

apter]schemelosScheme

**UNIVERSIDADE DE SÃO PAULO
ESCOLA DE ENGENHARIA DE SÃO CARLOS**

Jonathan Tobias da Silva

Análise de vulnerabilidades em redes OPC UA industriais

São Carlos

2023

Jonathan Tobias da Silva

Análise de vulnerabilidades em redes OPC UA industriais

Dissertação apresentada à Escola de Engenharia de São Carlos da Universidade de São Paulo, para obtenção do título de Mestre em Ciências - Programa de Pós-Graduação em Engenharia Elétrica.

Área de concentração: Sistemas Dinâmicos

Orientador: Prof. Dr. Ivan Nunes da Silva

São Carlos
2023

Jonathan Tobias da Silva

Análise de vulnerabilidades em redes OPC UA industriais

Dissertação apresentada à Escola de Engenharia de São Carlos da Universidade de São Paulo, para obtenção do título de Mestre em Ciências - Programa de Pós-Graduação em Engenharia Elétrica.

Data de defesa: 20 de fevereiro de 2024

Comissão Julgadora:

Prof. Dr. Ivan Nunes da Silva
Orientador

Prof. Dr. André Luís Dias
Convidado 1

Professor
Convidado 2

São Carlos
2023

Dedico este trabalho aos meus pais, Alessandra e Daniel, à minha noiva Carolina e ao meu irmão Nícolas. O apoio incondicional, amor e carinho que recebo de vocês são pilares fundamentais para me sustentar frente às adversidades da vida.

Muito obrigado!

AGRADECIMENTOS

Diante do desafio complexo enfrentado no desenvolvimento dessa dissertação de mestrado, envolvendo os mais variados obstáculos pessoais e profissionais, encontro-me, ao término dessa jornada, diante de uma oportunidade de expressar os sentimentos de gratidão que emergem dentro de mim.

*“The only way to do great work is to love what you do.
If you haven’t found it yet, keep looking. Don’t settle.
As with all matters of the heart, you’ll know when you find it.”*

Steve Jobs

RESUMO

SILVA, J.T. **Análise de vulnerabilidades em redes OPC UA industriais.** 2023. 64p. Dissertação (Mestrado) - Escola de Engenharia de São Carlos, Universidade de São Paulo, São Carlos, 2023.

O crescimento avançado da transformação digital, uma consequência direta da quarta revolução industrial, tem impulsionado de forma substancial a interconexão entre dispositivos e sistemas, introduzindo desafios significativos no âmbito da proteção de dados e sistemas críticos. A mudança de paradigma que caracteriza a convergência entre as tecnologias de informação e operacional requer uma análise criteriosa, sobretudo na indústria, cujos sistemas de automação e controle desempenham um papel central. Neste contexto, o protocolo OPC UA emerge como uma peça-chave ao permitir a transferência segura de informações entre uma variedade de dispositivos e sistemas. Não obstante, considerando a constante evolução das ameaças cibernéticas, é imprescindível adotar uma abordagem proativa na identificação e mitigação de vulnerabilidades. Esse estudo apresenta uma análise de vulnerabilidades em redes OPC UA, por meio da implementação de uma bancada experimental especialmente concebida para simular ataques cibernéticos. Os resultados da análise realizada na execução dos ataques de *sniffing* de pacotes, MITM e DoS, reforçam a resiliência destas redes e, simultaneamente, contribuem para o contínuo aprimoramento do protocolo em questão. Assim, a pesquisa desempenha um papel crucial ao proporcionar percepções valiosas e abordagens concretas para a proteção de IACSs em um ambiente caracterizado por uma rápida evolução tecnológica.

Palavras-chave: Segurança Cibernética. OPC UA. Vulnerabilidades. Ataques. IACS.

ABSTRACT

SILVA, J.T. **Vulnerability analysis in industrial OPC UA networks**. 2023. 64p. Dissertation (Master) - Escola de Engenharia de São Carlos, Universidade de São Paulo, São Carlos, 2023.

