Avaliação do Impacto da Arquitetura de Confiança Zero em Aplicações de Controle Industrial

Lucas S. Cruz e Iguatemi E. Fonseca

***Resumo*— A gestão eficiente dos equipamentos na indústria moderna é possibilitada pelo uso de aplicações de controle industrial para coletar e gerir dados. Com a integração de tecnologias de informação à tecnologia operacional, há um aumento significativo da malha de rede e a possibilidade de surgimento de vulnerabilidades. Este trabalho apresenta uma avaliação do impacto da arquitetura de segurança orientada a Confiança Zero em plantas industriais, utilizando métricas como latência, jitter e vazão na rede. Os resultados preliminares sugerem que a Confiança Zero permite um controle mais rigoroso na operação da rede, tendo pequena influência na resposta, no consumo de recursos computacionais e no desempenho da rede.**

***Palavras-Chave*— Redes industriais, Protocolo MODBUS TCP/IP, Confiança Zero, Segurança em redes de comunicação.**

***Abstract*— The efficient management of equipment in modern industry is enabled by the use of industrial control applications to collect and manage data. With the integration of information technology into operational technology, there is a significant increase in network infrastructure and the possibility of vulnerabilities emerging. This paper presents an evaluation of the impact of the zero-trust security architecture in industrial plants, using metrics such as latency, jitter, and network throughput. The preliminary results suggest that zero trust enables more stringent control in the network operation and may present a tiny impact in the response time, consume computational resources, and network performance.**

***Keywords*— Industrial networks, MODBUS TCP/IP protocol, Zero Trust, Security in communication networks.**

I. Introdução

As redes industriais apresentam desafios específicos no que diz respeito à segurança cibernética, uma vez que vulnerabilidades nos protocolos de comunicação podem expor os sistemas de automação industrial a riscos cada vez maiores. Em resposta a essa ameaça, uma abordagem emergente é a arquitetura de Confiança Zero (ZT - *Zero Trust*). Sendo esta uma metodologia de segurança que parte do pressuposto de que todo tráfego na rede é considerado suspeito, mesmo quando originado internamente. A arquitetura ZT implementa, portanto, controles rigorosos de autenticação, autorização e criptografia [1]. Pontos a serem avaliados estando em ambientes de redes de infraestruturas críticas de tempo real.

A adoção de práticas da arquitetura de segurança em pesquisa é uma forma promissora de mitigar riscos em segurança [2], conforme descrito em [3]. Em particular, redes industriais compartilham características com sistemas de controle de recursos energéticos, em que sensores, dispositivos de monitoramento e algoritmos de processamento de dados são usados para coletar informações em tempo real e otimizar a operação do sistema. Estudos, como os descritos em [4] e [5], têm explorado a implementação do modelo de segurança ZT em sistemas elétricos e identificado os desafios envolvidos. No entanto, um ponto crucial a ser considerado é a avaliação dos fatores após a implementação do modelo de segurança, especialmente em relação ao desempenho. Segundo o estudo [6], que utilizou simulações numéricas, foram observados impactos no tempo de resposta ao utilizar a abordagem ZT em infraestruturas críticas, sugerindo a importância de investigar outras métricas de rede relevantes para avaliação.

Este artigo apresenta informações sobre segurança em redes industriais na Seção II, que inclui um resumo dos protocolos utilizados na indústria e o protocolo empregado na pesquisa. Na Seção III, o ZT é apresentada como uma solução proposta para melhorar a segurança de dispositivos em redes industriais, com contexto e padronizações relevantes. A Seção IV detalha o processo de construção do ambiente de testes utilizado para avaliar a solução proposta, fornecendo dados preliminares rastreados ao longo da pesquisa. Finalmente, a Seção V apresenta as conclusões da pesquisa, destacando as principais descobertas e sugerindo possíveis direções para futuras pesquisas na área de segurança em redes industriais.

II. Segurança em Redes Industriais

A. Protocolos de Comunicação em Redes Industriais

Protocolos de comunicação são fundamentais para o funcionamento eficiente de redes industriais. Esses protocolos estabelecem as diretrizes necessárias para a comunicação entre dispositivos e sistemas de controle, garantindo que as informações sejam transmitidas de forma segura e precisa. Com o avanço da tecnologia, a complexidade da comunicação remota entre os elementos presentes nessas redes aumentou, tornando necessário o desenvolvimento de protocolos mais avançados para atender às novas demandas.

