UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
ESCOLA DE ENGENHARIA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

RODOLFO BRUNO HECHT

ANÁLISE DA LATÊNCIA NO ACESSO REMOTO À REDES SEM FIO INDUSTRIAIS POR MEIO DE REDES PRIVADAS SEGURAS

Porto Alegre
2021

RODOLFO BRUNO HECHT

ANÁLISE DA LATÊNCIA NO ACESSO REMOTO À REDES SEM FIO INDUSTRIAIS POR MEIO DE REDES PRIVADAS SEGURAS

Dissertação de mestrado apresentada ao Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal do Rio Grande do Sul como parte dos requisitos para a obtenção do título de Mestre em Engenharia Elétrica.
Área de concentração: Controle e Automação

ORIENTADOR: Prof. Dr. Ivan Müller

Porto Alegre
2021

RODOLFO BRUNO HECHT

ANÁLISE DA LATÊNCIA NO ACESSO REMOTO À REDES SEM FIO INDUSTRIAIS POR MEIO DE REDES PRIVADAS SEGURAS

Esta dissertação foi julgada adequada para a obtenção do título de Mestre em Engenharia Elétrica e aprovada em sua forma final pelo Orientador e pela Banca Examinadora.

Orientador: _____
Prof. Dr. Ivan Müller, UFRGS
Doutor pela Universidade Federal do Rio Grande do Sul – Porto Alegre, Brasil

Banca Examinadora:

Prof. Dr. Edison Pignaton de Freitas, UFRGS
Doutor pela Universidade de Halmstad – Suécia

Prof. Dr. Ivanovitch Medeiros Dantas da Silva, UFRN
Doutor pela Universidade Federal do Rio Grande do Norte – Brasil

Prof. Dr. Juliano Araújo Wickboldt, UFRGS
Doutor pela Universidade Federal do Rio Grande do Sul - Porto Alegre, Brasil

Coordenador do PPGEE: _____
Prof. Dr. Sérgio Luís Haffner

Porto Alegre, Julho de 2021.

AGRADECIMENTOS

Agradeço a minha esposa Elisete pelo apoio e companheirismo em estar sempre ao meu lado em todos os objetivos ao qual me proponho. Agradeço a minha filha Bruna por sempre me trazer palavras especiais para os momentos de maior ansiedade pelo nosso futuro. Agradeço meus pais por ter me proporcionado a vida.

Agradeço ao meu orientador que desde do início acreditou em mim, me proporcionou uma oportunidade única de realizar este mestrado e me apoiou como um ótimo professor e amigo.

Agradeço, também, aos colegas de laboratório, Max Feldman pela sua amizade e incansável disposição para ajudar, ao Ederson pelo apoio incondicional e palavras de incentivo, ao Tiago pela parceria, e companheirismo, ao Filipe pela sua simpatia e bom humor, e por fim ao Gustavo Cainelli que sempre disposto a me auxiliar nos testes do experimento.

RESUMO

Indústrias de diversos tipos necessitam que suas plantas estejam localizadas geograficamente em pontos distantes das sedes que controlam as suas operações administrativas. Como exemplo, industrias de base, como mineração, óleo & gás e de energia, que transformam matéria prima bruta para utilização em outros processos, comumente costumam ter suas instalações próximas às fontes primárias, impondo assim a necessidade de implantar uma estratégia de monitoramento de forma remota. Concentrar dados para tomada de decisões como modificar o comportamento de controladores à distância, é desejável, mas demanda operação robusta e segura. Nesse sentido, a chamada Indústria 4.0 tem, entre seus desafios, o desenvolvimento de sistemas de controle em rede, que possibilitam o monitoramento e manutenção remotos. Desta forma, acessar dados obtidos remotamente possibilita comparação com dados de outras plantas semelhantes, o que auxilia e agiliza tomadas de decisões. Este trabalho apresenta uma solução de interligação remota entre uma rede de dispositivos de automação industrial e um operador remoto, de forma segura e confiável, através do uso de uma rede virtual privada na Internet. Além disso, a análise da latência fim-a-fim é realizada, em tempo real, através de estratégias de coleta dos tempos em cada segmento do trajeto entre os dispositivos da rede de automação industrial e *host* remoto. Os dados coletados são tratados estatisticamente. Por fim, através do acesso remoto, o envio de comandos à rede de dispositivos de automação industrial abre horizontes para exercer supervisão e controle remoto de plantas industriais, e este é apresentado ao final do trabalho como complemento. Os resultados obtidos permitem concluir que é viável a utilização de acesso remoto através de redes privadas seguras cuja a latência interna é maior que o intervalo de latência medido, através da ferramenta produzida neste trabalho, na localização onde é realizado o acesso remoto.

Palavras-chave: Latência, VPN, Acesso remoto, *Wireless*HART, Sistema de controle

em rede.

ABSTRACT

Many types of industries require their plants to be located geographically far from the headquarters that control their administrative operations. For example, basic industries such as mining, oil & gas, and energy, which transform raw materials for use in other processes, often have their facilities close to primary sources, thus imposing the need to implement a remote monitoring strategy. Concentrating data for decision making, such as modifying the behavior of remote controllers, is desirable, but requires robust and safe operation. In this sense, Industry 4.0 has, among its challenges, the development of networked control systems that enable remote monitoring and maintenance. Thus, accessing data obtained remotely enables comparison with data from other similar plants, which helps and speeds up decision-making. This work presents a remote interconnection solution between a *Wireless*Hart device network and a remote operator, in a safe and reliable way, through the use of a virtual private network on the Internet. In addition, an end-to-end latency analysis is performed, in real time, through strategies of collecting the times in each path between the *Wireless*Hart devices and the remote host. The collected data is statistically treated. Finally, through remote access, sending commands to the *Wireless*Hart device network opens horizons for supervision and remote control of industrial plants is presented at the end of the work. The results obtained allow us to conclude that it is feasible to use remote access through secure private networks whose internal latency is greater than the measured latency interval, through the tool produced in this work, in the location where the remote access is performed.

Keywords: Latency, VPN, Remote access, *Wireless*HART, Network control system.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS

ASN	*Absolute Slot Number*
ANOVA	*Analysis of Variance*
CPS	*Cyber Physical Systems*
FD	*Field Device*
Hart-IP	*Hart-over-IP*
IEEE	*Institute of Electrical and Electronics Engineers*
IoT	*Internet of Things*
IIoT	*Industrial Internet of Things*
IP	*Internet Protocol*
IPv4	*Internet Protocol version 4*
LAN	*Local Area Network*
PING	*Packet Internet Groper*
NAT	*Network Address Translation*
NCS	*Networked Control Systems*
NTP	*Network Time Protocol*
RSFI	Rede Sem Fio Industriais
SDN	*Software Defined Networking*
TCP/IP	*Tramission Control Protocol/Internet Protocol*
UDP	*User Datagram Protocol*
USB	*Universal Serial Bus*
UTP	*Unshielded Twisted Pair*
VB	*Visual Basic*
VPN	*Virtual Private Network*
WAN	*Wide Area Network*
WH	*WirelessHART*

SUMÁRIO

1 INTRODUÇÃO

O estudo do acesso remoto em redes industriais tem atraído a atenção dos gestores de plantas industriais por permitir que as malhas de controle sejam operadas em locais distantes da produção mas próximos aos centros consumidores adaptando, instantaneamente, o ritmo de produção à demanda local. Além disso, o acesso remoto auxilia na manutenção da planta, possibilitando identificar e sinalizar às equipes de manutenção alguma situação que exija uma atuação preventiva ou corretiva.

1.1 Objetivos

De acordo com SILVEIRA (2016), os métodos de produção de fabricação tradicional irão passar por uma transformação e demandarão o uso de ferramentas da tecnologias da informação para conectar todos os subsistemas, processos internos e externos, fornecedores e clientes de forma que a troca de informações permeie toda a cadeia de valor construindo uma imensa base de dados e de computação em nuvem (CARMONA *et al.*, 2017). Atualmente a evolução da indústria vive um processo de implantação e uso intensivo das telecomunicações para atender tecnologias mais recentes, tais como, fábrica inteligente, *Internet of Services* (IoS), *Internet of Things* (IoT), *Cyber Physical Systems* (CPS), entre outros conceitos anteriores ou recentemente propostos.

Na estratégia de implantação de uma planta, onde busca-se que novas instalações industriais estejam localizadas de forma mais eficiente possível, em diversos aspectos, impõem-se a necessidade de realizar meios de interligação remota do controle dos processos produtivos. A interligação remota permite desta forma, o controle da planta industrial em uma localização diversa a da produção, por exemplo, próximo aos consumidores.

Considerando os argumentos apresentados anteriormente torna-se imprescindível a

indústria 4.0 vencer o desafio da comunicação industrial (GEAMPALIA *et al.*, 2017). Os novos meios de comunicação representam a possibilidade de se obter um aumento na disponibilidade dos dados da planta e permitir a implementação de novas aplicações que podem reduzir o envolvimento do operador humano. Também, será possível permitir uma integração direta dos dados em aplicativos de gerenciamento de ativos ou *Enterprise Resource Planning* (ERP) e, ainda, o uso de aplicativos móveis, que aumentarão a velocidade com que os gerentes das plantas são informados sobre a operação do processo.

Assim, realizar um monitoramento remoto no conceito da indústria 4.0 representa vantagens significativas tais como:

- **Dinamismo**

  Ter todos os dados analisados, de um determinado dispositivo de uma planta industrial ajuda a dinamizar a parada para execução de uma manutenção, preditiva ou corretiva e fazer um melhor aproveitamento do tempo da equipe técnica;

- **Alertas**

  Sistemas de monitoramento remoto já oferecem opções disparo de alertas por SMS ou e-mail em casos de criticidade de algum elemento operacional. Estes avisos permitem decisões mais assertivas e rápidas;

- **Eficiência**

  Com todos os dados obtidos em mãos mais rapidamente, é possível programar um ritmo de operação otimizado e eficaz de operação da planta.

Por exemplo, a aquisição remota de dados é um requisito essencial para usinas remotas automatizadas, como parques eólicos distribuídos, bombas de abastecimento de água, bombas de águas residuais e instalações de fornecimento de gás.

Em outro aspecto, os sistemas de controle em rede (NCS, *networked control systems*) tem desempenho otimizado se adaptações nos seus controladores são feitas em função de alterações nas redes industriais, especialmente as sem fio. Saber a latência dos eventos de comunicação fim-a-fim nas redes industriais é de suma importância aos projetistas de sistemas de controle em rede, uma vez que com este parâmetro é que conseguem projetar controladores estáveis. Ainda, uma possível realimentação do parâmetro latência aos controladores de sistemas de controle em rede é um campo a ser explorado. Neste contexto,

este trabalho foca em estudar o comportamento da latência de uma rede *Wireless*Hart (WH) sendo acessada remotamente e verificar a viabilidade de realizar o monitoramento e até mesmo o controle de um processo remotamente.

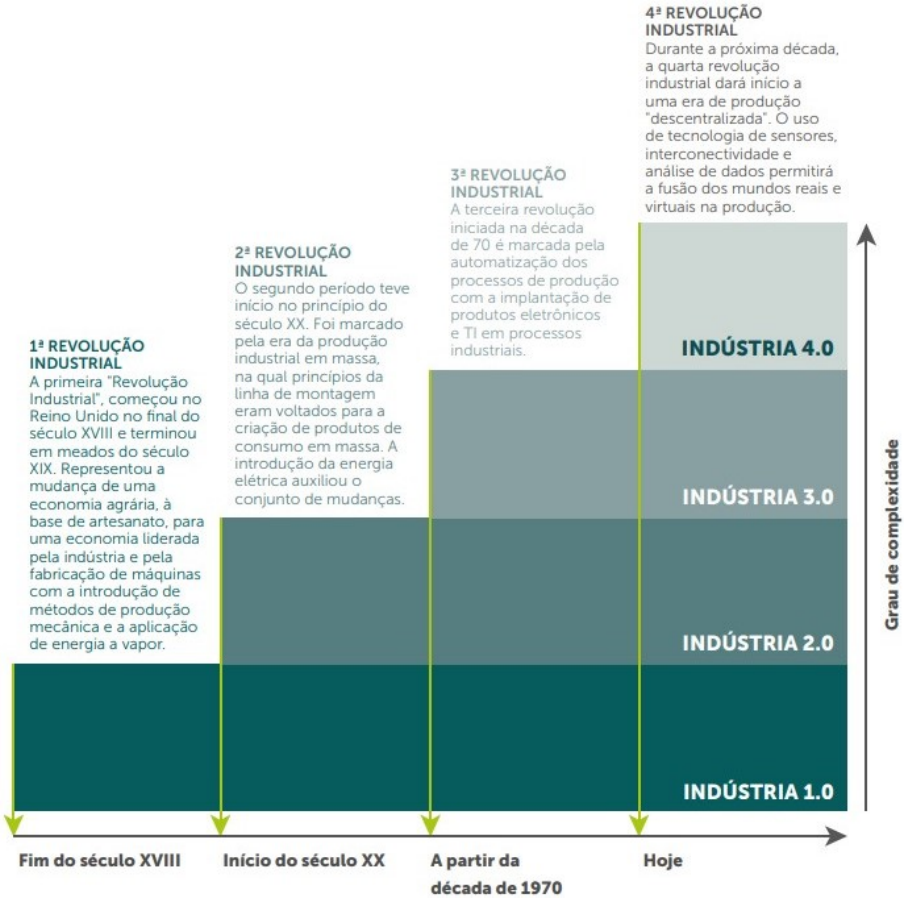
1.2 Motivação

Indústria é uma atividade econômica que surgiu no fim do século XVIII e início do século XIX na Inglaterra, com a finalidade transformar matéria-prima em produtos comercializáveis, utilizando força humana, máquinas e energia. Com o desenvolvimento da indústria ao longo dos séculos foi criada a expressão "planta industrial" que representa o local onde há o envolvimento de processos industriais, químicos ou mecânicos para produção de um determinado item de consumo (CARVALHO, 2014).

Para entendimento mais amplo, a seguir, está uma síntese da evolução da indústria na história da humanidade. Durante o século passado as indústrias e suas plantas industriais caminharam em direção ao desenvolvimento e implantação de estratégias de automação industrial, ou seja, utilização de máquinas eletromecânicas, softwares e equipamentos específicos para automatizar processos industriais obtendo resultados como aumento da eficiência, a maximização da produção, o menor consumo de energia, entre outros ganhos. Tarefas de controle e automação abriram campo para pesquisar melhorias nos processos técnicos industriais buscando redução da interferência humana e o aumento da precisão de equipamentos usados nesses processos. Sistemas que automatizam processos técnicos, chamados sistemas de automação, são compostos basicamente de dispositivos eletrônicos e mecânicos, os quais são capazes de realizar tarefas de forma mais precisa e mais rápida que humanos. Para atingir este desenvolvimento faz-se importante entender como ocorreram as etapas da evolução da indústria mundial (ARAUJO JUNIOR; DAS CHAGAS; FERNANDES, 2003). A primeira revolução industrial, iniciada no começo no século XVIII utilizou a energia a vapor e mecanização da produção. A seguir, a segunda revolução industrial ocorreu no século XVIII através da utilização da eletricidade e produção em linha de montagem. A terceira revolução industrial iniciou-se nos anos 70 através de automação parcial usando controles e computadores programáveis por memória. Atualmente, o movimento pelo desenvolvimento da indústria mundial está focado na implementação da quarta revolução industrial. Batizada como "Indústria 4.0", caracterizada pela aplicação de tecnologias de informação e comunicação à indústria (TOOLS, 2020). A Figura 1

ilustra a evolução da indústria até os dias de hoje.

Figura 1 – Evolução da indústria



Fonte:(GLOBAL, 2020)

Plantas industriais normalmente são estruturas altamente complexas projetadas em função dos seus principais processos, equipamentos e máquinas associados à sua função fabril. Neste cenário, há que se considerar que muitos tipos de indústrias necessitam que suas instalações sejam localizadas em locais específicos, geograficamente diferentes de seu mercado consumidor ou de seu gerenciamento fabril ou, ainda, por diversos outros motivos econômicos e estratégicos. Considerando esse contexto, a distribuição geográfica das atividades econômicas em geral e da indústria em particular começa a ser relacionada a uma série de variáveis e de suas combinações, como a fonte de matérias primas, a mão-de-obra, o mercado, os custos do transporte, a quantidade e qualidade dessas informações disponíveis, o capital e a tecnologia. A determinação dos custos de transporte, os impactos dos custos do trabalho e as forças da aglomeração e a polarização também são fatores considerados para o estudo de localização da indústria (VILAR, 2011). A observação da

distribuição geográfica das atividades econômicas entre as regiões em um país ou economia dificilmente guarda relação direta e proporcional com as diferentes dimensões físicas dessas regiões. Isto é, parece haver alguma regularidade nas tendências à especialização regional ou concentração geográfica das atividades econômicas. Três são os argumentos que podem ser identificados na teoria econômica para o entendimento de tal regularidade: a especialização e concentração a partir da dotação relativa de fatores da teoria das vantagens comparativas e a efetivação das economias de escala na presença de custos, tais como, de transportes (KRUGMAN, 1980). Por exemplo, indústrias de base, como a mineração, óleo e gás e energia renovável, transformam matéria-prima bruta em matéria-prima processada para a utilização por outras indústrias, realizam suas instalações próximas as fontes de suas matérias primas. A indústria de bens de intermediários, as quais produzem máquinas e equipamentos utilizados nas indústrias de bens de consumo, também buscam estar estrategicamente próximas aos seus principais clientes.

Desta forma, alguns setores industriais necessitam instalar suas plantas industriais em locais geograficamente diferentes de suas sedes gerenciais. Isto acontece por motivos tais como, conveniência da proximidade dos fornecedores da matéria prima principal, necessária para sua produção, pela proximidade do mercado consumidor, facilitando a logística de entrega, ou por fatores econômicos.

A tendência atual aponta para investimentos no modelo estrutural da Indústria 4.0, uma indústria totalmente conectada através de redes industriais, locais e remotas. Neste caminho, a conexão de plantas industriais que estejam geograficamente separadas do gerenciamento dos processos passa ser uma vantagem competitiva, uma vez que este gerenciamento poderá estar próximo a locais estratégicos como o mercado consumidor, regulando os processos conforme suas demandas locais.

Assim, este trabalho foi motivado na realização de uma análise prática da interligação entre gerenciador e planta industrial, através de um túnel seguro trafegando dados, como comandos e respostas dentro da Internet. Coletando latências, analisando estatisticamente e enviando comandos remotamente a um dispositivo em uma rede *Wireless*Hart, estabelece-se um caminho para entender como realizar monitoramento e controle remoto de plantas industriais.

1.3 Proposta

Este trabalho apresenta uma metodologia para obtenção das características de latência em uma solução de interligação de sistemas de comunicação, via Internet, de um dispositivo em uma rede *Wireless*Hart instalada em laboratório, utilizando uma solução de conexão remota, e ir além, buscando enviar comandos à rede industrial de forma a estudar a possibilidade de monitoramento e de controle de um processo à distância.

1.4 Organização do texto

Este trabalho está organizado da seguinte forma: no Capítulo 2, são apresentados os conceitos básicos da fundamentação teórica utilizados ao longo da dissertação. No Capítulo 3, é apresentada uma revisão bibliográfica referente a trabalhos anteriormente realizados. Os métodos e materiais utilizados são apresentados no Capítulo 4, já a implementação do sistema proposto neste trabalho é descrita no Capítulo 5. No capítulo 6 são relatados os estudo de caso e os resultados obtidos. Por fim, conclusões e trabalhos futuros são apresentados no Capítulo 7.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo é apresentada uma contextualização abrangente desde conceitos da indústria 4.0, redes virtuais privadas, sistemas de controle em rede, protocolo WH, e latência. É apresentada também uma revisão sobre técnicas de acesso remoto mais utilizadas. Por fim, são introduzidos os sistemas de controle em rede, fundamentais para o desenvolvimento da indústria 4.0, e que estão no escopo das possíveis aplicações desta dissertação.

2.1 A importância da Internet para Indústria 4.0

A denominação 4.0 deriva da quarta versão concebida para definição da nova revolução industrial, onde os mundos virtuais e físicos se fundem através da Internet (DAVIES, 2015).

Em HERMANN; PENTEK; OTTO (2016) foram identificados seis requisitos para a implementação da Indústria 4.0:

- **Interoperabilidade**: permitindo que todos os CPS de uma fábrica ou ambiente industrial, mesmo que descendentes de diversos fornecedores, possam se comunicar através das redes;
- **Virtualização:** possibilitando que os dados obtidos dos CPS nos produtos e equipamentos físicos sejam transmitidos aos modelos virtuais e em simulações, espelhando comportamentos reais no ambiente virtual;
- **Descentralização dos controles dos processos produtivos**: uma vez que os computadores embarcados em conjunto com a Internet das coisas gerarão produtos com tomadas de decisões na manufatura e nos processos de produção em tempo real;
- **Adaptação da produção em tempo real**: uma vez que os dados serão analisados

no instante em que são coletados, permitindo que a produção seja alterada ou transferida para outros sites em caso de falhas ou na produção de bens customizados;

- **Orientação a serviços**: dados e serviços serão disponibilizados em rede aberta, tornando a IoS ainda mais robusta. Dessa forma, a customização de processos de produção e operação terá maior flexibilidade de adaptação de acordo com as especificações dos clientes.

- **Sistemas modulares dos equipamentos e linhas de produção**: fábricas mais flexíveis e adaptáveis às alterações necessárias.

O crescimento rápido da utilização da Internet e o aumento do volume de dados trafegados impuseram estratégias para aliviar a necessidade de sistemas de hardware e software mais sofisticados para suportar e gerenciar as trocas de informações. Uma dessas estratégias é a computação em nuvem. Através da computação em nuvem, usuários podem acessar qualquer aplicação necessária ao controle e desenvolvimento de plantas industriais através da Internet.

