Implementação de Ambiente de Confiança Zero para Redes Industriais:

Desafios e Soluções em Aplicações de Sistemas de Controle Industrial

Lucas da Silva Cruz

CENTRO DE INFORMÁTICA
UNIVERSIDADE FEDERAL DA PARAÍBA

João Pessoa, 2024

Lucas da Silva Cruz

Implementação de Ambiente de Confiança Zero para Redes Industriais

Desafios e Soluções em Aplicações de Sistemas de Controle Industrial

Dissertação apresentada ao Programa de Pós-Graduação em Informática
do Centro de Informática, da Universidade Federal da Paraíba,
como requisito para a obtenção do grau de Mestre em Informática.

Orientador: Iguatemi Eduardo da Fonseca

Fevereiro de 2024

Catalogação na publicação
Seção de Catalogação e Classificação

C957i Cruz, Lucas da Silva.
Implementação de ambiente de confiança zero para redes industriais : desafios e soluções em aplicações de sistemas de controle industrial / Lucas da Silva Cruz. - João Pessoa, 2024.
74 f. : il.

Orientação: Iguatemi Eduardo da Fonseca.
Dissertação (Mestrado) - UFPB/CI.

1. Informática. 2. Sistema de controle industrial. 3. Confiança zero - Modelo de segurança. 4. Modbus TCP - Protocolo industrial. 5. Ataques cibernéticos. I. Fonseca, Iguatemi Eduardo da. II. Título.

UFPB/BC CDU 004(043)

Elaborado por Larissa Silva Oliveira de Mesquita - CRB-15/746

UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA

Ata da Sessão Pública de Defesa de Dissertação de Mestrado de Lucas da Silva Cruz, candidato ao título de Mestre em Informática na Área de Ciência da Computação, realizada em 31 de janeiro de 2024.

Aos trinta e um dias do mês de janeiro do ano de dois mil e vinte e quatro, às nove horas, reuniram-se os membros da Banca Examinadora constituída para julgar o trabalho do sr. Lucas da Silva Cruz, vinculado a esta Universidade sob a matrícula nº 20211021641, candidato ao grau de Mestre em Informática, na área de "Ciência da Computação", na linha de pesquisa "Sistemas de Computação", do Programa de Pós-Graduação em Informática, da Universidade Federal da Paraíba. A comissão examinadora foi composta pelos professores: Iguatemi Eduardo da Fonseca (PPGI), Orientador e Presidente da Banca; Fernando Menezes Matos (PPGI), Examinador Interno; e Waslon Terllizzie Araújo Lopes (UFPB), Examinador Externo ao Programa. Dando início aos trabalhos, o Presidente da Banca cumprimentou os presentes, comunicou a finalidade da reunião e passou a palavra ao candidato para que ele fizesse a exposição oral do trabalho de dissertação intitulado: "Implementação de Ambiente de Confiança Zero para Redes Industriais: Desafios e Soluções em Aplicações de Sistemas de Controle Industrial". Concluída a exposição, o candidato foi arguido pela Banca Examinadora que emitiu o seguinte parecer: "***aprovado***". Do ocorrido, eu, Fernando Menezes Matos, Coordenador do Programa de Pós-Graduação em Informática, lavrei a presente ata que vai assinada por mim e pelos membros da banca examinadora. João Pessoa, 31 de janeiro de 2024.

gov.br Documento assinado digitalmente
FERNANDO MENEZES MATOS
Data: 05/02/2024 10:51:10-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Fernando Menezes Matos

Prof. Iguatemi Eduardo da Fonseca
Orientador (PPGI-UFPB)

gov.br Documento assinado digitalmente
IGUATEMI EDUARDO DA FONSECA
Data: 31/01/2024 17:55:25-0300
Verifique em https://validar.iti.gov.br

Prof. Fernando Menezes Matos
Examinador Interno (PPGI-UFPB)

gov.br Documento assinado digitalmente
FERNANDO MENEZES MATOS
Data: 04/02/2024 10:52:03-0300
Verifique em https://validar.iti.gov.br

Prof. Waslon Terllizzie Araújo Lopes
Examinador Externo ao Programa (UFPB)

gov.br Documento assinado digitalmente
WASLON TERLLIZZIE ARAUJO LOPES
Data: 31/01/2024 22:06:11-0300
Verifique em https://validar.iti.gov.br

Nós só podemos ver um pouco do futuro,
mas o suficiente para perceber que há muito a fazer. - Alan Turing

DEDICATÓRIA

Aos meus Pais, Saraiva e Edna,

Este trabalho é dedicado a vocês, cujo amor e apoio incondicionais foram a base sólida sobre a qual construí minha jornada acadêmica. Suas palavras de incentivo, sacrifícios e constante encorajamento foram a luz que me guiou nos momentos mais desafiadores deste caminho.

Se não fosse pelo apoio e orientação que vocês me proporcionaram, esta conquista não seria possível. Cada página desta dissertação é um reflexo do profundo apreço que tenho por vocês e por tudo o que fizeram por mim.

Que esta dedicatória seja um humilde reconhecimento da minha eterna gratidão e amor por vocês. Vosso apoio foi a força motriz por trás de cada passo dado nesta jornada acadêmica. Desde a infância, vocês sempre me incentivaram a buscar o conhecimento e a perseguir meus sonhos.

Aos meus irmãos, Mateus e Sara,

Gostaria também de expressar minha sincera gratidão pela paciência e compreensão durante os momentos em que nossa relação de atenção foi distante devido às demandas deste percurso acadêmico. Sei que nem sempre pude estar tão presente quanto gostaria, mas o apoio silencioso e a compreensão que vocês demonstraram foram fundamentais para mim. Obrigado por entenderem os desafios que enfrentei e por sempre estarem ao meu lado, mesmo quando nossas interações foram limitadas. Saibam que cada conquista minha é também um reflexo do amor e apoio que recebi de vocês.

"O coração do homem planeja o seu caminho, mas o Senhor determina os seus passos" Provérbios 16:9 (NVI)

Com todo o meu carinho e admiração,

Lucas da Silva Cruz

AGRADECIMENTOS

Agradeço profundamente a todos que contribuíram para a realização deste trabalho, que representa uma etapa significativa em minha jornada acadêmica. Primeiramente, gostaria de expressar minha sincera gratidão ao meu orientador, Prof. Dr. Iguatemi Eduardo da Fonseca, pela orientação constante, apoio inestimável e insights valiosos ao longo deste processo. Sua orientação foi fundamental para moldar este trabalho e meu crescimento acadêmico.

À CAPES/CNPQ e ao PROAP/PPGI, expresso meu reconhecimento pelo suporte financeiro concedido, o qual viabilizou a realização deste mestrado. Sem esse apoio, esta pesquisa não seria possível.

Agradeço também aos professores do Centro de Informática da UFPB, cujo conhecimento e orientação enriqueceram minha formação acadêmica. Em especial a, Prof. Dr. Waslon Terllizzie e Prof. Dr. Fernando Matos, que ao participarem da banca, puderam compartilhar seus conhecimentos para aprimorar esta dissertação. Seus ensinamentos foram essenciais para o desenvolvimento deste estudo e para minha evolução como pesquisador.

Além disso, gostaria de reconhecer e agradecer à Sociedade Brasileira de Telecomunicações pelo apoio financeiro concedido para a participação no XLI Simpósio Brasileiro de Telecomunicação e Processamento de Sinais em 2023. Seu apoio tornou possível minha presença no evento e enriqueceu minha experiência acadêmica.

Por fim, expresso minha gratidão a todos os colegas, amigos e familiares que me apoiaram ao longo desta jornada. Seus encorajamentos e palavras de incentivo foram indispensáveis para superar os desafios e alcançar este marco.

Este trabalho não seria possível sem o apoio e contribuição de cada um de vocês. Sou imensamente grato por fazer parte de uma comunidade acadêmica tão inspiradora e colaborativa. Obrigado a todos pelo apoio e pela confiança em meu trabalho.

RESUMO

A integração da Tecnologia da Informação (TI) e Tecnologia Operacional (TO) na Indústria 4.0 levanta preocupações pertinentes sobre segurança cibernética. Diante da expansão de uma rede, torna-se necessário estabelecer uma cobertura abrangente contra eventos maliciosos. Esta dissertação se dedica à análise do Acesso Confiança Zero em Sistemas de Controle Industrial. Por meio de um ambiente simulado, foram realizados testes comparativos entre ambientes com e sem a implementação do Acesso Confiança Zero, seguidos por simulações de ataques cibernéticos clássicos. Os resultados contribuem para a compreensão aprimorada dos benefícios da arquitetura de Confiança Zero em redes industriais suscetíveis a ataques cibernéticos. Indicam que, embora o Acesso Confiança Zero permita um controle rigoroso, não acarreta impactos negativos. Esta conclusão encontra respaldo na estrutura implementada, onde políticas foram estabelecidas por meio de ferramentas de código aberto, e um meio de comunicação específico, com uso do protocolo Modbus TCP/IP, que demonstrou validação de identidade com impacto mínimo na rede. Os estudos realizados possibilitaram a simulação de um cenário industrial para uma escala menor, utilizando determinada rotina, considerada crítica pela pesquisa, específica e coletando dados relevantes para futuras investigações em escalas maiores, e questionamentos para pesquisa de novos modelos de controle de acesso. Além disso, os experimentos indicam que a implementação do modelo de Acesso Confiança Zero pode resultar em um leve aumento no tempo de resposta e, em certos casos, picos na latência. Esses resultados destacam a importância de considerar cuidadosamente a implementação, especialmente em infraestruturas críticas de tempo real, onde o atraso pode ser crucial. Os testes ressaltam a necessidade de avaliar outros fatores ao implementar soluções de segurança como o Acesso Confiança Zero em ambientes industriais. Enfatizam também a importância de realizar testes em cenários mais complexos, que envolvam múltiplos protocolos e um maior número de solicitantes, tanto legítimos quanto não legítimos, para uma compreensão abrangente do impacto da implementação do Acesso Confiança Zero na segurança e no desempenho da rede.

Palavras-chave: Sistema de Controle Industrial, Confiança Zero, Modbus TCP, Ataques Cibernéticos.

ABSTRACT

Integrating Information Technology (IT) and Operational Technology (OT) in Industry 4.0 raises pertinent concerns about cybersecurity. Faced with expanding networks, comprehensive coverage against malicious events becomes necessary. This dissertation analyzes Zero Trust in Industrial Control Systems. Comparative tests were conducted in a simulated environment between environments with and without the implementation of Zero Trust, followed by simulations of classical cyber-attacks. The results enhance understanding of the benefits of Zero Trust architecture in industrial networks susceptible to cyber-attacks. They indicate that while Zero Trust allows for stringent control, it does not entail negative impacts. This conclusion gains support from the implemented structure, where policies were established through open-source tools, and a specific communication medium, using the Modbus TCP/IP protocol, demonstrated identity validation with minimal impact on the network. The studies enabled the simulation of an industrial scenario on a smaller scale using a particular routine deemed critical by the research. This routine is specific, collecting relevant data for future investigations on larger scales and inquiries into research for new access control models. In addition, the experiments indicate that implementing the Zero Trust model may result in a slight increase in response time and, in some instances, spikes in latency. These results highlight the importance of carefully considering implementation, especially in critical real-time infrastructures where delay can be crucial. The tests underscore the need to evaluate other factors when implementing security solutions like Zero Trust in industrial environments. They also emphasize the importance of conducting tests in more complex scenarios with multiple protocols and a significant number of legitimate and illegitimate users for a comprehensive understanding of the impact of Zero Trust implementation on network security and performance.

Key-words: Industrial Control System, Zero Trust, Modbus TCP, Cyber Attacks.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS

CCZ - Central de Confiança Zero, em português.

DSR - Pesquisa em Ciência do Design, em português, ou Design Science Research, em inglês.

HMI - Interface Homem - Máquina, em português, ou Human Machine Interface, em inglês.

PLC - Controlador Lógico Programável, em português, ou Programmable Logic Controller, em inglês.

PE - Mecanismo de política, em português, ou Policy engine, em inglês.

PA - Administrador de políticas, em português, ou Policy administrator, em inglês.

PDP - Ponto de aplicação de política, em português, ou Policy enforcement point, em inglês.

HMI - Interface Homem - Máquina, em português, ou Human Machine Interface, em inglês.

ICS - Sistema de Controle Industrial, em português, ou Industrial Control System, em inglês.

IDS - Sistema de Detecção de Intrusão, em português, ou Intrusion Detection System, em inglês.

IP - Protocolo da Internet, em português, ou Internet Protocol, em inglês.

LAN - Rede de Área Local, em português, ou Local Area Network, em inglês.

MAC - Endereço de Controle de Acesso ao Meio, em português, ou Media Access Control, em inglês.

NIST - Instituto Nacional de Padrão e Tecnologia, em português, ou National Institute of Standards and Technology, em inglês.

PA - Administrador de políticas, em português, ou Policy administrator, em inglês.

PDP - Ponto de decisão de política, em português, ou Policy Decision Point, em inglês.

PEP - Ponto de aplicação de política, em português, ou Policy enforcement point, em inglês.

PE - Mecanismo de política, em português, ou Policy engine, em inglês.

PLC - Controlador Lógico Programável, em português, ou Programmable Logic Controller, em inglês.

RTU - Unidade Terminal Remota, em português, ou Remote Terminal Unit, em inglês.

SCADA - Sistemas de Supervisão e Aquisição de Dados, em português, ou Supervisory Control and Data Acquisition, em inglês.

TCP - Protocolo de Controle de Transmissão, em português, ou Transmission Control Protocol, em inglês.

TSBAC - Controle de Acesso Baseado em três Estado, em português, ou Three-State-Based Access Control.

TSN - Rede Sensível ao Tempo, em português, ou Time-Sensitive Networking, em inglês.

TTS - Tempo de Serviço , ou Time To Service, em inglês

ZTA - Arquitetura de Confiança Zero, em português, ou Zero Trust Architecture, em inglês.

ZTNA - Rede de Acesso de Confiança Zero, em português, ou Zero Trust Network Access, em inglês.

Sumário

1 Introdução

1.1 Contextualização

A rápida evolução da Indústria 4.0 impulsiona a integração entre Tecnologia da Informação (TI) e Tecnologia Operacional (TO), promovendo uma transformação profunda no cenário industrial. Essa integração viabiliza maior eficiência, automação na tomada de decisões e otimização de processos, incorporando dispositivos da Internet das Coisas Industrial (*Industrial Internet-of-Things* - IIoT) para a coleta de dados em tempo real. Contudo, essa convergência também apresenta desafios e preocupações significativos com a segurança cibernética, destacando-se como uma das principais.

Ataques direcionados a essas aplicações e dispositivos podem resultar em consequências potencialmente catastróficas, desde paralisações na produção até riscos para a segurança dos trabalhadores nas instalações fabris. Assim, vários setores, incluindo órgãos de padronização, instituições acadêmicas, o meio empresarial e o ambiente industrial, propõem a adoção de um novo paradigma de autenticação de ativos que apresenta uma abordagem inovadora: a Confiança Zero (*Zero Trust* – ZT).

A abordagem de Confiança Zero no contexto industrial representa um avanço significativo na garantia da segurança cibernética dos sistemas de controle. Essa perspectiva disruptiva, derivada do princípio da não confiança nos elementos, estipula que, em um ambiente interconectado, nenhum usuário ou dispositivo pode ser considerado intrinsecamente confiável, mesmo que tenham passado por processos de autenticação prévia (Rose et al. 2020).

A introdução dos dispositivos inteligentes em sistemas industriais, denominados IIoT, como elemento essencial da indústria inteligente, possibilitou a automação de processos, levando à criação de ambientes inteligentes e interconectados, capazes de adquirir e analisar dados em tempo real. Isso, por sua vez, permite o controle remoto, possibilitando uma administração eficaz dos processos (Ferencz, Domokos e Kovács 2021). Historicamente, os ambientes industriais foram concebidos para operar de maneira isolada, onde a segurança não era inicialmente considerada para dispositivos dispostos nessas redes. Portanto, ao serem introduzidos ao conceito de acesso remoto, tornou-se imprescindível a implementação de políticas de segurança, visando mitigar os potenciais efeitos adversos nas operações industriais (Wadsworth et al. 2019).

A literatura acadêmica tem amplamente abordado a segurança de ativos na era da Indústria 4.0. Diversas pesquisas têm se dedicado ao rastreamento dos principais fatores que contribuem para invasões de segurança relacionadas ao IIoT, incluindo a classificação e comparação de diferentes tipos de ataques (Jayalaxmi et al. 2021).

Adicionalmente, tem-se explorado a aplicação de um framework baseado em tec-

nologia blockchain para a integração segura de modelos de aprendizado federado em um contexto de IIoT (Kalapaaking et al. 2023). Alguns estudos recentes abordam temas relacionados às estratégias de mitigação de eventos por meio da arquitetura de Confiança Zero. Além disso, investigam como a ocorrência de eventos pandêmicos impulsionou a busca por abordagens inovadoras na prevenção de atividades maliciosas em aplicações industriais, a exemplo de sistemas SCADA (Trifonov et al. 2021).

1.2 Proposta da Pesquisa

Com base nas informações apresentadas e com o objetivo de abordar as dificuldades previamente mencionadas, esta dissertação propõe a criação e concepção de estados de confiança observáveis por meio do desenvolvimento de um modelo de controle de acesso baseado em três estados. Considerando que as redes industriais necessitam de comunicações confiáveis e de baixa latência (Bello e Steiner 2019), a criação de um ambiente de teste foi empreendida com o propósito de simular a comunicação de elementos presentes em redes críticas, empregando o protocolo industrial ModBus TCP. Essa estratégia surgiu como uma abordagem viável para analisar o comportamento por meio de métricas de rede. A solução ZT, com algoritmos baseados em atributos, foi inicialmente direcionada para os testes propostos, visando rastrear dados para fins de comparação.

Essa comparação irá avaliar o desempenho do algoritmo de confiança utilizado na pesquisa em diferentes cenários nesta dissertação e lançará as bases para uma nova abordagem de um modelo de Controle de Acesso Baseado em Três Estado (*Three-State-Based Access Contro* – TSBAC).

1.2.1 Objetivos

O propósito fundamental desta dissertação consiste na elaboração lógica da rastreabilidade contínua de segurança e na implantação de um controle de acesso dinâmico e avaliação contínua, juntamente com a avaliação do impacto resultante da inserção da arquitetura de Confiança Zero em um ambiente de rede industrial.

Adicionalmente, este trabalho visa fornecer diretrizes para estabelecer pré-requisitos iniciais necessários à incorporação do modelo de segurança nas redes industriais. Neste contexto, o objetivo é a concepção de uma estrutura que viabilize a avaliação contínua da segurança, denominada "Central de Confiança Zero".

Com o objetivo geral apresentado, desdobram-se os seguintes objetivos específicos:

- Identificar os elementos essenciais para a construção de um centro de Confiança Zero aplicável a redes industriais.

- Criar uma solução de interface homem-máquina que apresente rotinas compatíveis com o protocolo ModBus TCP, visando a utilização durante os testes em ambientes controlados.

- Realizar testes de desempenho em cenários normais e sob a influência de ataques, com o intuito de avaliar a eficácia das soluções propostas.

- Formular um modelo matemático para a criação da base de um modelo de controle de acesso baseado em estados observáveis que resulta no nível de confiança por meio da verificação de estados gerado a partir de transações.

- Desenvolver um controle de acesso baseado capaz de monitorar o estado, direcionado para a implementação em soluções especificamente projetadas para redes de infraestruturas críticas. O objetivo é introduzir o conceito de Confiança Zero nesse cenário, sem acarretar impactos significativos no desempenho.

1.3 Justificativa

A presente pesquisa se justifica devido à crescente diversidade de ataques direcionados a redes industriais, conforme destacado por (Jayalaxmi et al. 2021) em sua revisão de segurança em IIoT de 2021. A implantação de modelos de segurança desempenha um papel crucial na criação de ambientes seguros. Os questionamentos fundamentais que surgem durante este estudo estão relacionados à influência das regras de avaliação contínua de identidade, as quais, inicialmente, se baseiam em uma solução com algoritmo de confiança baseado em critérios. É relevante explorar como tais regras afetam o desempenho das rotinas, especialmente em cenários sob ataques, e considerar a possibilidade de conceber um modelo alternativo de avaliação baseado em estados de confiança.

A capacidade de fornecer informações que validem a segurança de uma transação em tempo hábil ou indiquem se o estado da mesma se encontra acima de um limiar seguro é essencial. Esse aprimoramento na capacidade de oferecer segurança tem o potencial de melhorar significativamente a solução em um contexto no qual as redes industriais demonstram ser particularmente sensíveis ao tempo, devido à crítica necessidade de comunicação entre os elementos presentes nesses ambientes.

1.4 Metodologia

A presente pesquisa se fundamenta na complexidade dos paradigmas, adotando a abordagem quantitativa, como indicado por (Martins e Theóphilo 2009), para a comparação das métricas de redes coletadas durante os testes. Paralelamente, adota a metodologia de Pesquisa em Ciência do Design (*Design Science Research* – DSR), como guia para

a avaliação de modelo especifico de segurança e direcionamento para nova estrategia de controle de acesso, conforme proposto por (Nunamaker e Chen 1990). Os procedimentos implementados na pesquisa e expostos são:

1. Revisão da literatura para compreender os elementos essenciais da abordagem em Redes de Confiança Zero.
2. Prototipagem de um ambiente de teste que simule uma rede industrial, com a seleção de um protocolo específico e a geração de tráfego entre cliente e servidor.
3. Seleção de soluções de código aberto para compor a "Central de Confiança Zero" (CCZ), alinhando-se aos pilares estabelecidos nas normas NIST 800-207 (Rose et al. 2020).
4. Organização lógica e topológica para a integração da CCZ no ambiente de simulação.
5. Avaliação do sistema em dois cenários: um com a presença de ZT (Zero Trust) em rotinas normais e outro com a introdução de ataques específicos descritos detalhadamente no Capítulo 3.
6. Desenvolvimento de um modelo matemático para modelo de controle de acesso, com base estados observáveis.
7. Elaboração da estratégia do modelo de controle de acesso.
8. Avaliação do Desempenho da estratégia.

Para avaliar o desempenho e comparar a visão em diversos cenários, utilizaram-se as seguintes métricas de rede: a média do atraso de ponta a ponta em várias séries avaliadas, a taxa de variação do atraso, a quantidade de dados transmitidos na rede e o tempo necessário para disponibilizar um serviço ou concluir uma tarefa de serviço (*Time To Service* – TTS).