Um dos protocolos mais eficientes utilizados em sistemas de controle industrial é o ModBus. Baseado no paradigma cliente-servidor, o ModBus permite a interação entre a Unidade Terminal Principal (MTU - *Master Terminal Unit*) e a Unidade Terminal Remota (RTU - *Remote Terminal Unit*) [7], gerando solicitações ao servidor ModBus para garantir uma comunicação eficiente. As mensagens de comunicação são compostas de Unidade de Dados de Protocolo (PDU - *Protocol Data Unit*) e a mecânica de solicitação/resposta é utilizada para garantir a eficiência da comunicação [8].

O ModBus evoluiu ao longo do tempo, destacando-se o ModBus TCP como uma das principais atualizações. Essa

Lucas S. Cruz e Iguatemi E. Fonseca, Centro de Informática, Universidade Federal da Paraíba, João Pessoa-PB, e-mail: ssh.lucascruz@gmail.com; iguatemi@ci.ufpb.br. Este trabalho foi parcialmente financiado pelo CNPq e CAPES.

atualização prioriza a confiabilidade da comunicação pela internet e rede interna, sendo essencial identificar características que possam influenciar o desempenho do sistema. Com o progresso da indústria e avanços tecnológicos, é necessário que o protocolo de comunicação em redes industriais acompanhe essa evolução para atender às demandas da indústria contemporânea, garantindo eficiência e segurança dos sistemas de controle industrial.

B. Modelo Tradicional de Segurança em Redes Industriais

A indústria atualmente adota um modelo organizacional e instrucional baseado na divisão da arquitetura de Sistema de Controle Industrial (ICS - *Industrial control system*) em duas grandes zonas: tecnologia da informação e tecnologia operacional. Cada uma dessas zonas é subdividida em seis níveis, cada um atendendo a necessidades específicas. Há trabalhos que visam compreender essa estrutura, como o CPwE (*Converged Plantwide Ethernet*) [9], que apresenta o modelo PERA (*Purdue Enterprise Reference Architecture* - Arquitetura de Referência Corporativa Purdue) para a hierarquia de controle [10], adotado para a segmentação de rede pela ISA/IEC 62443 (ISA - *International Society of Automation*) [11]. Em conjunto, esses elementos proporcionam um desenho da arquitetura de rede aplicado à indústria, no qual as operações resultam na criação de níveis com bordas lógicas de comunicação para controlar o acesso entre as camadas. Na área de segurança de redes, uma boa prática é segmentar e isolar dispositivos de TI (Tecnologia da Informação) e TO (Tecnologia da Operacional), considerando diversas características que permitam a classificação dos mesmos. Uma estratégia comum é o uso de modelos reconhecidos pelo setor, como o modelo PERA, níveis ISA-95 [12], arquitetura de sistema Internet das Coisas Industrial (IIoT - *Industrial internet of things*) de três camadas [13], ou uma combinação desses modelos para estruturar a segmentação de rede. Além disso, a adoção de zonas desmilitarizadas (DMZ – *Demilitarized Zone*) é uma opção interessante para garantir controle de acesso a informações e componentes, com ênfase na segurança e no desempenho operacional. Dessa forma, as organizações podem controlar e gerenciar o fluxo de dados, garantindo a integridade e a confidencialidade das informações e dispositivos envolvidos.

C. Confiança Zero

A arquitetura de ZT é uma tendência crescente na área de segurança cibernética. Seu modelo parte da premissa de que nenhum dispositivo pode ser considerado confiável por padrão, e que a concessão de permissões deve ser avaliada constantemente. Ao contrário do modelo anterior, que se baseava na criação de perímetros de defesa, essa visa oferecer oferecer proteção a partir de uma abordagem mais proativa, que considera a necessidade de proteger contra ameaças tanto internas quanto externas. Essa nova arquitetura de segurança apresenta desafios, mas também oportunidades para aprimorar a proteção de dados e sistemas críticos

A nova forma de autenticação com validações contínuas tem componentes lógicos padronizados, como a decisão da política e o seu ponto de execução, conforme a Fig. 1. Esses componentes seguem os princípios norteados pela norma

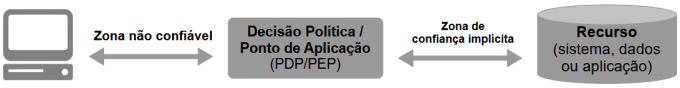

Fig. 1. Acesso através do Zero Trust. *Fonte:* NIST. Figura Adaptada.