Desde o início do século XXI, com a popularização da Internet e o surgimento de outras inovações tecnológicas, os níveis de produção industrial no mundo cresceram, visando atender uma demanda com um nível de exigência cada vez maior em um ambiente cada vez mais competitivo. A promessa é que a Indústria 4.0 fundamentada em inovação e melhoria contínua, possibilitará a criação de melhores produtos e serviços atendendo essa demanda cada vez maior e mais exigente. Nesta visão de futuro, ocorre uma completa descentralização do controle dos processos produtivos e uma proliferação de dispositivos inteligentes interconectados, ao longo de toda a cadeia de produção e logística. O impacto esperado na produtividade da indústria é comparável ao que foi proporcionado pela Internet em diversos outros campos, tais como no comércio eletrônico, nas comunicações pessoais e nas transações bancárias (HAHN FILHO, 2016).

A Indústria 4.0 adota de um conjunto de tecnologias emergentes das área da tecnologia da informação e automação industrial formando um sistema de produção físico-cibernético, com intensa digitalização de informações e interligação direta entre sistemas, máquinas, produtos e pessoas viabilizando a IoT. Assim, ambientes de manufatura se tornarão altamente flexíveis e autoajustáveis à demanda crescente por produtos cada vez mais necessitam ser customizados.

Para o sucesso do projeto, a consolidação de um único conjunto de padrões técnicos de comunicação e segurança será um elemento chave. Com ele, a troca de informações entre os diferentes tipos de sistemas e dispositivos será assegurada, eliminando-se as restrições relacionadas aos padrões proprietários vigentes (HAHN FILHO, 2016).

2.1.1 Vantagens da interligação remota de plantas industriais

Nos últimos anos o desenvolvimento da tecnologia da informação implementou conceitos como computação em nuvem, virtualização de equipamentos físicos e protocolos que, por sua vez, ampliou as conexões entre pessoas físicas e equipamentos. Desta forma cada vez mais estas interações permitem trocar informações entre si e/ou tomar decisões de forma autônoma, o paradigma denominado de IoT, que se estendeu ao ambiente industrial a toda e cadeia produtiva (DASTJERDI; BUYYA, 2016).

A integração dos meios de comunicação às tecnologias de automação industrial possibilita que sensores, máquinas fabris inteiras sejam monitoradas e controladas à distância, aspecto importante da atual revolução industrial. O acesso remoto a equipamentos industriais é definido pelos autores a seguir.

Em SOUPPAYA; SCARFONE *et al.* (2016) os autores afirmam que "A capacidade de usuários e operadores de uma organização de acessar seus recursos físicos, dados e sistemas particulares que residem em uma rede protegida fisicamente ou logicamente, a partir de redes externas que devem ser consideradas de fora da organização".

A interligação remota de controle de planta industrial através de acesso privado virtual pela Internet possibilita a troca de comandos e informações produzindo um rol de vantagens tais como:

- Aumento da produtividade e redução de custos ao integrar as redes dos sistemas de controle das unidades fabris, corporativas e externas;
- Agilidade na tomada de decisões e na manutenção de máquinas a distância;
- Virtualização de sistemas físicos, permitindo o monitoramento e controle remotos de unidades inteiras;
- Reposta mais rápida às mudanças nos processos produtivos e às demandas de mercado;

- Interoperabilidade entre unidades que possuem dispositivos e protocolos de comunicação diferentes.

Tais vantagens são motivadoras para o investimento nos assuntos relacionados ao controle e comunicação remota, desenvolvendo técnicas apropriadas, através de hardware e software específicos.

As soluções de acesso remoto normalmente precisam suportar vários objetivos de segurança. Soluções que podem ser realizadas através de uma combinação de recursos de segurança incorporadas nas técnicas de acesso remoto e controles adicionais de segurança aplicados aos dispositivos e outros componentes da solução de acesso remoto. Os mais comuns objetivos de segurança para tecnologias de acesso remoto são:

- **Confidencialidade**

  Segurança da informação envolve a proteção de dados e informações industriais confidenciais ou não, que transitam entre todos os seus setores e ainda entre a organização e seus parceiros. É fundamental a certificação de que as comunicações de acesso remoto e os dados armazenados do usuário não possam ser acessados por partes não autorizadas;

- **Integridade**

  A integridade é a proteção da informação. É garantir que a informação compartilhada foi enviada ao seu destino de maneira íntegra e plena, ou seja, sem alterações e entre máquinas e dispositivos incorruptíveis. Trata-se de um pilar da segurança da informação que visa assegurar que as informações da empresa serão disponibilizadas e compartilhadas da mesma forma que foram finalizadas e salvas em um sistema. Refere-se a maneira de proteger os dados e certificar de que eles não foram, nem serão modificados ou violados. É fundamental detectar quaisquer alterações intencionais ou não intencionais nas comunicações de acesso remoto que ocorram em trânsito;

Os aspectos relacionados aos temas acima descritos são apresentados na próxima subseção.

2.1.2 Acesso remoto em arquiteturas de sistemas de controle industrial

De uma perspectiva de definição, podemos pressupor que o acesso remoto é descrito, na sua forma mais simples, como um processo que conecta usuários remotos a redes e aplicações dentro do ambiente de uma organização.

A funcionalidade e os recursos de segurança de acesso remoto ajudam a criar caminhos eletrônicos para conceder acesso autorizado e autenticado a uma rede confiável a partir de um local que, de outra forma, seria considerado não confiável. Essa definição é útil para entender a necessidade de estabelecer vários elementos de segurança aplicáveis no uso do acesso remoto, levando em consideração que o acesso remoto pode ser interrompido, impedido, capturado ou sequestrado por meio de ações deliberadas de um invasor, sem que este tenha que contornar os controles de segurança físicos ou lógicos, especialmente quando as comunicações estiverem ocorrendo por um meio como a Internet.

A Figura 2 mostra uma arquitetura integrada que possui conexões de fontes externas, como a rede local corporativa ou *Local Area Network* (LAN), sites de fornecedores e a Internet. Ela ilustra o conceito de uma infraestrutura de comunicações externas, comum nas arquiteturas de sistemas de controle, estejam estas comunicações em localizações próximas ou distribuídas em áreas geográficas diversas.

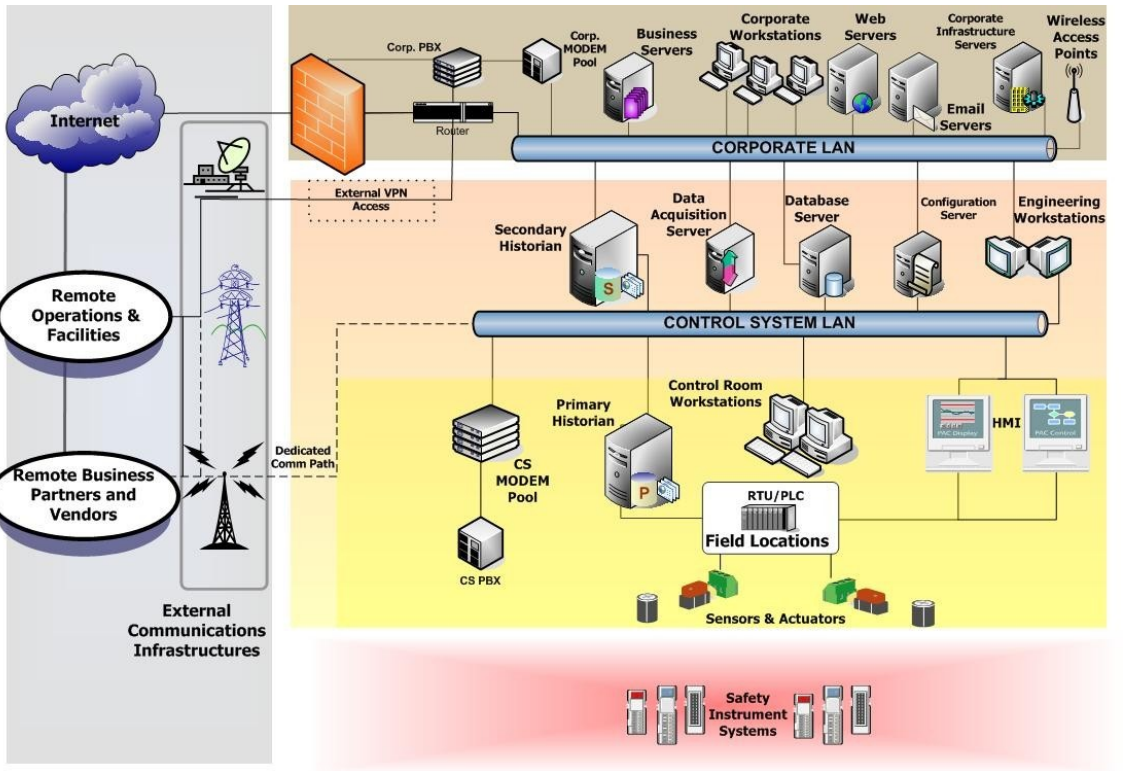
Normalmente, pode ser considerada como o ponto de conexão com a Internet, comum no atual processo que usuários remotos obtém acesso a negócios ou operações do sistema de controle (SECURITY-US, 2020).

A partir da análise de arquiteturas integradas ao acesso de comunicações de dados externos podemos entender que a existência de um invasor que obtivesse acesso a sistemas críticos, especialmente utilizando-se dos mecanismos de acesso remoto, suscitaria preocupações a respeito de como este invasor pode comprometer operações remotas de controle de uma planta industrial. Assim, questões de segurança mostram a importância da criação de soluções de acesso remoto eficazes e seguras ao lidar com sistemas, em especial, de controle de missão crítica (USA, 2020).

2.1.3 Requisitos gerais a serem considerados no acesso remoto

Basicamente as prioridades mais comuns nas infraestruturas tradicionais de comunicações que se preocupam com o acesso remoto são:

Figura 2 – Arquitetura industrial integrada



Fonte: (USA, 2020)

- Garantir acesso as informações e serviços essenciais de qualquer local;
- Garantir acesso as informações e serviços essenciais a partir de várias categorias de dispositivos;
- Garantir acesso autorizado das informações críticas apenas aos operadores autorizados a receber tais informações.

2.1.4 Tipos de soluções de acesso remoto

Todas as soluções de acesso remoto são essencialmente as mesmas em seu núcleo, pois fornecem uma conexão a uma distância entre um usuário (ou sistema) e outro usuário (ou sistema).

Porém existem três soluções mais comumente utilizadas, a saber:

- **Acesso ao desktop**

  Existem diversos softwares que permitem acesso ao desktop, tais como Logmein, Teamviewer, Anydesk, entre outros. Sua estratégia é o *host* remoto assumir o área

de trabalho, ou o ambiente terminal *host* acessado e comandando como se as operações fossem realizadas apenas pelo *host* acessado;

- **Acesso via *web broswer***

  Este acesso através de um servidor *web* será encontrado através endereçamento IP fixo na Internet, e através do navegador *web* um cliente poderá acessar um *front-end* onde poderá emitir comandos e acessar dados disponibilizados na aplicação do servidor *web*;

- **Acesso via Virtual Private Network (VPN)**

  Diversas soluções de VPN encontrem-se disponíveis tais como OpenVPN, NordVPN, SoftEther VPN entre outras. Suas estratégias são estabelecer acesso entre *host* remoto e *host* local inserindo em uma rede virtual com características semelhantes a uma rede local. Desta forma o *host* acessado pode atender comandos exercidos por um ou vários *host* remotos.

Neste trabalho foi utilizada a solução VPN, onde obtemos a opção de utilizar vários *host* remotos distribuídos em localizações geograficamente distintas e tratar suas conexões como uma rede local de forma segura.

2.2 Desafios relativos à segurança

Ataques externos intencionais podem alterar ou corromper os dados de processos em plantas industriais e produzir acidentes e prejuízos incalculáveis. As modernas técnicas de acesso remoto fazem uso de ferramentas e algoritmos com objetivo de proteger integridade das informações que são intercambiadas entre o exterior e as redes internas.

O controle de acesso previne pessoas não autorizadas a acessar e até corromper informações confidenciais, e garante que apenas os usuários autorizados tenham acesso a comunicação do acesso remoto.

Outro desafio a considerar é que a Internet é o principal meio pelo qual ocorrem as conexões remotas entre dispositivos físicos, e esta rede está sujeita a oscilações e interrupções na transmissão e recepção de dados (TANENBAUM; WETHERALL, 2003). Assim, é imprescindível considerar alternativas para mitigar a perda de informações de processos e impedir que a conexão esteja indisponível por tempo indeterminado.

Por fim, existe uma boa parte das plantas fabris ainda operam com dispositivos que não são compatíveis com os atuais protocolos de comunicação e não possuem, nativamente, infraestrutura para conexão à uma rede de dados ou rede Internet, que precisaram ser adaptados.

Os inúmeros métodos para controle e acesso remotos a equipamentos industriais possuem características comuns (XU *et al.*, 2014; SOUPPAYA; SCARFONE *et al.*, 2016):

- Necessitam garantir confidencialidade e integridade dos dados utilizando diferentes métodos de autenticação, senha e criptografia que podem ser combinados ou não;
- Devem manter um rastreamento e limitar as informações transmitidas de dentro para fora da rede interna para os usuários autorizados que, conforme seu nível de acesso, podem armazenar informações em seus equipamentos particulares;
- Manter uma latência aceitável na comunicação entre o cliente e o servidor, principalmente quando se necessita acompanhar em tempo real alguma operação ou extrair alguma informação em tempo conhecido.

Atualmente dispõe-se de tecnologias de comunicações que ampliaram a cobertura de serviço para atingir praticamente o planeta interligando dispositivos, bem como, o monumental incremento na velocidade de transmissão de dados comparado aos primórdios da comunicação de dados. Assim, plantas industriais que operam em áreas isoladas, podem se valer da troca de dados por meio de provedores de Internet através de fibra óptica e redes 3G, 4G ou 5G. Alternativas para comunicação remota de dados também estão sendo aplicadas nos projetos IoT e IIoT utilizando tecnologias consagradas ou emergentes, como WiFi, Bluetooth, ZigBee, LoRa, Sigfox, entre outras (KHODADADI; DASTJERDI; BUYYA, 2016).

Duas tecnologias evoluíram e convergiram para prover um alto grau de segurança. O tunelamento e técnicas de encriptação de dados técnicas se tornaram populares, e seus princípios são:

- **Tunelamento** é uma técnica que encapsula um protocolo dentro de outro de forma que o tráfego de dados não esteja visível no trajeto de transmissão entre redes ou dispositivos. Assim, o tráfego de dados fica transparente, indetectável e invisível em uma rede privada ou em uma rede pública, como a Internet;

- **Encriptação de dados** é o processo de codificação de mensagens ou arquivos gerando um código que permite que apenas que os dispositivos que possuam chaves de criptografia corretas tenham acesso àquelas informações. Desta forma a encriptação protege os dados digitais de serem entendidos caso tenham sido indevidamente interceptados no processo de seu envio. Algoritmos da criptografia provem verificação da origem da mensagem e a integridade da mesma, comprovando não ocorrer alteração em seu conteúdo.

Tecnologias que realizam conexões remotas, com alto grau de segurança, com utilização de recursos de autenticação de usuários, criptografia de dados transmitidos e tunelamento da conexão descrevem as conexões através de uma VPN. Uma rede privada virtual é considerada de acesso restrito, construído sobre a infraestrutura de uma rede pública (recurso público, sem controle sobre o acesso aos dados), normalmente a Internet, um tipo específico de ligação entre redes Intranet que utiliza a Internet como meio de conexão (WERNER, 1998).

2.3 Redes virtuais privadas

Uma VPN é uma conexão criptografada pela Internet entre dois dispositivo da rede. A conexão criptografada ajuda a garantir que os dados sejam transmitidos com segurança e confidencialidade. Ela evita que pessoas não autorizadas espionem o tráfego e permite que o usuário conduza o trabalho remotamente. A tecnologia VPN é amplamente utilizada em ambientes corporativos (SYSTEMS, 2021).

Redes de computadores sempre foram projetadas e desenvolvidas para compartilhar e distribuir serviços e recursos entre diversos usuários e proporciona vantagens tais como redução de custos de equipamentos, otimização de recursos, aumento de produtividade, entre outras. Uma rede local de computadores é composta de dispositivos computacionais como servidores, estações de trabalho, dispositivos de comunicação comutadores, roteadores, ponto de acesso de comunicação sem fio, placas de rede, cabos e diversos elementos para infraestrutura física.

A conexão da VPN liga computadores que estejam conectados fisicamente em provedores diferentes que dão acesso a rede mundial de computadores. A VPN estabelece um túnel virtual onde a informação trafega como se estivessem ligados lado a lado por um meio exclusivo, dividindo recursos somente entre estes (KOMPELLA, 2006).

A VPN dispõe de ferramentas para permitir o acesso de clientes remotos autorizados aos recursos da rede corporativa e viabilizar a interconexão de redes geograficamente distantes, de forma a possibilitar acesso de filiais à matriz. Em geral, uma VPN deve sempre possibilitar o compartilhamento de recursos e informações, além de assegurar privacidade e integridade dos dados que trafegam pela Internet (BORGES; FAGUNDES; DA CUNHA, 2019).

As técnicas de tunelamento, autenticação, transporte e encriptação de dados estão presentes na VPN atuando da seguinte forma:

- **Tunelamento** - Para que um datagrama seja enviado de um ponto a outro da VPN, ele precisa, primeiramente, ser encriptado para que fique ilegível para outros. Depois, precisa ser encapsulado, recebendo um cabeçalho adicional, para então ser enviado através da rede intermediária (por exemplo, a Internet). Ao chegar a seu destino na rede final, o datagrama é desencapsulado, desencriptado e encaminhado a seu destinatário final. Nos protocolos de tunelamento através da camada de enlace, os dados são trocados na forma de quadros PPP (*Point-to-Point Protocol*), que recebem um cabeçalho da camada de rede (IP) para serem transportados através da Internet;

- **Autenticação das extremidades** - Ao utilizar a autenticação das extremidades em uma conexão VPN garante-se que somente usuários validos estão participando da transmissão, através de protocolos de autenticação, que em sua maioria implementam algoritmos de *hash* como MD5, que garante a integridade das mensagens;

- **Transporte subjacente** - Devido ao protocolo TCP/IP ser a base da Internet, ele é amplamente utilizado para a comunicação entre redes. Entretanto, este protocolo é inseguro, por isso uma VPN utiliza a infraestrutura da rede já existente do TCP/IP, para transmitir os seus pacotes pela Internet adicionando cabeçalhos específicos, o que possibilita a instalação destes em qualquer parte da rede (KOLESNIKOV; HATCH, 2002);

- **Criptografia e autenticação de pacotes** - O uso de algoritmos criptográficos é um elemento essencial a interligação remota de redes industriais. A escolha do tipo algoritmo de criptografia depende dos recursos disponíveis nos dispositivos de comunicação e do nível de segurança que se deseja alcançar, pois a principal

ferramenta de encriptação, a chave para cifrar e decifrar. Quanto maior seu tamanho em bits, maior o consumo de tempo e de recursos computacionais são necessários para a comunicação, em contra ponto maior será a segurança.

Em relação as topologias, basicamente pode-se resumir em três modelos a seguir itemizados (BORGES; FAGUNDES; DA CUNHA, 2019):

- ***host-host***: Comunicação entre dois computadores separados fisicamente, podendo estar ou não em uma mesma rede;
- ***host*-gateway**: Conexão de um computador a uma rede fisicamente distante;
- **gateway-gateway**: Conexão entre duas redes, onde os gateways de VPN estarão sempre conectados.

Soluções VPN

As redes privadas virtuais apresentam ótima relação custo-benefício em comparação com os enlaces dedicados, apresentando menores custos e um nível de segurança na comunicação suficientemente razoável. O uso da Internet é uma vantagem importante uma vez que se encontra presente em todo o mundo, através de seus pontos de acesso espalhados por todos os lugares.

Com a utilização da criptografia nas informações e nas comunicações entre *host*s da rede privada é possível proporcionar um considerável nível de confidenciabilidade dos dados que trafegam pela rede. Ainda, com o uso do protocolo VPN é implementado um sistema de tunelamento para o tráfego dos dados de tal forma que estes podem ser enviados sem que outros usuários tenham acesso, e mesmo que os tenham, ainda os receberão criptografados. Por isso, é fundamental que os dispositivos responsáveis por cuidar da rede VPN devam ser capazes de garantir segurança e integridade das informações e dos dados que são transmitidos.

Através de (GOETHALS *et al.*, 2019) tem-se uma visão geral de algumas das mais utilizadas aplicações VPN .

- **OpenVPN** (INC., 2020a) é uma solução VPN amplamente usada. Usa padrões de criptografia abertos e oferece uma ampla gama de opções, sendo capaz de usar UDP e TCP para sua camada de transporte. Um ponto fraco do OpenVPN é que ela é de

thread único e, portanto, totalmente dependente da velocidade de um único núcleo do processador, não importa o quão poderoso seja o sistema;

- **WireGuard** (WIREGUARD, 2020) é uma solução VPN relativamente nova. Ela ainda não tem uma versão oficial estável pois ainda está em desenvolvimento;

- **ZeroTier** (INC., 2020b) é uma solução VPN desenvolvida pela ZeroTier Inc, apresentada pela primeira vez em 2011. ZeroTier ainda está em desenvolvimento ativo. A parte "*Zero*" de seu nome vem do fato de que ele requer configuração zero por padrão. Isso é conseguido por ter vários servidores *root*, chamados de "*Earth*" e gerenciados pela ZeroTier, que desempenham uma função semelhante aos servidores DNS da rede própria rede. Seu projeto também traz a vantagem de que nenhum *endpoint* precisa estar publicamente disponível, contanto que eles ainda estejam acessíveis através de algum endereço IP público via NAT. Sua operação é através de uma rede definida por software (*Software Defined Network*, SDN) seguindo suas regras de encaminhamento, o que elimina a necessidade de um servidor de VPN;

- **Tinc** (ORG, 2020a) é uma solução VPN anterior até mesmo ao OpenVPN, com lançamento inicial em novembro de 1998. A versão atual, 1.0.35, foi lançada em outubro de 2018, portanto, ainda está em desenvolvimento ativo. Como o OpenVPN, ele depende muito de padrões abertos. No entanto, ao contrário do OpenVPN, ele tem roteamento de malha completa por padrão, o que pode torná-lo mais eficiente em grandes redes com grandes quantidades de tráfego cliente-a-cliente;

- **SoftEther VPN** (ORG, 2020b) é uma solução VPN relativamente nova. Seu primeiro lançamento data de janeiro de 2014. A SoftEther é uma VPN multiprotocolo, com módulos para Open-VPN, L2TP / IPSec, MS-SSTP e seu próprio protocolo VPN SoftEther. Por padrão, ele usa o protocolo SoftEther VPN, que emula Ethernet sobre HTTPS. A vantagem de usar HTTPS para encapsular o tráfego VPN é tornar mais fácil contornar os *firewalls*, uma vez que as portas HTTPS são frequentemente acessíveis. Além de ser multiprotocolo, o SoftEther possui uma ampla gama de recursos, incluindo uma configuração de alta disponibilidade para seus terminais de servidor.