Os experimentos envolveram a criação de um ambiente de simulação para gerar pacotes do protocolo ModBus TCP entre cliente e servidor, avaliando a rotina de escrita de bobinas em ambientes com e sem a abordagem ZT. Em outro cenário, utilizando o mesmo ambiente de teste, conduziu-se outra série de testes, acionando determinados ataques detalhados no Capítulo 3.

1.5 Estrutura da dissertação

A estrutura deste documento é organizada como se segue:

Capítulo 2: Nesta seção, apresentam-se os pressupostos conceituais relacionados aos elementos fundamentais da pesquisa. São abordados conceitos relativos aos mecanismos tradicionais de autenticação do usuário e controle de acesso, bem como a abordagem inovadora de Confiança Zero. Também são discutidas as redes industriais, proporcionando uma base sólida para a compreensão dos capítulos subsequentes.

Capítulo 3: Este capítulo é dedicado ao desenho do ambiente para a realização das simulações, tanto com quanto sem a aplicação do conceito de Confiança Zero. O foco reside na condução de testes que geram conhecimento e servem como alicerce para a análise dos resultados parciais e as discussões subsequentes.

Capítulo 4: O desenho do ambiente para as simulações será abordado, incluindo detalhes sobre o hardware e software utilizados na implementação do modelo. O capítulo abrange a realização de testes e a coleta de métricas de redes, permitindo a obtenção de dados em diferentes cenários, como atividades rotineiras e a influência de ataques. Os dados coletados desempenharão um papel crucial na fundamentação dos resultados parciais e nas discussões que serão apresentadas no próximo capítulo.

Capítulo 5: O objetivo deste capítulo é apresentar os resultados da pesquisa, bem como expor as considerações finais e propor direções para trabalhos futuros.

2 Fundamentação Teórica

2.1 Mecanismos tradicionais de autenticação do usuário e controle de acesso

O campo da segurança cibernética tem demonstrado avanços significativos ao longo do tempo, à medida que a complexidade aumenta devido à proliferação de novas ameaças digitais. Garantir a segurança de ativos críticos nesse cenário tem proporcionado novos desafios que precisam ser superados. Nesse contexto, os tradicionais mecanismos de autenticação de usuários e controle de acesso desempenham um função crucial na mitigação de acessos não autorizados e na garantia da integridade dos dados. No entanto, diante das soluções apresentadas e das frequentes mudanças no cenário de segurança, é importante realizar uma análise crítica dos métodos utilizados, a fim de conceber novas estratégias para enfrentar as ameaças representadas por usuários maliciosos.

A autenticação é o processo pelo qual a identidade de um determinado agente é verificada para permitir o acesso a um recurso específico. O uso do termo genérico "agente" é intencional, pois representa que o acesso pode ser solicitado por qualquer elemento, seja um usuário ou um dispositivo, este último considerado sob a ótica da comunicação entre máquinas. Estabelecer a legitimidade do acesso é um dos primeiros passos essenciais para a construção de uma rede segura.

Introduzir inovações neste domínio sem antes explorar os mecanismos tradicionais resultaria em um contexto predominantemente comercial, em detrimento do caráter científico. Portanto, torna-se necessário apresentar o estado da arte, observando elementos fundamentais para o desenvolvimento de uma nova estratégia de autenticação para a indústria, que é o foco desta pesquisa.

Os métodos convencionais, voltados para o controle de acesso, delineados na literatura que norteia esta fase, incluem o Controle de Acesso Baseado em Identidade (*Identity-Based Access Control* – IBAC). Este mecanismo simplifica a autorização ao vincular diretamente o acesso a identificadores de usuários, utilizando listas de controle de acesso (*Access Control List* – ACL). No entanto, sua viabilidade em ambientes dinâmicos é comprometida pela necessidade constante de revisões de autorizações a cada nova mudança, desfavorecendo a escalabilidade (Hu 2014).

Outra abordagem presente na literatura é o Acesso Baseado em Função (*Role-Based Access Control* – RBAC). Diferentemente do IBAC, o RBAC gerencia o acesso por meio de funções atribuídas aos usuários, determinando, assim, o acesso a recursos. O RBAC possibilita a centralização sem depender de ACLs, permitindo a criação de ambientes com diversas camadas de funções e privilégios (Hu 2014). Contudo, quando confrontado com ambientes reais, especialmente em infraestruturas críticas, a necessidade de níveis detalhados para o acesso a recursos acaba por inviabilizar sua aplicação (Syed et al. 2022).

Outro modelo, presente na ferramenta Pritunl-Zero (Huff 2022), adotado pela pesquisa utiliza o Controle de Acesso Baseado em Atributos (Attribute-Based Access Control – ABAC), baseado em múltiplos atributos para conceder acesso (Hu 2014). Enquanto o IBAC foca na identidade do usuário e o RBAC na função que o usuário desempenha para determinar o acesso de um agente específico, seja ele um usuário ou um dispositivo, torna-se evidente a necessidade de abordar, em cada nova solicitação de acesso, desafios que nem o IBAC nem o RBAC conseguem enfrentar.

Esses desafios, encontrados tanto quando o controle é realizado por IBAC quanto por RBAC, referem-se à determinação de condições contextuais da ação desse agente, tais como elementos temporais, posicionamento na rede e níveis de risco associados a cada acesso. O controle por meio do ABAC possibilita a aplicação de políticas abrangentes e, certamente, complexas, resumindo as validações *booleanas* de cada atributo. Este conceito foi empregado de maneira simplificada no contexto do controle de acesso para proteção de sensores de Internet das Coisas (*Internet of Things* – IoT) onde foi observado menor tempo de interação em relação a outros (Monir 2016), oferecendo, por sua vez, possibilidades no âmbito da Internet Industrial das Coisas (*Industrial Internet of Things* – IIoT).

A etapa de controle de acesso, essencial para a criação de ambientes seguros, enfrenta desafios significativos ao lidar com a implementação de políticas de segurança em redes industriais. A escolha da estratégia adequada torna-se um elemento primordial nesse contexto, onde a preservação da integridade dos dados é imperativa. Uma decisão equivocada nesse âmbito pode desencadear uma cascata de intercorrências impactantes no cotidiano dos parques fabris.

Diversas abordagens se destacam no estado da arte, dentre elas, o uso do Controle de Acesso Baseado em Blockchain, que emprega contratos inteligentes para a aplicação de políticas de controle de acesso. Esta abordagem permitiu à pesquisa, conforme destacado por (Maesa, Mori e Ricci 2018), a verificação eficaz da implementação das políticas, incluindo a prevenção do acesso de terceiros mal-intencionados.

2.2 Confiança Zero

2.2.1 Fundamentação Teórica

A literatura apresenta o conceito de Confiança Zero como uma evolução das técnicas de autenticação do usuário e controle de acesso. Essa abordagem centraliza sua atenção na proteção de recursos, estabelecendo como princípio fundamental a concessão de permissões somente mediante avaliações contínuas, em vez de permitir implicitamente, como discutido em (Rose et al. 2020). Essa abordagem é válida tanto para usuários quanto para os recursos utilizados por eles.

Em contraste com a abordagem arquitetural anterior, que se baseava na criação de perímetros de segurança para os usuários, presumindo que um usuário com acesso a esses perímetros tivesse autorização para utilizar uma variedade de recursos, a arquitetura de Confiança Zero adota uma postura que questiona a confiabilidade de todos os dispositivos, mesmo quando eles estão dentro de ambientes corporativos e já foram previamente verificados (Rose et al. 2020).

No contexto da Confiança Zero (*Zero Trust* – ZT), destacam-se várias medidas e componentes que direcionam essa abordagem. Uma notável solução de código-fonte aberto é o "Pritunl-Zero" (Huff 2022), que se baseia em um conceito anterior (Spear et al. 2016). Essa solução elimina a necessidade de gerenciar chaves individuais armazenadas em arquivos em cada servidor, optando, em vez disso, por usar certificados SSH que são centralizados em uma autoridade de certificação (Ward e Beyer 2014). Esse enfoque inovador simplifica a gestão de chaves e reforça a segurança dos recursos, contribuindo para a implementação bem-sucedida do princípio da Confiança Zero.

Considerando o contexto da Confiança Zero e as medidas inovadoras destacadas anteriormente, é crucial apresentar o cenário tradicional, conforme descrito na evolução da indústria de firewalls. A segurança ainda enfrenta desafios, especialmente quando o usuário atinge a conclusão do processo, gerando permissões que inadvertidamente permitem movimentações não autorizadas.

Com o modelo predominante na estrutura de segurança da organização, é possível observar a presença de *firewalls* que delineiam o perímetro das instituições em relação aos acessos externos à rede local, conforme mencionado em (Cisco 2019). No entanto, essas regras de delimitação de perímetros mostraram-se insuficientes para conter possíveis ameaças internas e externas na rede local. Essa inadequação ganha destaque em cenários pandêmicos, como exemplificado pela COVID-19, devido ao aumento significativo do trabalho remoto e da utilização de dispositivos pessoais na rede corporativa. Isso torna ainda mais crucial a necessidade de proteção da rede, conforme indicado por (Haddon e Bennett 2021).

A crescente demanda por acesso externo aos recursos internos das empresas, impulsionada pelo advento do trabalho remoto, tornou essencial a expansão da área a ser monitorada para facilitar o acesso desses usuários. A ampliação da rede trouxe consigo desafios significativos na criação de ambientes seguros para as instituições.

Para elucidar os argumentos que serão desenvolvidos ao longo desta pesquisa, é pertinente apresentar, de forma concisa, as definições de Arquitetura de Confiança Zero e Confiança Zero conforme estabelecidas pelo NIST SP 800–207:

> "Todas as comunicações são protegidas, independentemente da localização da rede: as solicitações de acesso a ativos presentes na rede e de propriedade

da empresa deve atender a mesma segurança de elementos que solicitem o acesso e comunicação de qualquer outro. Ela não deve ser concedida de forma automática quando se está numa rede corporativa.

O acesso aos recursos da empresa individual é concedido em um por — base sessão: A confiança de quem está solicitando deve ser avaliada muito antes que o acesso seja concedido, a ideia de delimitar até onde e que tipo de acesso e permitido para qual aplicação e um exemplo do comportamento pós-autenticado.

O acesso aos recursos é determinado pela política dinâmica — incluindo o estado observável da identidade do cliente, aplicativo / serviço e o ativo solicitante – e pode incluir outros atributos comportamentais e ambientais: todos os elementos que permeia o usuário no momento que acessa um recurso deve ser extraído para ser avaliado como dispositivo que está sendo acessado, versão de software em uso, qual tipo de navegador foi permitido, horário e data de solicitação, credencias instaladas além de ser avaliado o comportamento em conflito com o acesso anterior.

A empresa monitora e mede a integridade e postura de segurança de todos os ativos próprios associados: A proposta segue a ideia de estabelecer no momento que se implementa uma arquitetura de Confiança Zero a necessidade de ter critérios de diagnósticos e mitigação continuada como forma de avaliar a postura de segurança de quem está solicitando o recurso. Entra na questão a ideia de relatórios sobre as atividades dos usuários para conflitar com o estado atual do solicitante.

Todas as autenticações e autorizações de recursos são dinâmicas e estritamente aplicadas antes que o acesso seja permitido: neste contexto e indicado que a empresa implemente uma arquitetura que possua gerenciamento de credencial de acesso e sistemas que gerencie ativos, incluindo até o uso de autenticação de vários fatores para acesso dos recursos da entidade. O monitoramento deve ser contínuo com possibilidade de revalidar autorizações de sessões conforme definido pela política da entidade que gira em fornece as aplicações apoiadas em questão de usabilidade, economia e disponibilidade.

A empresa coleta o máximo de informações possível sobre o estado atual dos ativos, infraestrutura de rede e comunicações e os usa para melhorar sua postura de segurança: Este tópico apresentado considera a empresa ter a possibilidade de coletar o máximo detalhes possíveis para ser possível identificar padrões e comportamentos para comparar com acessos anteriores e em certos momentos identificar possíveis pontos de vulnerabilidade com base no comportamento do usuário."(Rose et al. 2020, p. 15)

Os princípios apresentados na padronização proposta pelo NIST adotam uma perspectiva tecnologicamente agnóstica. Isso significa que esses princípios do ZT visam, em certa medida, fornecer elementos de natureza genérica, com o propósito de não constituírem um objetivo em si mesmos, mas sim um meio pelo qual se pode proceder à implementação de Arquiteturas de Confiança Zero (*Zero Trust Architecture* – ZTA). Nesse contexto, ZTA representa o plano de segurança a ser aplicado em uma rede específica, fazendo uso dos princípios do modelo, enquanto ZT abrange a coleção de conceitos e definições que orientam a construção de uma visão filosófica sobre esse enfoque de segurança.

2.2.2 Abordagens para implantação de Confiança Zero

Em um mundo cada vez mais direcionado para a segurança cibernética, a compreensão dos elementos essenciais que constituem um ambiente de Confiança Zero é de extrema importância. Para efeitos de investigações futuras em diversos campos, é crucial compreender os vários componentes lógicos que compõem um ambiente de Confiança Zero em organizações. A presente pesquisa apresenta esses elementos em um modelo ideal, fundamentado na interação entre eles. Os componentes lógicos em questão estão de acordo com as diretrizes estabelecidas através do documento, NIST SP 800–207, publicado pelo Instituto Nacional de Padrões e Tecnologia dos Estados Unidos (*National Institute of Standards and Technology* – NIST). Define o conceito:

> - Mecanismo de política (*Policy engine* – PE): componente responsável pela decisão final de concessão de acesso a determinado recurso, oferecendo a possibilidade de conceder, negar ou revogar acesso a recursos. Neste caso, o mecanismo trabalha em paralelo com outro componente a ser descrito, que é o administrador de políticas, onde o mecanismo toma e registra decisões, e a administração de políticas executa a decisão.
> - Administrador de políticas (*Policy administrator* – PA): é responsável por estabelecer a conexão ou encerrar o caminho de comunicação. Neste ponto, ocorre a transação de token que valida a sessão daquele usuário, por meio da troca de mensagens com o mecanismo de políticas, permitindo a criação da sessão ou encerramento da conexão.
> - Ponto de aplicação de política (*Policy enforcement point* – PEP): neste ponto, o sistema é responsável por habilitar, monitorar e encaminhar solicitações para que a comunicação se concretize.
>
> (Rose et al. 2020, p. 9)

Uma indústria que almeja implementar uma arquitetura de Confiança Zero envolve diversos componentes fundamentais (Rose et al. 2020). Essa abordagem pode ser puramente baseada em ZT, na qual todos os princípios são rigorosamente aplicados em sua estrutura, ou pode adotar um modelo híbrido, integrando elementos do modelo tradicional e incluindo um ou mais componentes, com ênfase em um motor de políticas sendo aplicado. Nesse contexto, a coleta de dados de várias fontes desempenha um papel central, fornecendo informações essenciais que embasam as decisões a serem tomadas relacionadas a novos acessos.

A implementação do modelo de pesquisa proposto pode ser compreendida a partir de três perspectivas distintas. São elas: acesso de rede baseado em ZT com o uso de

governança de identidade aprimorada, aplicando a microssegmentação da rede e, por fim, empregando infraestruturas de rede e perímetros definidos por software.

No contexto do acesso com governança de identidade aprimorada, é estabelecido que o acesso somente é concedido a atores previamente atribuídos com atributos que estão intrinsecamente ligados à sua identidade. A autorização de acesso é condicionada à avaliação do índice de confiança gerado a partir da análise de vários critérios, como a localização na rede, o dispositivo utilizado e o histórico do ator solicitante, a fim de conceder privilégios específicos para a utilização de recursos.

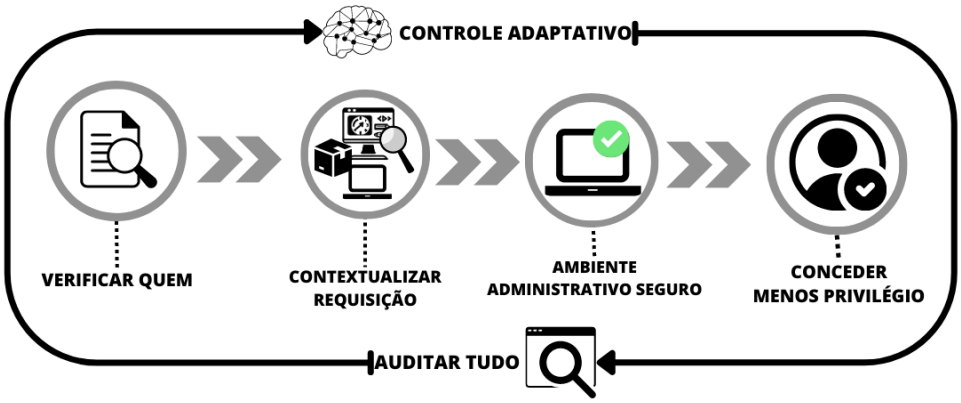

Figura 1: Resumo dos princípios do Zero Trust.
Fonte: Adaptado http://trendmicro.com.

No contexto da implementação através da microssegmentação, essa abordagem compartilha semelhanças conceituais com o isolamento de redes em ambientes industriais, através da criação de Zonas. Nestas Zonas, são utilizados Conduítes que estabelecem canais de comunicação entre elas, promovendo a inspeção e proteção das comunicações. O principal objetivo da microssegmentação é restringir o acesso a grupos específicos de recursos. Neste cenário, a estratégia baseia-se na utilização de *switches* e *firewalls* inteligentes, os quais desempenham o papel do Ponto de Aplicação da Política (*Policy Enforcement Point* – PEP), garantindo a proteção de recursos individuais ou conjuntos (Zaheer et al. 2019), (Rose et al. 2020).

Quando se trata de infraestruturas de redes e da criação de perímetros definidos por software para a implementação do Acesso a Rede de Confiança Zero (*Zero Trust Network Access* – ZTNA), conforme proposto pelo NIST (Chandramouli 2022), é introduzido o conceito de sobreposição de rede, com atuação na camada de aplicação do modelo OSI, ou até mesmo a nível da camada de rede. O Administrador de Políticas (*Policy administrator* – PA) é concebido como o controlador de rede responsável e deve se adaptar e configurar a rede com base nas diretrizes fornecidas pelo Mecanismo de Política (*Policy engine* – PE). Nesse modelo, os clientes interagem com os PEPs para solicitar acesso, enquanto a gestão da rede continua sendo por componentes do PA.

2.3 Redes Industriais

2.3.1 Arquitetura e Padronização de Redes Industriais

A complexidade inerente à organização das redes industriais contemporâneas, que demandam a transferência confiável de dados em larga escala, destaca a importância crucial da arquitetura e padronização dessas redes. Uma arquitetura bem delineada, fundamentada em conceitos discutidos na literatura, amplia a capilaridade da comunicação, estabelecendo conexões de alto impacto para otimizar as rotinas no chão de fábrica.

Essa abordagem viabiliza uma conectividade robusta e facilita o monitoramento ágil para atender demandas em constante evolução. A utilização de conceitos consolidados na construção dessas redes e a adoção de padronizações contribuem para a criação de bases sólidas, acessíveis a todo o setor industrial. Esse enfoque não apenas fomenta uma melhor interoperabilidade, mas também delineia claramente os passos futuros a serem seguidos por toda a indústria.

Diversas fontes de padronização para Sistemas de Controle Industrial (Industrial Control Systems - ICS) se propõem a orientar a construção de uma indústria segura, abordando tópicos que visam a escalabilidade e a entrega eficiente de resultados. Destaca-se, entre essas fontes, a norma IEC 61850 ((IEC) 2023), que define como deve ocorrer a comunicação, possibilitando a utilização de inúmeros dispositivos independentemente do fabricante.

No que diz respeito à organização de uma estrutura industrial com foco no nível de segurança, a norma ISA/IEC 62443 (ISA e IEC 2022) abrange os aspectos de segurança cibernética até o nível físico. Essa padronização baseia-se inicialmente no padrão ANSI/ISA95 ((ISA) 2019), conhecido como ISA 95, que introduziu o conceito de camadas, apoiando-se em um modelo de Arquitetura de Referência Empresarial Purdue (*Purdue Enterprise Reference Architecture* – PERA) (Williams 1993). No entanto, o modelo ISA/IEC 62443 enfatiza a construção de zonas e condutos para promover a interligação. O conceito de camadas fornece um contexto abstrato para apresentar membros-chave de cada camada de forma mais clara. Além das padronizações, existem entidades que fornecem orientações, como o NIST 800-20 (Standards e (NIST) 2023), servindo como fonte para a oferta de segurança para estrutura técnicos operacionais.

2.3.2 Protocolos de Comunicação em Redes Industriais

No contexto de um ICS, diversos elementos e componentes dependem da comunicação para executar suas funções. Cada um desses elementos opera por meio de protocolos específicos fornecidos por seus respectivos fabricantes, estabelecendo regras particulares para sua utilização. Como exemplo pode-se citar Modbus, Fieldbus e DNP3,

que são protocolos comuns na indústria, e mesmo com a coexistência de múltiplos fornecedores na industria, surgiu a necessidade de criar padrões abertos que promovam a interoperabilidade e otimizem os custos envolvidos

A comunicação nas redes industriais, de maneira simplificada, manifesta-se pela necessidade de determinados pontos, onde as ações de gestão se concentram, interagirem com pontos que fornecem e disponibilizam informações em tempo real sobre as operações no chão de fábrica. Isso é alcançado através de sensores e atuadores, contribuindo para a expansão da capacidade de controle de toda a cadeia de produção. Um exemplo desse processo de comunicação é a troca de informações entre Unidades Terminal Principal (Master Terminal Unit - MTU) e Unidades Terminal Remota (Remote Terminal Unit - RTU), estabelecida por meio de protocolos de comunicação específicos.

Historicamente, a comunicação entre os terminais e outras estruturas ocorria, por exemplo, através de instrumentos e relés de proteção que inicialmente estabeleciam comunicação remota utilizando a associação local RS232, um padrão de protocolo para a troca de informações por meio de dados binários, semelhante às portas seriais em computadores que seguem esse padrão (Buchanan 1999). Em alguns casos, também se valia da rede discada. No entanto, à medida que a complexidade dessa estrutura cresceu significativamente, tornou-se crucial migrar para protocolos mais avançados.