NIST 800-207 (NIST - *National Institute of Standards and Technology*), que incluem [1, p. 6]:

1) "Todas as fontes de dados e serviços computacionais são considerados recursos;"
2) "Todas as comunicações são protegidas, independentemente de sua localização;"
3) "O acesso aos recursos individuais da organização é concedido para cada sessão;"
4) "O acesso aos recursos é determinado por uma política atualizada dinamicamente;"
5) "A organização monitora e mede a integridade e a segurança de todos os ativos próprios e associados;"
6) "A autenticação e autorização de todos os recursos são dinâmicas e rigorosamente aplicadas antes do acesso ser concedido;"
7) "A organização coleta o máximo de informações possível sobre o estado atual dos ativos, infraestrutura de rede e comunicações e as utiliza para aprimorar sua política de segurança."

D. Confiança Zero em Redes Industriais

A arquitetura de ZT é uma tendência crescente na área de segurança cibernética, que tem ganhado destaque, em especial após os eventos pandêmicos [14]. A arquitetura ZT se baseia na premissa de que nenhum dispositivo é confiável por padrão e as permissões devem ser avaliadas continuamente. Ao contrário de modelos anteriores, a arquitetura ZT usa abstrações para criar novos perímetros de defesa, adotando abordagens proativas e contínuas para validar usuários e elementos ao redor. Isso torna o ambiente mais seguro e reduz o espaço para ameaças externas e internas. A abordagem ZT reconhece a necessidade de proteger contra ameaças internas e externas, representando uma mudança significativa na segurança cibernética. Embora essa nova arquitetura apresente desafios, também oferece oportunidades para aprimorar a proteção de dados e sistemas críticos.

A adoção do conceito de ZT tem se concentrado em soluções empresariais, especialmente em relação à segurança de dados. Estudos recentes indicam que a Indústria 4.0 também pode se beneficiar dessa arquitetura para enfrentar os desafios resultantes da convergência entre TO e TI.

Um exemplo de desafio que pode ser resolvido com a aplicação adequada da arquitetura de ZT é a validação da integridade do terminal utilizado pelo operador na camada de controle. É necessário garantir a integridade do dispositivo para acionar rotinas de alto grau de atenção. A aplicação de autenticação contínua, monitoramento constante das atividades do dispositivo e limitação das autoridades do usuário pode garantir que as ações decorrentes do dispositivo sejam seguras e confiáveis durante as rotinas [5].

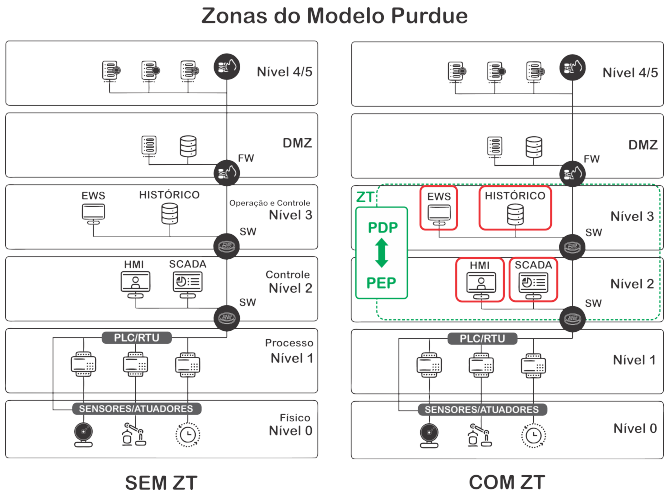

Fig. 2. Estrutura e localização do mecanismo de política seguindo modelo PERA em redes industriais.

No entanto, é importante destacar que a adoção da estratégia de ZT demanda tempo, recursos e uma extensa pesquisa de teorias sobre o assunto. Além disso, é fundamental avaliar a sua aplicação de acordo com o contexto de cada atividade fim, considerando pontos críticos do serviço e utilizando abordagens baseadas em riscos, como apresentado na Fig. 2 [15]. Implementar um novo modelo de segurança requer avaliação contínua para trazer vantagens competitivas e gerenciamento eficaz. Nesse sentido, a análise de métricas de rede pode ser utilizada para gerenciar eficazmente o desempenho do sistema, maximizando seus benefícios e minimizando riscos.