Foram estudadas e analisadas as arquiteturas de VPN acima e decidiu-se optar pela solução ZeroTier pelos seguintes motivos:

- Não necessitar de servidor VPN para estabelecer as conexões, pois a rede oferecida pela ZeroTier é controlada através de uma SDN que define regras para encaminhamento do tráfego. Desta forma, a comunicação tem baixa latência sem necessidade de ter um *host* controlador da conexão;
- Ser uma solução *Open Source*, ou seja, de código aberto;
- Apresentar alto nível de segurança;
- Facilidade de configuração e manejo;
- Não oferecer uma carga alta de processamento no *host* remoto ou local;
- Suporte a até 50 pontos de acesso identificados e conectados por um *NetworkID*, nome que identifica a VPN;
- Estar disponível para várias plataformas, tais como *Microsoft Windows*, *Apple Macintosh*, iOS para iPhone / iPad / iPod, sistemas operacionais *Linux*, entre outros, colocando à disposição para acesso remoto vários tipos de dispositivos.

2.4 Sistemas de controle em rede

Sistemas de controle em rede, do inglês *Networked Control Systems* (NCS), são sistemas de controle distribuído onde os sensores, atuadores e controladores estão alocados fisicamente em locais separados e são conectados através de uma rede de comunicação industrial (GODOY, 2011). O NCS representa a evolução das arquiteturas de controle em rede, fornecendo maior modularidade e descentralização do controle, facilidade de diagnóstico e manutenção e menor custo. O desafio no desenvolvimento de um NCS é contornar os efeitos degenerativos causados por fatores que afetam o seu desempenho e estabilidade. Assim, para o controle remoto de uma rede industrial é importante conhecer qual o valor de latência em sua comunicação de forma a identificar se estes efeitos podem ser degenerativos.

O sistema em rede industrial utilizado neste trabalho (WH) é uma Rede Sem Fio Industrial (RSFI). O uso das RSFI adquiriram uma enorme atenção devido a seus requisitos e desafios, pois oferecem alternativas atraentes com relação as redes cabeadas, pois, ajuda a melhorar a qualidade do produto, agiliza operações, acelera a produção, facilita a instalação, aumenta a flexibilidade e mobilidade nas fábricas, reduzindo os gastos

com infraestrutura e danos causados nos cabos em chão da fábrica, com a possibilidade de lidar com máquinas em movimento (MüLLER, 2012). Com a internacionalização e com o rápido desenvolvimento das RSFI, diversos protocolos de comunicação para este tipo de rede foram desenvolvidos, tais como, o WH, WIA-PA, ISA100.11a e ZigBeePRO (WANG; JIANG, 2016). Todos esses protocolos são baseados no padrão IEEE 802.15.4.

O protocolo WH é uma extensão sem fio do protocolo cabeado HART (FOUNDATION, 2009). O HART (*Highway Addressable Remote Transducer*) é sem dúvida o protocolo com maior número de aplicações em campo industrial, apresentando vantagens com os equipamentos inteligentes e utilizando-se da comunicação digital de forma flexível sob o sinal 4-20mA para a parametrização e monitoração das informações (COMPANY, 2021).

No desenvolvimento desta proposta, optou-se por utilizar o protocolo WH, para obter a latência dentro de um sistema de controle, a partir de um gateway. Alguns motivos conduziram a esta escolha, entre eles está o fato deste protocolo estar disponível em laboratório por trabalhos prévios e também por ser um protocolo amplamente empregado atualmente na indústria.

2.5 Latência

A latência ou atraso, definido como o tempo que um pacote leva para viajar da origem até o destino, tem sido um dos fatores críticos que afetam o desempenho das RSFI, podendo levar à instabilidade do sistema NCS (CHUNG *et al.*, 2016). O reconhecimento do atraso das comunicações é importante para investigar os efeitos que eles causam e suas consequências nos sistemas de controle em malha fechada (KRÖTZ, 2019).

Para sistemas de missão crítica e de controle de processos industriais, por exemplo, a automação de fábrica inclui aplicações operacionais com restrições de tempo, como aquelas usadas para controle de movimento e certas aplicações de eletrônica de potência. Desta forma, os requisitos de latência podem exigir que o valor esperado e a variação da latência permaneçam abaixo dos limites predefinidos. Para manter o desempenho de estabilidade e controle, aplicações de monitoramento e controle industrial impõem requisitos de atraso fim-a-fim rigorosos na comunicação de dados entre sensores e atuadores (SAIFULLAH *et al.*, 2015).

Conhecer e analisar a latência no acesso remoto a redes industriais torna-se impres-

cindível para garantir o sucesso no monitoramento e possível controle de processos industriais vinculados a estas redes. Portando, o trabalho apresentado nessa dissertação, busca avaliar a possibilidade de se realizar monitoramento e controle em tempo real de redes industriais através de acesso remoto pela Internet.

3 ANÁLISE DO ESTADO DA ARTE

Neste capítulo é realizada a análise do estado da arte, onde são apresentados alguns dos principais trabalhos relacionados com o tema desta pesquisa.

3.1 Acesso remoto via servidor web

Em BALASUBRAMANIAN; CELLATOGLU (2009) é relatado o desenvolvimento de hardware e software para controle remoto de unidades industriais que são controladas através da Internet. Três plantas modelo são levadas em consideração para ilustrar a atividade de controle remoto. A primeira é uma planta química com quatro processos, temperatura, nível de líquido, pressão pneumática e fluxo de líquido. A segunda, é uma planta de produção que envolve a produção de materiais para necessidades industriais, onde o processo é ajustado para seguir um pré-definido perfil de tempo de temperatura. A terceira aborda atividade de controle remoto de uma casa inteligente. Desta forma são validados três tipos de automação, de processos, fabril e residencial.

Sites são criados para monitoramento e emissão de comandos para as respectivas plantas modelo. O gerenciador destes sistemas está localizado remotamente com acesso à Internet, pode optar por escolher o *website* deseja operar bastando realizar sua autenticação de usuário e senha. Os comandos são encaminhados para o microprocessador correspondente anexado ao servidor web da planta. A página de login do usuário é construída com HTML e os problemas de senha são resolvidos com JAVA Script. Os autores não esclarecem como se realiza o acesso remoto, deixando aspectos como segurança, confiabilidade, entre outros carente de informações.

Em AL-KHATEEB; AL-KHATEEB; HAMEED (2009) os autores propõem um sistema com dispositivos elétricos e mecânicos que podem ser ligados, desligados e regu-

lados através de terminais distantes. Alegam que é possível executar monitoramento e também controle remoto de uma instalação industrial com várias unidades utilizando a Internet. Os autores informam que o sistema desenvolvido também é adequado para implementação de sistemas de segurança e SCADA. O experimento foi implementado e testado através de um ambiente simulado de residência, com dispositivos controlados, propondo simplicidade de operação através de um programa de fácil utilização, podendo ser adaptado para lidar com 256 unidades simultaneamente.

O protocolo de comunicação do controle de dispositivos implementado foi o protocolo X10. Este protocolo é utilizado geralmente para comunicação entre dispositivos eletrônicos usados para automação residencial (domótica), que usa como meio físico os fios de distribuição interna de energia elétrica para sinalização e controle.

Os transmissores enviam comandos como “ligar”, “desligar” ou “regular” precedidos da identificação da unidade receptora a ser controlada. Um console central abriga o controlador do sistema.

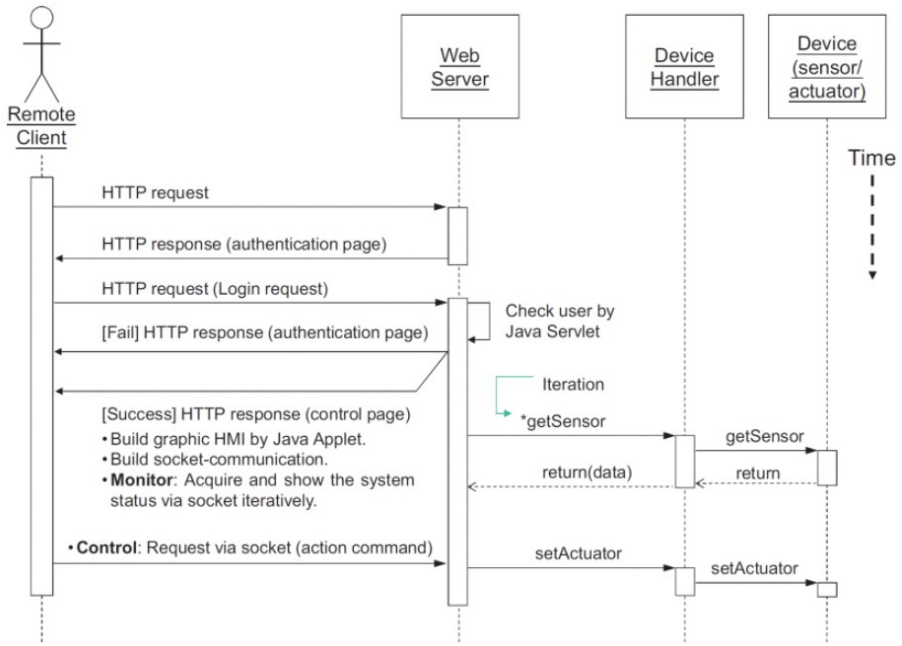
Um servidor web, protegido por senha e de simples configuração permite ao usuário controlar dispositivos X10. Os autores consideram a característica mais importante o site poder ser controlado de qualquer computador conectado à Internet, podendo todos os dispositivos aparecerem em uma página web, e todas as configurações serem feitas a partir do navegador web. O controle total de todos os dispositivos X10 é possível através de um endereço de rede privada, LAN ou Internet. Este endereço pode ser acessado diretamente pela Internet usando endereços de IP válidos e estáticos. No entanto a segurança ao acesso remoto pode estar prejudicada uma vez que servidores web com IP estático são vulneráveis a ataques na Internet. permitindo que qualquer usuário externo mal intencionado possa capturar eventos de comunicação, controlar o sistema ou derrubar seus serviços.

LEE; LEE (2013) propuseram uma abordagem sistemática para a modelagem de comportamento e controle remoto de sistemas transportadores industriais via Internet. Para demonstrar a abordagem proposta, uma aplicação ao sistema de transportador de sete posições e um protótipo foi realizado. Os comportamentos do sistema são modelados por meio de uma rede de Petri colorida de forma a lidar com a complexidade da modelagem em sistemas de grande escala com comportamentos semelhantes. Os autores afirmam que a técnica apresentada pode ser estendida para sistemas de transporte de grande porte. Foi utilizada uma arquitetura cliente-servidor para implementar o sistema operado remota-

mente. No lado do cliente, o operador remoto usa um navegador da web compatível com Java, como o Internet Explorer ou Firefox, para se conectar ao servidor web por meio da Internet. No lado do servidor, é empregado um PLC industrial com um servidor web integrado compatível com Java, designado para lidar com as solicitações do cliente. Dentro do PLC, um servlet Java trata da autenticação do usuário, um miniaplicativo Java fornece uma interface gráfica homem-máquina (HMI) e um diagrama de lógica Lader executa as operações detalhadas das tarefas solicitadas.

A Figura 3 modela a interação cliente-servidor usando diagramas de sequência do trabalho mencionado.

Figura 3 – Fluxo de sequência de mensagens do sistema operado remotamente.



Fonte: (LEE; LEE, 2013)

No trabalho de KOSHATWAR; SAWANT (2016) foi desenvolvido um sistema web embarcado usando processador ARM11 e um sistema operacional em tempo real, que possibilita a aquisição de dados e monitoramento e de status. Por meio de um navegador web convencional, pode-se acessar páginas da web desenvolvidas em HTML para apresentação dos dados e do monitoramento do status. O servidor da web incorporado é usado para compartilhar os dados com clientes on-line. Adicionalmente, a proposta oferece monitoramento por *streaming* de vídeo on-line. O sistema proposto se adapta aos requisitos estritos do sistema de aquisição e controle de dados, com boa confiabilidade, compacto e

de baixo custo, com acesso remoto.

Um sistema embarcado para monitoramento e controle remoto para o processo de bio-fermentação com acesso à Internet embarcada foi apresentado no trabalho de SUN; SHI (2018). O sistema proposto reduz o custo de comunicação, aumenta a estabilidade do controle e reduz significativamente o consumo de energia e o custo de armazenamento do produto.

O sistema possui circuitos de detenção e controle que analisam o efeito de parâmetros ambientais que afetam o metabolismo microbiano no processo de fermentação. A análise é feita através da coleta em tempo real da temperatura, do valor de pH, da concentração de oxigênio dissolvido e a altura da espuma. A plataforma do sistema utiliza o BOA server, um servidor web de pequeno processamento e código aberto bastante utilizado em sistemas embarcados. Desta forma, os usuários e operadores podem visitar e controlar remotamente o sistema por meio do navegador web na Internet. Operadores acessam remotamente o site do sistema de monitoramento e controle para monitorar e controlar o processo de fermentação em tempo real. Os operadores obtem informações sobre o estado da produção e controlam o processo de produção a qualquer momento e em qualquer lugar. Outros usuários acessar remotamente o site do sistema de monitoramento e controle para examinar o estado de bio-fermentação.

KOSTOLáNI; MURíN; KOZáK (2019) abordam o controle industrial convencional utilizando um controlador lógico programável (PLC), que foi aprimorado pelo uso de um gateway industrial inteligente. A plataforma Node-RED foi utilizada, baseada em aplicação web para fornecer interoperabilidade e sistema de controle robusto e confiável. O Node-RED, é uma ferramenta visual de ambiente de código aberto, que inicialmente foi desenvolvida para implementar, criar e/ou conectar dispositivos de IoT, tendo sido estendida posteriormente para hardwares, APIs e serviços web. Dados de processo coletados e parâmetros de sensores embutidos e outros dispositivos conectados podem ter seus dados rapidamente coletados, processados, transformados e usados para controle de equipamentos em ambiente de produção remoto. O acesso remoto ocorre por uma interface web com endereço IP e porta específicos. Os autores testaram o conceito em ambiente industrial real. Dados relevantes para controle remoto e visualização, como o estado atual dos dispositivos conectados ou dados do processo são obtidos diretamente do PLC para a Intranet ou Internet.

3.2 Acesso remoto via utilização de VPN e nuvem

O trabalho apresentado por HUANG; ZHANG; ZHU (2012) apresenta o desenvolvimento de um gateway de controle remoto de rede industrial com a finalidade de estudar e resolver os problemas de segurança gerados pela comunicação em rede entre o sistema SCADA e os computadores industriais provendo segurança afim de que a rede industrial se conecte à Internet com eficiência e confiabilidade.

Os autores levaram em consideração que os computadores industriais modernos já possuem pelo menos uma interface de rede. Porém esta interface é geralmente projetada para uso em LAN, não considerando a conexão com a Internet. Com esta limitação, a rede industrial, em geral, não suporta monitoramento remoto via Internet. Nesse sentido, os autores propõem um modelo de gateway de segurança de controle da rede industrial, e também um portal entre os equipamentos industriais e o sistema SCADA para monitorar os equipamentos industriais, encaminhar pacotes e bloquear dados não confiáveis, e ainda reportar eventos anormais.

Para o desenvolvimento da proposta foram projetados dois equipamentos *front-end* na rede industrial com a tarefa de gestão da segurança e troca de informações entre o computador industrial e o sistema SCADA. Estes equipamentos estão representados em dois nós e os nós são divididos em dois tipos, *super node e edge node*. O *edge node* foi instalado em PC local da indústria, e para acessar o sistema SCADA o *super node* foi instalado em PC remoto. Cada nó de borda também pode pertencer a mais de uma organização de rede (domínio). Foi desenvolvido um canal VPN de segurança para garantir a segurança dos dados entre o sistema SCADA e equipamentos industriais, o que permite resolver os problemas de comunicação remota entre o sistema SCADA e equipamentos industriais, fornecendo mecanismo de comunicação de segurança. Para garantir a segurança da transmissão de dados no túnel VPN, foi usado o algoritmo Twofish - um tipo de algoritmo de criptografia simétrica para criptografar os dados.

Ainda sobre o trabalho de HUANG; ZHANG; ZHU (2012), foi adotado um tipo de projeto de VPN de código aberto, o N2N. N2N é uma VPN ponto a ponto de camada dois, empregando o protocolo P2P. Como a rede é formada entre os dois nós da rede N2N, não é necessário o modelo de servidor e cliente.

A principal função do gateway é capturar e encaminhar pacotes diretamente relacionada ao desempenho do sistema industrial. A LAN industrial encaminha seus dados pelo

PC industrial local que participa da VPN e se conecta com a Internet diretamente. Assim, os equipamentos industriais podem trocar dados com o sistema SCADA.

O módulo de gerenciamento de nós é usado para gerenciar as informações de equipamentos industriais da LAN industrial. O gateway precisa monitorar o estado em tempo real de cada nó e criar uma tabela para armazenar as informações desses nós, como o endereço IP e o endereço MAC e a rede do nó. O gateway monitora a condição ativa dos nós e, em seguida, atualiza sua tabela.

A proposta desenvolvida nesta dissertação difere-se por utilizar acesso por VPN de código aberto, operando na camada 2, com sistema ponto a ponto, diferente do trabalho apresentado anteriormente, que utiliza uma VPN multiponto.

Em WHANG; ZHANG; CUI (2020) os autores propõem uma solução de sistema de gestão baseada em gateway de Internet industrial Este gateway é utilizado como um nó na ponta da rede para realiza funções de coleta, processamento e troca de informações.

O sistema consiste em três partes principais, os nós de coleta de dados do dispositivo, o gateway de Internet industrial e uma plataforma em nuvem. O gateway de Internet industrial conecta vários dispositivos de aquisição por meio de uma variedade de padrões de protocolo com e sem fio, tais como TCP, Modbus, porta serial, e outros. Vários equipamentos gateway podem ser colocados em cascata utilizando vários protocolos de comunicação de rede para prover a comunicação da Internet industrial. Nesta configuração, o gateway de Internet industrial atua na conexão com funções principais que incluem agregação, processamento, encaminhamento e monitoramento em tempo real dos dados do dispositivo subjacente. Além disso, o gateway se conecta à plataforma de nuvem pública e recebe as informações de controle emitidas e as processa de acordo.

Por fim, vários dados são agregados à plataforma de computação em nuvem por meio da estrutura de comunicação formada pelo gateway. A plataforma de dados processa os dados recebidos e os distribui na forma de um serviço em nuvem para uso por vários aplicativos, de modo que o aplicativo possa coletar dados da rede industrial de forma transparente e gerenciar o dispositivo em uma interface de chamada unificada. A plataforma de controle processa os comandos emitidos pelo usuário e os envia ao dispositivo de *downlink* correspondente para gerenciamento remoto. Os serviços em nuvem usam uma abordagem de “plataforma + aplicativo”. Ao fornecer uma plataforma estável, vários aplicativos podem ser acessados de forma flexível para oferecer suporte a mudanças

nos requisitos.

3.3 Resumo

Os trabalhos de AL-KHATEEB; AL-KHATEEB; HAMEED (2009), BALASUBRAMANIAN; CELLATOGLU (2009), LEE; LEE (2013), KOSHATWAR; SAWANT (2016), SUN; SHI (2018) e KOSTOLáNI; MURíN; KOZáK (2019), tratam de controle remoto industrial a partir de um endereço IP fixo disponibilizado na Internet para acesso via navegador web, possibilitando monitoramento e comandos de controle. O acesso por um IP fixo, muito comum no ambiente comercial, pode ser vulnerável necessitando a implantação de medidas extras como o uso de *Hyper Text Transfer Protocol Secure* (HTTPS) e *proxy*. Por fazer uso de VPN este trabalho evita a necessidade destas medidas extras uma vez que todas as conexões através da VPN são criptografadas, o que já traz muito mais segurança. Outro ponto positivo em priorizar o acesso remoto via VPN é o fato de as portas de acesso aos dispositivos não ficam expostas na internet.

A proposta de HUANG; ZHANG; ZHU (2012) proporciona o acesso de um sistema SCADA em localização remota, através de uma VPN - P2P, a LAN industrial. Utiliza servidores próprios para estabelecer a VPN diferente deste trabalho que utiliza uma rede SDN projetada para oferecer um acesso VPN sem necessidade de servidores locais. Este trabalho faz uso de uma VPN provida por uma rede SDN, o que evita a necessidade de servidores para estabelecimento da VPN e criação chaves criptográficas para as transmissões e recepção de dados. Por fim o trabalho de WHANG; ZHANG; CUI (2020) apresenta uma proposta de controle remoto industrial estabelecido em nuvem, onde uma rede de servidores alimenta de dados industriais a referida nuvem. O controle e acesso a dados acontece através da plataforma nuvem. Este trabalho apresenta uma proposta de acesso remoto direto entre usuário remoto e laço de controle não necessitando de uma plataforma em nuvem para troca de informações.

A tabela 1 apresenta o resumo dos trabalhos listados neste capítulo.