The rapid growth of digital transformation, a direct consequence of the Fourth Industrial Revolution, has substantially driven the interconnection of devices and systems, introducing significant challenges in the realm of data protection and critical system security. The paradigm shift characterizing the convergence of information and operational technologies demands careful scrutiny, particularly within the industrial sector, where automation and control systems play a central role. In this context, the OPC UA protocol emerges as a pivotal component, enabling secure information transfer among a variety of devices and systems. Nevertheless, given the constant evolution of cyber threats, it is imperative to adopt a proactive approach to identify and mitigate vulnerabilities. This study presents a meticulous analysis of vulnerabilities in networks OPC UA, implemented through a specially designed experimental setup to simulate cyberattacks. The results of the analysis, conducted through packet sniffing, Man in the Middle (MITM), and Denial of Service (DoS) attacks, reaffirm the resilience of these networks while simultaneously contributing to the ongoing improvement of the protocol in question. Thus, this research plays a crucial role in providing valuable insights and concrete approaches for safeguarding Industrial Automation and Control Systems (IACSs) in an environment characterized by rapid technological evolution.

Keywords: Cybersecurity. OPC UA. Vulnerabilities. Attack. IACS.

LISTA DE FIGURAS

Figura 1 – Número de publicações relacionadas ao OPC UA por ano	18
Figura 2 – Quantidade de publicações sobre a segurança em redes OPC UA nos últimos anos	20
Figura 3 – Quantidade de publicações sobre vulnerabilidades em redes OPC UA nos últimos anos	21
Figura 4 – Convergência de diferentes visões destacadas pela IoT	24
Figura 5 – Convergência dos tópicos de formação da IIoT	24
Figura 6 – Arquitetura Cliente-Servidor do OPC UA	28
Figura 7 – Infraestrutura de modelos do OPC UA	29
Figura 8 – Categorização da comunicação OPC UA no modelo de referência OSI .	30
Figura 9 – Processo de criação e encerramento de conexão no OPC UA	32
Figura 10 – Tópicos da convergência TI/TO	34
Figura 11 – Notificações de Incidentes recebidos pelo CERT.br nos últimos 10 anos	39
Figura 12 – Esquema geral da bancada experimental para ensaios de segurança cibernética	47
Figura 13 – Bancada experimental para ensaios de segurança cibernética	50
Figura 14 – Esquemático do ataque <i>Packet Sniffing</i>	51
Figura 15 – Resultados de captura do Wireshark durante o <i>sniffing</i> de pacotes . . .	51
Figura 16 – Esquemático do ataque MITM	52
Figura 17 – Esquemático do ataque DoS	53
Figura 18 – Fluxograma da metodologia proposta	57

LISTA DE TABELAS

Tabela 1 – Quantidade de publicações por categorias	19
Tabela 2 – Endereços IP e MAC dos equipamentos da rede OPC UA	57

LISTA DE QUADROS

Quadro 1 – Modos de segurança do OPC UA	33
Quadro 2 – Diferenças dos sistemas de TI e o IACS	35
Quadro 3 – Principais ataques cibernéticos industriais dos últimos anos	38
Quadro 4 – Metas estabelecidas para a pesquisa	63
Quadro 5 – Cronograma proposto para cumprimento das metas	64

LISTA DE ABREVIATURAS E SIGLAS

AI	<i>Artificial Intelligence</i>
ARP	<i>Address Resolution Protocol</i>
APT	<i>Advanced Persistent Threat</i>
CLP	Controlador Lógico Programável
CoAP	<i>Constrained Application Protocol</i>
DCS	<i>Distributed Control System</i>
IHM	Interface Homem-Máquina
IACS	<i>Industrial Automation and Control Systems</i>
SDI	Sistema de Detecção de Intrusão
IIoT	<i>Industrial Internet of Things</i>
IoT	<i>Internet of Things</i>
TI	Tecnologia da Informação
LGPD	Lei Geral de Proteção de Dados
MAC	<i>Media Access Control</i>
MQTT	<i>Message Queuing Telemetry Transport</i>
O-PAS	<i>Open Process Automation™ Standards</i>
OPAF	<i>Open Process Automation™ Forum</i>
OPC UA	<i>Open Platform Communications – Unified Architecture</i>
OSI	<i>Open Systems Interconnection</i>
TO	Tecnologia Operacional
SCADA	<i>Supervisory Control and Data Acquisition</i>
SOA	<i>Service Oriented Architecture</i>
TSN	<i>Time Sensitive Networking</i>
UTM	<i>Unified Threat Management</i>
XML	<i>Extensible Markup Language</i>