Na Fig. 2 é apresentada a estrutura e a localização do mecanismo de política seguindo o modelo PERA em redes industriais, que ilustra a importância de adotar abordagens baseadas em riscos e considerar pontos críticos do serviço para a implementação da arquitetura de ZT.

III. Estratégia de Inclusão de ZT em Ambiente Industrial: Avaliação de Tráfego

A estratégia Zero Trust (ZT) tem se mostrado uma abordagem atraente para proteger ativos críticos de infraestrutura e reduzir o risco de violações de segurança em redes industriais. Para implementá-la com sucesso, é essencial realizar uma avaliação detalhada da arquitetura a métricas de rede, identificando possíveis vulnerabilidades e a viabilidade do modelo ZT. Nesse contexto, esta pesquisa destaca a interação entre usuários e sistemas supervisórios como um ponto crucial para aplicação da abordagem ZT. Isso ocorre devido à importância de impedir que usuários não autorizados tenham acesso indevido e prejudiquem o funcionamento normal dos dispositivos que se comunicam com o Controlador Lógico Programável (PLC – *Programmable Logic Controller*).

Para atender a essa necessidade, foi utilizado um framework que permite a aplicação do contexto de ZT. Embora esse framework tenha sido originalmente desenvolvido para redes empresariais, sua utilização em redes industriais no nível operacional é possível, uma vez que existem elementos em comum, como a utilização de aplicações e software, além da presença de regras de segurança, como o firewall. Assim, a estratégia de ZT possibilitou a autenticação de usuários autorizados com papéis específicos para cada rotina, levando em conta informações como o dispositivo utilizado e suas características de segurança, sejam elas relacionadas ao hardware ou ao software.

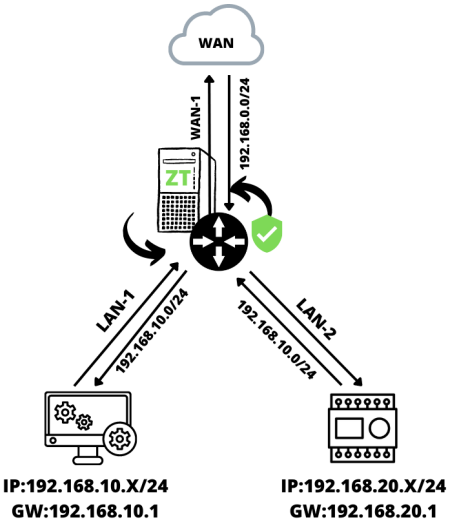

Fig. 3. Visualização da topologia do ambiente de teste (ZT).

Na implementação dessa estratégia em uma rede industrial, optou-se pela topologia ponto a ponto para o tráfego Modbus TCP, com uma arquitetura que incluiu a segmentação da rede e a implementação de um firewall, com a solução pfSense. Além disso, uma central de ZT foi adicionada para comunicar-se com o roteador e avaliar constantemente as autorizações de tráfego. A Fig. 3 ilustra o cenário topológico simulado.

A implementação da estratégia ZT em redes industriais requer a consideração de critérios essenciais para sua plena execução. Em primeiro lugar, é imperativo identificar os recursos e ativos disponíveis, incluindo dispositivos pertencentes à indústria e equipamentos pessoais utilizados pelos usuários. Essa identificação foi feita nos testes executados por meio da elaboração de um inventário de dispositivos e da criação de um banco de dados de usuários, permitindo a gestão eficiente desses ativos. Além disso, foi adotado nos testes mecanismos para identificar dispositivos e usuários que solicitam recursos, usando o *framework* específico como uma solução eficaz de gerenciamento que elimina a confiança implícita em todos os sujeitos envolvidos. Por meio dessa abordagem, todos os dispositivos, internos ou externos à rede industrial, foram tratados igualmente nos testes executados. Por fim, a segmentação, bem como a aplicação de VLAN, possibilitou a separação dos dispositivos em redes específicas, permitindo o isolamento e a criação de rotas específicas para a comunicação.