Tabela 1 – Trabalhos relacionados - resumo

Autores	*VPN*	*browser*	*NCS*	*Sistema controlado*
AL-KHATEEB; AL-KHATEEB; HAMEED (2009)	Não	Sim	Não	X-10 serial Interface
BALASUBRAMANIAN; CELLATOGLU (2009)	Não	Sim	Não	Microcontrolador
HUANG; ZHANG; ZHU (2012)	Sim	Não	Sim	PLC
LEE; LEE (2013)	Não	Sim	Sim	PLC
KOSHATWAR; SAWANT (2016)	Não	Sim	Não	Microcontrolador
SUN; SHI (2018)	Não	Sim	Sim	Microcontrolador
KOSTOLáNI; MURíN; KOZáK (2019)	Não	Sim	Sim	PLC
WHANG; ZHANG; CUI (2020)	Não	Não	Sim	Industrial Gateway
Proposta	Sim	Não	Sim	*Wireless*Hart

4 METODOLOGIA E IMPLEMENTAÇÃO

Este capítulo tem como objetivo apresentar o conjunto de métodos e materiais utilizados no desenvolvimento deste trabalho, sendo estes os equipamentos e software escolhidos. Também será detalhada a implementação da conexão remota entre o gateway da rede WH e o *host* remoto, bem como as características da aplicação desenvolvida para encaminhar comandos aos dispositivos da rede industrial simulada em laboratório. Por fim, são descritas as tarefas que envolvem a obtenção e análise da latência na implementação de comandos aos dispositivos de campo.

4.1 Visão do ambiente de conexão remota

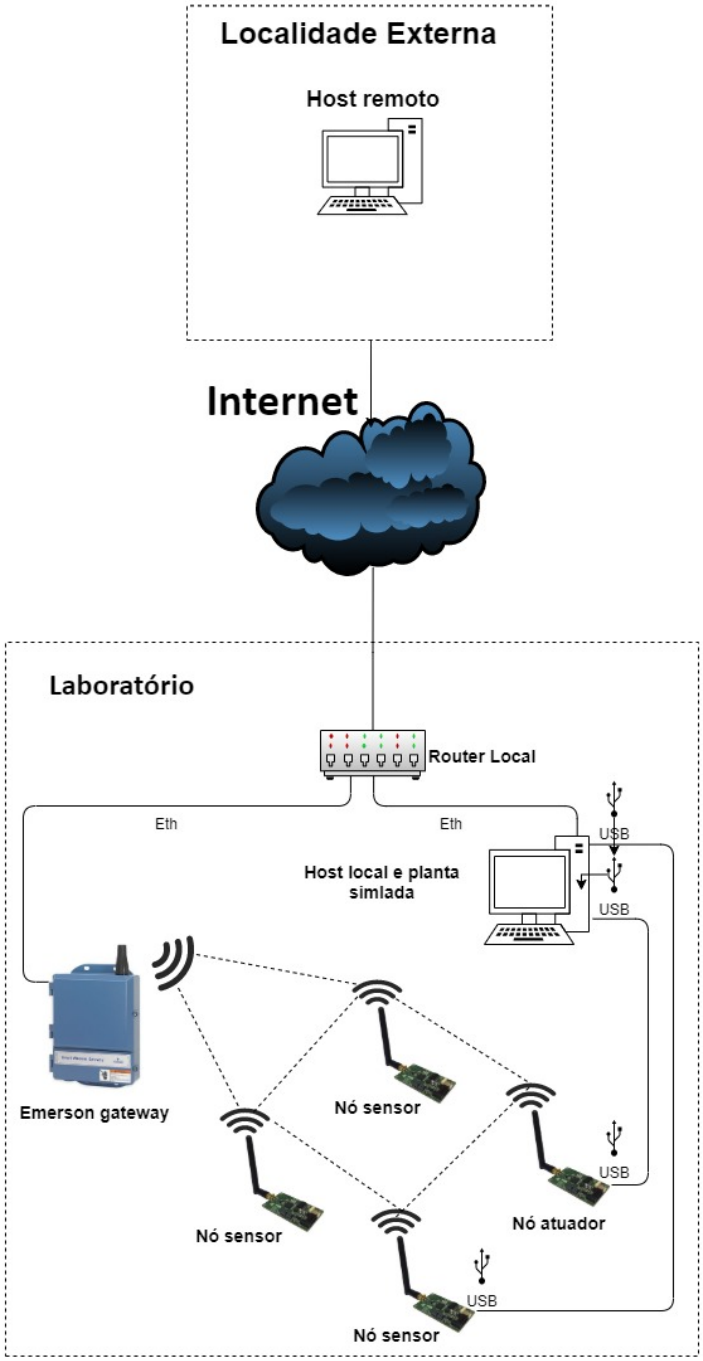
A arquitetura de rede total considerada nesse trabalho pode ser dividida em duas partes: a rede interna da planta e a rede externa, e ambas são conectadas entre si através da Internet. A rede interna é composta pelos dispositivos de campo WH comunicando-se com um gateway Emerson Rosemount modelo 1420, que é, além de gateway, gerenciador de rede e de segurança e ponto de acesso aos dispositivos de campo. O gateway é utilizado em ambiente de laboratório para pesquisas em automação industrial.

O gateway usa o padrão de comandos HART para transmitir e receber informações dos *field device* (FD), dispositivos de campo que atuam como sensores ou atuadores na planta. O equipamento utilizado tem uma de suas portas Ethernet ligada a uma rede local, e nesta, está ligado o dispositivo que atua como *host* local (PC). Este *host* possui portas USB disponíveis para conectar a alguns dos FD, que emulam sensores e atuadores de uma planta simulada com vistas a simular um NCS. Uma VPN interligando o *host* local e o remoto proporciona a conectividade necessária para que o *host* remoto possa comunicar-se com o gateway, e consequentemente com os FD. Através desta arquitetura

o *host* remoto, em uma posição geográfica qualquer, distante do laboratório, pode se comunicar com o gateway e os FD conectados a ele.

Uma visão geral da proposta deste trabalho pode ser obtida pela análise da Figura 4, onde os principais componentes da arquitetura podem ser vistos.

Figura 4 – Visão geral da proposta



Fonte: autor

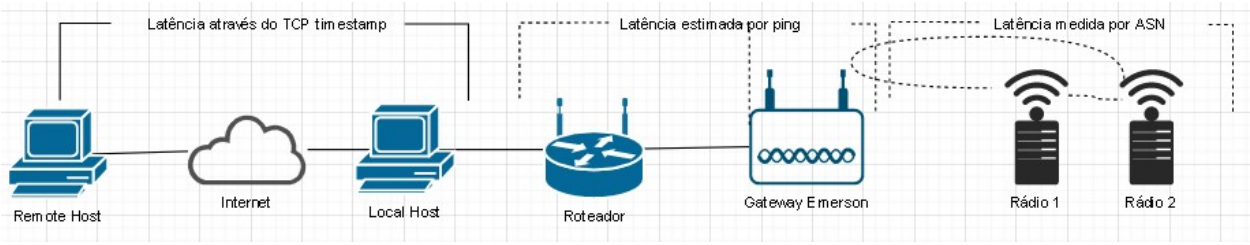
4.2 Estratégia de captura da latência

Para capturar a latência fim-a-fim medida entre o host remoto até o gateway e os dispositivos FD optou-se por separar as medições em três etapas com medições independentes:

- realizar medições de latência entre host remoto e host local - latência VPN;
- realizar medições de latência entre host local e gateway - latência rede local;
- realizar medições de latência entre gateway e FD conectados - latência WH.

A Fig. 5 revela como foi considerada a estratégia de captura da latência.

Figura 5 – Esquema de captura da latência *one-way*



Fonte: Autor

Esta estratégia foi necessária porque alguns componentes da interligação remota utilizam meios diferentes de conexão e de protocolos de comunicação.

4.3 Especificação dos elementos de hardware

Os dispositivos utilizados no experimento estão detalhados a seguir:

- **Gateway**

  O dispositivo comercial Emerson Wireless 1420A (EMERSON, 2020) que contém o *Network Manager*, o gateway em si e o ponto de acesso da rede WH. Sua capacidade de conexão e de até 100 dispositivos de campo. Possui recursos de configuração automática em rede WH utilizando rotas otimizadas e garantindo uma confiabilidade de até 99,3%. Dispõe, também, de uma interface homem-máquina provida por um servidor web interno onde é possível obter informações sobre os dispositivos da rede WH. Para monitoramento local do estado da rede, esta interface web é suficiente, pois a rede funciona basicamente como um sistema *convergecast*, onde os dados dos sensores são encaminhados ao gateway pela rede em malha

(KRÖTZ, 2019). O próprio gateway disponibiliza pela interface web, dados da taxa de atualização médias do tempo das comunicações, mas não realiza a coleta destes dados.

- **Dispositivos de campo**

  Os dispositivos de campo são oriúndos de projeto anterior do grupo de pesquisas, compatíveis com o protocolo WH (MüLLER *et al.*, 2010).

  Para a análise da latência das comunicações fim-a-fim dos dispositivos, foi necessária a alteração do *firmware* anteriormente desenvolvido (MüLLER, 2012), algo que só foi possível devido ao acesso a pilha do protocolo WH. Para adequar o *firmware* realizando as alterações nestes rádios foi utilizada a ferramenta IDE IAR *Embedded Workbench* 5.4. Estas modificações advém do trabalho de (KRÖTZ, 2019). Especificamente, as modificações no *firmware* permitem a obtenção dos ASN das mensagens que chegam e que saem do dispositivo, tanto em fluxo *uplink* quanto em *downlink*.

- ***Host* local e remoto**

  O *host* local faz o papel de um servidor para receber a comunicação do *host* remoto e encaminhar diretamente ao gateway, e tem as seguintes características:

  - Memória 4GB;
  - Processador Intel® Core i5™ CPU760 @ 2.80GHz $\times$ 4 núcleos;
  - Sistema Operacional Ubuntu 20.04.1 LTS tipo 64-bit;
  - Portas USB para acesso aos FDs sensores e atuadores.

  Os *hosts* remotos são equipamentos com características semelhantes ao *host* local.

- **Roteador**

  O roteador utilizado neste trabalho foi o TP-Link modelo WR740N que possui conexão de rede cabeada e *wireless* integrado com um roteador de compartilhamento de Internet e um *switch* de 4 portas. O roteador *wireless* é compatível com o padrão 802.11*b*, *g* ou *n* com enlaces de até 150Mbps brutos (TP-LINK, 2020).

4.4 Interligação física para acesso remoto

Os elementos necessários para interligação por acesso remoto estão detalhados a seguir.

4.4.1 Estabelecimento de conexão física-lógica entre *host* local, roteador e gateway

A conexão do *host* local ao gateway ocorre através de um enlace físico com cabo UTP (*unshielded twist pair*) conectado nas portas tipo *switch* do roteador formando a rede local.

O *host* local e gateway são configurados com endereços IPv4 conhecidos, fixos e registrados no serviço de DHCP (*Dynamic Host Configuration Protocol*) do roteador, facilitando a busca do *host* remoto e o encaminhamento de pacotes na rede local. O roteador estabelece o acesso à Internet através de sua porta nomeada WAN (*Wide Access Network*) com conexão por cabo UTP à rede local.

4.4.2 Estabelecimento de conexão *host* local - *host* remoto

O *host* remoto e o *host* local estão conectados pela internet através der uma VPN. Esta VPN configura uma interface lógica entre os *hosts* que conterá um endereço IP atribuído a cada *host* proporcionando comunicação de dados, criptografia de autenticação e comunicação.

4.4.3 Estabelecimento de Conexão da FD ao gateway

A conexão entre FD e gateway ocorre pela rede WH.

4.5 Preparação do ambiente de acesso remoto

O ambiente engloba a configuração de um caminho “contínuo” de comunicação entre um *host* remoto até um gateway e os FD conectados. Desta forma o ambiente de acesso remoto é preparado com a instalação da VPN. Para coleta de latência foi desenvolvido dois scripts na linguagem Python, um instalado no *host* remoto e outro instalado em um *host* local. Estas aplicações são responsáveis por encaminhar comandos do *host* remoto ao *host* local, ao gateway e aos dispositivos de campo interligados. O *host* local e gateway respondem com os valores de captura dos tempos nos trechos desta comunicação. Ao final, o script instalado no *host* remoto consolida as latências de todo o trajeto no *host*

remoto. Um terceiro script foi desenvolvido para envio de comando de leitura, de forma remota, de variável de processo de um FD.

Considerações sobre a VPN Zerotier

O hipervisor de rede ZeroTier é um mecanismo de virtualização de rede independente, que implementa uma camada de virtualização Ethernet semelhante ao VXLAN (protocolo de encapsulamento que fornece a conectividade de data centers usando o tunelamento para estender as conexões de Camada 2 em uma rede de Camada 3 subjacente) no topo de uma rede ponto a ponto criptografada global. O protocolo ZeroTier é original, embora seus aspectos sejam semelhantes a VXLAN e IPSec. Cada nó é identificado exclusivamente no VL1 por um endereço ZeroTier de 40 bits (10 dígitos hexadecimais). Este endereço é calculado a partir da parte pública de um par de chaves pública / privada. O endereço, a chave pública e a chave privada de um nó, juntos, formam sua identidade. Sua criptografia de chave pública assimétrica é Curve25519 / Ed25519, uma variante da curva elíptica de 256 bits. Cada pacote VL1 é criptografado ponta a ponta usando Salsa20 de 256 bits e autenticado usando o algoritmo de autenticação de mensagem (MAC) Poly1305 . O MAC é calculado após a criptografia (encrypt-then-MAC) e a composição de cifra / MAC usada é idêntica à implementação de referência NaCl .

A VPN ZeroTier combina as capacidades de VPN e SD-WAN, simplificando o gerenciamento da rede. Emula Layer 2 Ethernet com capacidades de multipatch, multicast e bridges. Assim a VPN ZeroTier oferece controle de rede e funcionalidade P2P, podendo criar redes descentralizadas acessando área de trabalho dos dispositivos, NAS (Network Attached Storage), e outros dispositivos de qualquer lugar. O mecanismo de regras ZeroTier VL2 difere da maioria dos outros firewalls e mecanismos de regras SDN de várias maneiras. O mais imediatamente relevante deles é que o mecanismo de regras ZeroTier não tem estado, o que significa que não possui rastreamento de conexão. Isso significa que a lista de permissões bidirecional não pode ser realizada simplesmente colocando pacotes de resposta na lista de permissões para conexões estabelecidas.

Configuração do túnel VPN entre host remoto e host local

O primeiro trecho a ser configurado é a conexão através da Internet do *host* remoto com o *host* local. O método de conexão remota ocorre através de um túnel VPN que permitir vincular os *host* através da Internet e tratá-los como se estivessem em um mesmo local. A VPN utilizada neste trabalho utiliza uma plataforma de operação “SDN-like”. A

tecnologia SDN tem como atrativo fornecer uma estrutura de rede dinâmica cuja existência é totalmente composta por software. Trata-se de uma tecnologia criptografada ponto a ponto, o que significa que, ao contrário de soluções tradicionais de VPN, as comunicações não precisam passar por um servidor central ou roteador, uma vez que toda a comunicação é administrada pelo sistema SDN. A VPN ZeroTier atua com doze servidores raiz organizados em dois *clusters* de seis membros distribuídos em todos os principais continentes e vários provedores de rede proporcionando uma latência de rede inferior a 100 ms de sua localização (INC., 2020b). Como resultado, a comunicação é muito eficiente e garante baixa latência.

A rede privada virtual escolhida para este trabalho foi pela ZeroTier que oferece uma VPN sem custos para até 50 *hosts* para uso não comercial. Desta forma, aproveitou-se de benefícios tais como a implantação e o processo de configuração simples do ZeroTier, manutenção simplificadas, permitindo o registro e gerenciamento centralizados de nós da rede, devidamente autorizados pelo console Web.

A plataforma ZeroTier fornece o ponto central de controle para sua rede definida por software acessada por um console aberto através de um navegador web onde é realizada abertura de conta, o gerenciamento de rede e dos dispositivos ligados a esta rede.

Basicamente, os principais itens a configurar no console web estão descrito no fluxograma da Figura 6.

Na Figura 7 pode-se observar a imagem após a criação da conta, criação da VPN, o nome da rede *UFRGS2020*, a atribuição de uma identificação *Network ID* para a rede, sua descrição e a escolha pela opção de uma rede privada (acesso restrito).

A Figura 8 apresenta a tela onde são realizadas as escolhas avançadas como a faixa IP dentre a uma variedade de intervalos oferecidos. É possível estabelecer eventuais rotas adicionais necessárias para acesso a redes locais específicas.

Configuração do host remoto e host local

Instalada a rede definida por software através da plataforma ZeroTier é necessária uma preparação em ambos os *host*. Para a configuração do *host* local e *host* remoto são considerados os seguintes requisitos:

- O *host* local e o *host* remoto devem executar o sistema operacional Ubuntu 20.04 com um usuário não raiz com privilégios (sudo);
- Tanto o *host* remoto, como o *host* local devem possuir a instalação da linguagem

Figura 6 – Fluxograma para estabelecimento de uma VPN ZeroTier-Basic

Fonte: Autor

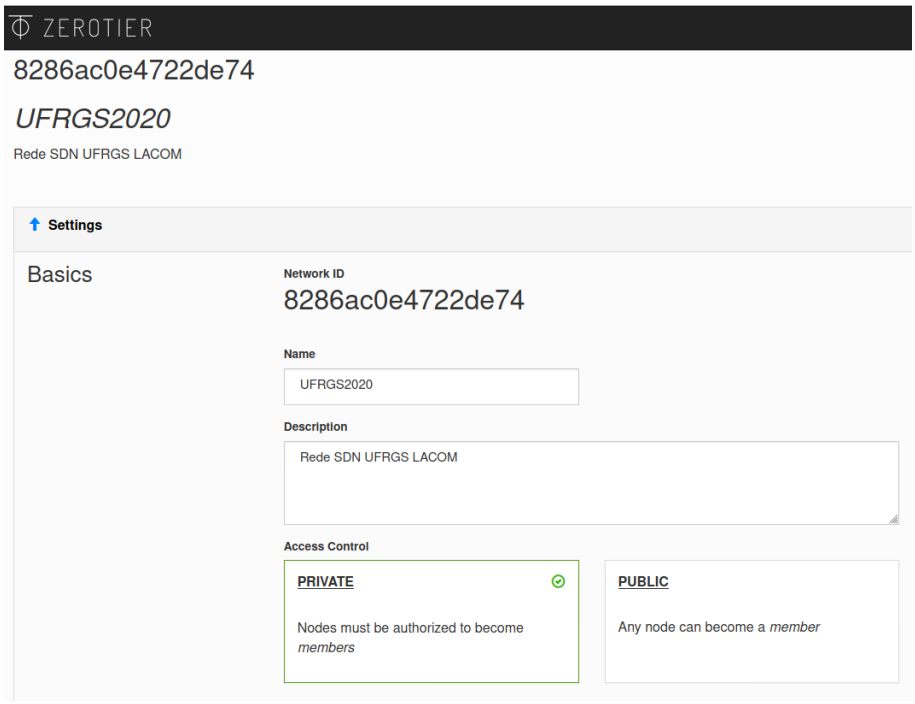
Python versão 3, ou superior;

- Complementando a preparação dos *host* é necessário a instalação dos módulos *numpy*, *socket*, *time*, *struct*, *os*, *datetime* e *reduce*.

A igualdade temporal entre *host* remoto e local é necessária para garantir a qualidade dos tempos de latência coletados. Para obtermos esta igualdade utiliza-se uma sincronização com um servidor que ofereça o protocolo NTP (*Network Time Protocol*), um protocolo que permite a sincronização dos relógios dos dispositivos de uma rede como servidores, estações de trabalho, roteadores e outros equipamentos à partir de referências de tempo confiáveis(NTP.BR, 2021).

A instalação do aplicativo Chrony é necessária para configurar o mesmo servidor NTP no *host* local e no *host* remoto. Este aplicativo realiza uma sincronização com servidores NTP, a cada solicitação de medição de latência proporcionando maior precisão na captura dos tempos.

Figura 7 – Imagem web gerenciamento ZeroTier- Basic



Fonte: Autor

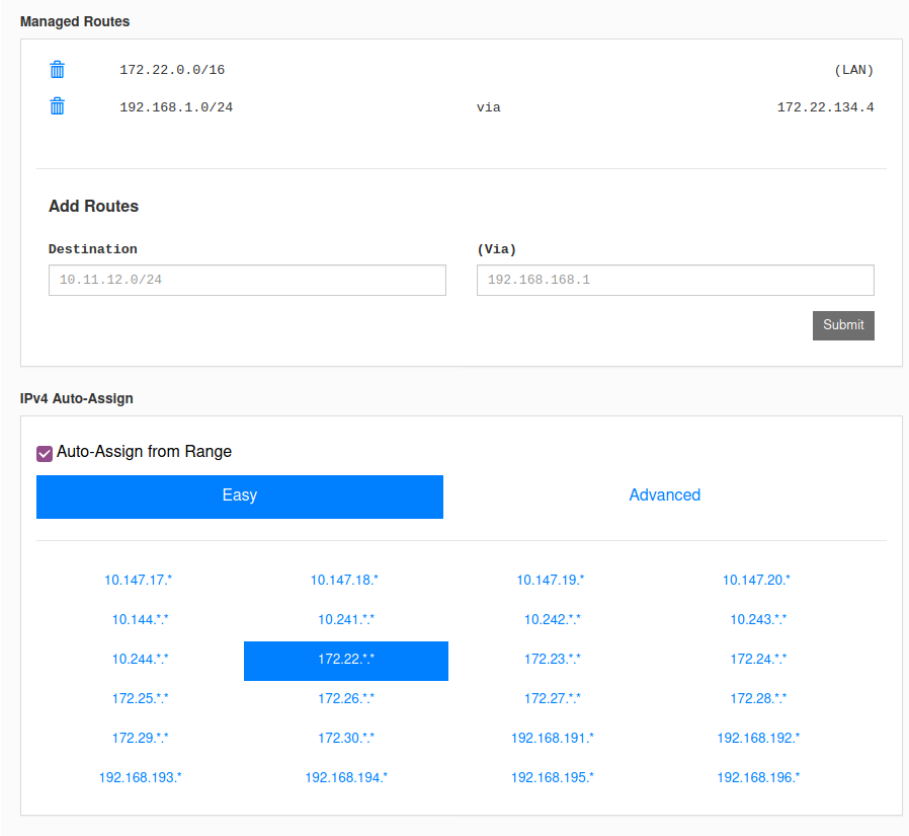
A preparação do *host* remoto e *host* local para ingressar na VPN é realizada com as seguintes operações realizadas através de um terminal console Ubuntu:

```
# Utilizando um certificado SSL para autenticar o site:
$ curl -s https://install.zerotier.com | sudo bash

# Utilizando a criptografica Linux GPG, uma opção mais segura
estiver disponível e utilizada neste trabalho:
$ curl -s  'https://raw.githubusercontent.com/zerotier/ZeroTierOne
/master/doc/contact\%40zerotier.com.gpg' | gpg --import \&\&

$ if z=\$(curl -s 'https://install.zerotier.com/' | gpg);
then echo "\$z"
```

Após a instalação e configuração do cliente VPN, é necessário obter um endereço ZeroTier e realizar a operação de *join* que realizará a junção na rede VPN. Para isso, usando, novamente, um console terminal é executado o seguinte comando:

```
$ curl -s 'https://pgp.mit.edu/pks/lookup?op=get\&search
```

Figura 8 – Imagem web gerenciamento ZeroTier - Avançada



Fonte: Autor

```
=0x1657198823E52A61'| gpg --import \&\& if z=$(curl -s
'https://install.zerotier.com/' | gpg); then echo "$z"
| sudo bash; fi

# Este comando o resultado aparece em duas linhas que mostram
o endereçamento de cliente VPN obtido na plataforma Zerotier:

Output:
*** Waiting for identity generation...
*** Success! You are ZeroTier address [ 916af8664d ].
```

A última operação necessária é a operação de *join*. Ao executar este comando é necessário inserir o endereço da VPN no lugar do *NetworkID*.

```
$ sudo zerotier-cli join NetworkID
Output:
```

```
200 join OK
```

O *host* remoto e o *host* local já são reconhecidos pela VPN, porém necessitam ser autorizados a realizar transmissões ou receber comunicações. Utilizando um navegador web é acessado o painel de gerenciamento da plataforma ZeroTier autorizando os endereços ZeroTier criados para o *host* remoto e *host* local. O painel de gerenciamento da plataforma ZeroTier já apresenta os novos *host* que ingressaram na rede faltando apenas assinalar a opção de "Auth?" para cada *host* que ingressou na VPN. O painel irá atribuir a cada *host* um IP válido para rede VPN liberando sua comunicação devidamente segura e criptografada.