LISTA DE SÍMBOLOS

Γ Letra grega Gama

Λ Lambda

ζ Letra grega minúscula zeta

\in Pertence

SUMÁRIO

1	INTRODUÇÃO	15
1.1	Motivação e Justificativa	17
1.2	Objetivos	22
1.3	Estrutura dos Capítulos	22
2	REFERENCIAL TEÓRICO	23
2.1	Protocolos IoT e IIoT	23
2.1.1	Principais Aspectos do Protocolo OPC UA	25
2.1.1.1	Espaço de Endereçamento e Modelo de Informação	27
2.1.1.2	Métodos de Comunicação	28
2.1.1.3	Escopo de Proteção	29
2.1.1.4	Processo de Conexão Segura	31
2.2	Cybersecurity	33
2.2.1	Ataques em Redes Industriais	36
2.2.2	Análise e Descoberta de Vulnerabilidades	41
2.3	Trabalhos Correlatos	43
3	DESENVOLVIMENTO	46
3.1	Aspectos da Bancada Experimental para Ensaios de Intrusão em Redes OPC UA	46
3.1.1	<i>Hardware</i>	46
3.1.2	<i>Software</i>	48
3.2	Ataques Cibernéticos em Redes Industriais OPC UA	49
3.2.1	<i>Packet Sniffing</i>	49
3.2.2	<i>Man in The Middle (MITM)</i>	52
3.2.3	<i>Denial of Service (DoS)</i>	52
3.3	Metodologia	56
3.3.1	Aquisição de Dados	56
4	RESULTADOS E DISCUSSÕES	60
4.1	Resultados Esperados	60
5	CONSIDERAÇÕES PARCIAIS	62
5.1	Conclusões	62
5.2	Trabalhos Futuros	62
6	CRONOGRAMA PROPOSTO	63

1 INTRODUÇÃO

A tecnologia atual tem impulsionado significativamente o nível da troca de informações nas mais diversas áreas do mundo, provocando mudanças substanciais em nossa forma de viver, enfrentar desafios e relacionar. Especialmente no setor industrial, essa transformação exige uma gestão de dados que esteja intrinsecamente vinculada ao aprimoramento da eficiência e produtividade.

Esse movimento de transformação digital ficou conhecido como a quarta revolução industrial, ou Indústria 4.0, caracterizando-se pela integração de tecnologias avançadas como a internet das coisas industrial (IIoT, do inglês *Industrial Internet of Things*), Inteligência Artificial (AI, do inglês *Artificial Intelligence*) e processamento de dados em larga escala (também denominados como *Big Data* e *Data Warehousings*).

À medida que o número de dispositivos interconectados e a quantidade de dados gerados por esses aumentam exponencialmente, a necessidade de estratégias robustas de segurança cibernética torna-se igualmente crucial, a fim de garantir a proteção da ampla exposição dessas informações às atividades maliciosas e ataques cibernéticos. De acordo com ??):

Conforme a sociedade continua a migrar para o mundo digital, a ameaça do crime cibernético se torna grande, custando rotineiramente às organizações dezenas – até mesmo centenas – de milhões de dólares. Os custos não são apenas financeiros: infraestrutura crítica, coesão social e bem-estar mental também estão em risco.

As redes de comunicação industriais não estão imunes aos desafios que surgem com o aumento exponencial na troca de informações. A interconexão de sistemas em um ambiente industrial requer uma abordagem especializada para enfrentar as crescentes ameaças cibernéticas que acompanham essa revolução tecnológica. Portanto, é imperativo que as empresas que operam nesse setor invistam e se desenvolvam em duas áreas de tecnologia fundamentais: da informação (TI) – que desempenha um papel crucial na gestão abrangente da informação – e operacional (TO) – que abrange os Sistemas de Automação e Controle Industrial (IACS, do inglês *Industrial Automation and Control Systems*) –, a fim de fortalecer os sistemas de defesas existentes ou desenvolver novas metodologias de defesa.