Em 1984, foi introduzido o modelo de Interconexão de Sistemas Abertos (*Open System Interconnection* – OSI), que descreve o processo de comunicação de dados em sete camadas distintas e delineia como os dados devem ser tratados em cada uma dessas etapas (Sheldon 2001). O uso de protocolos abertos incentivou a possibilidade de alcançar interoperabilidade entre dispositivos, reduzindo assim a dependência dos fornecedores.

Dentre os vários protocolos que adotam o modelo OSI e são aplicados em ICS, destaca-se a criação do protocolo Modbus pela empresa Modicon, atualmente Schneider Electric UK (Electric 1999). Esse protocolo é projetado para viabilizar a troca de mensagens na camada de aplicação (Modbus 2004), permitindo a conexão de dispositivos eletrônicos e facilitando as interações entre o MTU e RTU.

O Modbus é um protocolo proprietário baseado no paradigma cliente-servidor, em que o cliente Modbus é responsável por gerar solicitações ao servidor Modbus. Esse protocolo opera por meio de um mecanismo de solicitação/resposta e disponibiliza serviços específicos identificados por códigos de função. Esses códigos constituem elementos das unidades de dados de protocolo (*Protocol Data Units* – PDUs) utilizadas na comunicação por meio do Modbus.

Uma característica notável da rede que utiliza o protocolo Modbus é a capacidade de um cliente interagir com um máximo de duzentos e quarenta e sete servidores RTUs (Unidades Remotas de Terminais) (Modbus 2004). Essas unidades estão orientadas para

responder a questionamentos específicos, evitando assim respostas a transmissões indiscriminadas. Dentre os comportamentos habilitados pelas mensagens de comunicação, destacam-se as solicitações/respostas de/para MTUs, mensagens de confirmação de recebimento bem-sucedido de mensagens MTU e RTUs. Quando o MTU envia mensagens para o servidor, atribui um endereço a cada um dos servidores, respeitando o limite máximo estabelecido pelo protocolo.

Esta pesquisa adota o padrão Modbus TCP/IP, uma evolução do Modbus tradicional destinada a aprimorar a confiabilidade da comunicação em redes industriais, como protocolo para a criação do ambiente de teste. O protocolo oferece diversas vantagens, como maior confiabilidade, segurança, escalabilidade e interoperabilidade.

O protocolo Modbus TCP utiliza métodos de detecção de erros presentes no quadro Ethernet, sendo a Verificação de Redundância Cíclica (*Cyclic Redundancy Check* 32 – CRC-32) (Modbus 2004). Não é acrescentado ao quadro um campo para checagem de erro no protocolo em si, o que deve ser considerado ao explorar vulnerabilidades Ethernet, apresentando riscos e fornecendo um ponto de pesquisa, dada a forma como ocorre a verificação de cada pacote. Uma vez que o protocolo utiliza o meio físico Ethernet, está sujeito ao Acesso Múltiplo por Detecção de Portadora com Detecção de Colisões (*Carrier Sense Multiple Access with Collision Detection* – CSMA-CD). O protocolo em questão tem a finalidade de evitar colisões, garantindo que, quando uma estação transmite um sinal, ela só o faz quando o canal está livre.

Em pesquisas anteriores sobre Sistemas de Controle em Rede (Networked Control Systems - NCS), essa abordagem foi explorada devido à necessidade de precisão temporal durante a sincronização entre dispositivos para assegurar uma operação efetiva. Foram realizadas comparações entre os protocolos CSMA-CD e TDMA, analisando aspectos relacionados à segurança. No entanto, ambos os protocolos tornaram-se suscetíveis a ataques de dessincronização maliciosa (Junior e Souza 2012).

Este aspecto ganha relevância devido à potencial influência no desempenho da rede, sugerindo-se como tema para pesquisas futuras a análise do protocolo em questão e a viabilidade da evolução do protocolo com uma camada de segurança antes de disponibilizar o acesso ao cabeçalho do Modbus TCP, especialmente em ambientes de infraestruturas críticas orientados ao modelo ZTNA.

2.3.3 Segurança em Redes Industriais

Os Sistemas de Controle Industrial, reconhecidos como componentes cruciais para o funcionamento eficiente e ininterrupto de infraestruturas críticas, desempenham um papel crucial, sobretudo na gestão das operações de supervisão e recebimento de dados. Essas funções, aliadas a soluções específicas, possibilitam o gerenciamento e a administração

de processos em uma indústria. Uma das características fundamentais desses sistemas reside em sua concepção original, voltada para garantir a continuidade operacional e a segurança.

Entretanto, é crucial observar que esses sistemas não foram originalmente projetados para enfrentar ameaças provenientes de invasões maliciosas, uma vez que sua operação pressupõe a criação de ambientes isolados por meio de zonas de atuação, apresentando conectividade escassa ou nula com redes externas à indústria.

À medida que a indústria evoluiu, com a introdução de novas tecnologias e protocolos nos ICS, houve aperfeiçoamentos significativos nos tempos de resposta e na qualidade das transações de dados. Contudo, essa evolução também inseriu os sistemas em um contexto que exige uma atenção redobrada à segurança dos dispositivos, especialmente devido à crescente interconexão com elementos externos que, anteriormente, eram isolados.

O modelo tradicional de ICS, seguindo padrões como o ISA95/IEC-62264, busca aprimorar a eficiência e interoperabilidade entre diferentes níveis, sem, contudo, influenciar a escolha da topologia de rede a ser adotada. Nas aplicações industriais, as topologias de barramento, estrela e anel são frequentemente empregadas, cada uma apresentando características distintas e diversos níveis de segurança.

Entretanto, todas essas topologias podem apresentar vulnerabilidades e serem propensas a ataques maliciosos. Por exemplo, em uma topologia de barramento, o compartilhamento do cabo pode facilitar a interceptação e modificação não autorizada dos dados em trânsito. Em uma topologia em estrela, embora a segurança seja mais pronunciada, o dispositivo central torna-se um ponto crítico de falha e um alvo potencial para ataques.

Na topologia em anel, apesar de sua robustez, também pode ser vulnerável a ataques, especialmente se um dispositivo for comprometido. Dessa forma, a implementação de medidas de segurança apropriadas, como criptografia e monitoramento em tempo real, revela-se essencial para mitigar os riscos associados a essas configurações.

Os ataques cibernéticos em ambientes industriais têm se tornado uma preocupação cada vez mais significativa devido ao papel crucial dos Sistemas de Controle Industrial no funcionamento eficiente e confiável das infraestruturas críticas. Diversas estratégias são adotadas por indivíduos mal-intencionados, sejam eles agentes isolados ou conglomerados de grande porte.

Entre as metodologias existentes, uma se destaca por guiar os gestores na identificação até o momento de contramedidas, a *Cyber Kill Chain* (Martin 2014). Também conhecida como Cadeia de Ataques Cibernéticos, sua estrutura possibilita definir cenários para ações contra, guiando a geração de ataques no ambiente de teste, conforme ilustrado na Figura 2. Essa abordagem permitiu descrever uma tentativa de invasão de forma precisa, fornecendo informações que possibilitam a adaptação para os ambientes.

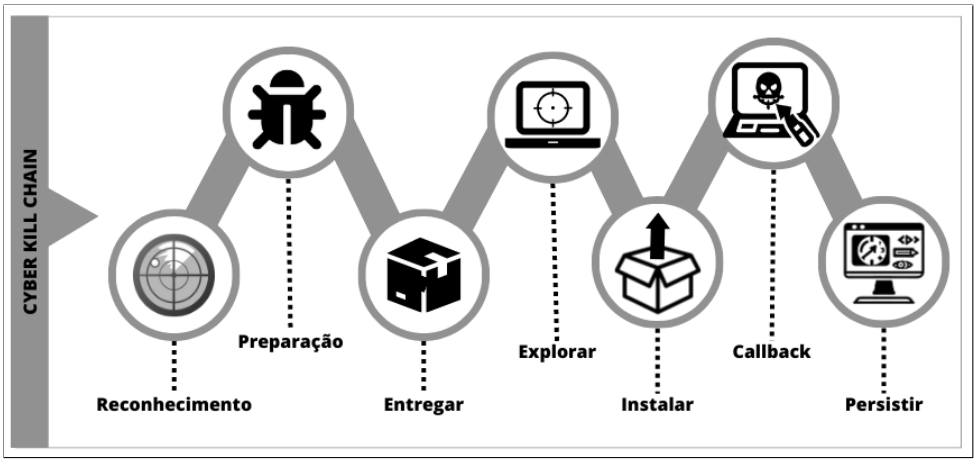

Figura 2: Representação das etapas do "Cyber Kill Chain".
Fonte: Adaptado de (Martin 2023).

A segurança na indústria enfrenta diversas ameaças maliciosas, conforme apontado nos relatórios do primeiro semestre de 2023 da empresa de segurança Kaspersky (CERT 2023). Entre as principais causas de comprometimento das empresas, destacam-se ações como negação de serviço, vazamento de credenciais, vazamento de dados e ransomware. Outro relatório relevante, divulgado pela Fortinet (Fortinet 2023), ressalta a persistência de ameaças como malware e phishing, que continuam a representar desafios significativos. Através desses métodos, os invasores conseguem obter privilégios para a execução de códigos arbitrários.

O mesmo relatório da Fortinet apresenta dados intrigantes, indicando que mais de 50% dos Controladores Lógicos Programáveis ou Unidades Terminais Remotas utilizam criptografia, autorização de usuário e autenticação de usuário para dispositivos. Contudo, é crucial observar criticamente que as atividades maliciosas destacadas pelo relatório sugerem um padrão recorrente na aquisição de credenciais pelos atacantes.

Nesse contexto, a presente pesquisa assume uma posição crítica, reconhecendo que o modelo adotado pode desempenhar um papel fundamental na mitigação de ações prejudiciais à rede. Destaca-se a importância de aprimorar as práticas de controle de acesso, monitoramento de eventos e resposta a incidentes, a fim de prevenir e combater efetivamente as crescentes ameaças à segurança cibernética na indústria.

2.3.4 Confiança Zero em Redes de Controle Industrial

A estratégia Confiança Zero emerge como uma abordagem para a salvaguarda de ativos críticos de infraestrutura, visando mitigar os riscos inerentes a violações de segurança em redes industriais. Para sua implementação bem-sucedida, apresenta-se a necessidade da condução de uma avaliação minuciosa da arquitetura existente, identificando possíveis vulnerabilidades e avaliando a viabilidade do modelo proposto.

Neste contexto, o rastreamento da interação entre usuários e sistemas supervisórios deve ser um ponto crucial para a aplicação da abordagem ZT. Isso decorre da importância em coibir acessos indevidos por parte de usuários não autorizados, preservando, assim, o funcionamento ininterrupto dos dispositivos que mantêm comunicação com o Controlador Lógico Programável (*Programmable Logic Controller* – PLC).

A validação de dispositivos surge como um ponto crucial a ser meticulosamente considerado, uma vez que, conforme preconizado pelo NIST (Rose et al. 2020), não se deve tacitamente aceitar a legitimidade das ações provenientes de usuários e dispositivos.

Nesse contexto, a confirmação das identidades, que são possíveis de serem forjadas no instante da bidirecionalidade de requisições entre cliente-servidor, com ataque do tipo homem do meio (*Man-In-The-Middle* – MITM), torna-se essencial para prevenir a possibilidade de falsificação dessas identidades. A adulteração abriria caminho para a validação errada de ações provenientes de IIoT, tornando crucial a implementação de dispositivos resilientes à falsificação, conforme apresentado em (Syed et al. 2022).

Para atender a esta demanda da pesquisa, optou-se pela implantação de uma ferramenta específica (Pritunl 2022), que viabiliza o controle de acesso através da validação de atributos, propiciando a integração eficaz do contexto de Confiança Zero. Apesar de sua concepção inicial voltada para ambientes empresariais, sua adaptação para redes industriais em nível operacional se mostra factível, uma vez que compartilham elementos comuns, como a utilização de diversas aplicações e a presença de atributos atrelados ao hardware e software suscetíveis de questionamento.

A presença de inúmeros atributos possibilitou a aplicação de uma política de avaliação constante, conforme oferecida pela solução utilizada. Assim, a estratégia de Confiança Zero possibilita a autenticação de usuários autorizados com papéis específicos para cada rotina, levando em consideração informações como o dispositivo utilizado e suas características de segurança, tanto relacionadas ao hardware quanto ao software.

3 Ambiente de Teste: Confiança Zero para Redes Industriais

3.1 Técnicas propostas e desenvolvimento

A presente seção expõe a metodologia empregada no desenvolvimento deste estudo, utilizando ambientes simulados para a proposição de testes, permitindo a construção de conhecimento por meio de uma pesquisa experimental com elementos quantitativos e um nível de profundidade, sob a forma exploratória. Dada a natureza abstrata da abordagem Confiança Zero (*Zero Trust* – ZT) na indicação de medidas de segurança, optou-se pela estratégia de Acesso de Confiança Zero à Rede (*Zero Trust Network Access* – ZTNA) para inserir essa abordagem em um contexto de restrição de acesso a recursos, conforme as decisões de políticas de acesso.

Para o desenvolvimento do ambiente de simulação industrial para testes, foram utilizadas as seguintes estruturas:

O equipamento base, Dell G3 3590 com as seguintes especificações:

- Sistema Operacional: Windows 11 Home
- Processador: Intel® Core™ i5-9300H CPU @ 2.40GHz (8MB Cache, OverClock até 4.1 GHz)
- Núcleos: 4
- Processadores Lógicos: 8
- Memória Física (RAM) Instalada: 8,00 GB
- Memória Virtual: 12,1GB
- HD: 1 TB

Configuração das Instâncias:

As instâncias foram criadas utilizando o VMware Workstation 17, seguindo a regra de utilização de instâncias virtuais idênticas. Cada uma das instâncias utilizou o sistema operacional Debian versão 10, com as seguintes configurações:

- Processador: 1 GHz
- Memória RAM: 2 GB
- Espaço em Disco: 10 GB

Nas seções subsequentes, são detalhadas a implementação das técnicas ZT, a descrição da ferramenta utilizada, e a apresentação de propostas fundamentadas no que foi evidenciado ao longo dos testes.

3.1.1 Implementação de Técnicas de Confiança Zero

As atividades propostas, alinhadas aos pilares do ZT, incluíram a utilização de autenticação de dispositivos, micro-segmentação da rede, auditoria contínua de acesso e a possibilidade de autenticação multifatorial. Para estabelecer ambientes experimentais equivalentes nos dois cenários propostos, buscou-se garantir a identidade de configuração das bases de cada instância virtualizada, replicando a máquina base para diversos propósitos. Isso assegurou critérios consistentes nos testes administrados em relação ao equipamento.

No que diz respeito à central ZTNA e às políticas implementadas, as políticas foram elaboradas mediante o monitoramento do fluxo de trabalho e das mensagens, o que ocorreu por meio da tomada de decisão de política centrada em critérios presentes no cliente. Simultaneamente à análise das credenciais do usuário, foram validados os critérios dos equipamentos que requeriam serviço. Dispositivos com configurações específicas tinham a capacidade de fornecer entradas para as variáveis do algoritmo de confiança.

Algoritmo 1: Alteração da Inicialização do app em Flask para uso Multithreading

```
from control import *

# Run App BEGIN
if __name__ == "__main__":
    app.run(host=WEB_CLIENT_HOST, port=WEB_CLIENT_PORT, debug=False, threaded=True)
# Run App END
```

Usuários que utilizavam a plataforma com credenciais específicas eram obrigados a fornecer outras informações, como dados telemétricos de dispositivos, a fim de validar suas ações. As requisições com um protocolo específico foram codificadas em Python, utilizando a biblioteca PyModbus, e apresentadas por meio de uma interface homem-máquina implementada em Flask, com a opção de *threading* ativada "threaded=True" para permitir concorrência, conforme apresentado no Algoritmo 1 . Essa interface fornecia exemplos de rotinas.

A interface possibilitava a interação do usuário, permitindo o envio de requisições para a instância designada ao PLC. Com o intuito de evitar que serviços terceiros presentes nas instâncias virtuais interferissem na coleta de dados, foram monitorados e desativados aqueles considerados desnecessários. Essa abordagem evitou comportamentos anômalos durante os testes de coleta de dados.

Nos cenários avaliados entre as requisições disponíveis na Interface Homem-Máquina (*Human Machine Interface* – HMI) para o dispositivo com simulação de um Controlador lógico programável (*Programmable Logic Controller* – PLC), com uso da biblioteca PyModBus, são disponibilizadas as ações "Write Single Coil" e "Read Coils", sendo utilizada a primeira ação na investigação propostas sobre diferentes cenários.

Algoritmo 2: Código JavaScript para Automação de Atividades no HMI/PLC

```
1: let myVar = setInterval(myTimer, 1000);
2: function myTimer() {
3:   document.getElementById("btn_coilSet").click();
4:   // ...
5:   document.getElementById("btn_receiveCoils").click();
6: }
```

Essas ações são enviadas por meio de uma rotina com tempo determinado e intervalos pré-definidos entre cada requisição. Isso possibilita a execução de ações no HMI/PLC, proporcionando uma análise mais eficiente e precisa das interações no contexto do estudo. Por meio de um código específico, as interações no HMI/PLC são automatizadas, conforme exemplificado no Algoritmo 2.

A telemetria dos equipamentos nos testes foi coletada por agentes instalados nas instâncias virtualizadas participantes. Esses agentes transmitiam, em tempo real, os dados para o dispositivo designado como base da coleta, fornecendo informações instantâneas.

Nas atividades de coleta da telemetria e análise de dados, foi empregado o Zabbix, uma ferramenta de código aberto voltada para monitoramento de ativos na rede. De forma simultânea, o Wireshark foi utilizado para analisar o tráfego de rede durante os testes, permitindo a visualização de métricas de desempenho da rede em ambos os cenários.

Em busca de estabelecer condições mínimas para a conformidade com o ZT, foram implementadas regras para definir perímetros utilizando a ferramenta escolhida. Com o auxílio do dispositivo equipado com o PFSENSE, foi possibilitada a microssegmentação por meio da criação de redes locais virtuais. Essa abordagem direcionada à segmentação de perímetro permitiu a criação de zonas para simulação de rede industrial.

Além da autenticação do usuário, observou-se, por meio dos relatórios da instância designada para ser o ponto central ZTNA, que os critérios do plano de controle inteligente adotado eram verificados a cada transação.

Para o plano de controle, definimos regras específicas, como restrições de acesso com base nas credenciais apresentadas e nos atributos rastreados dos dispositivos previamente autorizados sendo observado se estes estão presente no histórico do usuário em questão. Essas regras de segurança permitem que as ações que o usuário pode executar através do HMI sejam apresentadas em uma tela conforme ilustrado na Figura 3, e são observadas pela Central ZT.

Para utilizar um determinado recurso, o dispositivo era avaliado continuamente à medida que ocorria a solicitação de uso do mesmo. Cada transação, conforme o algoritmo implementado no framework, passava por uma verificação na qual eram considerados os critérios preestabelecidos. Caso esses critérios não fossem atendidos, ocorria a negação do

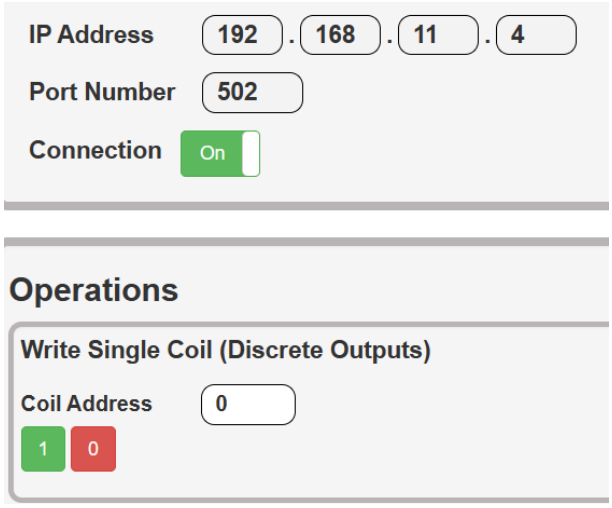

Figura 3: Tela com a opção "*Write Single Coin*".

recurso.

Para simular as rotinas industriais, foram empregadas regras que possibilitaram a implementação das atividades pertinentes à segurança de Sistema de Controle Industrial (*Industrial Control System* – ICS) sob a abordagem ZT. Dentre as regras definidas, foram considerados e estabelecidos os seguintes fatores:

- Seleção de uma rotina ou atividade específica para ser avaliada;
- Verificação se o ambiente atende aos requisitos propostos pela abordagem;
- Devido à complexidade de simular implementações presentes em plataformas reais localmente, foram empregadas ferramentas de virtualização como suporte;
- Configurações otimizadas nas instâncias virtualizadas para garantir uma coleta de dados livre de influências de contextos;
- Utilização de dispositivos equipados com agentes para disponibilizar dados de telemetria.

Para configurar as máquinas virtuais com serviços específicos, foi elaborado o seguinte mapeamento dos dispositivos, conforme a Figura 4:

- Máquina A: Configurada para disponibilizar recursos, originados do uso de um microframework, e gerar a Interface Homem-Máquina - (*Human Machine Interface* – HMI).
- Máquina B: Ambiente implantado para atuar como ponto de decisão e aplicador de políticas, utilizando ferramenta que fornece atividades características da arquitetura ZT, com o PRITUNL-Zero.

- Máquina C: Configurada para simular dispositivo receptor de instruções via protocolo Modbus TCP, atuando como PLC, servidor, e podendo ser utilizada em ambos os cenários.
- Máquina D: Dispositivo utilizado pelo usuário para interagir com o HMI/MTU, dispondo de um navegador específico, Firefox, e com sistema operacional Windows com endereçamento de IP pré-definido.
- Máquina E: Utilizada como base para coleta de dados apoiado a ferramentas como Wireshark e Zabbix.
- Máquina G: Disponibilizado para atuar no papel de Firewall e Roteador através da solução PFSENSE.
- Máquina F: O dispositivo utilizado foi configurado com o sistema operacional Kali Linux, que inclui as ferramentas necessárias para a aplicação de ataques. Além disso, foi empregada a solução open-source Infection Monkey (Akamai 2023), uma plataforma de autopropagação e mapeamento de rede que oferece técnicas de pentest para a exploração de falhas conhecidas (Yarali e Sahawneh 2019), com o propósito de avaliar o nível de maturidade do modelo ZT.