Verificação da conectividade entre host remoto e host local

A conectividade entre os *host*s é verificada através do uso do aplicativo *ping* a partir de um *host* remoto apontando para o endereço IP do *host* local com sucesso na resposta do aplicativo.

Conexão host local ao gateway

O gateway está conectado a rede local em ambiente de laboratório com endereçamento 192.168.1.0/24 disponibilizado pelo roteador local. Como os demais endereços da rede local não são acessíveis para a VPN, é necessário estabelecer um roteamento entre esta rede local e a VPN para que os *host* remotos possam acessar o gateway WH.

Para encaminhar o tráfego da VPN para a rede local LAN foi feita uma configuração especial no *host* local alterando instruções no controle *iptables*. Foi ativado o serviço *network address translation* (NAT) e o serviço *Masquerade* do *host* local ligado ao gateway, para que os pacotes TCP endereçados ao gateway sejam encaminhados corretamente.

Verificação da conectividade entre host remoto e o gateway

A conectividade entre o *host* remoto e o gateway foi verificada através do uso aplicativo *ping* a partir de um *host* remoto apontando para o endereço IP do gateway na rede local e obtendo resposta com sucesso.

4.6 Scripts de captura de latência

Para verificar a viabilidade do uso da mesma em sistemas de monitoramento e controle a medida que os eventos ocorrem remotamente, com NCS como controlador local ou até mesmo remoto, e analisar a latência desta comunicação, foram desenvolvidos dois scripts

na linguagem Python que realizam todas as funções de captura e consolidação dos valores de latência a cada medição realizada. Esses scripts realizam todas as funções de envio de comandos ao NCS, captura e consolidação dos valores de latências.

Os dois script desenvolvidos em Python atuam em conjunto da latência atuam da seguinte forma:

4.6.1 Descoberta dos FD ativos na rede WH

O envio, através do script principal, do comando 814 ao gateway, terá como resposta a identificação dos FD ativos na rede naquele momento, apresentando resultado em tela. Esta operação também garante a conectividade de todo o trajeto entre *host* remoto até os FD da rede WH.

4.6.2 Coleta dos tempos de latência

- *Latência entre host remoto e host local*

  Neste trecho da rede, é obtida a latência da VPN que interliga estes dispositivos através de soquete de domínio Unix (socket) que estabelece um ponto final de comunicações troca de dados. Estes soquetes de domínio Unix permitem que dois processos abram o mesmo soquete para poder comunicar. A cada ciclo de coleta, o script principal, realiza a diferença entre o valor coletado no comando *time.time()* e o valor recebido do *host* remoto para este mesmo comando. Foi considerado o uso do protocolo da ferramenta OWAMP para analise da latência, mas como está ferramenta apenas poderia ser implementada neste trecho optou-se por manter a análise baseada na medição dos tempos de cada *host* sincronizado com um servidor NTP a cada ciclo de medição.

  O script utiliza o comando *time.time()* do módulo *datetime* importada para uso em linguagem *Python*. O módulo *datetime* converte *Epoch* em *Datetime* em *Python*. *Epoch* é um termo para o número de segundos que decorreram desde 1º de Janeiro de 1970, a data de lançamento do sistema operacional UNIX. O tempo de época é também chamado alternativamente de UNIX *timestamp* (DELFTSTACK, 2021). Ao iniciar cada ciclo de medição de latência, o script obtém o valor do tempo, obtido junto ao módulo *datetime* é obtido no *host* remoto e depois no *host* local para calcular a latência neste trecho da comunicação. Os valores recebidos estão

em milissegundos e fazem parte do cálculo da latência total consolidada a cada final de ciclo.

- *Latência entre o host local e o gateway*

  A cada ciclo de coleta, o script principal recebe do script instalado no *host* remoto a estimativa da latência desse trecho em milissegundos. O tempo de latência é medido a cada ciclo através de uma estimativa utilizando a metade do tempo obtido executando o comando *ping* direcionado ao endereço IP do gateway. O comando *ping* no sistema operacional Linux mede o tempo de ida e volta de um pacote teste entre dois dispositivos. O uso do comando *ping* foi necessário para estimar a latência no trecho *host* local e gateway, uma vez que o gateway não permite rodar um script, internamente. Os valores recebidos estão em milissegundos e fazem parte do cálculo da latência total consolidada a cada final de ciclo.

- *Latência entre o gateway e o FD*

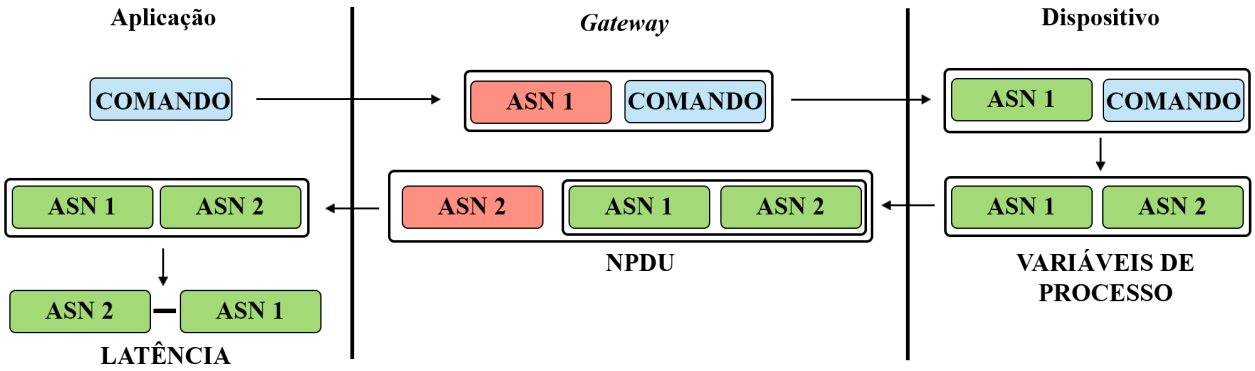
  Entre o *host* remoto e o gateway, o protocolo de transporte é TCP/IP. Os pacotes enviados e recebidos do gateway utilizam o protocolo *HART-over-IP* (Hart-IP) e estão encapsulados pelo protocolo TCP/IP. Esta é uma técnica de tunelamento, que suporta tanto o protocolo TCP quanto o UDP (FOUNDATION, 2009). Entre o gateway e os FD, a conexão ocorre através da utilização do protocolo de comunicação WH. Para obter esta latência, foi utilizada a estratégia descrita em (KRÖTZ, 2019), onde através da análise da diferença do valor do ASN (*Absolute Slot Number*) obtido no gateway e do ASN do FD durante a execução de um comando WH. O ASN é um *nonce*, iniciado no momento da criação de uma rede WH e incrementado a cada número de *slot*. Trata-se de um contador que começa com um valor igual a 0 e a cada *slot* transmitido dentro dos superquadros em uma rede WH, seu valor é incrementado em uma unidade. Os *slots* têm intervalos padronizados de 10 ms no WH, assim, o resultado da diferença entre o valor de ASN no momento em que um comando é recebido e encaminhado pelo gateway e o valor do ASN no momento que este comando é recebido pelo FD, indica o tempo de latência de comunicação dentro da rede WH.

  Uma modificação foi feita no *firmware* dos FD para que estes possam receber comandos diretamente do *host* remoto que normalmente são restritos ao gerenciador

da rede e ao gateway. Desta forma, foi implementado um comando especial para que o gateway e os FD possam revelar sua uma estampa temporal das mensagens das mensagens recebidas.

Assim, a cada ciclo de captura, a latência entre o gateway e o FD modificado é obtida utilizando dois comandos WH especiais implementados, 130 e 131, que respondem com os valores de ASN do gateway e do FD encaminhando ao *host* remoto para consolidação. O comando especial 130 foi implementado para escrita em variáveis de processo de um dispositivo. Este comando é utilizado para obter o ASN das comunicações de um dispositivo. O comando especial 131 tem a finalidade de leitura das variáveis de processo de um dispositivo. Assim como o comando especial 130, foi modificado para obter o ASN obtido pelo comando 130. Os comandos modificados obtém os valores atribuídos de ASN1 obtidos na chegada do comando ao gateway e os valores de ASN2 de chegada do comando ao FD destinado. O script do *host* remoto ao receber as informações ASN realiza a operação subtração dos valores de ASN2 e ASN1, obtendo um valor numérico referente ao número de *slots* ocorridos entre o recebimento da comunicação pelo gateway e depois ao chegar no FD. A Figura 9 explicita o método para determinar o valor de latência utilizando valores de ASN.

Figura 9 – Método para determinar a latência WH fim-a-fim



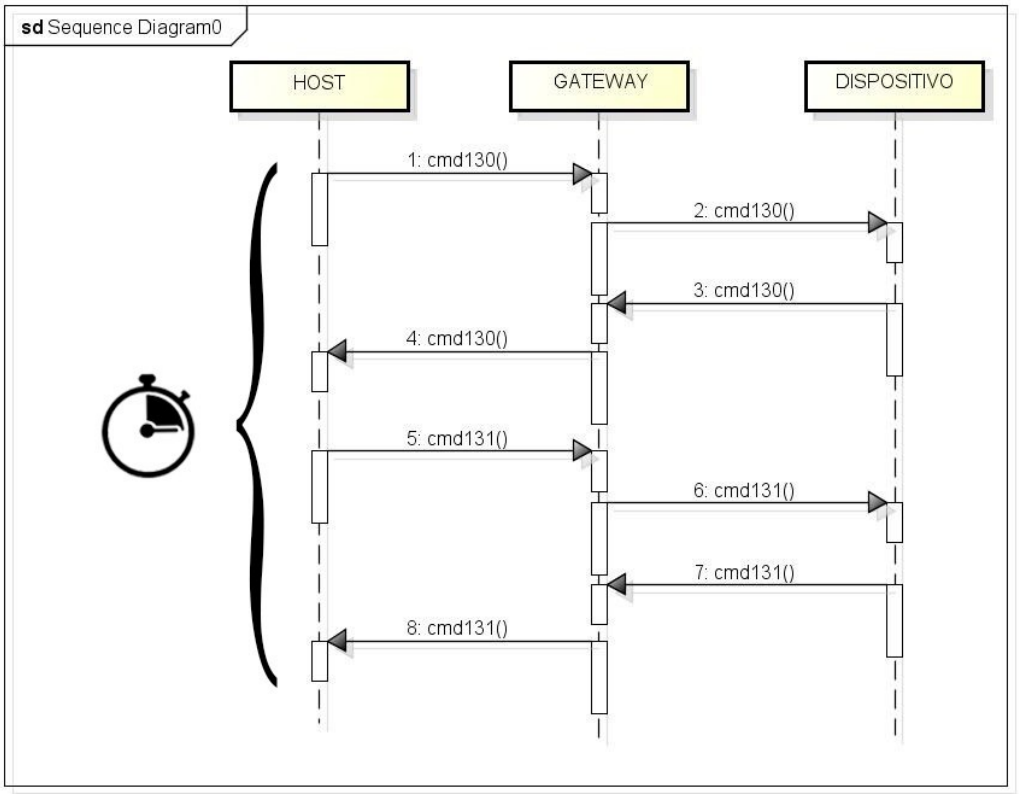
Fonte: (KRÖTZ, 2019)

Como cada *slot* tem um tempo fixo de 10 ms, utilizou-se esta métrica para obter a latência entre gateway e FD com a multiplicação do valor encontrado entre a diferença de ASN2 e ASN1 por 10 ms. Assim, uma parte do script implementado no *host* remoto utilizou o trecho de captura da latência entre o gateway e um FD

escolhido.

A Figura 10 demonstra como ocorre a obtenção da latência WH *one-way*.

Figura 10 – Ciclo para obtenção da latência WH fim-afim



Fonte: (KRÖTZ, 2019)

Em resumo, no *host* remoto, é executado o script principal com as seguintes funções:

- Consulta ao gateway, identificando os dispositivos de campo ativos na rede WH de forma a conhecer e confirmar o alcance da comunicação entre *host* remoto e os FD;
- Solicita ao operador a quantidade de medições a serem realizadas em determinado FD ativo;
- Executa o ciclo de medições de tempos na quantidade de medições solicitada no passo anterior realizando as seguintes tarefas:
  - conexão ao script instalado no *host* local;
  - sincronismo do relógio do *host* remoto com um servidor externo através de *Network Time Protocol* NTP;
  - consulta de latência de um FD, da rede WH, através dos comandos especiais 130 e 131;
  - solicita ao segundo script a medição do tempo do *host* local e a estimativa da latência entre gateway e o *host* local;
  - consolida o cálculo da latência total com os dados coletados;
  - apresenta os resultados;
  - registra os resultados em arquivo tipo planilha;
- Consolida a planilha com os resultados obtidos;
- Encerra o processamento.

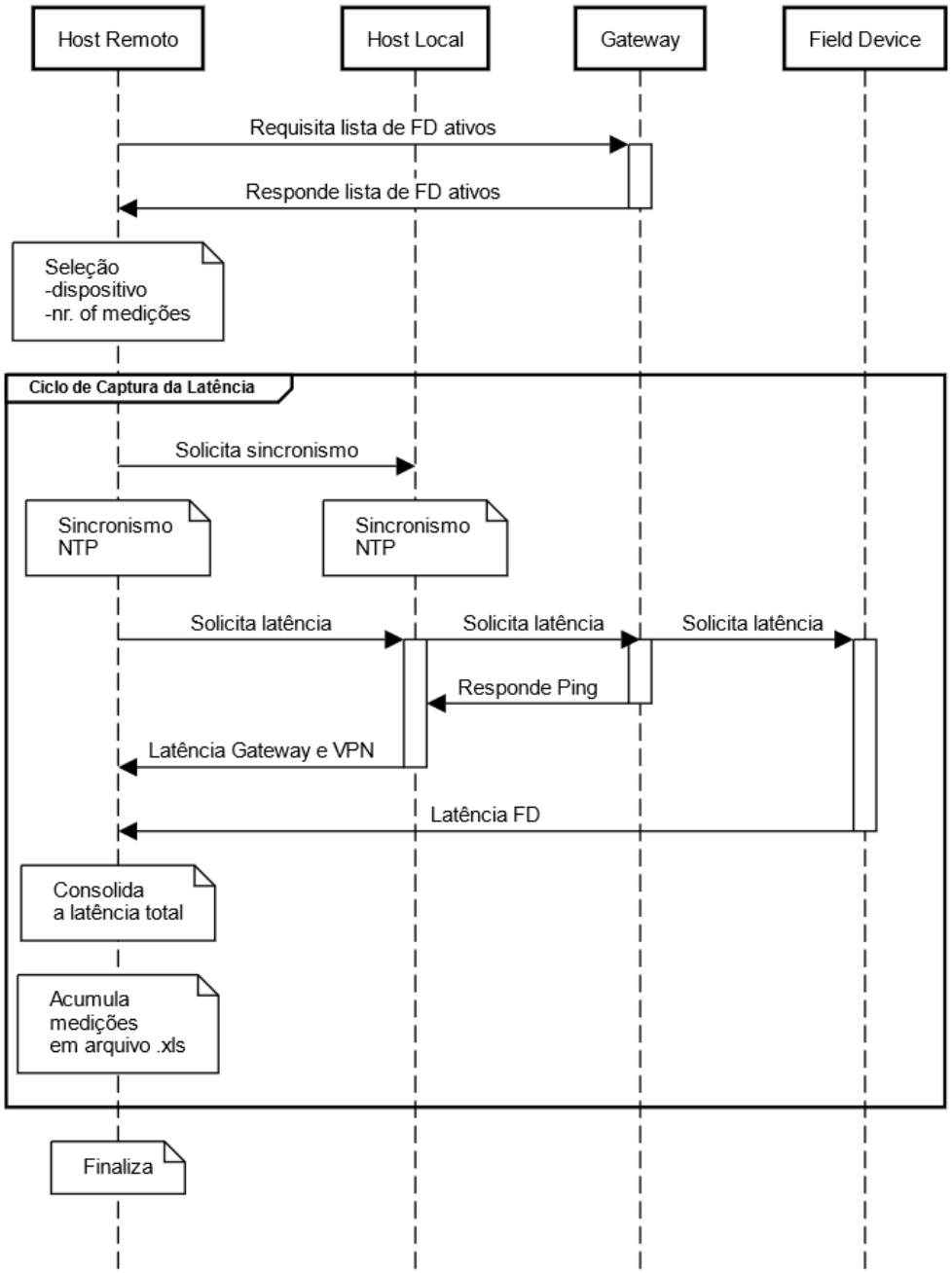
O segundo script, localizado no *host* local, aguarda permanentemente o acionamento pelo primeiro, realiza, a cada ciclo de medição, as seguintes tarefas:

- Responde a conexão solicitada pelo script principal;
- Sincroniza o relógio do *host* local com um servidor NTP;
- Coleta o tempo do relógio sincronizado do *host* e encaminha ao script principal;
- Realiza a estimativa do valor da latência entre *host* local e gateway e envia ao script principal;

- Encaminha os dados coletados ao script principal, aguardando a próxima requisição.

A Figura 11 apresenta o diagrama sequencial de operação dos scripts descritos.

Figura 11 – Diagrama Sequencial da captação da latência fim-afim



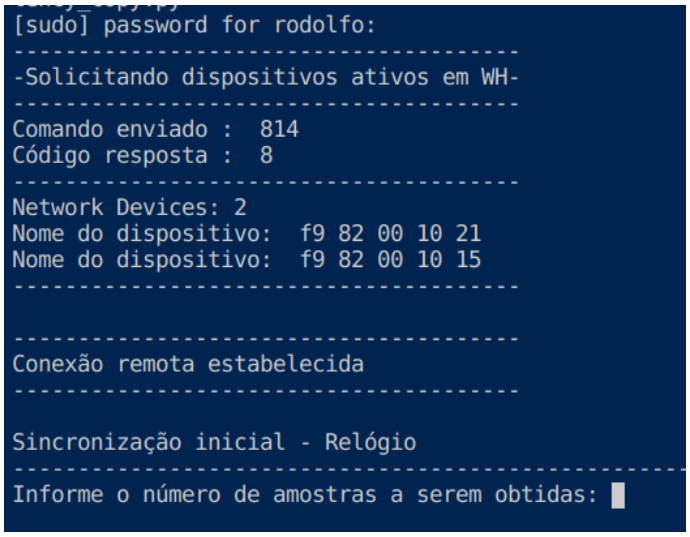
Fonte: Autor

A análise de testes realizados em scripts escritos em Python com várias execuções de loops foram feitos para estudar o tempo médio da operação do script Python. Os testes geraram resultados na ordem de poucas dezenas de microssegundos com um desvio

padrão de centenas de nanossegundos (SCIENCE, 2021). Desta forma a influência do tempo de execução do script Python na medição de latência foi desprezada uma vez que a ordem de grandeza das medições de latência em redes industriais WirelessHART é de milissegundos.

Na figura 12 pode-se observar o script principal, instalado no host remoto, iniciar a execução realizando uma consulta dos dispositivos ativos de rede através dos comando 814 recebendo o código de resposta 8, indicando sucesso na consulta. A figura também mostra que a resposta do gateway informa que a rede WH possui dois dispositivos ativos naquele momento, cujos *tags* são 1021 e 1015. Um aviso de sincronização com um servidor NTP para ajuste do tempo do *host* remoto e local é mostrado. Por fim, o script envia uma solicitação ao operador para inserir a quantidade de amostras de latências a serem coletadas.