Outro aspecto relevante nos experimentos foi a apresentação dos papéis e comportamentos adotados na utilização de aplicativos e fluxos de trabalho, por meio de um ponto de aplicação de política. Esse procedimento foi realizado de forma didática, usando formulários disponibilizados no *front-end* do *framework*. Todas as solicitações autorizadas e autenticadas foram delegadas aos serviços em execução no *backend*. O mecanismo de política executa a autorização de nível de serviço, concedendo ou negando o acesso, como ilustrado na

Fig. 4. O acesso do usuário foi também analisado, em relação à versão do sistema operacional ao navegador utilizado para uso da aplicação Interface Homem-Máquina (HMI - *Human Machine Interface*), no uso da rotina *"Write Single Coil"* e à sua disposição dentro da rede. É monitorado também o endereço IP que previamente é atrelado a esse usuário por meio da lógica do *framework* utilizado, que armazena os detalhes do usuário para definir padrões de comportamento de origem de recursos.

Por fim, vale ressaltar que, para acesso a redes ZT, todas as comunicações são criptografadas, garantindo a confidencialidade e integridade dos dados transmitidos. No contexto da conexão entre o cliente e o servidor por meio da instância reservada para o *framework* utilizado, também conhecido como central ZT empregada neste trabalho, o processo de autenticação sendo autorizado e aprovado a conexão faz o uso de múltiplas chaves criptográficas para garantir a segurança da conexão. Para autenticar a solicitação, o *framework* utiliza chave secreta SHA512-HMAC para assinar cada solicitação de conexão. Chaves assimétricas estão presente onde solicitação de conexão e da resposta é realizada por meio do uso de chave pública NaCl disponível no perfil de cada usuário.

IV. Resultados Experimentais

A. Cenários dos Experimentos e Métricas

Para construir o ambiente experimental, foram configuradas instâncias virtuais com condições iniciais idênticas, garantindo a uniformidade da base de equipamentos utilizada. O sistema operacional Debian na versão estável dez, com processador de $1\ GHz$, $2\ GB$ de RAM e $10\ GB$ de espaço em disco foram utilizados como condições iniciais.

Por meio da ferramenta VMware Workstation 16, quatro instâncias foram criadas. As primeiras duas máquinas foram destinadas à primeira série de testes sem a abordagem ZT. O objetivo foi coletar dados gerados de requisições entre cliente-servidor sob protocolo ModBus TCP, utilizando a ferramenta Wireshark, que serviriam como valores-base para comparação na segunda etapa dos testes. Na segunda etapa, foram realizados testes com novas regras de autenticação, incluindo validação contínua do usuário em tempo real.

A simulação do ambiente para sistemas de controle industrial foi organizada seguindo o modelo de estrutura PERA e a topologia escolhida foi ponto a ponto [16]. Ademais, a telemetria foi coletada pela ferramenta Zabbix, com agentes dispostos em todas as instâncias.Para os testes realizados, a única requisição disponível na HMI [8], presente no protocolo ModBus, que foi alternadamente acionada.

Cada cenário proposto foi executado por $100\ min$, com intervalos pré-definidos de $1000\ ms$ entre cada requisição. Simulando a interação de um operador com uma HMI por meio de uma ferramenta de supervisão e controle, como, por exemplo, o Controle de Supervisão e Aquisição de Dados (SCADA -*Supervisory Control and Data Acquisition*) [17]. Essa rotina é comumente presente em processos industriais e a repetição era capaz de gerar tráfego, sobre o protocolo MODBUS TCP, utilizado para avaliação através de métricas de rede.

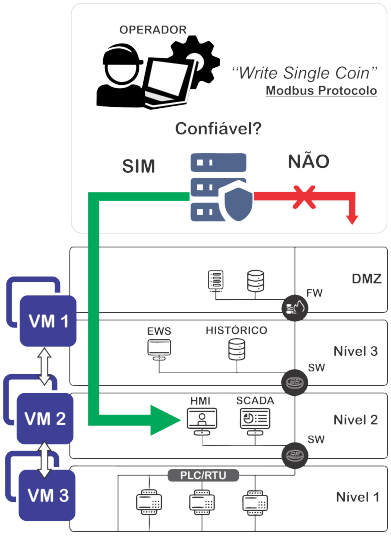

Fig. 4. Estrutura e localização do mecanismo de política seguindo modelo PERA em redes industriais.

É importante destacar que, embora outras rotinas estivessem disponíveis na interface, foi disponibilizada apenas a escrita de bobina para manter a consistência nos testes realizados e evitar a introdução de variáveis que pudessem afetar os resultados.