Até muito recentemente, essas duas áreas de tecnologia (TI e TO) eram separadas nos níveis técnico e organizacional. A transformação digital supracitada, gerou alguns gatilhos, principalmente no setor industrial, obrigando as organizações a reverem esse paradigma e liderar projetos de convergência entre os dois mundos (??). A convergência

TI/TO, conforme definida na literatura (??????), apresenta um desafio significativo para as empresas ao propor a descompartimentação dos dados e a intercambialidade de pilares (*e.g.*, a implementação da computação em nuvem no monitoramento dos processos de IACS).

À medida que os processos oriundos dessa convergência se tornam mais precisos e complexos, aumenta-se a relevância da transmissão de dados entre os equipamentos que os controlam. Assim, os protocolos de comunicação emergem como componentes de importância primordial na convergência TI/TO, pois desempenham um papel fundamental na viabilização da integração eficiente e segura entre esses dois domínios de tecnologia. A interoperabilidade e intercambialidade de um sistema, antes não apresentadas por protocolos industriais proprietários, passam a ser características fundamentais nesse contexto. Desse modo, o protocolo OPC UA (do inglês *Open Platform Communications Unified Architecture*) assume uma posição de destaque e relevância ao estabelecer as bases para a troca de informações contínua, segura e confiável entre dispositivos e sistemas de diferentes origens e finalidades.

O OPC UA é um protocolo de comunicação amplamente utilizado para aplicações IIoT e de automação industrial, no qual foi projetado para fornecer uma camada de comunicação segura e confiável para cenários da Indústria 4.0. Sua construção baseou-se nas seguintes preocupações de segurança, de acordo com ??): autenticação de usuários/instâncias de aplicativos (software), confidencialidade e integridade ao assinar e criptografar mensagens, disponibilidade por processamento mínimo antes da autenticação e auditabilidade por eventos de auditoria definidos para operações OPC UA. Assim, o OPC UA é amplamente reconhecido como um protocolo seguro, uma vez que incorpora todos os elementos fundamentais para assegurar a comunicação industrial, conforme identificado por ??). Esse conjunto de medidas de segurança o torna um pilar confiável para a infraestrutura de comunicação em ambientes industriais modernos, cuja integridade e segurança dos dados são de suma importância.

No entanto, a despeito dessa concepção robusta emeticulamente direcionada para a segurança que caracteriza o protocolo OPC UA, é imperativo reconhecer a dinamicidade do cenário atual de segurança cibernética. A evolução tecnológica supramencionada e as táticas adversárias à ética podem resultar no surgimento de novas ameaças e vulnerabilidades a esse protocolo, além da possibilidade de ser significativamente afetado por várias opções de configuração de segurança. Logo, uma postura proativa é crucial para continuar mitigando as ameaças emergentes e assegurando a resiliência desse ecossistema industrial. A vigilância e a análise de novas vulnerabilidades são requisitos indispesáveis para o aprimoramento contínuo do OPC UA.

A análise sistemática de vulnerabilidades proporciona uma visão crítica das possíveis brechas que possam surgir, permitindo uma abordagem preventiva e corretiva na

implementação de soluções adequadas. Ao identificar potenciais pontos de risco no protocolo industrial, é possível adotar medidas de segurança proativas, tais como: atualizações sistêmicas ou estruturais, ajustes de configuração e o estabelecimento de políticas rigorosas. Essa análise, uma vez bem executada, não apenas identifica fragilidades, mas também orienta as estratégias de proteção, concebendo à organização uma posição privilegiada para se comportar de maneira ágil e eficaz contra uma ameaça ou ataque cibernético.