Figura 12 – Imagem mostrando os dispositivos ativos em rede WH



Fonte: Autor

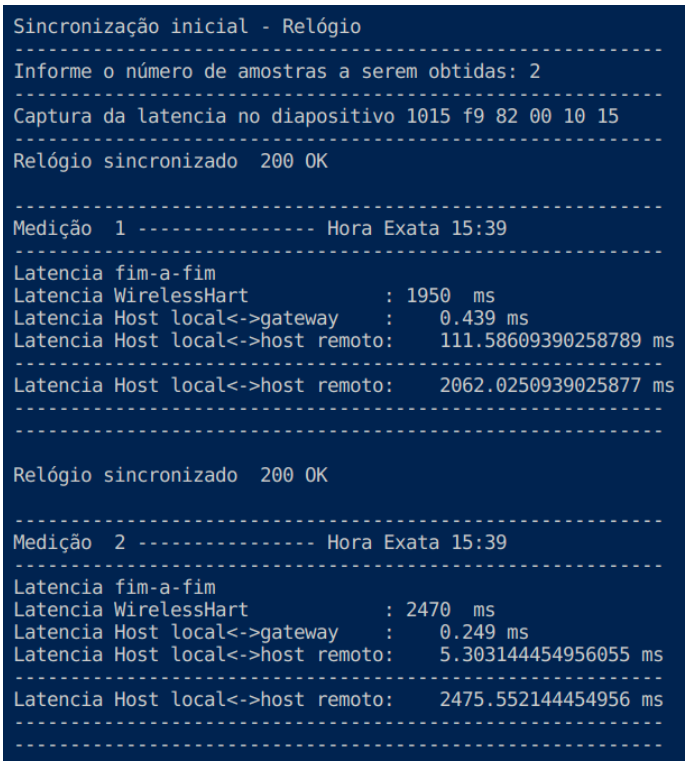
A Figura 13 mostra, em tela, o resultado de duas coletas de latências dos trechos e sua totalização.

4.7 Atuação do script para leitura de variável em FD

Utilizando o acesso remoto à rede WH via VPN, foi preparado mais um script Python com a finalidade de enviar um comando de leitura de variável de um determinando FD, possibilitando a supervisão remota de um processo em uma rede WH.

Para testar a atuação de vários acessos remotos executando simultaneamente, a leitura de variável de um determinado FD na rede WH, foi feito uso da tecnologia de virtualização por contêineres. O uso de contêineres é uma abordagem de desenvolvimento de software na qual um aplicativo ou serviço, suas dependências e suas configurações (abstraídos como arquivos de manifesto de implantação) são empacotados juntos como uma

Figura 13 – Imagem mostrando os resultados de latência do dispositivo da rede WH



Fonte: Autor

imagem de contêiner. O aplicativo em contêineres pode ser testado como uma unidade e implantado como uma instância de imagem de contêiner no SO (sistema operacional) do *host*. Os contêineres também isolam os aplicativos uns dos outros em um sistema operacional compartilhado. Os aplicativos em contêineres são executados com base em um *host* do contêiner que por sua vez é executado no sistema operacional (Linux ou Windows). Cada contêiner pode executar um aplicativo web ou um serviço inteiro (MICROSOFT, 2021). Com o *hypervisor*, é possível criar máquinas virtuais, as quais possuem recursos virtuais isolados a partir de recursos físicos individuais (VERAS, 2016)

Utilizou-se o benefício da escalabilidade no uso de contêineres para criar várias instâncias executando o script de leitura de variável de um FD simultaneamente, acessando a VPN com endereços IP distintos simulando, assim, vários usuários obtendo dados de monitoramento de uma rede WH.

5 ESTUDOS DE CASO

Neste capítulo são apresentados os resultados dos experimentos realizados juntamente com o detalhamento da análise e estatística de latência obtida nas medições.

5.1 Avaliação experimental

Tendo em vista avaliar o desempenho da técnica proposta, foi projetado e executado um experimento de acesso remoto em uma rede WH real para realizar a coleta de dados de latência total de forma rápida e analisar seus resultados. Pretendeu-se com isso avaliar a possibilidade de executar monitoramento e/ou controle remoto em plantas industriais. Os objetivos do experimento são:

- Verificar se há uma diferença significativa nas medições de latência de um acesso remoto realizado diretamente dentro da rede local industrial, ligada diretamente ao gateway industrial quando comparados ao acesso remoto externo, em localização regional, nacional ou internacional;

- Determinar qual trecho componente da medição de latência total em acesso remoto de uma rede industrial tem maior significância;

- Verificar o efeito das medidas de latência total com a alteração da topologia da rede WH, impondo a um determinado FD, rota de comunicação indireta com o gateway;

- Demonstrar a leitura de variável de processo de um FD dentro da rede WH, por meio de vários acessos remotos simultâneos, possibilitando uma múltipla supervisão remota de uma rede WH.

A bancada experimental utilizada inclui os seguintes equipamentos:

- Cinco FD que atuam como dispositivos de campo com o *firmware* modificado para que aceitem os comandos especiais 130 e 131 de forma a capturar e transmitir os valores de ASN para poder consolidar o valor da latência até a rede WH;
- Um PC para atuar como *host* local e para executar as coletas de latência local, além do gateway.

A Figura 14 mostra o *set-up* de laboratório.

Figura 14 – Bancada experimental

Fonte: Autor

Foram realizadas medições de latência nas localidades listadas abaixo:

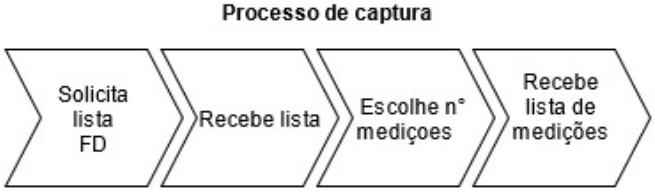
- Brasil - Porto Alegre - Bairro Mont' Serrat;
- Brasil - Natal - Universidade Federal do Rio Grande do Norte;
- Chile - Santiago - Universidad de Concepcion;
- Alemanha - Magdeburg - Saxônia-Anhalt.

A operação do *script* é descrita de forma simplificada na Figura 15.

Os dados coletados representam as latências obtidas durante o acesso remoto desde todas as localidades citadas.

Foram feitas 100 medições de latências dentro do laboratório e, sucessivamente, mais 100 medições desde os locais remotos disponíveis para análise deste trabalho.

Figura 15 – Operação do script



Fonte: Autor

Com as medições coletadas nas localidades, procedeu-se uma análise inicial sobre os dados coletados e percebeu-se que as amostras capturadas na Universidade Federal do Rio Grande do Norte tinham valores de latências cerca de 100 vezes mais altas que as medições nas outras localidades. A investigação revelou que o computador oferecido pela instituição para realização da coleta apresentou um erro de relógio de cerca de 5 a 6 minutos, independente das ações de correção, ou comando inserido no script de coleta de latências para realizar o sincronismo com servidores NTP a cada amostra de latência capturada. Desta forma foi necessário desconsiderar as medições desde a cidade de Natal.

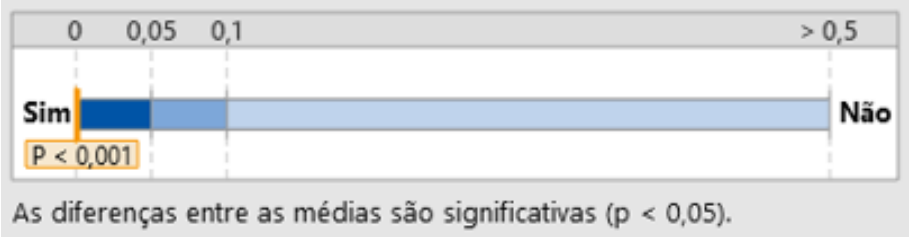
5.2 Estudo de caso: análise das latências medidas no acesso remoto

Neste estudo de caso, o objetivo foi verificar se há uma diferença significativa no latência de um acesso realizado diretamente dentro da rede local industrial, ligada diretamente ao gateway industrial, quando comparado ao acesso remoto externo, em localização regional, nacional ou internacional.

Uma análise de variâncias (ANOVA - *Analysis of Variance*) considerando como fator controlável “local” e a análise da resposta “latência total” permite avaliar as diferenças significativas. Através do conceito de inferência estatística pode-se afirmar que as medidas obtidas representam as características deste tipo de medição nas localidades. Um teste de hipóteses apoia o objetivo proposto e verifica se há uma diferença significativa nas medidas de latência local com um acesso direto à rede WH e os acessos remotos. Em estatística, entende-se que a potência estatística de um teste de hipóteses é a probabilidade de rejeitar H_0 quando H_0 é falsa (MONTGOMERY; RUNGER, 2003). Este teste é importante para obter um poder estatístico suficiente para uma análise acertada, ou seja, estimar se o número de medições realizadas são suficientes para um teste de hipótese apresentar, ou não, uma diferença específica. Para este experimento a hipótese nula é confirmar que

todas as médias nas localidades são iguais, já a hipótese alternativa preconiza que nem todas as médias são iguais. Para determinar se alguma das diferenças entre as medianas é estatisticamente significativa, é comparado o valor-p com o seu nível de significância. Um nível de significância (denotado como α) de 0,05 é usual. Um valor-$P \leq \alpha$ significa que as diferenças entre algumas das medianas são estatisticamente significativas (LLC., 2021). A análise de variância demonstra que valor-$P = 0$ é menor que α. Isto fica bem evidenciado na Figura 16.

Figura 16 – Análise de significância



Fonte: Autor

Para auxiliar nesta tarefa, foi feito uso do software estatístico Minitab. O Minitab calcula, a partir de informações de variabilidade e potência estatística desejada, o tamanho que a amostra deve ter para que um teste com o seu poder especificado detecte cada diferença encontrada. Como os tamanhos amostrais são números inteiros, o poder real do teste pode ser um pouco maior que o valor de poder que foi especificado, de forma que aumentando o tamanho amostral, o poder do teste também aumentará (LLC., 2021). A partir do software estatístico é possível estabelecer a informação da análise de variância e potência estatística, e representar a probabilidade do teste detectar uma diferença significativa nas medias de latência por localidade.

Resultados

Os valores resultantes da ANOVA obtida estão apresentados na tabela 2 e observa-se que o valor de P é igual a zero.

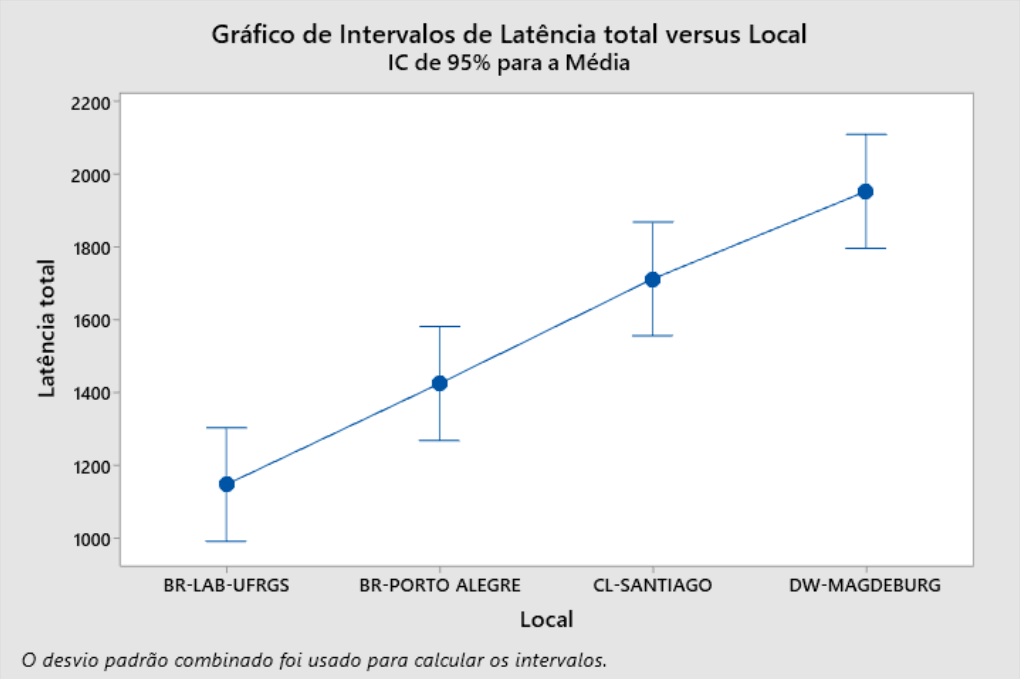
Tabela 2 – Análise de variância

Fonte de variação	*Graus de liberdade*	*Soma dos Quadrados*	*Média Quadrática*	*Valor de F*	*Valor de P*
Local	3	36602414	12200805	19,32	0,000
Erro	396	250102853	631573		
Total	399	286705267			

A análise de significância permite afirmar que existem diferenças significativas entre as médias das medidas de latência total em todas as localidades.

No gráfico de intervalos da Figura 17 cada ponto representa uma média da amostra e cada intervalo é um intervalo de confiança de 95% para a média de um grupo. É possível afirmar que se tem 95% de confiança de que a média do grupo não está dentro do intervalo de confiança do grupo confirmando diferenças estatisticamente significativas.

Figura 17 – Intervalos temporais da latência total



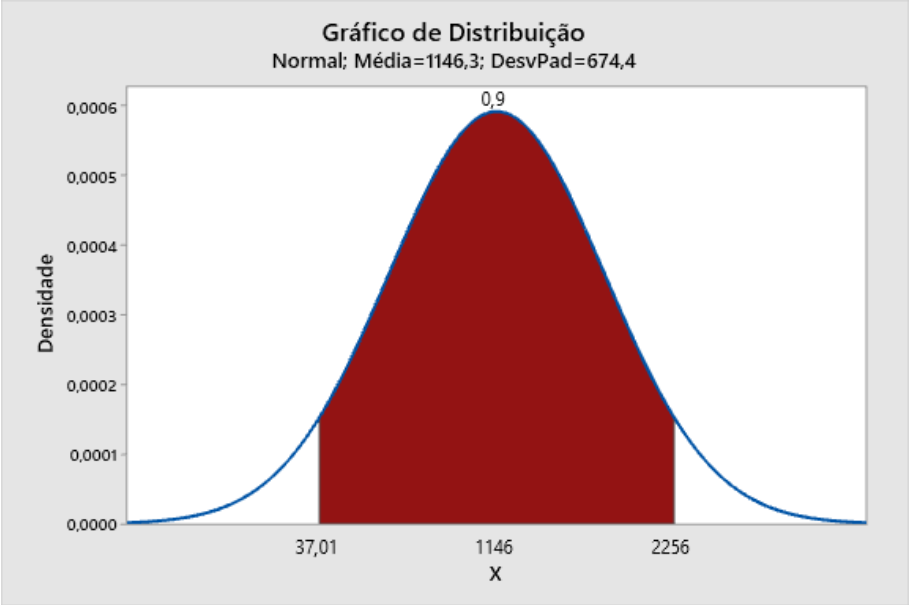
Fonte: Autor

Analisando o tipo de distribuição obtida nos conjuntos de amostras de latência em cada localidade percebe-se que são do tipo Gaussiana ou normal, pois apresenta uma curva simétrica em torno do seu ponto médio, apresentando assim seu famoso formato de sino. Para entender o comportamento dos limites de latência que poderiam servir como parâmetros de tempo de latência em projetos de controle utilizados foram gerados gráficos de distribuição de probabilidade. Estes gráficos descrevem a função distribuição acumulada (FDA) que calcula a probabilidade acumulada para um determinado valor de medição de latência.

A figura 18 apresenta o gráfico da função de distribuição acumulada das medições no laboratório da UFRGS. Pelo gráfico observa-se que a probabilidade de um valor de medição de latência escolhido aleatoriamente deve estar entre 37,01 ms e 2256 ms.

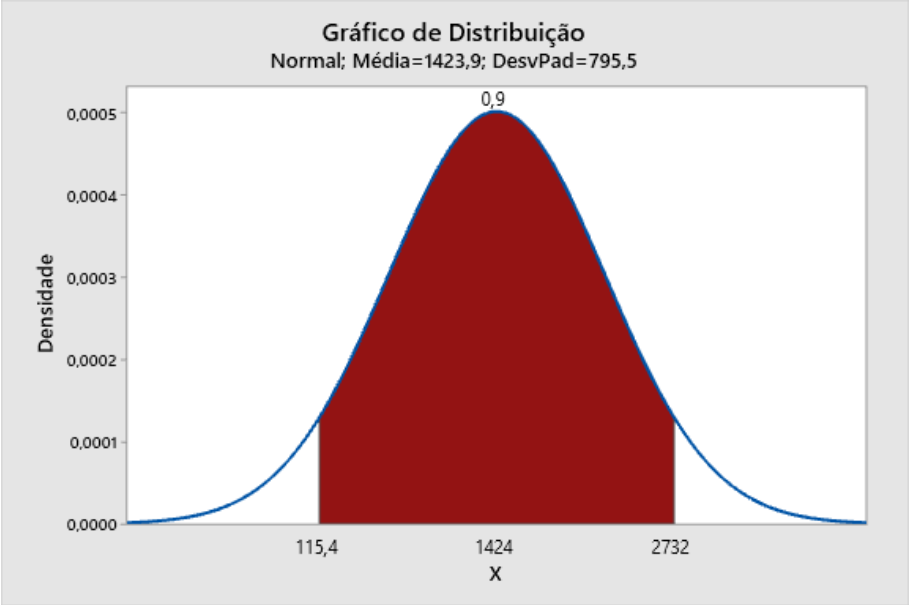
Na figura 19 mostra o gráfico da função de distribuição acumulada das medições em localidade na cidade de Porto Alegre, onde observa-se que a probabilidade de um valor de medição de latência escolhido aleatoriamente deve estar entre 115,4 ms e 2732 ms.

Figura 18 – Gráfico de distribuição acumulada - medições - UFRGS



Fonte: Autor

Figura 19 – Gráfico de distribuição acumulada - medições - Porto Alegre

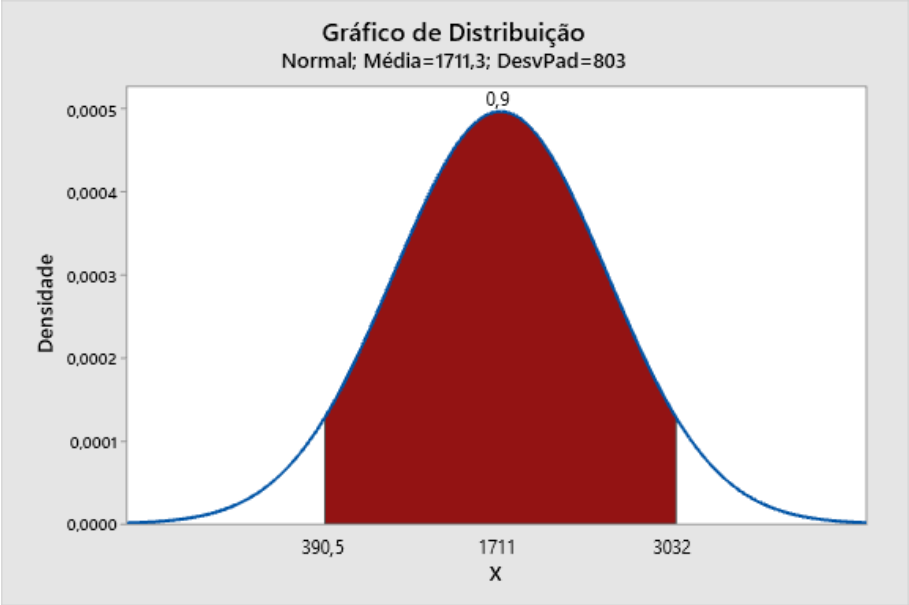


Fonte: Autor

Na figura 20 mostra o gráfico da função de distribuição acumulada das medições no Chile, onde observa-se que a probabilidade de um valor de medição de latência escolhido

aleatoriamente deve estar entre 390,5 ms e 3032 ms.

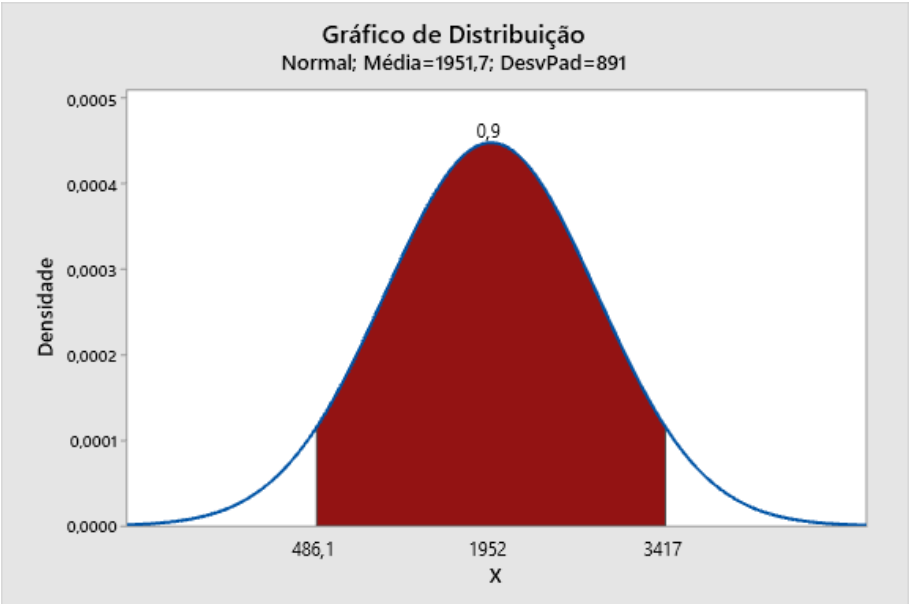
Figura 20 – Gráfico de distribuição acumulada - medições - Chile



Fonte: Autor

Por fim, na figura 21 mostra o gráfico da função de distribuição acumulada das medições no Chile, onde observa-se que a probabilidade de um valor de medição de latência escolhido aleatoriamente deve estar entre 486,1 ms e 3417 ms.