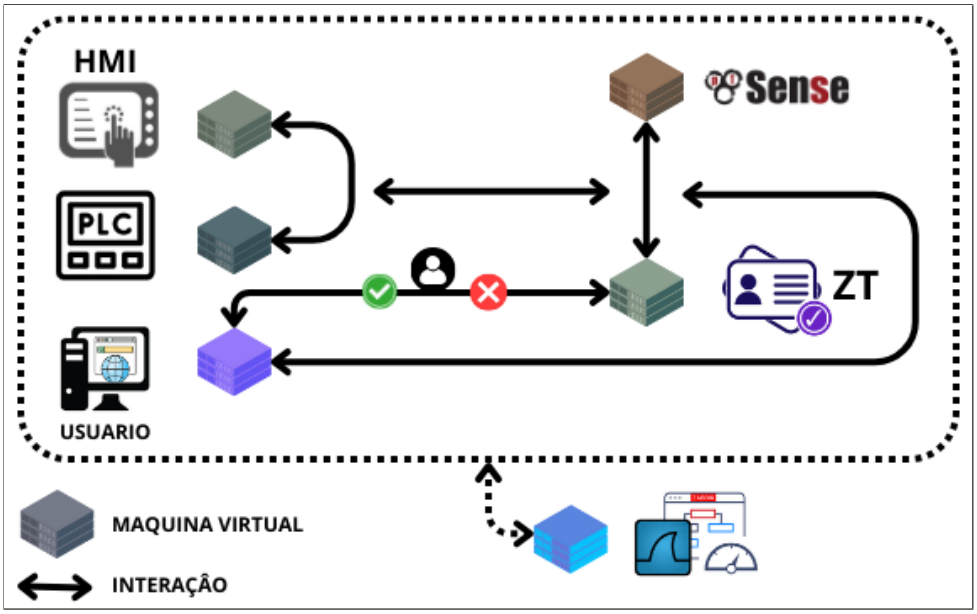

Figura 4: Comunicação entre maquinas virtuais com a presença das soluções.

Ao adotar a ferramenta com abordagem ZT, foram realizadas algumas adaptações, que incluíram o uso de certificados digitais para assegurar uma comunicação segura entre as transações. O ambiente criado enfrentou um desafio no uso desses certificados digitais, demandando a criação de chaves por meio da ferramenta MKCERT, uma solução voltada para a geração de chaves locais e autênticas (Valsorda 2023).

A utilização desta solução permitiu a incorporação de assinaturas autoassinadas, fornecendo uma camada adicional de segurança tanto para a gestão da central ZTNA quanto para o ambiente de interação do usuário. Foram estabelecidas duas rotas de acesso: uma delas direcionando para a sala de controle das políticas aplicadas no ambiente (https://zero.pritunl), e a outra atuando como um porteiro para redirecionar ao recurso (https://zero-user.pritunl). O recurso disponibilizado era a interface homem-máquina para interagir e enviar comandos para o PLC.

A ferramenta utilizada para gerir as políticas, Pritunl-Zero, é apresentada como uma evolução da ferramenta Pritunl (Huff 2022), e sua principal função é oferecer uma abordagem ZT semelhante ao contexto proposto na pesquisa BeyondCorp, uma implementação da Google para o conceito de segurança de ativos em rede (Ward e Beyer 2014).

Ambos os projetos, Pritunl e BeyondCorp, fornecem um sistema de controle de acesso autenticado e seguro a servidores, sem a necessidade de gerenciar chaves SSH. Eles promovem uma rede ZT (Spear et al. 2016), similar ao contexto de micro perímetros. Sua estrutura inicialmente pode ser tratada como semelhante ao modelo tradicional mas o que se difere é a aplicação a um nível mais estratégico da abordagem.

Ao verificar as configurações internas na plataforma, é possível observar o uso de micro segmentação com monitoramento contínuo das autorizações. As ações internas presentes na plataforma, como definir recursos, papéis, usuários e especificações sobre o ponto de origem das solicitações, oferecem a capacidade de criar uma divisão lógica dos papéis e recursos. Adicionalmente, o algoritmo de confiança por critérios promove o acesso seguro de acordo com a padronização ZT pelo NIST. A seguir estão os princípios que foram utilizados para atingir a abordagem ZT:

A) Identidade

   (a) A validação da identidade é um elemento importante na abordagem ZTA. O acesso a recursos só é possibilitado quando o usuário devidamente registrado utiliza suas credenciais no endereço específico, sendo concedido o acesso por sessão.

   (b) Um gestor de identidade e acesso autoriza ou nega o acesso ao recurso, somado à validação com autenticação multifator, especificamente através da autenticação por SSH. A ferramenta também permite o uso de outras formas, como código temporário, Google Authenticator, ou código por SMS, DUO.

B) Dispositivos

   (a) A autorização dos dispositivos é outro ponto crucial para a estratégia adotada, e a autorização ocorre com base nos detalhes dos equipamentos a nível de ferramenta de acesso.

(b) O posicionamento na faixa de rede e informações do sistema operacional são coletados para comparação, determinando se o perfil de acesso está autorizado a acionar o recurso a partir daquele dispositivo.

(c) Entre os critérios estão o navegador, versão do navegador, endereço IP permitido para aquele recurso, lista de IPs não permitidos, sistema operacional com versão, entre outros. Ao final da pesquisa, uma atualização da ferramenta permitiu testar o uso de TPM para validação do dispositivo.

C) Aplicações

(a) A camada de aplicação é protegida com a implementação do ZTNA, onde a proposta é criar limites de acesso a determinados recursos autorizados com base na necessidade de determinada função do usuário.

(b) Os usuários são vinculados aos tipos de serviços que podem utilizar, direcionando-os, uma vez autenticados, para a aplicação correspondente.

D) Dados

(a) Para manter a integridade dos dados, foi necessário identificar, dentro de um cenário industrial, elementos a serem escolhidos para criar os teste.

(b) Foi identificado um ponto sensível de dados para a aplicação do ZTNA, escolhendo uma rotina crítica, como atribuir sinal de desligamento para o PLC, para ser monitorada. Durante os testes, a proposta foi manter o dispositivo sempre ligado e, em cenários de ataque, impedir o religamento após o comando de desligar, por negação de serviço, e em outro cenário, fazer a injeção de comando de desligar para o PLC.

E) Infraestrutura

(a) Para o ambiente de simulação, todo o acesso aos recursos oferecidos pelo HMI passava por ações de *proxy* reverso, e os ambientes virtualizados eram devidamente configurados com rotinas para atualizações e desativação de serviços que poderiam comprometer a coleta de dados.

(b) Durante os testes com ataques, houve a necessidade de ampliar a configuração da máquina virtual destinada para o HMI, PLC e demais, de 1 GB cada para 1.5 GB.

F) Redes

(a) Com a topologia escolhida, que utiliza a estrutura em estrela devido à comunicação envolvendo poucos elementos, e com o objetivo de centralizar a aquisição para o mecanismo de política, optou-se por empregar o PFSENSE

para promover a microssegmentação da rede e aplicar uma barreira para outras portas. É importante ressaltar que a topologia em estrela pode ser considerada um ponto vulnerável, e sua utilização em cenários reais deve ser estrategicamente organizada para evitar a indisponibilidade da estratégia oferecida pela Central ZT, utilizando redundância, quando necessário.

(b) Foram criadas duas zonas, uma destinada para o nível operacional e controle (faixa 192.168.10.0/24) onde se posicionava a ferramenta Pritunl-Zero e a solução HMI, e outra para o nível de controle (faixa 192.168.11.0/24) com a presença da solução PLC. Na faixa 192.168.0.0/24, eram disponibilizados dispositivos onde o operador acessava para interagir com o HMI remoto.

G) Auditoria e Relatórios

(a) Em relação à auditoria, a ferramenta utilizada guardava e listava para o gestor um painel com detalhes de todas as ações dos usuários, identificando momentos em que não houve a validação de credenciais, com o ID daquela sessão e detalhes sobre qual recurso foi utilizado.

(b) Em paralelo, a ferramenta, operando com o conceito de disponibilizar agentes na borda do nível de operação e controle, incorporou o Zabbix para fornecer agentes destinados à aquisição de telemetria dos dispositivos. Uma vez que o Acesso por Confiança Zero (*Zero Trust Network Access* - ZTNA) não é uma solução única capaz de abranger todos os objetivos, diversas outras soluções foram adotadas, incluindo o PFsense, certificados digitais e a própria ferramenta Pritunl-Zero em conjunto.

(c) Existe a possibilidade de integrar a base de dados gerada pela ferramenta Pritunl-Zero como o Grafana para auxiliar como monitor de atividades, que só foi utilizado logo apos a conclusão da pesquisa.

3.1.2 Ferramenta: Modelo de Controle de Acesso Baseado em Atributos

A configuração do ambiente demandou a definição de políticas de acesso por meio da ferramenta empregada nos testes. A arquitetura desta solução engloba a Gerenciamento de identidade e acesso dos usuários (*Identity and Access Management* – IAM), com regras de acesso a recursos e a descrição correspondente ao dispositivo do solicitante.

A lista de usuários proporciona relatórios em tempo real sobre o acesso, detalhando os serviços e sessões mais recentes. O código organiza os usuários e políticas de maneira estruturada. A estrutura do usuário inclui campos como ID, tipo, provedor, nome de usuário, *token*, configurações e senha, sendo esta última gerada através da função *Bcrypt* que é uma implementação do seguinte trabalho (Provos e Mazieres 1999). Em relação

Algoritmo 3 - Estrutura da Classe 'User' - Fonte: (Pritunl Zero 2023)

```
1: Type Policy {
2:    Id primitive.ObjectID
3:    Name string
4:    Disabled bool
5:    Services []primitive.ObjectID
6:    Authorities []primitive.ObjectID
7:    Roles []string
8:    Rules map[string]*Rule
9:    AdminSecondary primitive.ObjectID
10:   UserSecondary primitive.ObjectID
11:   ProxySecondary primitive.ObjectID
12:   AuthoritySecondary primitive.ObjectID
13:   AdminDeviceSecondary bool
14:   UserDeviceSecondary bool
15:   ProxyDeviceSecondary bool
16:   AuthorityDeviceSecondary bool
17:   AuthorityRequireSmartCard bool
18: }
```

Algoritmo 4 - Função `ValidateUser` em `Check` - Adaptado Fonte: (Pritunl Zero 2023)

```
1: function ValidateUser(db: database.Database, usr: user.User, r: http.Request):
   (errData: errortypes.ErrorData, err: error)
2:    for each rule in p.Rules do
3:       if rule.Type is OperatingSystem then
4:                                          ▷ Lógica para o tipo Sistema Operacional
5:          ...
6:       else if rule.Type is Browser then
7:                                                  ▷ Lógica para o tipo Navegador
8:          ...
9:       else if rule.Type is Location then
10:                                                 ▷ Lógica para o tipo Localização
11:         ...
12:         ...
13:      end if
14:   end for
15:   ...
16: end function
```

à estrutura da política, esta abrange elementos como ID, nome, estado de desativação, serviços, autoridades, funções e regras, conforme ilustrado no Algoritmo 3.

Na ferramenta utilizada, a classe "*check*" contém a função *ValidateUser*, incumbida de validar a conformidade do usuário com as regras da política (Pritunl Zero 2023). Essa função percorre as regras, aplicando lógicas específicas para diferentes parâmetros, tais como sistema operacional, navegador, localização e redes permitidas ou proibidas.

Esses elementos fornecem um arcabouço para o gerenciamento de usuários e a aplicação de políticas de segurança, apoiando-se nos pilares propostos pelo ZT, como ilustrado no Algoritmo 4. A estratégia para a validação do usuário utiliza respostas que determinam a confiança na requisição, considerando critérios como hardware, software e geolocalização. A validação contínua, especialmente em ambientes industriais, requer um algoritmo com visão holística dos elementos físicos e virtuais do cliente, capaz de operar em sistemas críticos.

Diante da necessidade de validar tanto o dispositivo quanto o agente que ativa a funcionalidade para o PLC, este estudo abordou a seleção de uma solução de código aberto como componente essencial na estrutura ZT. Esse componente desempenha um papel crucial na gestão de identidade e na realização de auditorias, sendo decisivo para assegurar a integridade e a segurança do sistema. Outros elementos compõem a estrutura ZT, não sendo ela a única promotora da abordagem. Entre eles, destaca-se a solução PFSense para criação da microssegmentação e aplicação de regras de firewall compatíveis com a solução. Além disso, foi utilizada a ferramenta de auditoria em cada instância, com agentes pré-configurados que forneciam dados em tempo real, como utilização da CPU e taxa de transferência, para apresentar outros elementos explicativos durante as observações. Por fim, mas não menos importante, foi utilizada uma solução para verificar a maturidade do ZT, com o uso da ferramenta *InfectMonkey* (Akamai 2023).

3.2 Implementação do Protocolo Modbus TCP/IP

A fim de investigar possíveis cenários de desempenho durante a utilização de protocolos em aplicações ICS, optou-se por analisar a geração de tráfego de rede por meio das rotinas oferecidas pelo protocolo Modbus TCP.

Dentre as diversas rotinas presentes no protocolo Modbus, foi selecionada a operação de leitura e escrita, *write single coin*. Essa rotina possibilita, respectivamente, a função de escrever uma única saída "On" ou "Off" em um dispositivo remoto sendo especificado o endereço da bobina a ser forçada (Modbus 2004).

As atividades escolhidas seguem o fluxo padrão do protocolo Modbus, e o resultado do envio da instrução é um eco da consulta, conforme ilustrado na Figura 5.

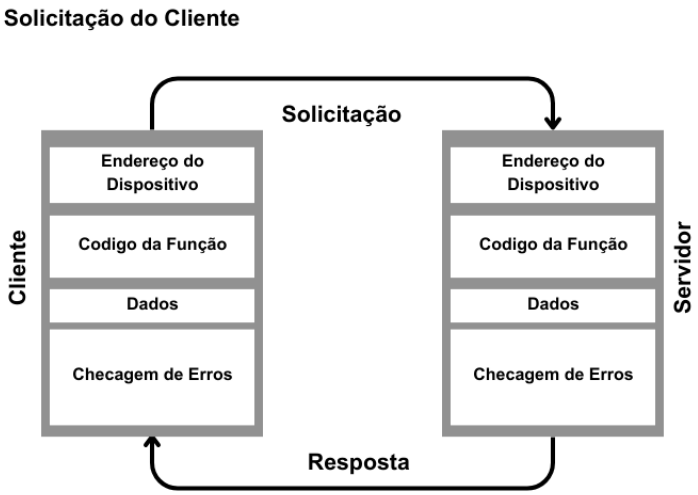

Figura 5: Quadro de mensagens do Modbus.
Fonte: (Modbus 2004).

A solução adotada para a apresentação da HMI incluiu diversas funcionalidades destinadas ao operador. Cada uma dessas funcionalidades permitia a utilização dos códigos funcionais documentados pelo protocolo Modbus, os quais possibilitam a execução de instruções remotas no PLC.

Essa abordagem viabilizou a representação contínua das operações de acionamento. Devido ao fato de que valores diferentes de *write single coil* em formato hexadecimal são considerados inválidos e não impactam na saída, visto que esse comando aceita apenas as ações de ligar e desligar, tornou-se viável gerar tráfego de forma contínua. Isso permitiu a observação dos dados transacionados entre o cliente e o servidor por meio de ferramentas de monitoramento de tráfego de rede, possibilitando a análise do comportamento das transações em resposta a diversos testes propostos para esse tráfego.

O código empregado implica em uma ação específica de alto impacto, requerendo privilégios elevados para sua execução. Nesse sentido, este componente é exemplar devido à sua relevância crítica e impacto significativo, podendo ser avaliado em variados contextos, tanto com a abordagem ZT quanto sem ela.

4 Resultados

4.1 Definição do Ambiente de Testes

O ambiente experimental consistiu em seis instâncias virtualizadas, todas configuradas de forma idêntica, incluindo o sistema operacional Debian 10, CPU de 1 GHz, espaço em disco de 10 GB e 1 GB de RAM. Duas máquinas foram alocadas para a primeira série de testes, sem a implementação da abordagem ZT, enquanto uma terceira foi reservada para manter histórico e realizar avaliações por meio do software Wireshark, conforme ilustrado na Figura 6.

A configuração da máquina utilizada para criar as instâncias virtualizadas possuía a seguinte configuração: Intel(R) Core(TM) i5-9300H CPU @ 2.40 GHz, com overclock de 4.1 GHz, 4 núcleos e 8 threads, 1 TB de disco, 8 GB de RAM e placa de vídeo NVIDIA GTX 1050.

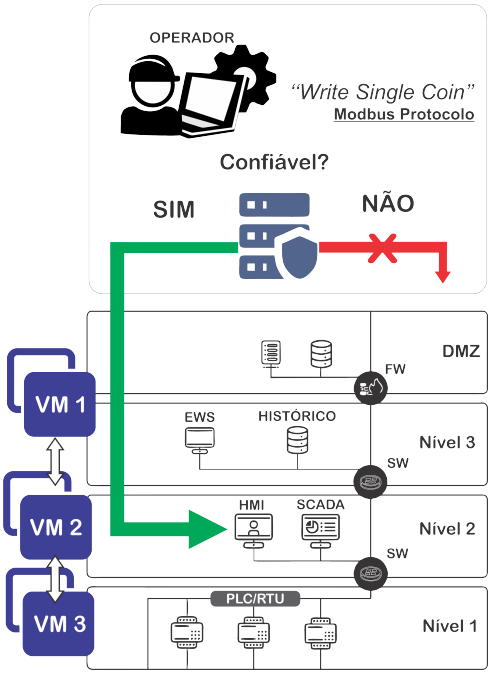

Figura 6: Estrutura e localização do mecanismo de política seguindo modelo PERA em redes industriais.

As requisições do protocolo foram conduzidas por interfaces que possibilitaram à máquina, desempenhando o papel de servidor, receber essas requisições. Serviços dispensáveis foram desativados em todas as instâncias virtuais, a fim de prevenir a influência de comportamentos anormais nas máquinas sobre os dados coletados.

Para facilitar a comunicação na topologia desejada, empregou-se a ferramenta Virtual Network Editor, disponível na solução VMWARE Workstation. Através dessa ferramenta, foi possível configurar a rede para cada dispositivo utilizado.

As validações da topologia escolhida seguiram inicialmente as orientações presentes nas diretrizes da terceira revisão do NIST 800–82 (Stouffer et al. 2022). Além disso, fundamentaram-se as escolhas em trabalhos anteriores. No cenário sem a implementação de Zero Trust, adotou-se a topologia ponto-a-ponto com o HMI ao lado do PLC, conectados por um módulo de comunicação, como ilustrado na Figura 7.

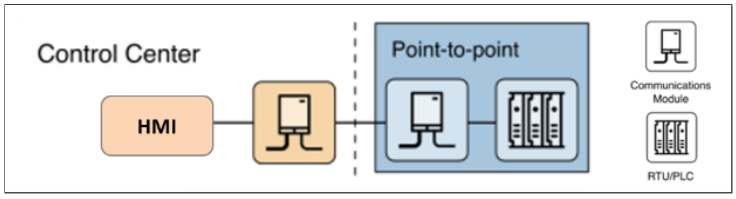

Figura 7: Topologia ponto a ponto.
Fonte: (Stouffer et al. 2022).

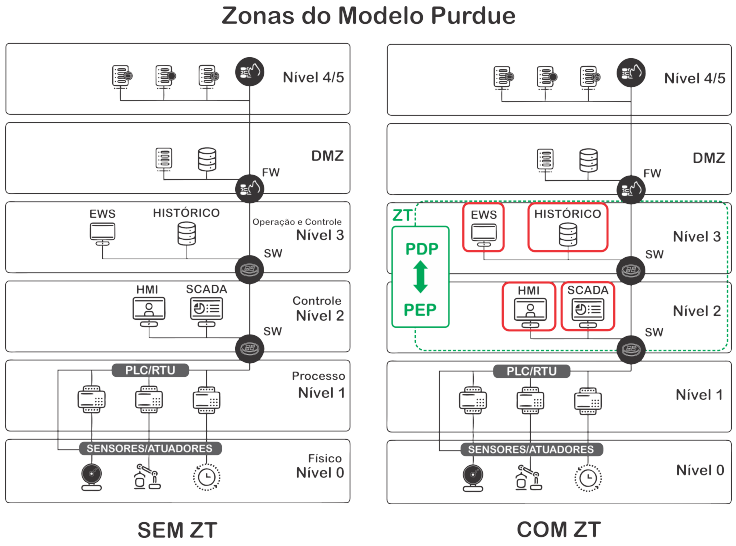

Figura 8: Estrutura e Localização do ZT no Modelo PERA

A escolha da topologia em estrela para a abordagem Zero Trust (ZT) também é contemplada em redes industriais. A designação de uma região específica e centralizada para a aplicação de políticas proporcionou uma aproximação do ambiente de simulação criado com a realidade industrial, alinhando-se à abordagem ZT. A interação entre o HMI/PLC, presente no nível de controle, e o PLC, no nível de processo, seguindo o modelo de referência Arquitetura de Referência Empresarial Purdue (*Purdue Enterprise Reference Architecture* – PERA), conforme mostrado na Figura 8, foi estrategicamente adotada.

A conformidade com a padronização apresentada pelo NIST em sua terceira revisão para topologias auxiliou na fundamentação e aproximação da realidade da indústria (Stouffer et al. 2022) na construção do ambiente pretendido para os testes.