Neste trabalho, uma análise de vulnerabilidades em redes industriais OPC UA é realizada com o intuito de fornecer uma abordagem estruturada de avaliação da segurança do protocolo. Adota-se a criação de uma bancada experimental como ambiente industrial de simulação de ataques cibernéticos. Ao aplicar a abordagem proposta, pretende-se contribuir para o fortalecimento da resiliência dessas redes, assim como colaborar com o desenvolvimento do OPC UA.

1.1 Motivação e Justificativa

A investigação de trabalhos na comunidade científica foi utilizada como justificativa da dissertação e motivação ao tópico proposto. Duas buscas principais foram realizadas para que o tema do trabalho fosse definido: a primeira (I) relacionada ao panorama, desafios e oportunidades do protocolo OPC UA no cenário atual, e a segunda (II) com foco no principal gargalo do protocolo observado na pesquisa anterior.

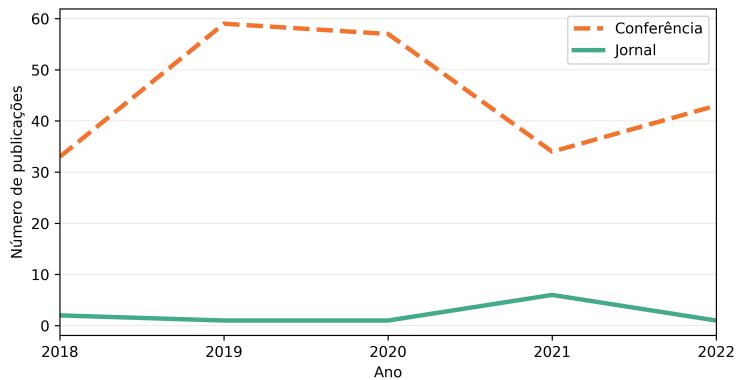
Mediante uma pesquisa sistemática de publicações relacionadas ao protocolo OPC UA na base de dados IEEE Xplore, considerando publicações entre os anos 2018 e 2022, escritas em inglês e aplicando critérios de exclusão, 238 publicações (Artigos, Jornais, Revistas, Atas de Conferências, etc.) foram classificadas em categorias, e seus resultados apresentados e discutidos a fim de fornecer uma visão geral do protocolo e investigar os desafios e oportunidades de sua aplicação em ambientes industriais atuais.

Inicialmente, utilizaram-se diferentes formas de escrita para o termo ‘OPC UA’ como *Author Keywords* nessa pesquisa inicial, como: ‘OPC-UA’, ‘OPC:UA’ e ‘OPC Unified Architecture’, resultando em 263 publicações. A relevância das publicações foi avaliada e, posteriormente, os seguintes critérios de exclusão foram aplicados para eliminar as publicações que não forneciam informações pertinentes:

- O foco principal da publicação não é em redes de comunicação industrial ou em Internet das Coisas (IoT, do inglês *Internet of Things*), apesar do OPC UA ser utilizado no projeto de pesquisa;
- O OPC UA é referenciado na publicação, mas não é um tópico relevante da mesma;
- Publicações que se concentram em *marketing* de produtos e não priorizam o OPC UA como protocolo central ou recurso.

Após a aplicação dos critérios supracitados, um total de 238 publicações foram identificadas e submetidas a uma análise quantitativa. Entre as publicações selecionadas, 227 (95%) foram publicadas em anais de conferências, enquanto 11 (5%) foram publicadas em revistas científicas. A distribuição das publicações por jornais e conferências por ano é ilustrada na Figura 1.

Figura 1 – Número de publicações relacionadas ao OPC UA por ano



Fonte: elaborada pelo autor.