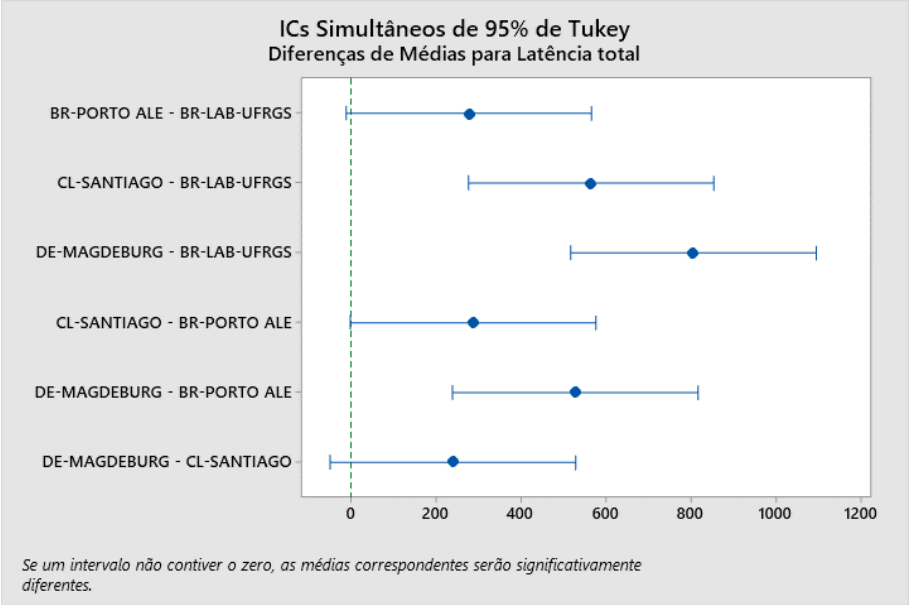
Figura 21 – Gráfico de distribuição acumulada - medições - Alemanha



Fonte: Autor

Tukey é o método usado em ANOVA para criar intervalos de confiança para todas as diferenças pareadas entre as médias dos níveis dos fatores, controlando a taxa de erro global para um nível de significância especificado. É importante considerar a taxa de erro global ao efetuar comparações múltiplas, porque as chances de cometer um erro do tipo I para uma série de comparações é maior do que a taxa de erro para uma comparação separada. Para compensar essa alta taxa de erro, o método de Tukey ajusta o nível de confiança para cada intervalo individual de forma que o nível de confiança simultâneo resultante seja igual ao valor especificado (LLC., 2021). Na análise pelo método Tukey apresentado na Figura 22 o eixo vertical apresenta os pares de localidades considerados. No eixo horizontal representa as diferenças das médias do pares e seus intervalos de confiança, menos a diferença mínima significativa entre os valores medidos em cada localidade.

Figura 22 – Comparações pelo método Tukey



Fonte: Autor

As variações que não incluem zero indicam que a diferença é estatisticamente significativa entre os os pares medidos.

A tabela 3 indica os pares de localidades onde podemos afirmar que as diferenças de suas medições de latência são significativamente diferentes. O nível de confiança simultâneo de 95% indica que é possível ter 95% de confiança de que todos os intervalos de confiança contêm as verdadeiras diferenças.

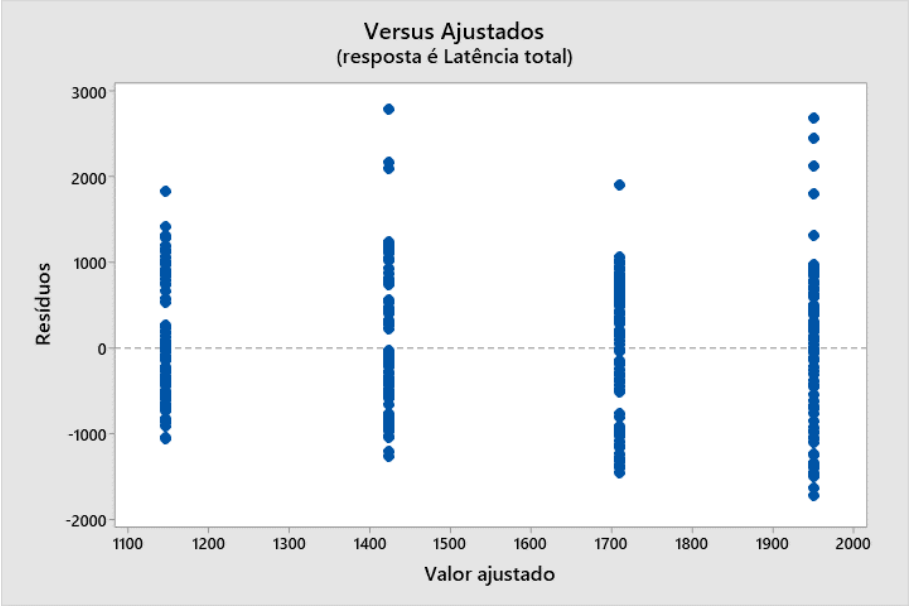
Para determinar se o modelo estatístico escolhido atende às suposições da análise,

Tabela 3 – Comparação da significância dos pares nas localidades

Local	***Local***	***Significância***
BR-Porto Alegre-Home	BR-LABORATÓRIO	Não significativa
CL-Santiago	BR-LABORATÓRIO	Significativa
DE-Magdeburg	BR-LABORATÓRIO	Significativa
CL-Santiago	BR-Porto Alegre-Home	Não significativa
DE-Magdeburg	BR-Porto Alegre-Home	Significativa
DE-Magdeburg	CL-Santiago	Não significativa

utilizou-se o gráfico de resíduos. O gráfico de resíduos ajuda a determinar se o modelo é adequado e satisfaz aos pressupostos da análise. A análise do gráfico de resíduos apresentado na Figura 23 demonstra que os pontos caem aleatoriamente em ambos os lados de 0, sem padrões reconhecíveis nos pontos, confirmando que os pressupostos foram satisfeitos e o modelo pode ajustar bem os dados.

Figura 23 – Comparações pelo método Tukey



Fonte: Autor

Uma análise do poder estatístico dos resultados assegura que a quantidade de medições foi suficiente para sustentar os resultados encontrados. As informações de variabilidade estão diretamente relacionadas com o tamanho amostral e por isso sua estimativa deve ser adequada. Para o cálculo do tamanho amostral, foram inseridas na aplicação as

informações das 100 medições preliminares sobre a variabilidade dos dados, que inclui o desvio padrão e a diferença entre as médias que se quer detectar. Os valores da análise de variância e das estatísticas da tabela 4 apoiam a estimativa do poder estatístico para as 100 medições realizadas em cada local.

Tabela 4 – Estatística de 100 medições

Local	***Medições***	***Média[ms]***	***D.P.[ms]***
BR-Porto Alegre-LAB.	100	1146,3	674,4
BR-Porto Alegre-Home	100	1423,9	795,5
CL-Univer. Conception	100	1711,3	803,0
DE-Magdeburg	100	1951,7	891,0

A raiz quadrada da média do erro (631573) estima o diferença máxima entre as médias das medições e resulta em 794,72. Na tabela 4 observa-se que o maior desvio padrão entre as localidades é DE-Magdeburg com 891 ms, portanto este é o valor escolhido para diferença máxima no cálculo do poder estatístico.

Tabela 5 – ANOVA 1 fator α = 0,05- Desvio padrão assumido= 794,72

Diferença Máxima	***Tamanho Amostral***	***Poder***
891,0	100	0,981292

Com 100 medições obteve-se a potência estatística de 98,1%, conforme mostra a tabela 5. Desta forma, foi confirmada uma potência estatística adequada para definir a existência de diferenças significativas da médias obtidas nas medições das diversas localidades.

***Resultados*:** Em cada localidade foi gerado um conjunto de 100 amostras cujo o resultado estatístico desta medições estão representados na tabela 4. É possível declarar que o valor de P é igual a zero, ou seja, menor que o nível de significância (α), concluindo, com 95 % de confiança, e 98% de potência estatística, que a localização geográfica do acesso remoto afeta significativamente a variável de resposta latência total, fim-a-fim, medida e obtida na casa dos milissegundos.

5.3 Estudo de caso para determinar trecho de latência mais relevante

A análise apresentada nessa seção tem como objetivo determinar qual trecho de medição de latência em um acesso remoto tem maior significância para o sistema de monitoramento e controle industrial remoto. Para esta determinação foi feito o cálculo das médias dos trechos que compõe o cálculo da latência em cada amostra, ou seja, a latência entre *host* remoto e local, entre *host* local e gateway e entre gateway e FD medido.

Tabela 6 – Médias da latência trecho-a-trecho

Trecho medido	***Total de Medições***	***Média*** [ms]	***D.P.***[ms]
Latência *gateway*-FD	400	1422,3	811,2
Latência *host* local-*gateway*	400	0,26	0,037
Latência *host* remoto-local	400	135,7	167,5
Latência total	400	1558,3	847,7

***Resultados*:** A tabela 6 apresenta as médias de cada trecho que compõe a latência total. Percebe-se que o valor medido dentro da rede WH representa 91,27% da latência total média medida e evidencia ser este trecho o mais significativo na composição da latência total fim-afim do acesso remoto a uma rede industrial com este tipo de protocolo.

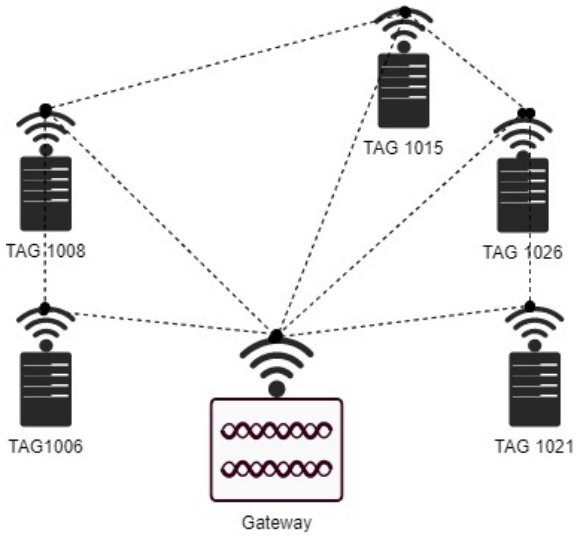
As demais latências, entre a *host* remoto e local (representando a VPN) tem um impacto de 8,71% sobre o valor da latência total, e entre *host* local e gateway aproximadamente 0,02% o que pode ser considerada desprezível quando comparada aos outros valores.

5.4 Estudo de caso - Efeito da latência na alteração da topologia WH

Nas análises de tempos de latência anteriores foi considerada uma topologia conforme a apresentada na Figura 24, em que um FD (TAG 1015), alvo das medições, estava conectado diretamente a ao gateway que realiza a formação e manutenção da rede WH. Neste estudo foi feita uma comparação das medidas de latência alterando a topologia da rede WH de tal forma que o FD alvo da medição, de tal forma a não se comunicar diretamente com o gateway.

Nesta nova topologia, mostrada na Figura 25, o FD (TAG 1015) foi forçado a procurar uma rota de acesso ao gateway através da conexão com outros FD da mesma rede. Isto

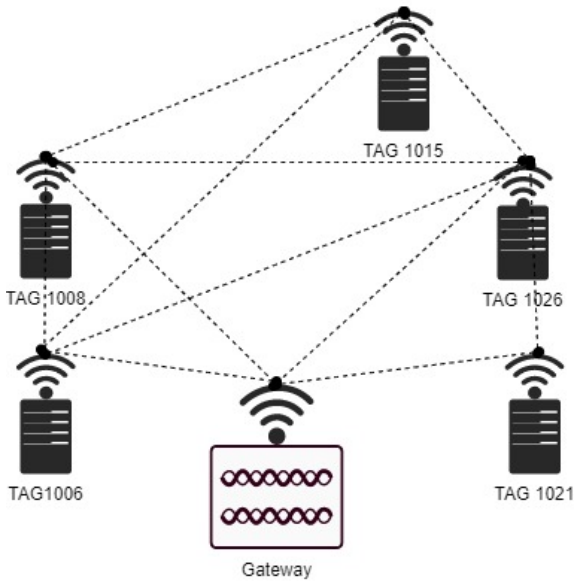
Figura 24 – Topologia Original



Fonte: Autor

foi feito afastando o FD do gateway, além de reduzir sua potência de transmissão.

Figura 25 – Nova topologia



Fonte: Autor

Agora o FD necessita acessar ao gateway indiretamente para enviar seus dados, utilizando os suas conexões com os FD TAG 1006, TAG 1008 e TAG 1026. A Figura 26 mostra imagem do *webserver* do gateway 1420. Nesta imagem observa-se que em sua terceira coluna que o FD TAG 1015 não está mais conectado ao gateway. Sua comunicação se dá pelos FD ativos da vizinhança, com identificações TAG 1026 e TAG 1008.

Figura 26 – Imagem dos FD conetados ao gateway e seus vizinhos

HART Tag	Node state	Active neighbors	Neighbors
TAG 1006		wihartgw TAG 1026 TAG 1008 TAG 1015	4
TAG 1008		wihartgw TAG 1006 TAG 1015 TAG 1026	4
TAG 1015		TAG 1008 TAG 1026 TAG 1006	3
TAG 1021		wihartgw TAG 1026	2
TAG 1026		wihartgw TAG 1021 TAG 1006 TAG 1008 TAG 1015	5

Fonte: Autor

As comparações são realizadas analisando as medições com a topologia de rede original e alterada nas seguintes localidades:

- BR - Porto Alegre - Local;
- BR - Porto Alegre - Remoto;
- DE - Magdeburg.

Para comparar e avaliar as medidas, foi utilizado o modelo estatístico de uma ANOVA balanceada. A ANOVA balanceada ajusta modelos de mínimos quadrados para determinar se as médias de dois ou mais grupos variam quando se tem fatores categóricos e uma resposta contínua. Neste modelo, uma análise de variância determina a existência de diferença significativa entre as medidas de latência trecho a trecho do acesso remoto considerando a topologia original e a nova topologia.

Resultados obtidos

No modelo ANOVA balanceada a análise de variância determinou a existência de diferença significativa entre as medidas de latência trecho a trecho do acesso remoto considerando a topologia original e a nova topologia.

- Análise nova topologia x topologia original

A tabela 7 apresenta a análise de variância da medida de latência do trecho entre o gateway e o FD, considerando os valores obtidos com a topologia original e a nova topologia. Como resultado, o valor de P é zero, indicando que existe diferença significativa nas medidas deste trecho considerando as duas topologias.

Tabela 7 – Análise de variância - trecho gateway-FD

Fonte de variação	*Graus de liberdade*	*Soma dos Quadrados*	*Média Quadrática*	*Valor de F*	*Valor de P*
Local	1	369974402	369974402	287,20	0,000
Erro	198	255061798	1288191		
Total	199	625036200			

A tabela 8 apresenta a análise de variância da medida de latência do trecho entre o gateway e o *host* local, considerando os valores obtidos com a topologia original e a nova topologia. Como resultado, o valor de P é diferente de zero, indicando que não existe diferença significativa nas medidas deste trecho considerando as duas topologias.

Tabela 8 – Análise de variância - trecho gateway-*host* local

Fonte de variação	*Graus de liberdade*	*Soma dos Quadrados*	*Média Quadrática*	*Valor de F*	*Valor de P*
Local	1	0,02430	0,024299	8,56	0,005
Erro	198	0,56226	0,02840		
Total	199	0,58656			

A tabela 9 apresenta a análise de variância da medida de latência do trecho entre o *host* local e o *host* remoto, considerando os valores obtidos com a topologia original e a nova topologia. Como resultado o valor de P é diferente de zero indicando que não existe diferença significativa nas medidas deste trecho considerando as duas topologias.

Tabela 9 – Análise de variância - trecho *host* local-*host* remoto

Fonte de variação	*Graus de liberdade*	*Soma dos Quadrados*	*Média Quadrática*	*Valor de F*	*Valor de P*
Local	1	0,02430	0,024299	8,56	0,005
Erro	198	0,56226	0,02840		
Total	199	0,58656			

Por fim, a tabela 10 apresenta a análise de variância da medida de latência total considerando os valores obtidos com a topologia original e a nova topologia. Como resultado

o valor de P é zero indicando que existe diferença significativa nas medidas deste trecho considerando as duas topologias.

Tabela 10 – Análise de variância - Latência total

Fonte de variação	*Graus de liberdade*	*Soma dos Quadrados*	*Média Quadrática*	*Valor de F*	*Valor de P*
Local	1	369981220	369981220	287,21	0,000
Erro	198	255057856	1288171		
Total	199	625039076			

Análise nova topologia x topologia original BR-Porto Alegre

A tabela 11 apresenta a análise de variância da medida de latência do trecho entre o gateway e o FD, considerando os valores obtidos com a topologia original e a nova topologia. Como resultado o valor de P é zero indicando que existe diferença significativa nas medidas deste trecho considerando as duas topologias.

Tabela 11 – Análise de variância - trecho gateway-FD

Fonte de variação	*Graus de liberdade*	*Soma dos Quadrados*	*Média Quadrática*	*Valor de F*	*Valor de P*
Local	1	272634601	272634601	397,77	0,000
Erro	198	135711219	685410		
Total	199	408345820			

A tabela 12 apresenta a análise de variância da medida de latência do trecho entre o gateway e o *host* local, considerando os valores obtidos com a topologia original e a nova topologia. Como resultado o valor de P é zero indicando que existe diferença significativa nas medidas deste trecho considerando as duas topologias.

Tabela 12 – Análise de variância - trecho gateway-*host* local

Fonte de variação	*Grau de liberdade*	*Soma dos Quadrados*	*Média Quadrática*	*Valor de F*	*Valor de P*
Local	1	0,09886	0,098857	35,29	0,000
Erro	198	0,55458	0,002801		
Total	199	0,65344			

A tabela 13 apresenta a análise de variância da medida de latência do trecho entre o *host* local e o *host* remoto, considerando os valores obtidos com a topologia original e a nova topologia. Como resultado, o valor de P é zero, indicando que existe diferença significativa nas medidas deste trecho considerando as duas topologias.

Tabela 13 – Análise de variância - trecho *host* local-*host* remoto

Fonte de variação	*Grau de liberdade*	*Soma dos Quadrados*	*Média Quadrática*	*Valor de F*	*Valor de P*
Local	1	813742	813742	1548,20	0,000
Erro	198	104070	526		
Total	199	917812			

Por fim, a tabela 14 apresenta a análise de variância da medida de latência total considerando os valores obtidos com a topologia original e a nova topologia. Como resultado, o valor de P é zero, indicando que existe diferença significativa nas medidas deste trecho considerando as duas topologias.

Tabela 14 – Análise de variância - Latência total

Fonte de variação	*Grau de liberdade*	*Soma dos Quadrados*	*Média Quadrática*	*Valor de F*	*Valor de P*
Local	1	303248846	303248846	443,87	0,000
Erro	198	135271124	683187		
Total	199	438519970			

Análise nova topologia x topologia original DE-Magdeburg

A tabela 15 apresenta a análise de variância da medida de latência do trecho entre o gateway e o FD, considerando os valores obtidos com a topologia original e a nova topologia. Como resultado, o valor de P é zero, indicando que existe diferença significativa nas medidas deste trecho considerando as duas topologias.

Tabela 15 – Análise de variância - trecho *gateway*-FD

Fonte de variação	*Grau de liberdade*	*Soma dos Quadrados*	*Média Quadrática*	*Valor de F*	*Valor de P*
Local	1	146581442	146581442	159,84	0,000
Erro	198	255061798	1288191		
Total	199	625036200			

A tabela 16 apresenta a análise de variância da medida de latência do trecho entre o gateway e o *host* local, considerando os valores obtidos com a topologia original e a nova topologia. Como resultado, o valor de P é diferente de zero, indicando que não existe diferença significativa nas medidas deste trecho considerando as duas topologias.

A tabela 17 apresenta a análise de variância da medida de latência do trecho entre o *host* local e o *host* remoto, considerando os valores obtidos com a topologia original e

Tabela 16 – Análise de variância - trecho *gateway-host* local

Fonte de variação	*Grau de liberdade*	*Soma dos Quadrados*	*Média Quadrática*	*Valor de F*	*Valor de P*
Local	1	0,1100	0,11003	2,01	0,158
Erro	198	10,8517	0,05481		
Total	199	10,9617			

a nova topologia. Como resultado, o valor de P é diferente de zero, indicando que não existe diferença significativa nas medidas deste trecho considerando as duas topologias.

Tabela 17 – Análise de variância - trecho *host* local-*host* remoto

Fonte de variação	*Grau de liberdade*	*Soma dos Quadrados*	*Média Quadrática*	*Valor de F*	*Valor de P*
Local	1	21940	21940	0,76	0,386
Erro	198	5748505	29033		
	199	5770444			

Por fim, a tabela 18 apresenta a análise de variância da medida de latência total considerando os valores obtidos com a topologia original e a nova topologia. Como resultado, o valor de P é zero, indicando que existe diferença significativa nas medidas deste trecho considerando as duas topologias.

Tabela 18 – Análise de variância - Latência total

Fonte de variação	*Grau de liberdade*	*Soma dos Quadrados*	*Média Quadrática*	*Valor de F*	*Valor de P*
Local	1	143024706	143024706	151,44	0,000
Erro	198	186998806	944438		
	199	330023511			

Um resumo dos resultados obtidos nas análise dos resultados da ANOVA é apresentado na tabela 19.