Na bateria de testes, utilizou-se a solução ZT com o *framework* PRITUNL-Zero que adota um algoritmo de confiança baseado em atributos [18]. Antes de serem executadas no PLC, as requisições foram validadas pela central ZT e implementadas por meio da biblioteca PyModBus, sendo apresentadas por meio de uma HMI em Flask ofertada ao navegador do operador/usuário. Esse tipo de teste é importante para avaliar a eficiência do protocolo utilizado na comunicação entre os dispositivos, bem como para verificar se a implementação de estratégias de segurança, como o modelo Zero Trust, afetam significativamente o desempenho do sistema.

No que tange aos fatores relacionados à comunicação cliente-servidor, a avaliação concentrou-se na comparação entre resultados de métricas de rede, tais como atraso, variação do atraso e tráfego de rede. A escolha dessas métricas é fundamental para a avaliação de desempenho em sistemas de comunicação cliente-servidor, principalmente em cenários industriais, nos quais a disponibilidade e a confiabilidade são fatores críticos. O atraso, por exemplo, é uma métrica importante que indica o tempo decorrido desde o envio de um pacote até sua chegada ao destino.

B. Desempenho observado entre ambientes

Foram avaliadas as médias de atraso em cinco séries de testes, em dois cenários distintos. Conforme ilustrado na Fig. 5, 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 [19]. É possível inferir que a implementação do modelo ZT na rede pode introduzir uma leve sobrecarga e ocasionar um discreto aumento na latência.

A Fig. 6 apresenta a média de jitter em diversas séries de dados, um parâmetro crucial para avaliar o desempenho de

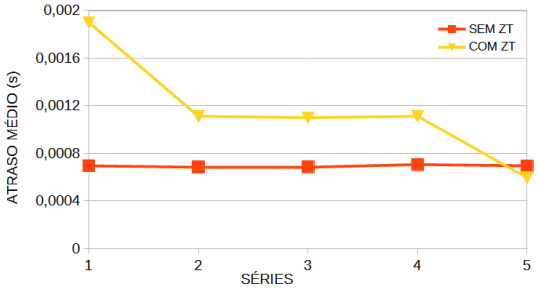

Fig. 5. Média do Atraso durante os testes.

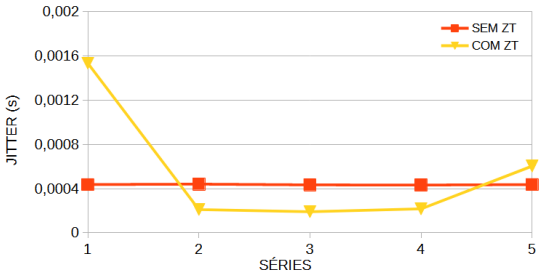

Fig. 6. Média da variação do Atraso durante os testes.

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 Fig. 7, não foi possível concluir de forma significativa as diferenças entre as abordagens SEM ZT e COM ZT em termos de taxa de transferência, devido às pequenas diferenças encontradas, todas na ordem de 156 $bytes/s$. Na série 4, observa-se uma diferença maior, mas vale destacar que em termos de escala, a diferença em relação à série anterior é $0,013$ $bytes/s$. Portanto, os resultados apontam que a implantação do modelo de segurança ZT em ambiente industrial pode ser viável.

V. Conclusões

Este estudo apresenta uma avaliação do desempenho de um modelo de segurança ZT em uma infraestrutura crítica de tempo real. Os testes realizados indicaram que a implementação do modelo ZT gerou um aumento leve no atraso, quando comparado a um ambiente sem ZT. Em relação à taxa de transferência, no geral, os valores foram semelhantes em todos os testes realizados. Dependendo da padronização ou organização da rede, esses valores podem ser considerados muito próximos, o que pode não reproduzir efeitos em larga escala. Os resultados apresentados destacam a importância de considerar novas soluções para tornar ambientes mais seguros e confiáveis nas redes industriais. Como trabalho futuro, propõe-se a criação de um algoritmo de confiança baseado em pontuação, bem como a execução de experimentos com ataques à planta industrial.