A partir das instâncias criadas, duas máquinas foram designadas para a primeira série de testes, sem a implementação do modelo de segurança em questão. A intenção era

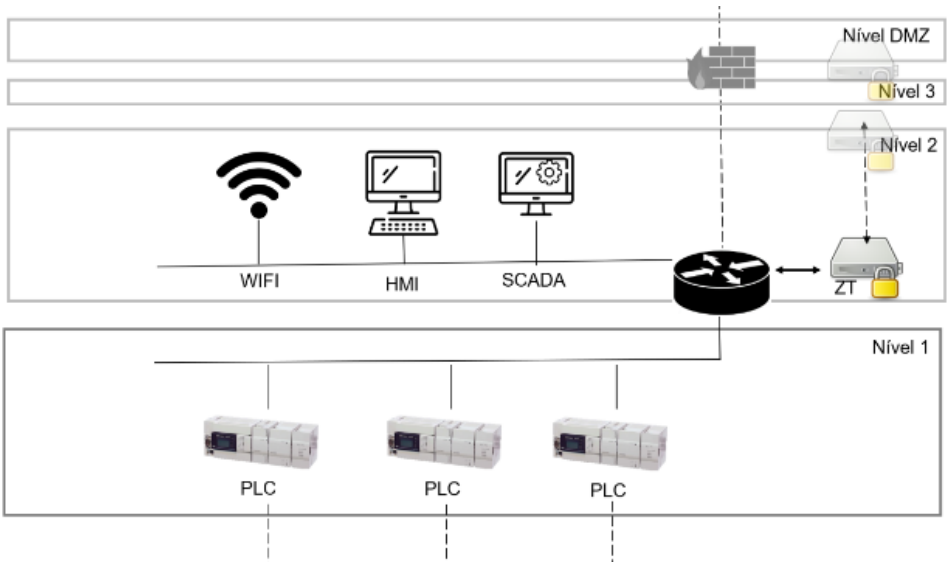

Figura 9: Posição de atuação do mecanismo de política.

coletar dados iniciais que serviriam como valores-base para comparação na segunda etapa dos testes, agora sob novas diretrizes.

A segunda bateria de testes foi conduzida com base na hipótese de que as ações resultantes das rotinas disponibilizadas pelo HMI/PLC seriam validadas pela abordagem ZTNA antes da efetiva execução das ordens no PLC. Essa comunicação ocorreu por meio da intermediação de uma terceira instância virtual responsável por receber as ações de comunicação entre os dispositivos, desempenhando o papel de central autenticadora de requisições, conforme detalhado na próxima seção. Essa instância validava as ações dos usuários junto ao HMI, garantindo a autenticidade no acionamento de recursos.

Os dados coletados ao longo da execução foram registrados pelo Wireshark, configurado com filtros específicos para identificar o protocolo Modbus/TCP. Ferramentas adicionais, como Collectl e bMon, foram empregadas para monitorar em tempo real as taxas de uso da CPU, memória e a taxa de utilização da rede, a fim de avaliar os momentos nos quais ocorria a comunicação entre o HMI e o PLC.

4.1.1 Escopo: Central de Acesso por Confiança Zero

O ponto central da tomada de decisões foi designado como “Central ZT”. Para garantir uma verificação contínua da identidade e avaliar as transações, foram implementadas ferramentas específicas para apoiar a implementação da abordagem ZT.

Como evidenciado na Figura 9, a Central foi estrategicamente posicionada no ambiente de teste para interagir continuamente na comunicação entre os níveis de operação e controle. Para viabilizar esse controle, adotou-se a estratégia de integrar várias soluções *opensource* para criar condutos lógicos seguros para o trajeto das transações.

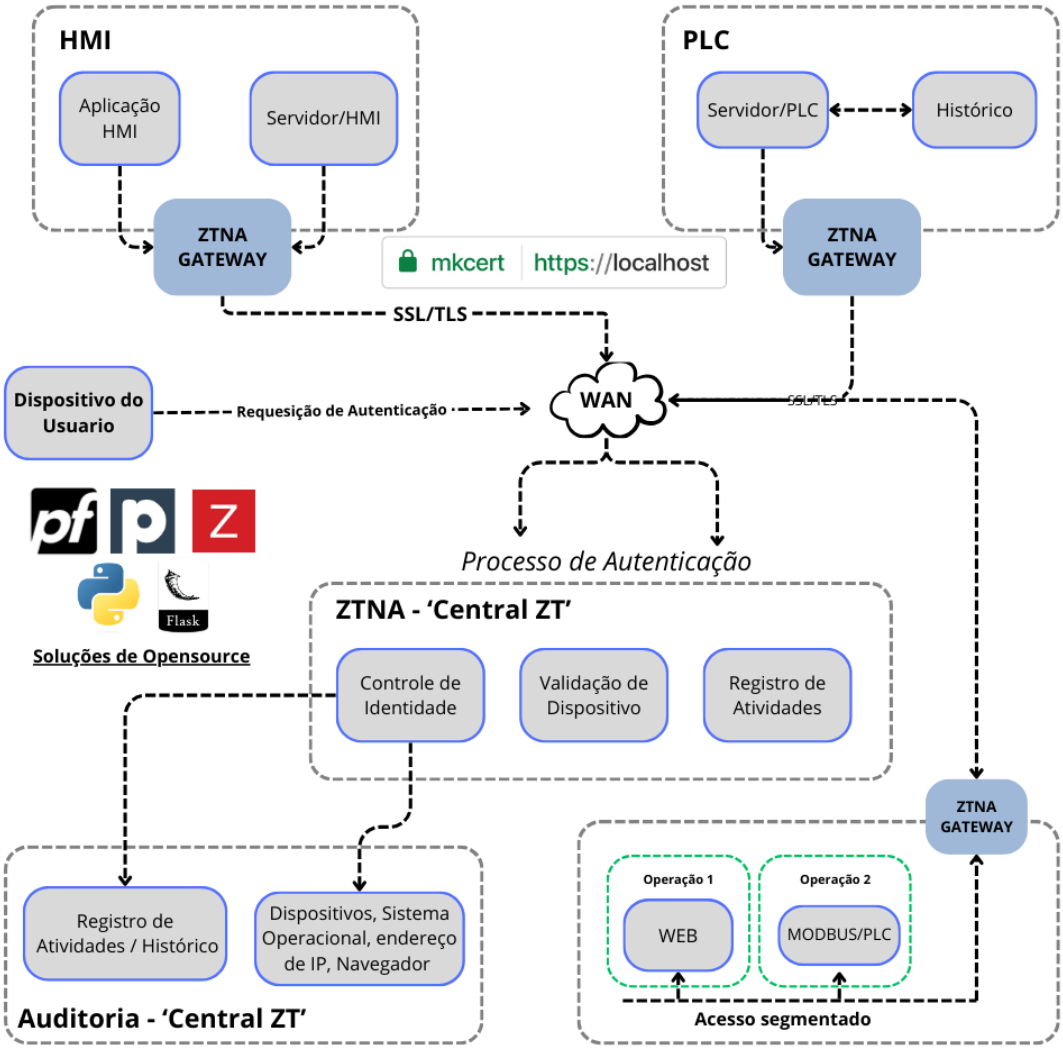

Figura 10: Direção do envio de dados para a Central ZT.

A configuração do PFSENSE contemplou a separação em vias da rede, onde cada faixa possuía um único gateway para a troca de dados. Dada a quantidade de elementos presentes no ambiente de teste, conforme ilustrado na Figura 10, foi implementado o bloqueio de portas, permitindo apenas aquelas consideradas essenciais para o pleno funcionamento, tais como 502 (PLC), 8080 (HMI), 443 (Pritunl-zero), 22 (Pritunl-zero). No entanto, o acesso às portas, como PLC e HMI, estava disponível apenas para usuários validados pelo IAM.

Durante os testes, as comunicações seguiram um procedimento estabelecido. O operador do sistema, denominado usuário, munido de um dispositivo informático específico, iniciava a interação ao acessar um endereço designado por meio do navegador para uma página simulando o HMI, apresentando atividades a serem acionadas. Para automatizar uma atividade rotineira, simulou-se um operador junto ao HMI, com instruções em *Javascript* diretamente no navegador, servindo como um acionamento recorrente por parte do usuário para manter uma constante interação entre o HMI e o PLC.

É relevante destacar que o endereço acionado pelo usuário direcionava-se a um proxy-reverso. Dada a origem das ações provenientes de máquinas externas às faixas de redes destinadas ao HMI, era necessário redirecioná-las para uma página gerada pela ferramenta IAM. Nesse contexto, solicitava-se que o usuário inserisse suas credenciais. Após a confirmação, o usuário era redirecionado para a solução web prevista no plano de controle, que disponibilizava rotinas específicas ao utilizar o protocolo Modbus/TCP. O operador, então, acionava as atividades específicas, a serem enviadas para o PLC, que respondia à requisição e confirmava a ação para o HMI.

4.1.2 Composição da solução de Confiança Zero

Nos testes em ambiente controlado, foram estabelecidos pontos específicos para acompanhar as estratégias da abordagem ZT, conforme proposto pela pesquisa. Internamente, foram definidas especificações durante os testes sobre o uso de um determinado recurso disponível na rede:

- Orientação do usuário para uma atividade específica.
- Identificação abrangente do recurso de forma nominal: "Modbus/TCP" – uso do serviço presente em um determinado endereço IP, neste caso, a localização do HMI.
- Definição de atributos estáticos para usuários com atributos: versão do sistema operacional, versão do navegador, faixa de endereçamento de IP.
- Verificação do usuário, padronizada pela ferramenta: através do uso das credenciais no momento da autenticação e a cada instante que houver requisição ou a cada intervalo de 30 segundos.

Durante os testes iniciais, observou-se a geração de um histórico de acesso para cada usuário, incluindo detalhes do dispositivo utilizado. Para confirmar a validação contínua do usuário, foram realizados testes nos quais o gestor altera as opções do usuário em tempo real, resultando na compreensão imediata pelo algoritmo das novas regras e na impossibilidade de uso de determinado recurso.

Com a validação da ferramenta para o fim proposto, foi criado um roteiro para definir as atividades durante os testes, como atribuir ao usuário o recurso Modbus/TCP para utilizar o serviço HMI/MTU, exigindo acesso via Firefox em um sistema Linux.

As etapas para definir políticas da ferramenta específica seguem um fluxo interno:

1. Início das configurações e instalação do certificado de segurança pelo administrador.
2. Criação do acesso ao serviço ou recurso, indicando o papel necessário.

3. Definição dos recursos autorizados para o usuário.

4. Direcionamento do recurso com indicação do endereço IP e das portas de acesso.

5. Atribuição de critérios para definir a estratégia, incluindo detalhamento de hardware e software a ser questionado durante os desafios de segurança oferecidos pela ferramenta.

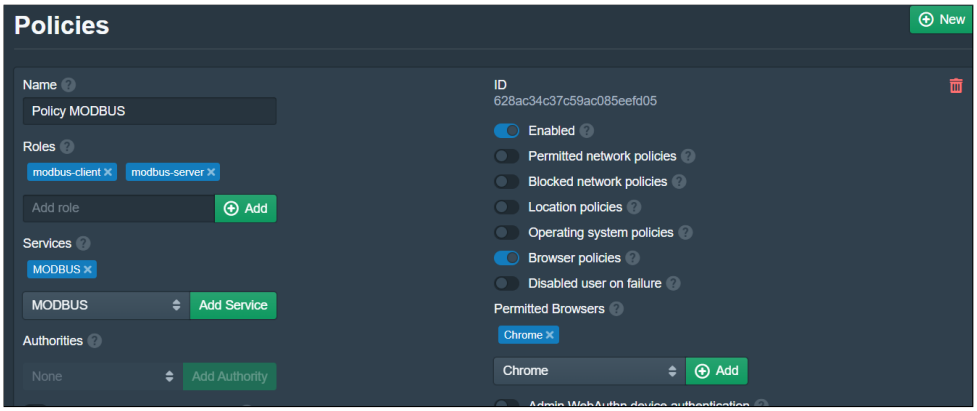

Figura 11: Tela de Politicas da ferramenta utilizada nesta pesquisa.
Fonte: Adaptado de (Pritunl Zero 2023).

4.1.3 Topologias e Métricas de Redes

A topologia em ambientes de rede aplicados a negócios permite a implementação de diversas abordagens, como árvore, estrela e malha completa. No contexto industrial, as redes ICS possibilitam a utilização simultânea de múltiplas topologias, adaptando-se às necessidades específicas. A presença de conectividade na indústria exige medidas para assegurar a integridade dos dados, incluindo práticas como filtragem e identificação de pontos de acesso.

Dentre as topologias existentes na literatura, a estrela destaca-se em ambientes ICS e para o presente estudo foi utilizado uma versão hibrida, conforme ilustrado na Figura 12, favorecendo a criação de redes centralizadas para aplicação do contexto da Central ZT. Os efeitos das topologias ultrapassam os protocolos, considerando custos, distribuição geográfica e compartilhamento de variáveis para uma gestão eficiente, impactando na construção de zonas seguras para um controle preciso do fluxo de informações.

Na aplicação desta estratégia em um ambiente de simulação para o contexto industrial, optou-se pela configuração estrela na transmissão de tráfego Modbus/TCP. Esta escolha implicou na segmentação da rede e na implementação de um firewall com a ferramenta de validação de credenciais para usuários requisitantes de recursos, representando, assim, a topologia do ambiente de simulação.

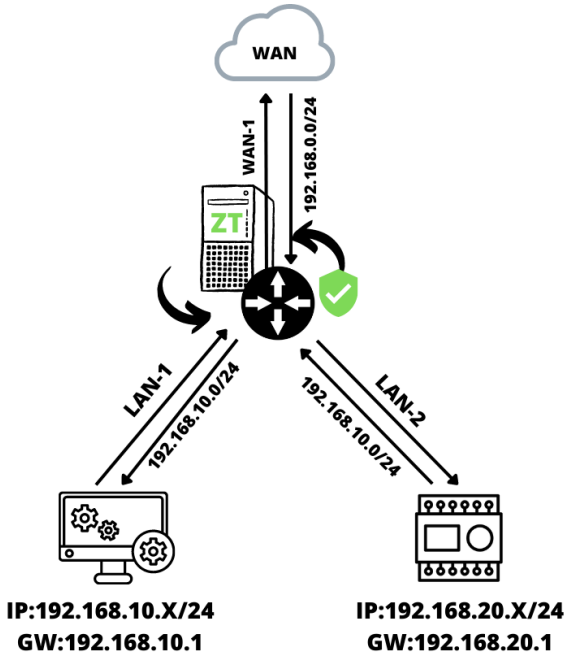

Figura 12: Visualização da topologia do ambiente de teste (ZT).

Após apresentar a topologia alvo para o ambiente de teste, concentrou-se a atenção nas métricas de redes que oferecem informações sobre o funcionamento da rede industrial. Ambientes industriais são permeados por grandezas como confiabilidade, disponibilidade e manutenibilidade, todas voltadas para garantir uma operação fluida nos parques fabris. Esses aspectos validam a busca pela avaliação de desempenho dessas redes industriais, conforme será detalhado na próxima seção.

A escolha da topologia da rede pode implicar no desempenho, sendo crucial para a criação de redes que simulem um contexto abrangente da indústria. A atividade escolhida e a quantidade de elementos nos testes estabelecem uma base onde as interações são sensíveis a mudanças de valores em diferentes cenários.

As métricas de rede selecionadas, como atraso, variação do atraso, vazão, tempo de ida e volta e tempo para serviço (TTS), possibilitam a apresentação de indicadores-chave de desempenho dessas redes. Isso permite que os dados visualizados por meio desses indicadores sejam questionados de forma consistente em diversos cenários.

4.2 Análise dos Resultados de Desempenho

O estágio inicial da pesquisa foi selecionado como ponto de partida para a criação de cenários experimentais, com o objetivo de investigar a interação entre HMI e PLC. Nesse contexto, definiu-se que a requisição a ser utilizada seria o comando "*Write Single Coil*". Esse procedimento foi conduzido ao longo de um período específico, com intervalos determinados entre cada requisição. Os resultados apresentados nos cenários subsequentes

refletem os testes iniciais realizados durante um breve período de dez minutos, o que permitiu a coleta de mais dados, uma vez que as instruções eram automatizadas e exigiam menos recursos computacionais devido ao tempo limitado previamente, durante o qual as instruções foram ativadas, conforme visualizado na Figura 13:

1. Cenário - Requisição do protocolo Modbus/TCP sem abordagem ZT (Rotinas e Ataques)
   Os resultados revelaram que o tempo de resposta variou entre 0,6 e 1,4 milissegundos, com uma instrução sendo acionada em um loop a cada cinco segundos. Através das ferramentas de monitoramento dos dispositivos, como Collectl, bMon e Zabbix, observou-se que a taxa de uso da CPU ficou abaixo de 6%, e o consumo de memória RAM abaixo de 0,9 GB.

2. Cenário - Requisição de protocolo com abordagem de ZT (Rotinas e Ataques)
   No segundo cenário, observou-se que o tempo de resposta variou entre 0,7 e 1,4 ms. Comparativamente ao primeiro cenário, cada requisição de comunicação entre as máquinas apresentou um aumento no tempo de execução de cada instrução. O uso da CPU ficou abaixo de 5%. No entanto, durante os testes, foram identificados picos de consumo máximo da capacidade do processador em momentos em que a pesquisa aplicava testes de stress, os quais foram realizados para simular cenários de ataque. Além disso, o consumo de memória RAM atingiu sua capacidade total em determinados momentos da pesquisa.

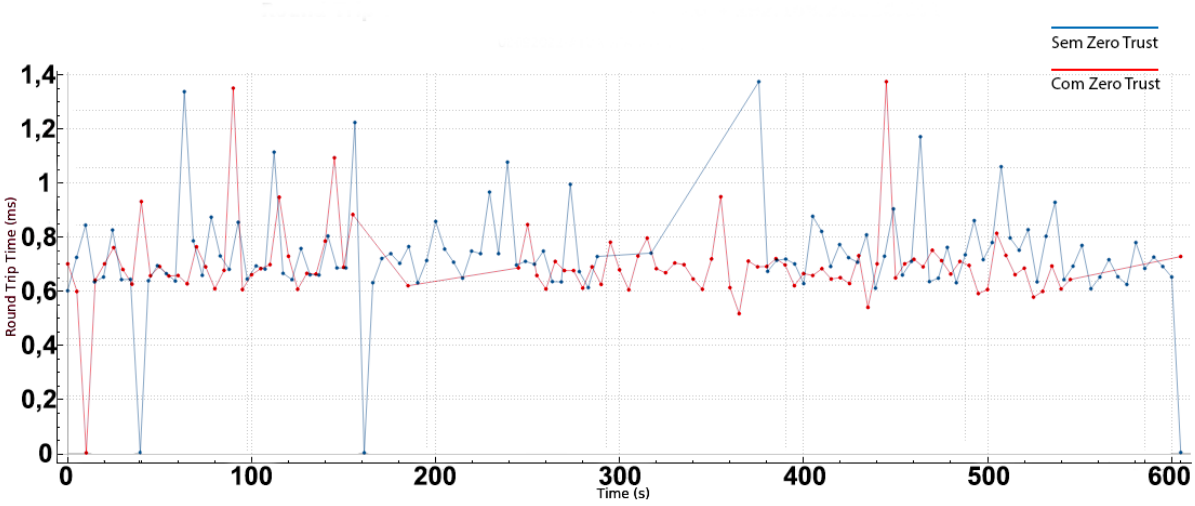

Figura 13: Round Trip Time para os cenários com e sem ZT.

A escolha de investigar o Tempo de Ida e Volta (*Round Trip Time* – RTT) no estudo decorre de sua importância como métrica em comunicações. Esse parâmetro é particularmente relevante na observação de protocolos industriais como o MODBUS/TCP,

onde a comunicação entre dispositivos é crítica. O RTT possibilita ações para avaliar o desempenho do sistema, garantir a qualidade das comunicações, diagnosticar problemas de rede ou de dispositivos e, por fim, otimizar o serviço, seja por meio de ajustes de parâmetros ou da atualização de equipamentos, conforme necessário.

Simulações numéricas sugeriram a ocorrência de picos no tempo de resposta das requisições em cenários nos quais o conceito ZT foi implantado, em comparação com cenários sem essa abordagem. Foi possível verificar o aumento do intervalo de tempo para cada instrução no cenário em que ZT foi implementada, indicando possíveis irregularidades sistêmicas nos dispositivos destinados à gestão da identidade dos usuários para acesso ao HMI. Esses picos na latência e o aumento no tempo de resposta das transações podem gerar interferências, especialmente quando somados a outros protocolos e ações que permeiam aplicações robustas, como SCADA.

A pesquisa propôs a realização de testes ao longo de um período mais extenso para avaliar a consistência dos resultados iniciais em diferentes momentos. Apesar de a avaliação inicial ter identificado aumentos significativos, os testes subsequentes não reproduziram essas variações, sugerindo que os resultados iniciais podem ter sido influenciados pela configuração inicial do ambiente, a qual serviu para reformular o ambiente.

No que concerne aos fatores vinculados à comunicação cliente-servidor, a avaliação direcionou-se à comparação entre métricas de rede, tais como atraso, variação do atraso e tráfego de rede. Estes resultados corroboram as descobertas de (Thrybom e Prytz 2009), que identificou, em sua pesquisa realizada em 2009, a necessidade de observar redes industriais a longo prazo, aproximando-se da Tecnologia da Informação e, com isso, gerando ambientes de protocolo misto. Nesse contexto, torna-se necessário o emprego adequado de métricas presentes em Qualidade de Serviço (*Quality of Service* - QoS) para manter sob monitoramento requisitos exigentes como latência, jitter e perda de pacotes nos protocolos Ethernet Industrial.

Com o objetivo de alcançar um bom desempenho e uma comunicação eficiente, observamos, no entanto, que, diferentemente do estudo apresentado, a eficiência da comunicação está diretamente relacionada ao grau de personalização da estrutura original do ambiente industrial. Essas discrepâncias podem ser explicadas pelo fato de que, para atender às exigências da indústria contemporânea em relação à segurança da informação, as métricas de rede surgem como guias para mudanças estruturais físicas e lógicas, a fim de cumprir os objetivos previstos no campo das telecomunicações em QoS.

O atraso, por exemplo, é uma métrica crucial que indica o tempo decorrido desde o envio de um pacote até sua chegada ao destino. A escolha dessas métricas durante os testes se deu pela relevância ao avaliar o desempenho, sem se limitar apenas a essas.

Para as novas baterias de testes, além de tempos superiores aos primeiros testes du-

rante as avaliações, foram propostas estratégias que, novamente, envolveram dois cenários distintos, mas com um número superior de requisições. No segundo momento, já com a configuração dentro das especificações da central ZT, ambos os cenários foram acionados pela mesma quantidade de tempo previsto de 100 min, com intervalos pré-definidos de 1000 ms entre cada requisição.

Em redes industriais, onde a disponibilidade e a confiabilidade são fatores críticos, as médias de atraso foram avaliadas em cinco séries de testes. Conforme ilustrado na Figura 14, constatou-se que a média de atraso sem a utilização do modelo ZT é levemente inferior em comparação com a abordagem ZT. Observa-se uma diferença da ordem de 0,5 ms, a qual não representa um impacto negativo para a operação da rede industrial (Seno, Tramarin e Vitturi 2012). É possível inferir que a implementação do modelo ZT na rede pode introduzir uma leve sobrecarga e ocasionar um discreto aumento na latência.