Após uma leitura e análise cuidadosas, as publicações identificadas foram classificadas nos tópicos sugeridos, conforme apresentado abaixo, seguidos da sua respectiva descrição:

- Integração e Teoria (TI): integração do protocolo com diferentes sistemas, dispositivos e aplicativos por meio de um modelo de dados comum, assim como sobre sua teoria baseada em padrões como IEC 61499 e IEC 62541 e trabalhos de pesquisa existentes;
- Desenvolvimento de Produto (PD): criação de novos servidores, clientes, *frameworks* e modelos de informação para expandir a funcionalidade e compatibilidade do OPC UA, fornecendo uma base para novos sistemas e aplicativos industriais;
- Segurança (S): enfatiza significativamente a segurança, ao utilizar autenticação, criptografia e controle de acesso para proteger os dados e sistemas industriais contra ameaças cibernéticas, ou analisar as implicações de segurança da implementação do protocolo em um sistema;
- Análise de Desempenho (PA): análise do desempenho do protocolo, identificação de gargalos e indicação de possíveis melhorias para o desempenho geral do sistema, utilizando medidas como latência, variação de latência, perda de pacotes, taxa de

transferência, entre outras métricas para avaliar o comportamento do sistema e verificar a conformidade com os requisitos aplicáveis;

- Comparação de Protocolo (PC): comparação com outros protocolos de comunicação industrial e IoT, principalmente com base em indicadores de desempenho;
- Diagnóstico e Monitoramento (DM): oferece recursos de diagnóstico e monitoramento, tais como: monitoramento da saúde do sistema, gerenciamento de alarmes e notificação de eventos, a fim de garantir a disponibilidade do sistema e reduzir o tempo de inatividade;
- Comunicação Wireless (W): principal característica da rede é a utilização do protocolo OPC UA através de uma comunicação sem fio;
- Outros (O): abrange uma ampla gama de áreas de pesquisa relacionadas à tecnologia OPC UA, como modelagem de dados, interoperabilidade semântica, virtualização, computação em nuvem e computação de borda.

A presente análise tem implicações significativas para identificar lacunas no estado atual da pesquisa na comunidade científica. Um artigo foi desenvolvido, submetido à *IEEE/IAS International Conference on Industry Applications* e aceito para publicação, cuja discussão mais integralizada em relação aos trabalhos atuais para cada categoria é apresentada. A literatura existente sobre OPC UA é notavelmente carente de trabalhos que explorem a intersecção entre segurança e comunicação sem fio, o que representa uma lacuna crítica. A Tabela 1 fornece um resumo abrangente dos tópicos abordados nas publicações identificadas ao longo do período estudado, permitindo uma avaliação sistemática das tendências e padrões na comunidade científica ao longo dos últimos anos.

Tabela 1 – Quantidade de publicações por categorias

Ano	TI	PD	S	PA	PC	DM	W	O
2018	14	12	4	5	2	2	2	6
2019	21	20	6	10	10	10	8	10
2020	22	13	6	8	10	13	6	15
2021	17	16	4	12	6	3	7	3
2022	12	18	5	7	7	5	3	10
Total	86	79	25	42	35	33	26	44

Fonte: elaborada pelo autor.

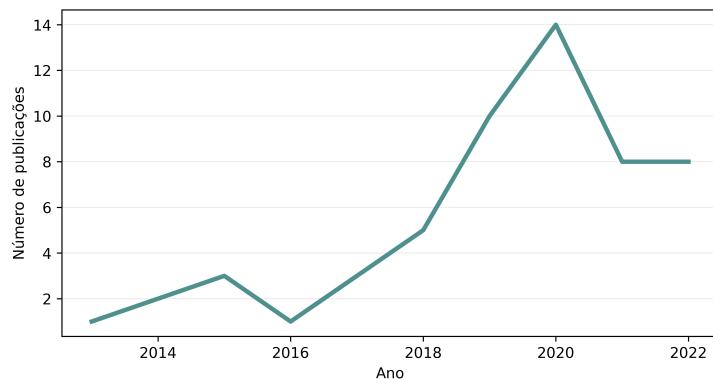
A segurança tem historicamente recebido uma proporção menor de atenção na área de pesquisa. Isso pode ser atribuído ao fato de que o OPC UA foi projetado para

incorporar medidas de segurança, incluindo criptografia, autenticação e autorização (??). Tal abordagem abrangente de segurança, aliada às recomendações e diretrizes de melhores práticas fornecidas pela fundação desenvolvedora, a *OPC Foundation*, contribuiu para uma redução notável na quantidade de pesquisas dedicadas a esse tópico específico.