Tabela 19 – Análise das diferenças das médias

Trecho medido	*BR-Laboratório*	*BR-Porto Alegre*	*DE-Magdeburg*
Latência *gateway*-FD	Significativo	Significativo	Significativo
Latência *host* local-*gateway*	Não Significativo	Significativo	Não Significativo
Latência *host* local-*host* remoto	Não Significativo	Significativo	Não Significativo
Latência Total	Significativo	Significativo	Significativo

5.5 Estudo de caso - leitura da variável primária de um FD por acesso remoto

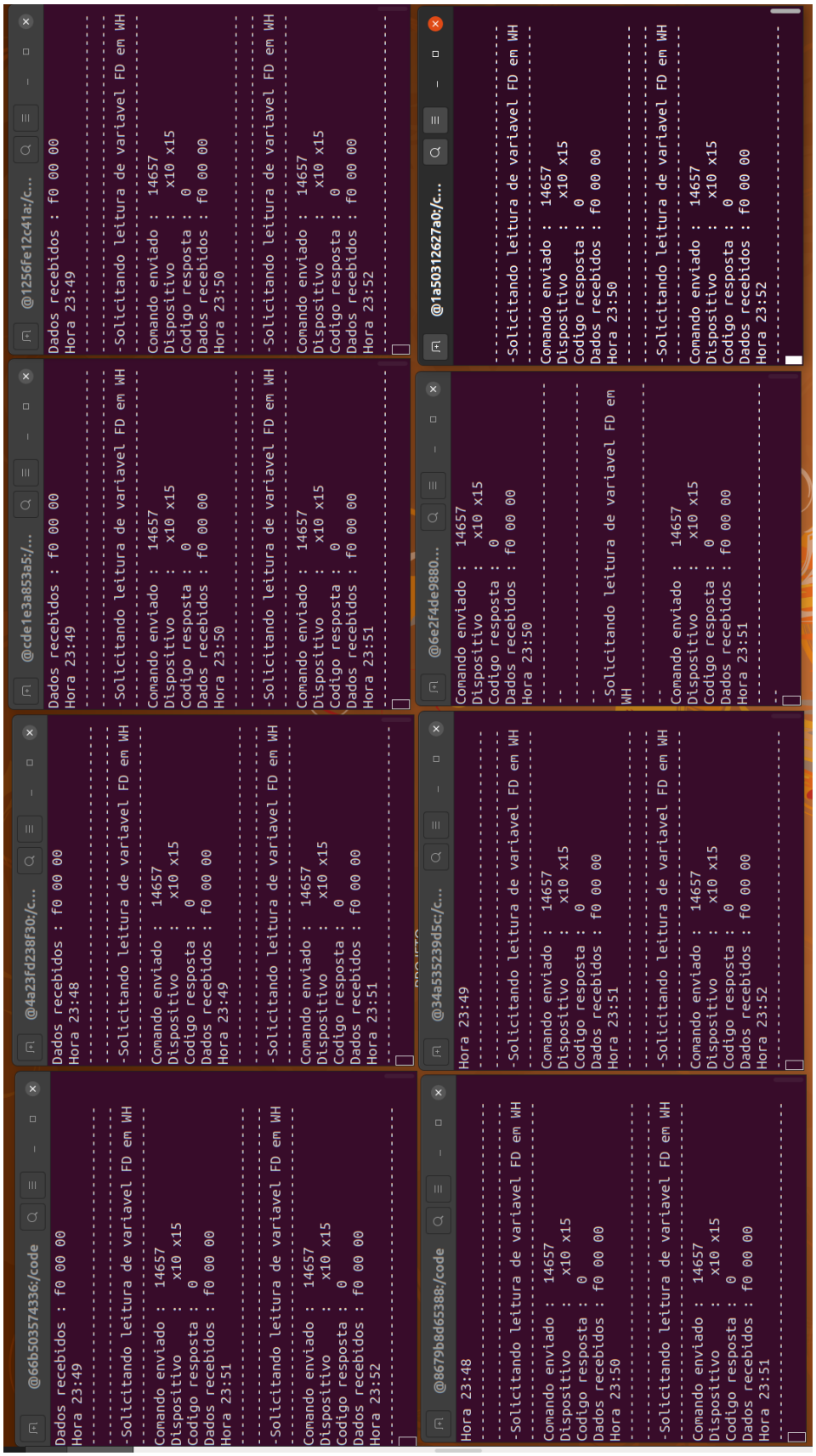
Para analisar a possibilidade do experimento de acesso remoto a uma rede industrial poder exercer monitoramento ma medida que os eventos ocorrem ou até mesmo controle de processos industriais, um *script* em linguagem Python foi preparado de forma a realizar consultas, periódicas a uma variável primária de um FD dentro da rede industrial. O *script* foi preparado para enviar o comando HART 1 a um FD escolhido. Este comando lê o valor da variáveis primária do dispositivo interoperável, respondendo com o valor da leitura. Um FD tipo sensor pode enviar sua variável de medida para um sistema de supervisão remota. Assim, através do uso de virtualização foram criados oito acessos remotos consultando o FD 1015, que reponde a todos os acessos com o valor da variável.

A possibilidade de envio de um comando para um FD atuador pode também ser realizada através do acesso remoto configurando um sistema de controle industrial operado remotamente.

Resultados obtidos

Para conseguir realizar o acesso simultâneo foi utilizada e estratégia de virtualização, através do uso de conteinerização. O teste foi realizado em Porto Alegre, com sucesso em todas consultas. Na Figura 27 pode-se observar as consultas realizadas através de oito *containers* com acessos remotos simultâneos e com endereçamento IP independentes.

Figura 27 – Leitura de variável de um FD através de vários acessos remotos simultâneos



Fonte: Autor

6 CONCLUSÕES

Este trabalho objetivou verificar a possibilidade de se realizar o monitoramento e controle de processos por meio de redes industriais de forma segura, analisando as latências de comunicação impostas pelo acesso remoto. Foi proposta uma técnica de acesso remoto utilizando uma VPN provida por um ambiente SDN, interligando um *host* remoto instalado geograficamente distante da rede industrial, a uma gateway industrial instalado em ambiente de laboratório. A VPN provida pelo sistema SDN elimina a necessidade de manter servidor para sustentar aplicação de estabelecimento da VPN em si. Foram desenvolvidos *scripts* que realizam a capturas dos tempos e latência para cada trecho da trajetória do acesso remoto. Foram apresentados estudos de caso com análises da latência do acesso remoto a partir de posições geográficas diferentes, nacionais e internacionais. Foram coletadas 100 medições de latência fim-a-fim, através de um acesso remoto por VPN, interligando cada localidade à rede WH instalada em laboratório. Na sequência, foi desenvolvido um *script* para envio, a um determinado FD, de comando para leitura da sua variável primária emitido por vários acessos simultâneos na VPN para comprovar a possibilidade de supervisão e controle a dispositivos de campo em rede WH, remotamente. Os dados coletados serviram de base para as conclusões listadas a seguir.

Análise das latências medidas no acesso remoto.

O acesso remoto a uma rede WH funcionou corretamente e pôde ser analisado através de ferramenta estatística. Pela análise de variância das medidas obtidas que o acesso remoto das localidades comprovou-se que estas medidas possuem intervalos de latência diferentes, significando que para realização de monitoramento e controle, remotamente, de processos em dispositivos de uma rede WH considere-se que os intervalos de latência obtidos através do acesso remoto deveram ser menores que os parâmetros de latência suportas pelo sistema supervisionado ou controlado. Não se leva em consideração aqui o

tempo de atualização das variáveis de processo industriais, mas sim, se os *deadlines* são atendidos. Nesse sentido, para processos industriais lentos, como os de indústria óleo e gás (refinarias) ou de tratamento de efluentes, é sim possível realizar o monitoramento e até mesmo controle remoto em malha fechada. Subentende-se também, que o controlador projetado para o sistema de controle em rede é capaz de lidar com eventuais perdas de pacote, mas ainda exige o requisito tempo real, atendido pela proposta aqui analisada (*soft real time*).

Determinação do trecho de latência mais relevante

Na análise de variância do experimento realizado conclui-se que as médias das medidas de latência são diferentes em cada localidade, como esperado, uma vez que dependem do tipo de infraestrutura de rede disponível. A partir desta conclusão, foi feita uma análise nas somas das médias totais obtidas para determinar qual o trecho que poderia impor as diferentes análises de variância em cada localidade. Percebeu-se que a latência entre gateway e FD representa 91,27% das médias totais. Este valor também era esperado, uma vez que a rede WH é de baixa dinamicidade e alta confiabilidade, adequada para atender monitoramento e controle de processos industriais. A latência entre *host* remoto e *host* local, ou seja, o acesso remoto por VPN, apresentou um valor de 8,71% sobre a latência total demonstrando que a VPN proporciona uma relevância baixa nos intervalos de latência de todas as localidades.

Efeito da latência com a alteração da topologia da rede WH

A topologia da rede WH nos testes de latência ligavam todos FD diretamente ao gateway. Isto é inerente deste tipo de rede, centralizada, onde o gerenciador de rede sempre busca manter os caminhos para comunicação os mais curtos e confiáveis o possível. Para avaliar o efeito de uma mudança na topologia da rede WH, o FD, alvo das medidas, foi afastado fisicamente até que seu acesso ao gateway fosse realizado pela conexão intermediária com outro FD (rota alternativa). Foram analisadas novas medidas de latência para as localidades Porto Alegre - laboratório, Porto Alegre - remoto e Magdeburg, Alemanha. Com as novas medidas fez-se um comparativo estatístico dos obtidos antes da mudança de topologia e com a nova topologia. Nesta comparação observou-se que os trechos entre gateway e *host* local e entre *host* local e *host* remoto passaram a não serem mais significativos. Ou seja, a mudança de topologia da rede interfere, apenas, nas médias de latência no acesso aos dispositivos de campo da rede WH. Concluindo que a mudança de topo-

logia de um dispositivo em rede WH, impacta apenas os valores da latência dentro desta rede, não afetando os valores de latência dos demais trechos medidos.

Leitura de variável primária de um FD por acesso remoto

Outra possível aplicação avaliada de forma simples foi o acesso remoto para monitoramento de variáveis de processo por diversos clientes. Baseado no *script* para coleta de latências, alterou-se o comando a ser enviado para um FD, comando este que devolve o valor da variável de processo de qualquer FD. Através da aplicação de oito *containers*, todos conectados à VPN de acesso remoto, cada um com um IP distinto do outro para acessar um determinado FD da rede WH, com cada *container* contendo um *script* que solicita ao FD a reposta para um comando de leitura da variável primária, pode-se concluir que é possível realizar o monitoramento remoto a partir de locais diferentes, simultaneamente.

As ferramentas criada nesse trabalho, através dos *scripts* de captura de latência, servem como uma ferramenta de monitoramento e manutenção de redes WH ou outras redes semelhantes, testando regularmente o comportamento da latência em um acesso remoto à dispositivos de campo de uma rede WH. Desta forma é possível monitorar estas redes de foma remota e estabelecer limites de latência aceitáveis para operação de sistemas de controle em rede.

Com a possibilidade de monitoramento através de acessos remotos simultâneos realizando leitura da variável primária de um FD, através de comando, cria-se a possibilidade de monitoramento de um sistema de controle em varias localidades distintas em tempo real.

Trabalhos futuros

Outras abordagens poderão complementar os *scripts* de acesso remoto com outros comandos de leitura e de escrita variáveis para FD de uma rede WH para apoiar um projeto para uma aplicação de um sistema de controle em rede operado remotamente. Uma ferramenta que permita descobrir o caminho feito pelos pacotes desde a sua origem até o seu destino, tal como Traceroute, pode ser utilizado para detectar falhas em dispositivos tais como, por exemplo, gateways intermediários que descartam pacotes ou rotas que excedem a capacidade de um datagrama IP, pode complementar a ferramenta de captura de latência. Ainda, sugere-se a investigação dos requisitos de segurança de rede, com relação à ataques realizados por elementos que participem da rede VPN, a vulnerabilidade a

eles e os efeitos na latência das comunicações remotas. O uso dos datasets, obtidos pela ferramenta desenvolvida, poderiam ser utilizados para o treinamento de Redes Neurais com objetivo de realizar a previsão da latência em sistemas de controle. Outra possibilidade de trabalho é a utilização de modelos baseados em redes de Petri generalizadas utilizando mais nodos de na rede a partir dos modelos obtidos nas projeções gráficas das funções de densidade de probabilidade apresentados. Também este trabalho pode avançar através do uso da plataforma de código aberto escrita em linguagem Python, conhecida como Apache Airflow, que pode gerenciar o fluxo de consultas dos scripts de captura de latência e de monitoramento e gerenciamento de um sistema industrial. Outra complementação deste trabalho pode ser obtida habilitando os acessos remotos obtidos pela VPN Zerotier comunicar-se através vários caminhos físicos simultaneamente, Isto faria o balanceamento de carga automaticamente de acordo com a intensidade do caminho. Por fim, a utilização do mecanismo de regras SDN pode realizar listas brancas para o tráfico TCP ou bloquear o tráfego UDP desnecessário.

REFERÊNCIAS

AL-KHATEEB, K. A. S.; AL-KHATEEB, W. F.; HAMEED, S. A. Implementation of Internet based remote control and monitoring. *In*: IEEE CONFERENCE ON INDUSTRIAL ELECTRONICS AND APPLICATIONS, 2009., 2009. **Proceedings [...]** [S.l.: s.n.], 2009. p. 1513–1516.

ARAUJO JUNIOR, A. P.; DAS CHAGAS, C. V.; FERNANDES, R. G. Uma rápida análise sobre automação industrial. **Redes para Automação Industrial – 2003.1**, [S.l.], v. 1, 2003.

BALASUBRAMANIAN, K.; CELLATOGLU, A. Remote control techniques for selected applications performed through internet. *In*: INTERNATIONAL CONFERENCE ON CONTROL, AUTOMATION, COMMUNICATION AND ENERGY CONSERVATION, 2009., 2009. **Proceedings [...]** [S.l.: s.n.], 2009. p. 1–6.

BORGES, F.; FAGUNDES, B. A.; DA CUNHA, G. N. Vpn: protocolos e segurança. **S/D**, [S.l.], v. 10, 2019.

CARMONA, A. L. M. *et al.* **Análise dos impactos da indústria 4.0 na logística empresarial**. 2017. TCC (graduação) — Universidade Federal de Santa Catarina, 2017.

CARVALHO, J. F. d. Energia e sociedade. **Estudos avançados**, [S.l.], v. 28, p. 25–39, 2014.

CHUNG, T. D. *et al.* Effect of network induced delays on WirelessHART control system. *In*: INTERNATIONAL CONFERENCE ON INTELLIGENT AND ADVANCED SYSTEMS (ICIAS), 2016., 2016. **Proceedings [...]** [S.l.: s.n.], 2016. p. 1–5.

COMPANY, S. T. **WirelessHART^{TM} - Características, tecnologia e tendências**. 2021.

DASTJERDI, A. V.; BUYYA, R. Fog Computing: helping the internet of things realize its potential. **Computer**, [S.l.], v. 49, n. 8, p. 112–116, Aug 2016.

DAVIES, R. Industry 4.0 Digitalisation for productivity and growth. **European Parliamentary Research Service**, [S.l.], v. 1, 2015.

DELFTSTACK. **Convert Epoch to Datetime in Python**. 2021.

EMERSON. **Process Management, Gateway Smart Wireless**. 2020.

FOUNDATION, H. C. **Network Management Specification, HCF SPEC-085 Revision 1.2**. 2009.

GEAMPALIA, G. *et al.* Communication Technologies for Complex Industrial Systems. *In*: INTERNATIONAL CONFERENCE ON CONTROL SYSTEMS AND COMPUTER SCIENCE (CSCS), 2017., 2017. **Proceedings [...]** [S.l.: s.n.], 2017. p. 401–405.

GLOBAL, D. **Industry 4.0 Challanges and solutions for the digital transformation and use of exponential technologies - 24 de outubro de 2014**. 2020.

GODOY, E. P. **Desenvolvimento de sistemas de controle via rede (NCS) para aplicações em redes com protocolo CAN**. 2011.

GOETHALS, T. *et al.* Scalability evaluation of VPN technologies for secure container networking. *In*: INTERNATIONAL CONFERENCE ON NETWORK AND SERVICE MANAGEMENT (CNSM), 2019., 2019. **Proceedings [...]** [S.l.: s.n.], 2019. p. 1–7.

HAHN FILHO, J. R. A Era da Internet Industrial e a Indústria 4.0. **Produção em Foco**, [S.l.], v. 6, n. 3, 2016.

HERMANN, M.; PENTEK, T.; OTTO, B. Design Principles for Industrie 4.0 Scenarios. *In*: HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES (HICSS), 2016., 2016. **Proceedings [...]** [S.l.: s.n.], 2016. p. 3928–3937.

HUANG, Y.; ZHANG, Z.; ZHU, P. The Design of an Industrial Remote Control Network Gateway Based on P2P VPN. *In*: INTERNATIONAL CONFERENCE ON INTELLIGENT HUMAN-MACHINE SYSTEMS AND CYBERNETICS, 2012., 2012. **Proceedings [...]** [S.l.: s.n.], 2012. v. 2, p. 140–143.

INC., O. **Securing Remote Access Using VPN**. 2020.

INC., Z. **ZeroTier Manual**. 2020.

KHODADADI, F.; DASTJERDI, A.; BUYYA, R. Chapter 1 - Internet of Things: an overview. In: BUYYA, R.; Vahid Dastjerdi, A. (Ed.). **Internet of Things**. [S.l.]: Morgan Kaufmann, 2016. p. 3–27.

KOLESNIKOV, O.; HATCH, B. **Building Linux virtual private networks (VPNs)**. [S.l.]: Sams Publishing, 2002.

KOMPELLA, K. **Transport networks supporting virtual private networks, and configuring such networks**. US Patent 7,136,374.

KOSHATWAR, R. G.; SAWANT, S. D. Remote monitoring and control of industrial parameters using embedded web server. *In*: INTERNATIONAL CONFERENCE ON INTELLIGENT SYSTEMS AND CONTROL (ISCO), 2016., 2016. **Proceedings [...]** [S.l.: s.n.], 2016. p. 1–4.

KOSTOLáNI, M.; MURíN, J.; KOZáK, v. An effective industrial control approach. *In*: FEDERATED CONFERENCE ON COMPUTER SCIENCE AND INFORMATION SYSTEMS (FEDCSIS), 2019., 2019. **Proceedings [...]** [S.l.: s.n.], 2019. p. 911–914.

KRÖTZ, C. A. **Ferramenta e método para obtenção de parâmetros de confiabilidade fim-a-fim de redes industriais sem fio**. 2019. Dissertação de Mestrado — Universidade Federal do Rio Grande do Sul, 2019.

KRUGMAN, P. Scale Economies, Product Differentiation, and the Pattern of Trade. **The American Economic Review**, [S.l.], v. 70, n. 5, p. 950–959, 1980.

LEE, J.-S.; LEE, Y.-F. Behavior modeling and remote control of industrial conveyor systems via internet. *In*: IEEE 8TH CONFERENCE ON INDUSTRIAL ELECTRONICS AND APPLICATIONS (ICIEA), 2013., 2013. **Proceedings [...]** [S.l.: s.n.], 2013. p. 387–392.

LLC., M. **Interpretar todas as estatísticas e gráficos para Poder e Tamanho de Amostra para Teste t Pareado**. 2021.

MICROSOFT. **Introdução aos contêineres e ao Docker**. 2021.

MONTGOMERY, D. C.; RUNGER, G. C. Estatística aplicada e probabilidade para engenheiros, 2ª. **Edição. Rio de Janeiro: Editora LTC**, [S.l.], 2003.

MüLLER, I. **Gerenciamento descentralizado de redes sem fio industriais segundo o padrão WirelessHART**. 2012. Tese de Doutorado — Universidade Federal do Rio Grande do Sul, 2012.

MüLLER, I. *et al.* Development of a WirelessHART compatible field device. *In*: IEEE INSTRUMENTATION MEASUREMENT TECHNOLOGY CONFERENCE PROCEEDINGS, 2010., 2010. **Proceedings [...]** [S.l.: s.n.], 2010. p. 1430–1434.

NTP.BR. **O NTP**. 2021.

ORG, S. **Design and Implementationof SoftEther VPN**. 2020.

ORG, T. **Setting up a Virtual Private Network with tinc**. 2020.

SAIFULLAH, A. *et al.* End-to-End Communication Delay Analysis in Industrial Wireless Networks. **IEEE Transactions on Computers**, [S.l.], v. 64, n. 5, p. 1361–1374, May 2015.

SCIENCE, T. D. **Measure the execution time of your Python codes**. 2021.

SECURITY-US, N. I. **Configuring and Managing Remote Access for Industrial Control Systems**. 2020.

SILVEIRA, C. B. O que é indústria 4.0 e como ela vai impactar o mundo. **Acesso em**, [S.l.], v. 15, 2016.

SOUPPAYA, M.; SCARFONE, K. *et al.* Guide to enterprise telework, remote access, and bring your own device (BYOD) security. **NIST Special Publication**, [S.l.], v. 800, p. 46, 2016.

SUN, X.; SHI, Q. Remote Monitoring and Control System for Bio-fermentation Process Based on Embedded Internet. *In*: IEEE 4TH INFORMATION TECHNOLOGY AND MECHATRONICS ENGINEERING CONFERENCE (ITOEC), 2018., 2018. **Proceedings [...]** [S.l.: s.n.], 2018. p. 513–516.

SYSTEMS, C. **What Is a VPN? - Virtual Private Network**. 2021.

TANENBAUM, A. S.; WETHERALL, D. **Redes de computadores. [Sl]**. [S.l.]: Pearson-Prentice Hall, 2003.

TOOLS, D. I. **Revolução Industrial - Da Indústria 1.0 à Indústria 4.0**. 2020.

TP-LINK. **Roteador Wireless N 150Mbps**. 2020.

USA, C. . I. A. H. S. **Configuring and Managing Remote Access for Industrial Control Systems**. 2020.

VERAS, M. **Virtualização**: tecnologia central do datacenter. [S.l.]: Rio de Janeiro: Brasport, 2016.

VILAR, J. W. C. **Geografia da Produção, Circulação e Consumo**. Aula 5.

WANG, Q.; JIANG, J. Comparative Examination on Architecture and Protocol of Industrial Wireless Sensor Network Standards. **IEEE Communications Surveys Tutorials**, [S.l.], v. 18, n. 3, p. 2197–2219, thirdquarter 2016.

WERNER, J. Tecnologias para Implantação de Redes Virtuais Privadas. **Fórum Nacional sobre Segurança de Redes e Telecomunicações**, [S.l.], v. 20, 1998.

WHANG, H.; ZHANG, W.; CUI, E. The Research and Design of the Management and Control System Based on the Industrial Internet Gateway. *In*: INFORMATION COMMUNICATION TECHNOLOGIES CONFERENCE (ICTC), 2020., 2020. **Proceedings [...]** [S.l.: s.n.], 2020. p. 12–16.

WIREGUARD. **WireGuard**: next generation kernel network tunnel. 2020.

XU, L. *et al.* Information Security in Big Data: privacy and data mining. **IEEE Access**, [S.l.], v. 2, p. 1149–1176, 2014.