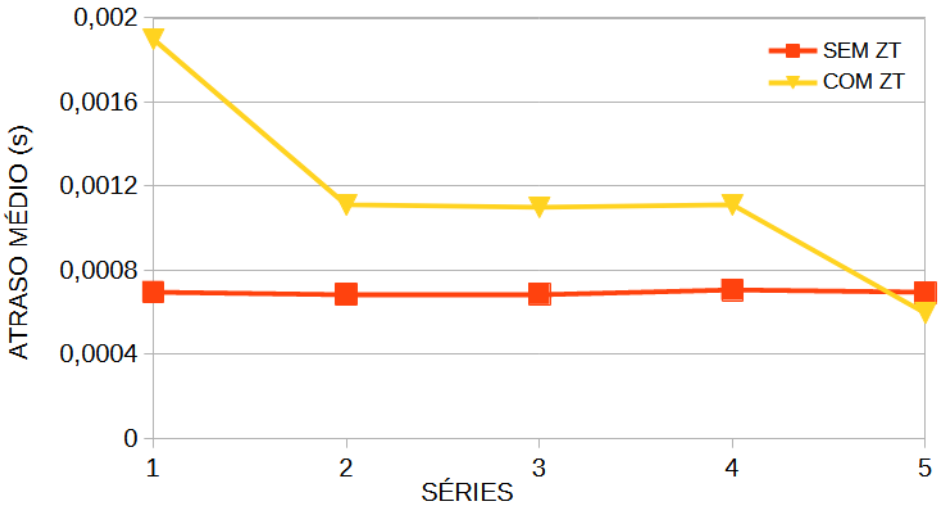

Figura 14: Média do Atraso durante os testes.

A Figura 15 apresenta a média de jitter em diversas séries de dados, um parâmetro crucial para avaliar o desempenho de redes de computadores e comunicação, uma vez que o jitter se refere à variação do atraso na transmissão de dados. A figura exibe os valores para cinco séries distintas, comparando os valores obtidos com e sem a implementação da estratégia ZT. Observou-se que, em geral, os valores de jitter apresentados nas séries de dados são baixos em ambas as situações, de maneira similar aos resultados do atraso.

Os resultados sugerem que a implementação do modelo de segurança ZT apresentou leve impacto no atraso médio no sistema. No entanto, ao observar a Figura 16, não foi possível concluir de forma significativa as diferenças entre as abordagens sem e com ZT em termos de taxa de transferência, devido às pequenas diferenças encontradas, todas na ordem de 156 B/s. Na série 4, observa-se uma diferença maior, mas vale destacar que em termos de escala, a diferença em relação à série anterior é 0,013 B/s. Portanto, os

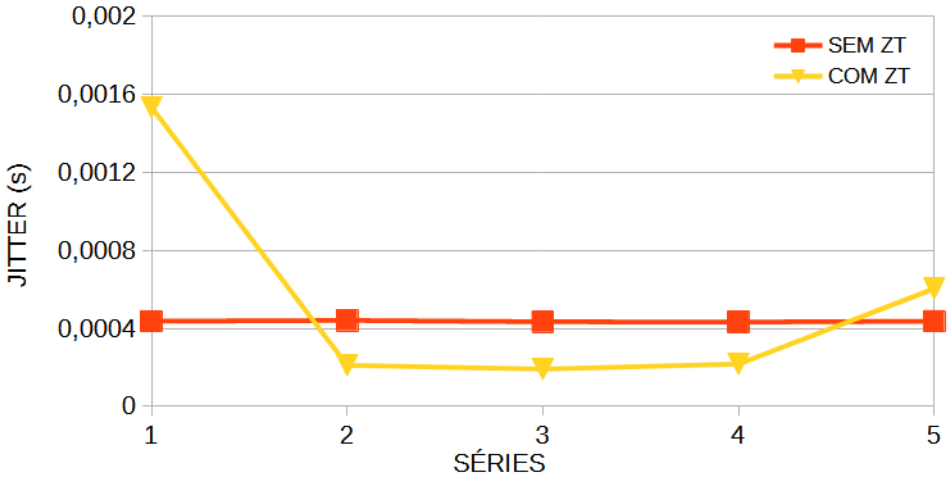

Figura 15: Média da variação do Atraso durante os testes.

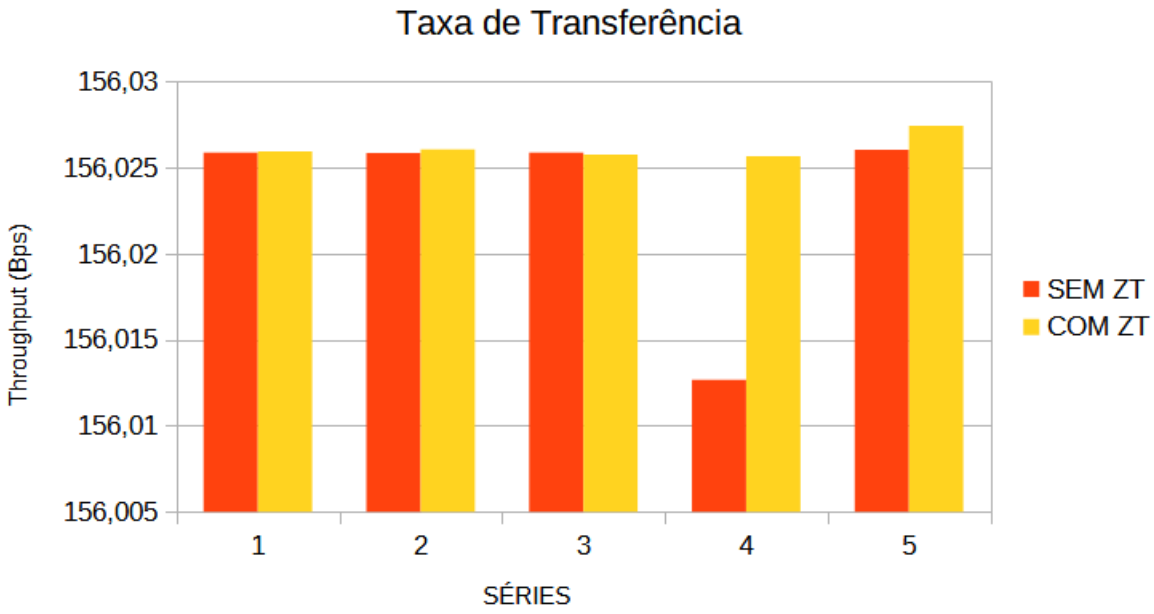

Figura 16: Vazão na rede.

resultados apontam que a implantação do modelo de segurança ZT em ambiente industrial pode ser viável.

4.3 Análise dos Resultados de Segurança

O estudo gerou tráfego legítimo Modbus/TCP na rede, utilizando o protocolo mencionado (Modbus/TCP) (Modbus 2004), confirmado por meio da análise realizada com a ferramenta de monitoramento de rede, Wireshark. Durante os testes, a comunicação foi devidamente acompanhada e avaliada.

Testes foram realizados em vários cenários para comparar a eficácia do ZT em ambientes com e sem ataques, empregando ferramentas como nmap, ettercap e etterfilter. Os resultados demonstraram que o ZT proporcionou estabilidade e consistência na transferência de dados, exibindo uma menor variação no jitter, mesmo diante de ataques.

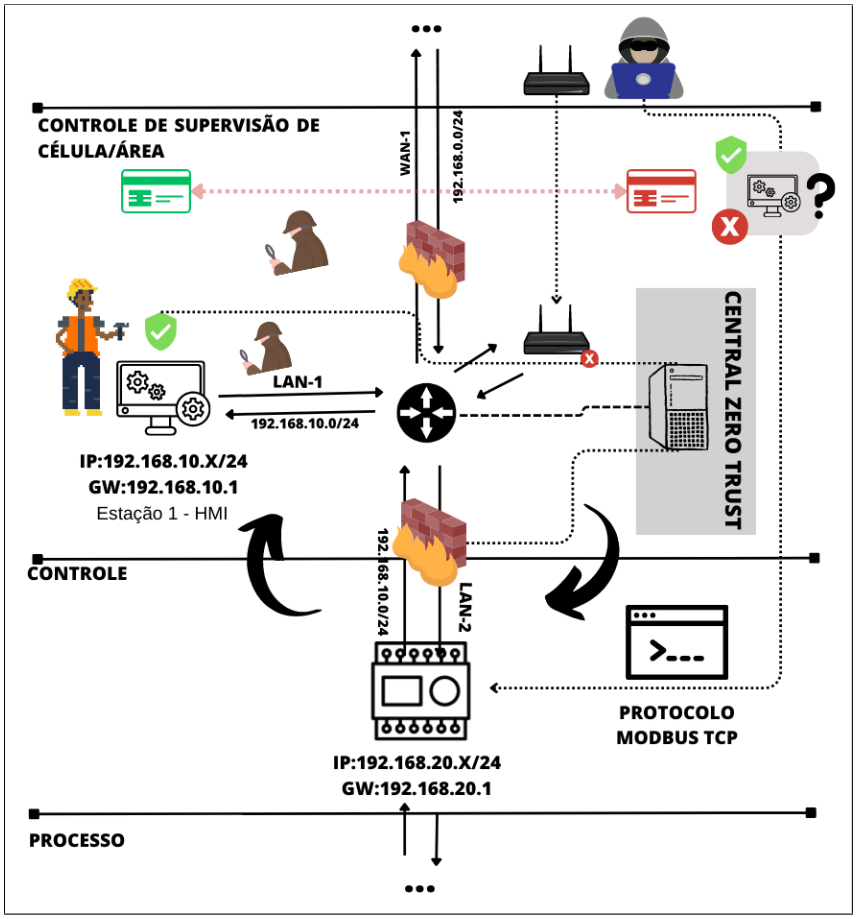

Figura 17: Simulação de Rede industrial com ataque em curso e abordagem ZT.

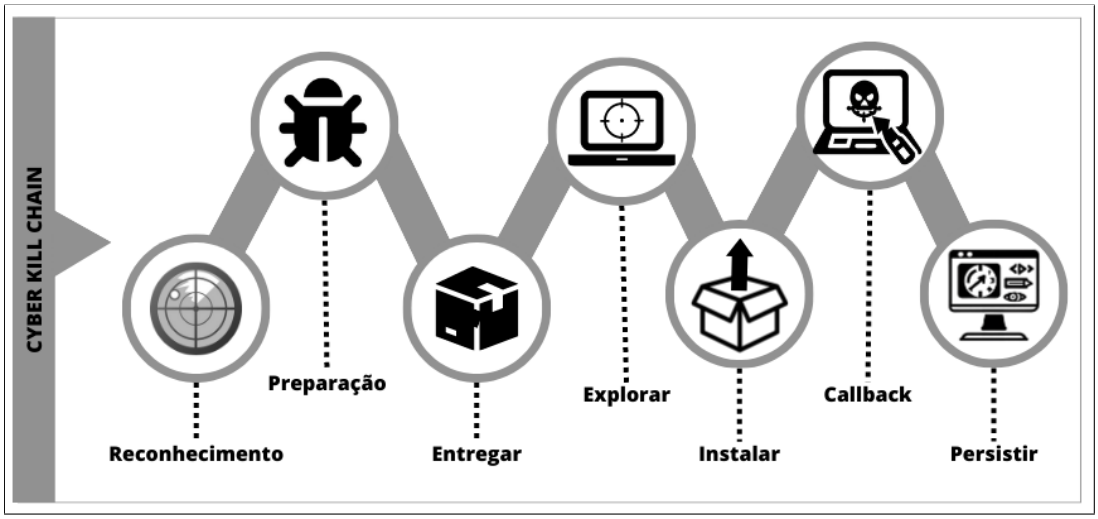

Figura 18: Etapas presente no framework Cyber Kill Chain®.

As ações dos ataques nos cenários propostos abrangeram desde Negação de Serviço (DoS - *Denial of Service*) até a injeção de instruções por meio da técnica de homem-do-meio 17. A escolha por essas formas de ataques parte do princípio abordado no estudo de Jayalaxmi et al. (Jayalaxmi et al. 2021) que apresentou diversos tipos de ataques nos quais a indústria é alvo, enquanto o estudo de Rahman et al. (Rahman et al. 2022) demonstrou a necessidade de implementar políticas de segurança para proteger as rotinas contra ações maliciosas. A pesquisa também identifica protocolos de comunicação em redes industriais, como o Modbus TCP, como suscetíveis a certos tipos de ataques.

O tráfego gerado sobre o protocolo Modbus/ TCP foi utilizado para aplicar o framework Cyber Kill Chain®, conforme ilustrado na Figura 18. Este framework abrange etapas como Reconhecimento, Preparação, Entrega, Exploração, Instalação, Callback e Persistência (Martin 2014).

A aplicação dos teste com uso de ataques específicos partiu da hipótese de que o atacante já havia adquirido acesso à rede industrial e estava monitorando-a por meio da exploração de vulnerabilidades em dispositivos sem fio, o que possibilitou direcionar para as etapas de retorno da chamada e persistência.

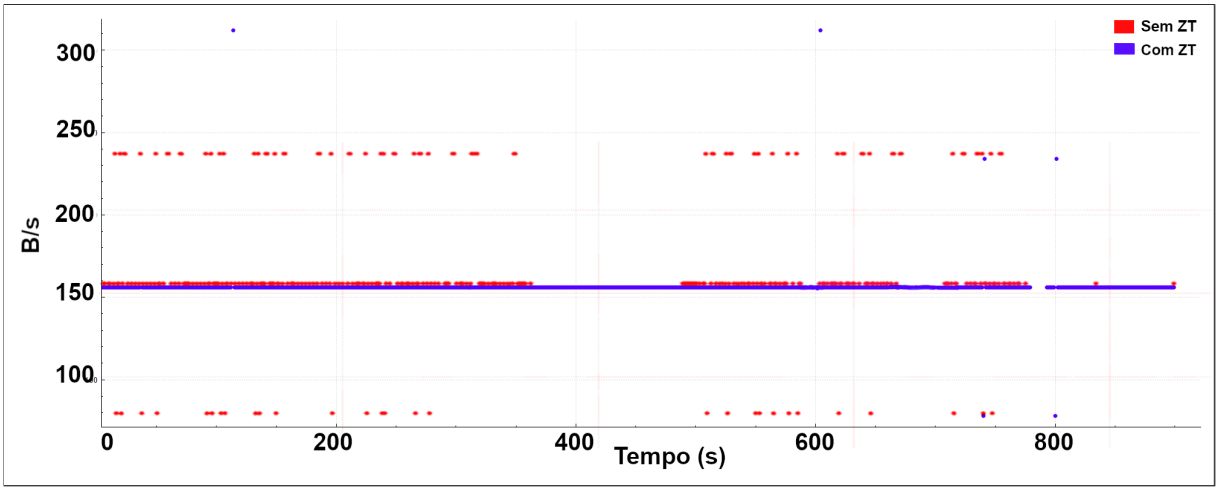

Figura 19: Tráfego sem ataque durante os testes com e sem Zero Trust.

Conforme ilustrado na Figura 19, verificou-se que a taxa de transferência com a utilização do modelo ZT é semelhante à abordagem sem ele. Durante os testes sem a presença de ataques e sem a aplicação do modelo ZT, foram observados picos na taxa de transferência, possivelmente atribuíveis a outros fatores, como a ação da inicialização a frio do sistema durante o teste.

Foi proposta uma nova abordagem de teste para investigar a possibilidade de o estado anterior ter sido afetado por uma inicialização fria. Foram realizados novos testes de rotina, conforme ilustrado na Figura 20. Observa-se que o sistema já estava em funcionamento, demonstrando estabilidade na troca de dados. Em ambos os testes, contudo,

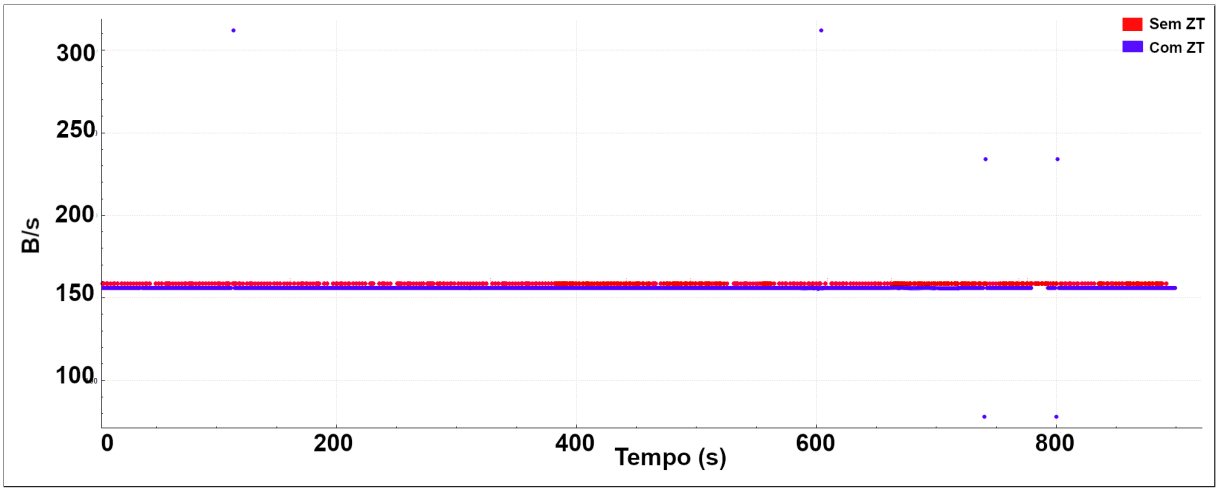

Figura 20: Nova geração de tráfego sem ataque durante os testes com e sem Zero Trust.

a configuração sem ZT apresentou um leve aumento em comparação com a configuração com ZT.

Importa ressaltar que a disparidade entre os dois cenários não implica em um impacto negativo substancial na operação da rede industrial, dado que os testes foram conduzidos em um ambiente simulado. É pertinente levar em conta os aspectos práticos e ambientais ao avaliar o desempenho de sistemas de comunicação industrial, conforme apontado em um estudo prévio (Seno, Tramarin e Vitturi 2012). Ao observar a comparação entre os dois cenários, nota-se uma taxa de aproximadamente 150 B/s.

Executaram-se rotinas de "Write Single Coil" a cada intervalo de 1 s, sendo que cada cenário teve a duração de 15 min, com intervalos de 1 s entre as requisições para o PLC. Os resultados foram obtidos por meio da ferramenta Wireshark.

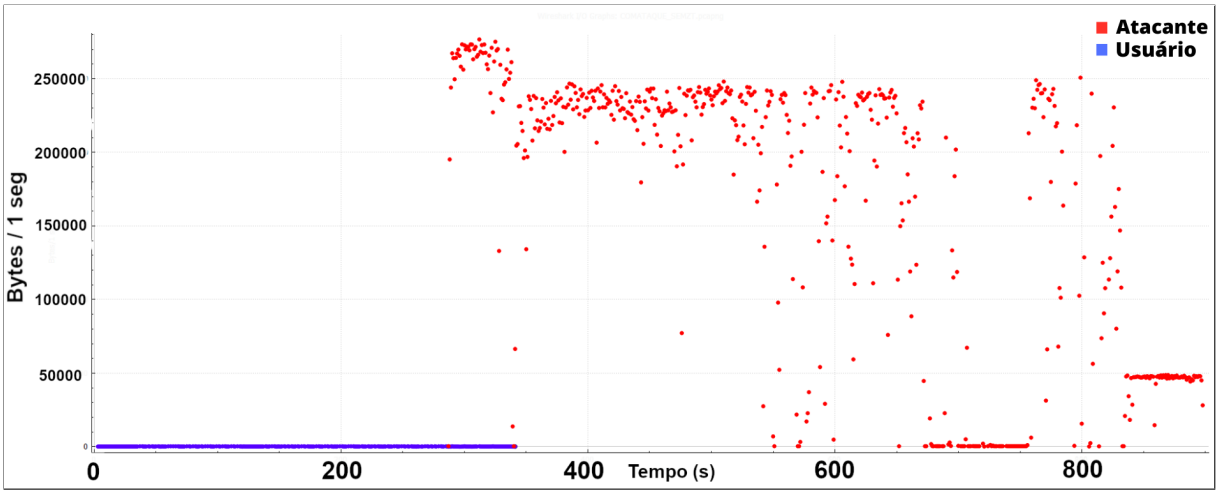

Figura 21: Tráfego Sob Ataque: Denial-of-Service (DoS) de Origem, Iniciado Após Cinco Minutos em Ambiente Desprovido de Zero Trust.

Em relação ao ataque de negação de serviço, sem a utilização do ZT, o HMI tornou-

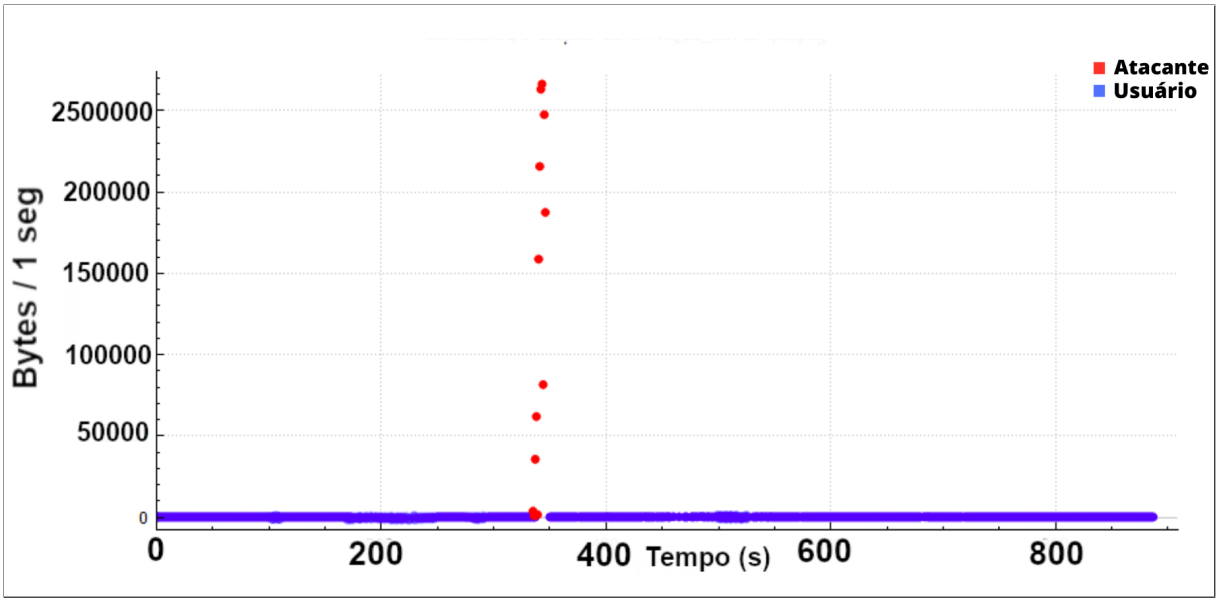

Figura 22: Tráfego Sob Ataque: Denial-of-Service (DoS) de Origem, Iniciado Após Cinco Minutos em Ambiente com Zero Trust.

se indisponível, como ilustrado na Figura 21. No entanto, ao empregar o ZT, o ataque foi detectado e bloqueado após 11 segundos, reduzindo significativamente a indisponibilidade da comunicação cliente-servidor, conforme mostrado na Figura 22.

