escola de Engenharia de São Carlos, Universidade de São Paulo, São Carlos. 2014.

[18] Application Layer protocol for decentralized periphery and distributed automation, Techinical Specification for PROFINET IO. Profibus International, versão 2.3. 2012.

[19] FERRARI, P.; FLAMMINI, A.; MARIOLI, D.; TARONI, A.; VENTURINI, F. *Evaluation of timing characteristics of a prototype system based on PROFINET IO RT_Class 3.* Emerging Technologies and Factory Automation, 2007c. IEEE, 2012, p.1254-1261.

[20] BELIE, F.; MARTINOVIC, G. *Model of Influence of MRP on Network Performance*. IEEE, 2013.

[21] FELSER, M. *Media Redundancy for PROFINET IO*. IEEE, 2008

[22] IEC 61784-2. Industrial Communication Networks – Profiles – Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3. International Eletrotechnical Commission, 2007.