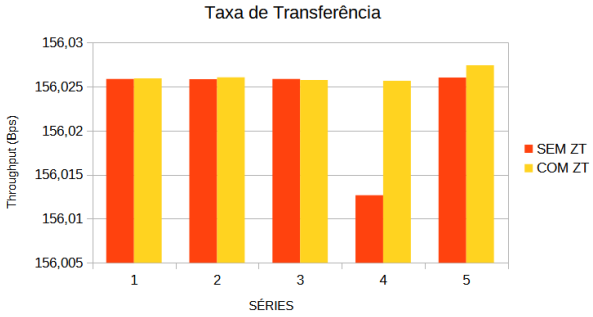

Fig. 7. Vazão na rede.

Referências

[1] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," Tech. Rep. NIST Special Publication (SP) 800-207, National Institute of Standards and Technology, Aug. 2020.

[2] R. Trifonov, G. Tsochev, S. Manolov, R. Yoshinov, and G. Pavlova, "Cyber Trends in Industrial Control Systems," in *2021 25th International Conference on Circuits, Systems, Communications and Computers (CSCC)*, pp. 41–45, July 2021.

[3] A. Kerman, O. Borchert, S. Rose, E. Division, and A. Tan, "Implementing a Zero Trust Architecture," tech. rep., National Institute of Standards and Technology, 2020.

[4] Z. E. Mrabet, N. Kaabouch, H. E. Ghazi, and H. E. Ghazi, "Cyber-security in smart grid: Survey and challenges," *Computers & Electrical Engineering*, vol. 67, pp. 469–482, Apr. 2018.

[5] Y. Chen, X. Zhou, J. Zhu, and H. Ji, "Zero Trust Security of Energy Resource Control System," in *2022 IEEE 5th International Electrical and Energy Conference (CIEEC)*, (Nangjing, China), pp. 5052–5055, IEEE, May 2022.

[6] C. Lucas S., F. Iguatemi E., and F. Camilla E. J. F., "Impacto em Aplicações de Controle Industrial Operando em Ambientes Orientado a Confiança Zero," *Conferência Nacional em Comunicações, Redes e Segurança da Informação – Encom*, pp. 37–38, 2022.

[7] D. Trung, "Modern SCADA systems for oil pipelines," in *Industry Applications Society 42nd Annual Petroleum and Chemical Industry Conference*, pp. 299–305, Sept. 1995. ISSN: 0090-3507.

[8] I. D. A. Modbus, "Modbus specification v1.1b," 2004.

[9] R. Automation, "Converged Plantwide Ethernet (CPwE) Design and Implementation Guide," *Design and implementation guide, Rockwell Automation*, p. 564, 2011.

[10] T. J. Williams, "The Purdue Enterprise Reference Architecture," *IFAC Proceedings Volumes*, vol. 26, pp. 559–564, July 1993.

[11] I. E. Commission *et al.*, "Iec 62443: Industrial communication networks—network and system security," *IEC Central Office: Geneva, Switzerland*, 2010.

[12] ISA, "Isa95: Enterprise-control system integration," *ISA Standard*, no. ANSI/ISA-95-2010, 2010.

[13] S.-W. Lin, B. Miller, J. Durand, R. Joshi, P. Didier, A. Chigani, R. Torenbeek, D. Duggal, R. Martin, G. Bleakley, *et al.*, "The Industrial Internet Reference Architecture," *Industrial Internet Consortium (IIC), Tech. Rep*, 2022.

[14] S. Mandal, D. A. Khan, and S. Jain, "Cloud-Based Zero Trust Access Control Policy: An Approach to Support Work-From-Home Driven by COVID-19 Pandemic," *New Generation Computing*, vol. 39, pp. 599–622, Nov. 2021.

[15] Z. A. Collier and J. Sarkis, "The zero trust supply chain: Managing supply chain risk in the absence of trust," *International Journal of Production Research*, vol. 59, pp. 3430–3445, June 2021.

[16] K. Stouffer, S. Lightman, V. Pillitteri, M. Abrams, and A. Hahn, "Guide to Industrial Control Systems (ICS) Security," Tech. Rep. NIST Special Publication (SP) 800-82 Rev. 2, National Institute of Standards and Technology, June 2015.

[17] A. Daneels and W. Salter, "What is SCADA?," *CERN Document Server*, 1999.

[18] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Zero Trust Architecture (ZTA): A Comprehensive Survey," *IEEE Access*, vol. 10, pp. 57143–57179, 2022.

[19] L. Seno, F. Tramarin, and S. Vitturi, "Performance of industrial communication systems: Real application contexts," *IEEE Industrial Electronics Magazine*, vol. 6, no. 2, pp. 27–37, 2012.