O outro ataque proposto, que envolveu a técnica combinada de envenenamento da tabela ARP em conjunto com o Ataque do Homem no Meio (*Man-In-The-Middle* – MITM), foi conduzido por meio da manipulação de pacotes enviados ao PLC, com o objetivo de alterar seu estado de ligado para desligado. O cenário do teste foi configurado para que o operador, através do IHM, enviasse uma instrução para manter a bobina no estado ligado, cujo valor hexadecimal correspondente era "FF00". Durante o teste, o atacante interceptava a instrução, que era filtrada com o uso do ettercap, e alterava o valor da bobina para desligado, representado em hexadecimal como "0000". O ataque proposto permitiu compreender o funcionamento da atividade manipulação do estado do PLC, bem como avaliar diferentes cenários, tanto com a utilização da abordagem ZT quanto sem ela, conforme investigado nesta pesquisa.

No entanto, a presença da estrutura de confiança do ZT impediu a execução das ações, pois o atacante não possuía especificações compatíveis com as autorizações necessárias. A arquitetura adotada foi eficaz na detecção e prevenção dessas alterações maliciosas, preservando a integridade dos dados por meio de uma avaliação criteriosa. A existência de características distintas nos dispositivos previamente cadastrados na central ZT obstruiu as ações do atacante, impossibilitando que atendesse aos requisitos para ser considerado seguro.

Foram conduzidos testes em diversos cenários para comparar a eficácia do modelo

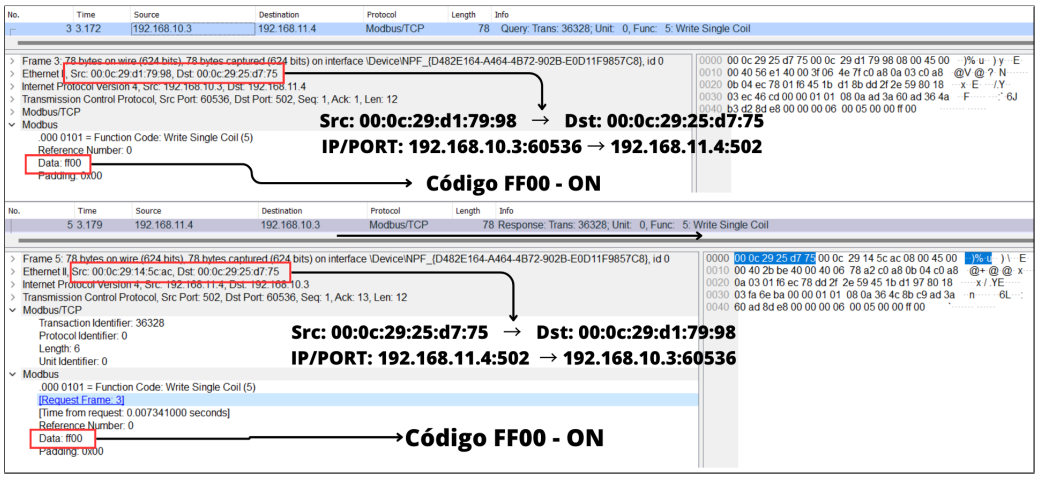

Figura 23: Tráfego legitimo de envio do comando "ON" via protocolo Modbus/TCP semelhante em ambos ambientes.

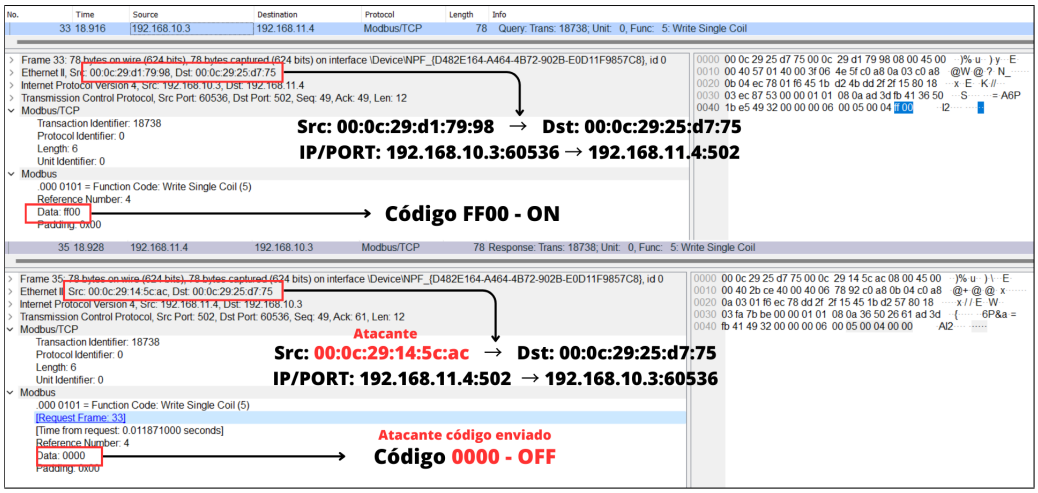

Figura 24: Tráfego não-legitimo com injeção de comando "ON" para "OFF" por meio do MITM sem ZT.

ZT em situações com e sem ataques, incluindo ataques de negação de serviço, manipulação de pacotes usando MITM com envenenamento da tabela ARP e injeção de comandos em registradores específicos disponíveis no PLC. Para realizar esses ataques, foram utilizadas as seguintes ferramentas: nmap, para descoberta de serviços, enumeração de portas e mapeamento da rede; ettercap, para execução de ataques de homem-do-meio com criação de filtros específicos, e etterfilter, para manipulação de pacotes.

Outro ponto observado diz respeito aos ataques de negação de serviço sem o uso de ZT, nos quais não é necessário que o atacante esteja na mesma rede do PLC para resultar na indisponibilidade do mesmo, caso o foco seja o dispositivo do operador do IHM. Destaca-se que o atacante é capaz de obter êxito na interrupção da comunicação entre o IHM e o PLC, resultando na interrupção do tráfego legítimo, conforme ilustrado na Figura 21. Essa indisponibilidade foi provocada mediante a execução de instruções de escrita aleatória, por meio do acionamento de um exploit, que faz uso da biblioteca pyModbus

(Collins 2013), envolvendo 20 agentes durante os testes. O acionamento ocorreu após os primeiros 5 minutos de um total de 15 minutos.

No cenário da Figura 22, foi constatado um intervalo menor de indisponibilidade de sinal, atingindo um pico de 2500000 B/s. No entanto, ao utilizar o ZT, a solução identificou a falta de padrões de critérios estáticos esperados para os dispositivos autenticados com aquelas credenciais. A conexão do atacante foi encerrada após 11 segundos.

Nas situações em que o ZT estava ativo, o jitter apresentou menor variação em comparação ao cenário sem a utilização do modelo, indicando maior estabilidade e consistência na transmissão de dados. É importante ressaltar que, no contexto de negação de serviço em um ambiente ZT, são necessários estudos adicionais para compreender os possíveis comprometimentos quando as ações apresentam características distribuídas, resultando em um alto volume de requisições.

Essa questão não foi abordada nesta pesquisa específica. No entanto, em um cenário real, no qual a presença de redes de *botnets* é uma realidade, é fundamental conduzir uma investigação aprofundada sobre as estratégias de mitigação durante ataques, apoiando-se em soluções de balanceamento de carga e espelhamento do serviço de autenticação. No ataque de manipulação de pacotes por meio do envenenamento da tabela ARP, o processo envolveu a obtenção dos endereços MAC das máquinas-alvo para iniciar a interceptação dos sinais.

Com o uso do ettercap, foi possível redirecionar as ações entre o HMI e o PLC para rotinas específicas pretendidas pelo atacante. Uma vez que os dados do pacote eram reconhecidos, o conteúdo era alterado para exibir informações diferentes no painel do HMI. Analisando o tráfego, foi possível distinguir dois momentos: um com tráfego legítimo, em que o valor enviado para o PLC era o esperado, e outro momento ilegal, em que ocorria o envio de um valor correto ao PLC, mas o valor percebido no painel do HMI era diferente. O objetivo era a gravação de bobinas para os estados "ON" e "OFF" usando o protocolo Modbus/TCP, conforme o Algoritmo 5.

Algoritmo 5 - Instrução apresentada no "Modbus.filter"

```
if (ip.proto == TCP && tcp.dst == 502) {
  if (search(DATA.data, ''\xff\x00'')) {
    msg(''Identificado ON trocando para OFF'');
    replace(''\xff\x00'', ''\x00\x00'');
  }}
```

No contexto do tráfego legítimo, a alteração do campo de gravação na bobina, localizado no registrador 0, consistia na inserção de um código hexadecimal "FF00" no campo de dados, conforme descrito na Tabela 1. A ação teve como objetivo manter a bobina permanentemente no estado "ON". No entanto, durante um ataque de MITM,

o invasor empregava um filtro, conforme demonstrado no algoritmo da Figura 24, para modificar continuamente o estado, enviando o valor "OFF" para o controlador lógico programável sempre que o dado específico era identificado. Isso resultava na transição de "**FF**00" para "**00**00". Com a aplicação da abordagem ZT, essa mudança não ocorria nem era permitida, pois o usuário era comparado com sessões anteriores, e caso o critério do algoritmo de confiança não fosse atendido, a requisição do atacante não era considerada.

Tabela 1: Representação do Protocolo Modbus/TCP

Cabeçalho do Protocolo de Aplicação Modbus				Unidade de Dados de Protocolo	
Transação ID	Protocolo ID	Tamanho	Unidade ID	Código de Função	Dados

Como resultado, foi possível observar, por meio das capturas de tráfego, as alterações, demonstrando a efetividade das técnicas no contexto apresentado com o uso do ZT. Ao acionar a abordagem ZT, não foram observadas essas alterações nos valores que estavam presentes nos momentos sem ZT. Os testes propostos permitiram identificar esses dois momentos, conforme ilustrado nas Figuras 23 e 24, que mostram os quadros das solicitações. A primeira ocorreu durante o ataque em um ambiente sem ZT, enquanto a segunda ocorreu dentro do ambiente protegido pelo ZT.

É possível visualizar a forma como ocorre o reconhecimento entre as máquinas para a interação na execução do comando "ON" no tráfego legítimo e a alteração para "OFF" no tráfego ilegítimo como visto na Figura 25 que representa as mensagens trocadas nos dois momentos.

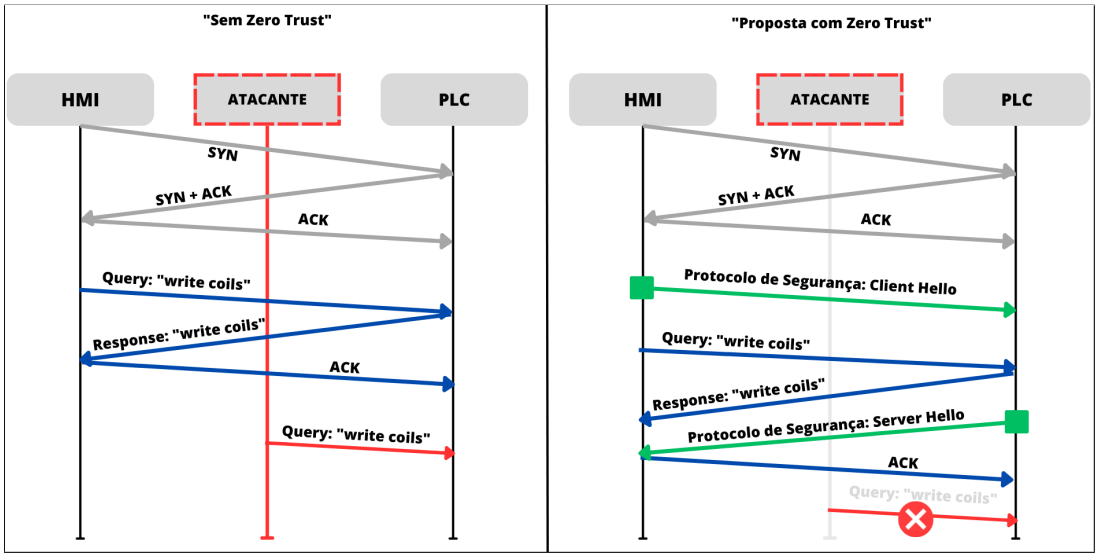

Figura 25: Aperto de mão de três vias - Estabelecendo conexão nos dois cenários com a presença do atacante (MITM).

No contexto do ataque de "*device spoofing*" com a injeção de código, foi proposto um cenário em que o atacante possui credenciais válidas, mas o seu dispositivo não atende

aos critérios esperados para validação pela central ZT. As políticas disponibilizadas pelo *framework* utilizado nesta pesquisa fornecem apenas informações estáticas sobre o dispositivo utilizado pelo usuário, tais como tipo de navegador, sistema operacional, localização na rede e geolocalização. Vale ressaltar que a última informação não foi testada devido ao custo associado ao uso de uma API de geolocalização, sendo adotadas apenas as soluções disponíveis opensource.

Quando apresentado sem a abordagem ZT, o atacante pode explorar a rede em busca de dados presentes nos campos de autenticação que não foram tratados, possibilitando o acesso direto à interface homem-máquina, principalmente em serviços com baixa segurança que são suscetíveis a violações de segurança, como evidenciado em (CVE-2021-26828 2021). Por outro lado, ao adotar uma abordagem ZT e utilizar algoritmos baseados em desafios como critérios de segurança, o processo de estabelecimento de conexão se torna mais lento, uma vez que é necessário atender a todos os critérios do perfil do usuário.

Portanto, pesquisas futuras específicas serão necessárias para explorar possíveis quebras de múltiplas soluções de segurança em ambientes ZT. Além disso, a quantidade de tentativas executadas por um atacante seria facilmente observada por sistemas de detecção de intrusões atualmente utilizados na indústria.

Nesta pesquisa, foram realizados alguns testes em que um usuário malicioso, possuindo credenciais de login e senha, tenta superar os desafios propostos pelo algoritmo, como o uso de um navegador específico com uma determinada versão e sistema operacional. Para atender aos critérios propostos pela política de autenticação com a abordagem ZT, foi utilizado o Burp Suite Proxy para estabelecer a interceptação local das requisições.

Dessa forma, foi possível modificar as requisições de autenticação de acordo com os critérios desejados. Essa abordagem permitiu realizar testes e verificar a eficácia das medidas de segurança implementadas. No entanto, não foram obtidos êxito com ataques em ambiente ZT conforme a Figura 26, que encerrou a conexão já na etapa de autenticação uma vez que não foi superada.

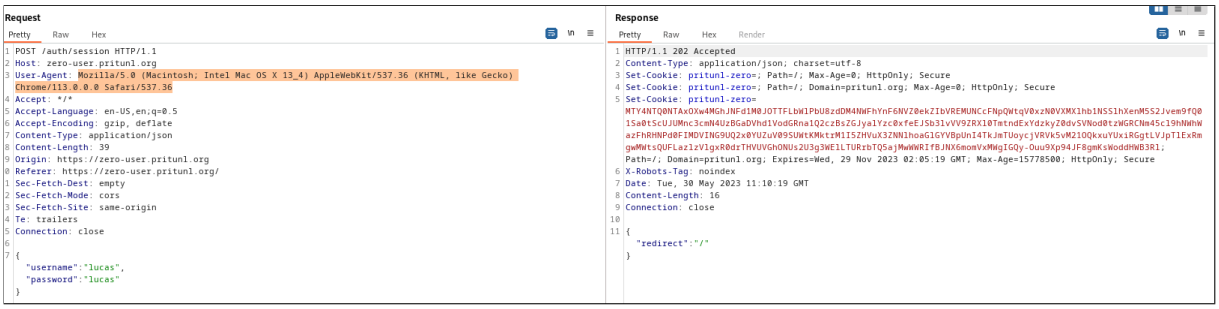

Figura 26: Tentativa de acesso negada ao errar campos estáticos do perfil com credenciais válidas.

Identificou-se apenas uma falha de segurança que poderia resultar em uma inundação

de sessões na ferramenta escolhida, o "Pritunl-Zero". Durante os ataques, observou-se que, mesmo quando o usuário fornece informações sobre as sessões abertas e métodos para encerrá-las, um número excessivo de sessões ainda poderia comprometer o gestor de identidades, inviabilizando a rede ao ser necessário passar por um controle de credenciais sobrecarregado por usuários duplicados em várias sessões. Isso poderia assemelhar-se a um possível ataque de negação de serviço direcionado a usuários que não conseguiriam acessar o recurso. Essa potencial falha sugere, como medida de mitigação, a adoção de conceitos como descentralização, contratos inteligentes ou espelhamento do serviço.

Tabela 2: TSS e Jitter para os testes com e sem o ataque DoS.

Teste - Cenários propostos	**Jitter (s)**	**TTS (s)**
SEM ATAQUE/SEM ZT	$\approx 0,0003$	$\approx 0,0012$
SEM ATAQUE/COM ZT	$\approx 0,0036$	$\approx 0,0029$
COM ATAQUE/SEM ZT	∞	∞
COM ATAQUE/COM ZT	$\approx 0,0097$	$\approx 0,0051$

Os resultados evidenciam que a implementação do modelo Zero Trust pode proporcionar benefícios significativos para a proteção da rede industrial contra ataques de negação de serviço, mesmo considerando uma leve sobrecarga e um discreto aumento no Tempo de Serviço (*Time To Service* – TTS), conforme apresentado na Tabela 2. Torna-se necessário realizar avaliações em cenários que abranjam múltiplos protocolos e envolvam um maior número de solicitantes, tanto legítimos quanto não legítimos. A presente pesquisa abordou cenários que incluem rotinas sem ataque, com um único usuário, e com ataques, envolvendo múltiplos usuários de forma concorrente.

5 Trabalhos Futuros e Conclusões

5.1 Proposta: Modelo de Controle de Acesso Baseado em Estados Observáveis

A ferramenta utilizada demonstrou eficácia em sua proposta inicial de prover segurança aos usuários, levando em consideração suas características específicas para o uso de determinado recurso. Quando aplicada em contextos relacionados a redes industriais, especialmente no âmbito da Tecnologia da Informação, a utilização de soluções como a mencionada permite a implementação de microperímetros autorizados para o acesso de usuários a dispositivos no nível de operação/controle.

No entanto, ao lidar com níveis mais elevados, como o controle e o de processo, que se aproximam das redes TO, surgem desafios adicionais com especificidades que dificultam a aplicação eficiente da ferramenta escolhida.

A verificação contínua de identidade para cada transação em infraestruturas críticas cria uma dinâmica complexa. Validar cada solicitação de recurso proveniente de dispositivos torna-se altamente sensível a questões relacionadas ao tempo, o que demanda a necessidade de adotar padrões, como os de redes sensíveis ao tempo. Esses padrões têm sido objeto de estudo e padronização na nova indústria, visto que as redes industriais atuais, onde os dispositivos utilizam o padrão *Ethernet* para a troca de mensagens, começam a apresentar um conjunto de normas denominado redes sensíveis ao tempo.

Essa temática tem sido discutida em grupos de trabalho que buscam a padronização desse aspecto (IEC/IEEE 60802 TSN Profile for Industrial Automation 2023). Os desafios de implementação desta solução e as dificuldades na leitura de todos os dispositivos, como sensores e atuadores, abrangem desde obstáculos na criação de microperímetros até a cobertura de dispositivos não-IIoT. Um padrão relevante, como o 802.1AR-2018, propõe que dispositivos IEEE 802 definam identificadores e os vinculem criptograficamente ao dispositivo, além de estabelecer uma forma de autenticação para conceder validação à identidade daquele dispositivo (IEEE 2018).

Em linha com a tendência de cada vez mais implementar redes industriais seguras, surge a necessidade de validar as ações de recursos presentes nos níveis de operação, controle e acesso, sem prejudicar o tempo entre as comunicações. A estratégia utilizada durante os testes revelou, em certo cenário, uma leve inserção de aumento em valores de certas métricas de rede, conforme detalhado no Capítulo 4.

No entanto, é crucial destacar que, dado que foi utilizado apenas um protocolo específico, o Modbus/TCP, isso não reflete totalmente o que é transmitido em uma rede industrial de forma mais ampla. Nas redes industriais, há uma diversidade de dispositivos e protocolos presentes no nível de controle e processo, como sensores e atuadores, os quais

não foram abordados durante a pesquisa.

Olhando para o futuro, observa-se que na abordagem ZT há um momento durante a implementação e construção da lógica de segurança a utilização de algoritmo de confiança para apoiar a decisão do mecanismo de política. De acordo com o NIST (Rose et al. 2020), são indicadas formas de alcançar esse objetivo com estratégias como critério, semelhante à ferramenta utilizada, em que a confiança pode ser vista de forma singular ou em contexto.

A aplicação de algoritmos de confiança com base em critérios, de forma singular, evidencia a necessidade de um nível mais detalhado de informações, o que poderia resultar em um aumento do poder computacional necessário para a resolução das atividades de segurança, impactando outros fatores.

Portanto, uma proposta de direcionamento surge na medida em que a tendência de padronização a longo prazo aponta para dispositivos únicos e validados, integrados em redes sensíveis ao tempo para automação industrial. Nesse contexto, a validação dos equipamentos para o cenário atual da indústria, que busca incorporar a abordagem ZT, pode considerar a indicação de graus temporários de confiança. A ideia é que a validação de cada transação ocorra por meio da transição de estados, estabelecendo estados observáveis para a validação da confiança em solicitações de recursos, tanto entre usuário e dispositivo quanto entre dispositivos.

Para pesquisas futuras, a definição de limiares de confiança entre equipamentos distribuídos, considerados de forma singular ou em zonas, surge como uma proposta a ser considerada. Os dispositivos poderiam comunicar seus estados ao mecanismo de políticas, que, por sua vez, indicaria o grau de confiança dessas transações. Esta proposta se alinha e gera um novo formato de controle de acesso de dispositivos alinhado nos pilares do ZT.

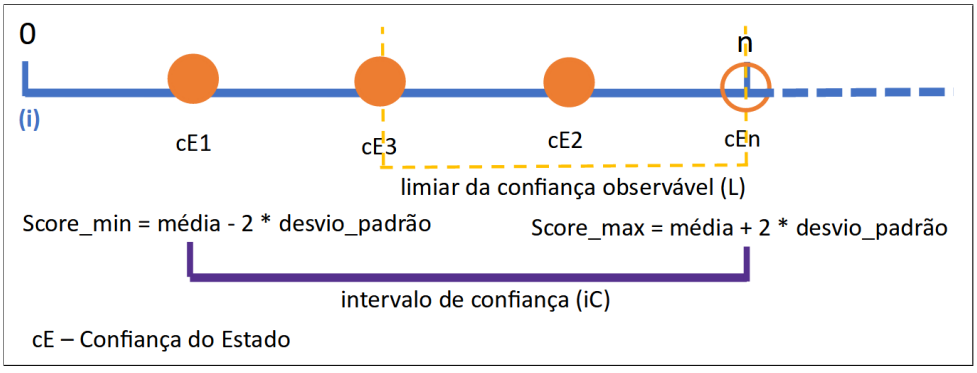

Figura 27: Representação do Modelo de Controle de Acesso Baseado por Três Estados.

Um exemplo prático envolve a transação de um pacote Modbus/TCP encapsulado, que inclui o estado e é apresentado com um certo nível de confiança. O mecanismo de políticas recebe as duas primeiras transações, cada uma com seu estado calculado, a fim de estabelecer um limiar de confiança observável. Quando a próxima transação é recebida,

o estado desta última é calculado e comparado com o limiar de confiança para verificar se está dentro ou além dos limites máximo e mínimo dos estados calculados anteriormente.

O intervalo de confiança proposto é de 95% devido à estratégia de propor limite superior como a média mais duas vezes o desvio padrão, e o limite inferior como a média menos duas vezes o desvio padrão. Em caso de superação, novos pontos de máximo e mínimo são atribuídos e apresentado a um novo limiar de confiança, como na Figura 27.

Os estados seriam calculados através de coeficientes de ponderação aplicados à probabilidade condicional com uma função linear simples, onde o resultado indicaria um ponto de confiança para os próximos dois subsequentes, conforme visto na figura acima. A reordenação dos estados evidenciaria padrões e comportamentos no transacionamento, o que possibilitaria a indicação de alertas.

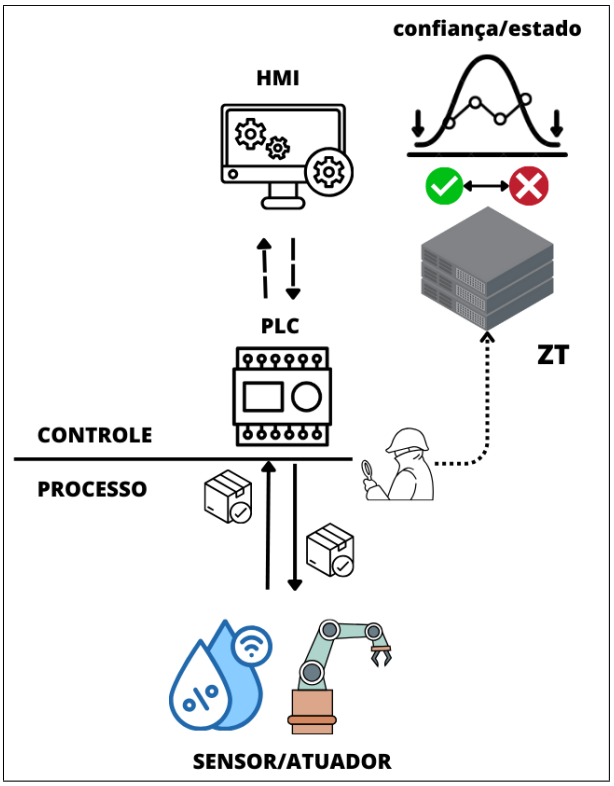

Figura 28: Representação da presença de agentes na borda do nível controle.

Para que seja possível a aplicação dessa teoria, existiria a necessidade de agentes, com única instrução de fazer a aquisição dos dados em tempo real, na borda do nível de controle, com ligação direta à central ZT para que o nível de confiança seja verificado. Ao menor sinal de incongruência ou mesmo atuação ilícita, um alerta seria enviado aos gestores da rede em questão, conforme visto na Figura 28. Para auditoria, restaria apenas a indicação do momento e do dispositivo que iniciou a indicação negativa da confiança.

5.2 Conclusões

Em síntese, as investigações realizadas durante esta pesquisa destacam a importância da implementação do modelo de ZTNA na rede das redes industriais. Os resultados evidenciam que a adoção desse modelo pode aprimorar a segurança, prevenindo ataques e assegurando uma transferência de dados mais estável e confiável. Contudo, as pesquisas também apontam desafios e limitações, ressaltando a necessidade de investigações adicionais em cenários mais próximos da realidade.

Os experimentos realizados indicam que a implementação do modelo pode resultar em um leve aumento no tempo de resposta e, em certos casos, picos na latência. Esses resultados destacam a importância de considerar cuidadosamente a implementação, especialmente em infraestruturas críticas de tempo real, onde o atraso pode ser crucial. Em testes de carga, por meio do uso de ataques específicos, foi demonstrada uma aproximação entre os valores das métricas de rede nos dois ambientes utilizados nos testes. No entanto, os valores encontrados refletem o ambiente de teste simulado proposto, sendo necessário implementar testes em cenários mais próximos da realidade industrial.

O estudo revela que o ZT proporcionou estabilidade e consistência na transferência de dados, mesmo durante a ocorrência de ataques. Em particular, a capacidade do ZT de detectar e bloquear rapidamente ataques de negação de serviço foi destacada como um ponto positivo na proteção da rede industrial, apoiado ao contexto proposto para a criação dos cenários onde a proteção era sugerida. Essa avaliação foi realizada com base na estratégia da solução opensource utilizada para avaliar a integridade do equipamento que estaria acessando o HMI.

Foram identificados cenários em que a implementação do ZT impediu com sucesso a execução de ações maliciosas, como injeção de comandos e manipulação de pacotes. Além disso, foi destacada a importância de conduzir estudos adicionais para compreender possíveis comprometimentos durante ataques distribuídos e explorar estratégias de mitigação, como balanceamento de carga e espelhamento do serviço de autenticação. Foi observado um ponto de vulnerabilidade da solução utilizada no tratamento de sessões geradas por manipulação de credenciais, onde, apesar de poder ser identificado e encerrado de forma simples, o encerramento ocorreria de forma manual em vez de ser identificado e encerrado automaticamente.

Os testes ressaltam a necessidade de avaliar fatores práticos e ambientais ao implementar soluções de segurança como o ZT em ambientes industriais. Além disso, enfatizam a importância de realizar testes em cenários mais complexos, que envolvam múltiplos protocolos e um maior número de solicitantes, tanto legítimos quanto não legítimos, para uma compreensão abrangente do impacto da implementação do ZT na segurança e no desempenho da rede. A abordagem do Acesso a Redes por ZT pode ser uma estratégia eficaz

para fortalecer a segurança das redes industriais, embora seja necessário um equilíbrio cuidadoso entre segurança e desempenho.

Adicionalmente, sugere-se a realização de experimentos com hardware específico e a investigação de novos tipos de ataques que possam surgir direcionados a ambientes com ZT. O desenvolvimento de um algoritmo de confiança específico, apoiado ao Controle de Acesso Baseado em Três Estados proposto para validar transações em redes industriais, especialmente em redes sensíveis ao tempo (Time-Sensitive Networking – TSN), é visto como potencial e significativo para avanços na comunicação segura na indústria a longo prazo. Isso visa não apenas a busca por impactos menores no contexto da comunicação em redes industriais, mas também o aprimoramento da detecção de ameaças e a redução de falsos positivos.

Durante a condução desta pesquisa, as investigações anteriores resultaram na aceitação de quatro artigos científicos que foram apresentados em sequência:

1. Impacto em Aplicações de Controle Industrial Operando em Ambientes Orientado a Confiança Zero. Lucas S., Cruz Iguatemi E., Fonseca e Camilla E. J. F., Figueiredo, p. 37–38, 2022 - XII Conferência Nacional em Comunicações, Redes e Segurança da Informação – Encom - em outubro de 2022 - Guaramiranga - CE (S., E. e F. 2022)

2. Avaliação do Impacto da Arquitetura de Confiança Zero em Aplicações de Controle Industrial - Lucas S., Cruz e Iguatemi E., Fonseca - XLI Simpósio Brasileiro de Telecomunicações e Processamento de Sinais - Sociedade Brasileira de Telecomunicações – SBRT - em outubro de 2023 - São José dos Campos - SP (S. e E. 2023)

3. Sistemas de Controle Industrial com Arquitetura de Confiança Zero: Analise de Resposta a Ataques - Lucas S., Cruz e Iguatemi E., Fonseca - XIII Conferência Nacional em Comunicações, Redes e Segurança da Informação - Encom - em outubro de 2023 - Belém - PA (S. e E. 2023)

4. L. S. Cruz and I. E. Fonseca, "Industrial Control Systems in Environments with Zero Trust Architecture: Analysis of Responses to Various Attack Types," 2023 Workshop on Communication Networks and Power Systems (WCNPS) – IEEE, Brasília, Brasil, 2023, pp. 1-7 (Videoconferência) (Cruz e Fonseca 2023).

Em resumo, os resultados obtidos indicam que a adoção do modelo de confiança zero é uma medida promissora para aprimorar a segurança nas redes industriais, mas sua implementação requer considerações detalhadas e adaptações contínuas para enfrentar desafios específicos e garantir a eficácia desejada na proteção contra ameaças.

REFERÊNCIAS

Akamai 2023 AKAMAI. *Infection Monkey: Breach and Attack Simulation Platform*. Akamai, 2023. Disponível em: ⟨https://www.akamai.com/infectionmonkey⟩.

Bello e Steiner 2019 BELLO, L. L.; STEINER, W. A perspective on ieee time-sensitive networking for industrial communication and automation systems. *Proceedings of the IEEE*, v. 107, n. 6, p. 1094–1120, 2019.

Buchanan 1999 BUCHANAN, B. Rs-232. In: _____. *Handbook of Data Communications and Networks*. Boston, MA: Springer US, 1999. p. 610–632. ISBN 978-1-4757-0905-6. Disponível em: ⟨https://doi.org/10.1007/978-1-4757-0905-6_47⟩.

CERT 2023 CERT, K. I. *H1 2023 – a brief overview of main incidents in industrial cybersecurity*. [S.l.], 2023. Disponível em: ⟨https://ics-cert.kaspersky.com/publications/reports/2023/10/05/h1-2023-a-brief-overview-of-main-incidents-in-industrial-cybersecurity/⟩.

Chandramouli 2022 CHANDRAMOULI, R. *Guide to a Secure Enterprise Network Landscape*. [S.l.], 2022.

Cisco 2019 CISCO. *Firewalls - The Future of the Firewall White Paper — cisco.com*. [S.l.], 2019. [Accessed 22-Jun-2023].

Collins 2013 COLLINS, G. *Pymodbus Documentation*. [S.l.]: June, 2013.

Cruz e Fonseca 2023 CRUZ, L. S.; FONSECA, I. E. Industrial control systems in environments with zero trust architecture: Analysis of responses to various attack types. In: *2023 Workshop on Communication Networks and Power Systems (WCNPS)*. [S.l.: s.n.], 2023. p. 1–7.

CVE-2021-26828 2021 CVE-2021-26828. *CVE-2021-26828*. 2021. Available from MITRE, CVE-ID CVE-2021-26828. Disponível em: ⟨https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26828⟩.

Electric 1999 ELECTRIC, S. *Modicon is now Schneider Electric UK*. 1999. Disponível em: ⟨https://www.se.com/uk/en/about-us/company-profile/brands/modicon.jsp⟩.

Ferencz, Domokos e Kovács 2021 FERENCZ, K.; DOMOKOS, J.; KOVáCS, L. Review of industry 4.0 security challenges. In: *2021 IEEE 15th International Symposium on Applied Computational Intelligence and Informatics (SACI)*. [S.l.: s.n.], 2021. p. 245–248.

Fortinet 2023 FORTINET. *Relatório sobre o estado da segurança cibernética de TI operacional*. [S.l.], 2023. Disponível em: ⟨https://www.fortinet.com/content/dam/fortinet/assets/reports/pt_br/report-state-ot-cybersecurity.pdf⟩.

Haddon e Bennett 2021 HADDON, D.; BENNETT, P. The emergence of post covid-19 zero trust security architectures. In: _____. *Information Security Technologies for Controlling Pandemics*. Cham: Springer International Publishing, 2021. p. 335–355. ISBN 978-3-030-72120-6. Disponível em: ⟨https://doi.org/10.1007/978-3-030-72120-6_13⟩.

Hu 2014 HU, C. T. Attribute based access control (abac) definition and considerations. Chung Tong Hu, 2014.

Huff 2022 HUFF, Z. *PRITUNL-ZERO*. 2022. Disponível em: ⟨https://docs.pritunl.com/docs/pritunl-zero⟩.

(IEC) 2023 (IEC), I. E. C. *Communication Networks and Systems for Power Utility Automation-All Parts*. Geneva, Switzerland, 2023.

IEC/IEEE 60802 TSN Profile for Industrial Automation 2023 IEC/IEEE 60802 TSN Profile for Industrial Automation. IEEE 802.1, 2023. Disponível em: ⟨https://1.ieee802.org/tsn/iec-ieee-60802⟩.

IEEE 2018 IEEE. Ieee standard for local and metropolitan area networks - secure device identity. *IEEE Std 802.1AR-2018 (Revision of IEEE Std 802.1AR-2009)*, p. 1–73, 2018.

ISA e IEC 2022 ISA; IEC. *Security for Industrial Automation and Control Systems (ISA/IEC 62443)*. Research Triangle Park, NC, USA, 2022.

(ISA) 2019 (ISA), I. S. of A. *Enterprise-Control System Integration (IEC 62264-1:2019 and ISA95.00.01-2013 Edition 2)*. Research Triangle Park, NC, USA, 2019.

Jayalaxmi et al. 2021 JAYALAXMI, P. et al. A taxonomy of security issues in industrial internet-of-things: Scoping review for existing solutions, future implications, and research challenges. *IEEE Access*, v. 9, p. 25344–25359, 2021.

Junior e Souza 2012 JUNIOR, E. M. de O.; SOUZA, M. L. d. O. e. A brief comparison of security aspects of time synchronization in networked control systems using csma/cd versus tdma protocols. *XIV Simposio de Aplicações Operacionais em Áreas de Defesa*, 2012.

Kalapaaking et al. 2023 KALAPAAKING, A. P. et al. Blockchain-based federated learning with secure aggregation in trusted execution environment for internet-of-things. *IEEE Transactions on Industrial Informatics*, v. 19, n. 2, p. 1703–1714, 2023.

Maesa, Mori e Ricci 2018 MAESA, D. D. F.; MORI, P.; RICCI, L. Blockchain based access control services. In: *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. [S.l.: s.n.], 2018. p. 1379–1386.

Martin 2014 MARTIN, L. Cyber kill chain. *URL: http://cyber. lockheedmartin. com/hubfs/Gaining the Advantage Cyber Kill Chain. pdf*, 2014.

Martin 2023 MARTIN, L. *Cyber Kill Chain*. 2023. Disponível em: ⟨https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html⟩.

Martins e Theóphilo 2009 MARTINS, G. d. A.; THEóPHILO, C. R. *Metodologia da investigação científica para ciências sociais aplicadas*. [S.l.]: Atlas, 2009.

Modbus 2004 MODBUS, I. D. A. *Modbus application protocol specification v1.1b*. North Grafton, 2004. Disponível em: ⟨http://www.modbus.org/specs.php⟩.

Monir 2016 MONIR, S. *A Lightweight Attribute-Based Access Control System for IoT*. Tese (Doutorado) — University of Saskatchewan, 2016.

Nunamaker e Chen 1990 NUNAMAKER, J.; CHEN, M. Systems development in information systems research. In: *Twenty-Third Annual Hawaii International Conference on System Sciences*. [S.l.: s.n.], 1990. v. 3, p. 631–640 vol.3.

Pritunl 2022 PRITUNL. *Documentation - Security — Pritunl*. Pritunl, 2022. Disponível em: ⟨https://docs.pritunl.com/docs/security⟩.

Pritunl Zero 2023 PRITUNL Zero. GitHub, 2023. Disponível em: ⟨https://github.com/pritunl/pritunl-zero⟩.

Provos e Mazieres 1999 PROVOS, N.; MAZIERES, D. A future-adaptable password scheme. In: *USENIX Annual Technical Conference, FREENIX Track*. [S.l.: s.n.], 1999. v. 1999, p. 81–91.

Rahman et al. 2022 RAHMAN, A. et al. Launch of denial of service attacks on the modbus/tcp protocol and development of its protection mechanisms. *International Journal of Critical Infrastructure Protection*, v. 39, p. 100568, 2022. ISSN 1874-5482. Disponível em: ⟨https://www.sciencedirect.com/science/article/pii/S187454822200052X⟩.

Rose et al. 2020 ROSE, S. et al. *Zero Trust Architecture*. [S.l.], 2020. Disponível em: ⟨https://csrc.nist.gov/publications/detail/sp/800-207/final⟩.

S. e E. 2023 S., C. L.; E., F. I. Avaliação do Impacto da Arquitetura de Confiança Zero em Aplicações de Controle Industrial. *Sociedade Brasileira de Telecomunicações – SBRT*, p. 4, 2023. Disponível em: ⟨https://biblioteca.sbrt.org.br/articlefile/4421.pdf⟩.

S. e E. 2023 S., C. L.; E., F. I. Sistemas de controle industrial com arquitetura de confiança zero: Analise de resposta a ataques. *Conferência Nacional em Comunicações, Redes e Segurança da Informação – Encom*, p. 117, 2023. Disponível em: ⟨https://www.iecom.org.br/encom2023/files/anais_encom2023.pdf⟩.

S., E. e F. 2022 S., C. L.; E., F. I.; F., F. C. E. J. Impacto em Aplicações de Controle Industrial Operando em Ambientes Orientado a Confiança Zero. *Conferência Nacional em Comunicações, Redes e Segurança da Informação – Encom*, p. 37–38, 2022. Disponível em: ⟨http://iecom.org.br/encom2022/files/anais_encom2022.pdf⟩.

Seno, Tramarin e Vitturi 2012 SENO, L.; TRAMARIN, F.; VITTURI, S. Performance of industrial communication systems: Real application contexts. *IEEE Industrial Electronics Magazine*, v. 6, n. 2, p. 27–37, 2012.

Sheldon 2001 SHELDON, T. *McGraw-Hill Encyclopedia of Networking & Telecommunications*. Osborne/McGraw-Hill, 2001. ISBN 9780072122701. Disponível em: ⟨https://books.google.com.br/books?id=RzvPtAEACAAJ⟩.

Spear et al. 2016 SPEAR, B. et al. Beyondcorp: The access proxy. *Login*, 2016.

Standards e (NIST) 2023 STANDARDS, N. I. of; (NIST), T. *Guide to Operational Technology (OT) Security*. 2023.

Stouffer et al. 2022 STOUFFER, K. et al. *Guide to Operational Technology (OT) Security*. [S.l.], 2022.

Syed et al. 2022 SYED, N. F. et al. Zero Trust Architecture (ZTA): A Comprehensive Survey. *IEEE Access*, v. 10, p. 57143–57179, 2022. ISSN 2169-3536. Disponível em: ⟨https://ieeexplore.ieee.org/document/9773102/⟩.

Thrybom e Prytz 2009 THRYBOM, L.; PRYTZ, G. Qos in switched industrial ethernet. In: *2009 IEEE Conference on Emerging Technologies & Factory Automation*. [S.l.: s.n.], 2009. p. 1–8.

Trifonov et al. 2021 TRIFONOV, R. et al. Cyber Trends in Industrial Control Systems. In: *2021 25th International Conference on Circuits, Systems, Communications and Computers (CSCC)*. [S.l.: s.n.], 2021. p. 41–45.

Valsorda 2023 VALSORDA, F. *Mkcert*. GitHub, 2023. Disponível em: ⟨https://github.com/FiloSottile/mkcert⟩.

Wadsworth et al. 2019 WADSWORTH, A. et al. Development of iiot monitoring and control security scheme for cyber physical systems. In: *2019 SoutheastCon*. [S.l.: s.n.], 2019. p. 1–5.

Ward e Beyer 2014 WARD, R.; BEYER, B. Beyondcorp: A new approach to enterprise security. *;login:*, Vol. 39, No. 6, p. 6–11, 2014.

Williams 1993 WILLIAMS, T. J. The Purdue Enterprise Reference Architecture. *IFAC Proceedings Volumes*, v. 26, n. 2, Part 4, p. 559–564, jul. 1993. ISSN 1474-6670. Disponível em: ⟨https://www.sciencedirect.com/science/article/pii/S1474667017485326⟩.

Yarali e Sahawneh 2019 YARALI, A.; SAHAWNEH, F. G. Deception: Technologies and strategy for cybersecurity. In: *2019 IEEE International Conference on Smart Cloud (SmartCloud)*. [S.l.: s.n.], 2019. p. 110–120.

Zaheer et al. 2019 ZAHEER, Z. et al. Eztrust: Network-independent zero-trust perimeterization for microservices. In: *Proceedings of the 2019 ACM Symposium on SDN Research*. New York, NY, USA: Association for Computing Machinery, 2019. (SOSR '19), p. 49–61. ISBN 9781450367103. Disponível em: ⟨https://doi.org/10.1145/3314148.3314349⟩.