As descobertas desse estudo inicial foram significativas ao fornecer uma visão geral e atual do protocolo OPC UA, destacando a necessidade de manter um interesse vigilante na área de segurança, a fim de garantir resiliência do protocolo frente às ameaças constantes a esses sistemas. Assim, uma nova análise quantitativa foi realizada visando o aprofundamento nos trabalhos com esse foco, especificamente naqueles atinentes à segurança cibernética nesse tipo de rede. Para isso, utilizou-se as bases de dados: IEEE Xplore, Web of Science e Scopus.

Em uma pesquisa inicial, os termos ‘OPC UA’ e ‘*Security*’ foram empregados como *Keywords*, repetindo os mesmos critérios de inclusão relatados na pesquisa anterior. Entretanto, não se aplicou nenhum critério de exclusão. A Figura 2 apresenta os resultados separados por ano, de 2013 até o de 2022.

Figura 2 – Quantidade de publicações sobre a segurança em redes OPC UA nos últimos anos



Fonte: elaborada pelo autor.

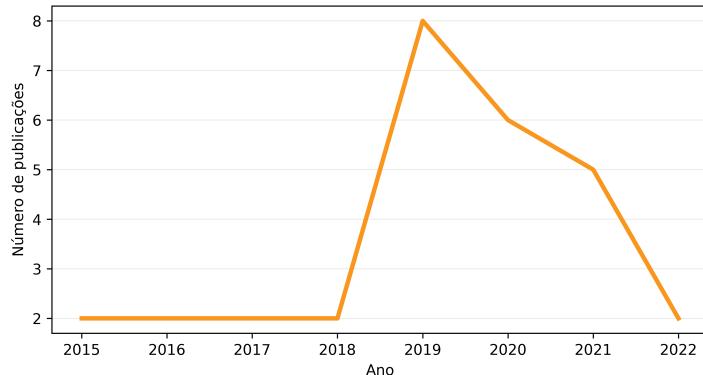
A análise sobre o panorama das publicações relacionadas à segurança em redes OPC UA ao longo da última década, evidencia um notável crescimento na quantidade de trabalhos sobre o tema, indicando um interesse crescente e uma conscientização ampliada acerca dos desafios de segurança envolvendo esse protocolo. No entanto, a partir do ano de 2021, observa-se um fenômeno de diminuição e posterior estagnação nessa produção acadêmica e técnica. Essa tendência decrescente pode derivar de uma combinação de fatores, como: a possibilidade de que muitos aspectos cruciais tenham sido já discutidos e explorados, a influência de outros tópicos emergentes na segurança cibernética, ou até

mesmo considerações externas que impactaram a dinâmica da pesquisa e publicação (*e.g.*, pandemia de COVID-19).

Seguidamente, a estrutura de pesquisa abaixo foi empregada a fim de filtrar aqueles trabalhos relacionados à análise de vulnerabilidades em redes OPC UA, aplicando como critérios de inclusão: publicações no período de 2013 a 2022, escritas em inglês. Entende-se ‘TKA’ pela junção dos campos *title*, *keywords* e *abstract*. Os resultados estão descritos na Figura 3.

```
("TKA":"OPC UA" OR "TKA":"OPC-UA" OR "TKA":"OPC:UA" OR "TKA":"OPC Unified
→ Automation") AND ("TKA":"Vulnerabilities" OR "TKA":"Vulnerabilities
→ Analysis" OR "TKA":"Vulnerabilities Assessment")
```

Figura 3 – Quantidade de publicações sobre vulnerabilidades em redes OPC UA nos últimos anos



Fonte: elaborada pelo autor.

A avaliação desses resultados conduz a uma conclusão que, embora semelhante à anterior, revela uma oscilação notória. No ano de 2019, um pico significativo na quantidade de artigos publicados denota um interesse acentuado e um maior reconhecimento por parte da comunidade científica acerca das vulnerabilidades associadas ao OPC UA. Entretanto, a partir de 2020, constata-se uma inversão na tendência, com uma redução na quantidade de publicações. Esse declínio pode estar relacionado a diversos fatores interconectados, conforme descrito anteriormente. Contudo, vale ressaltar a importância do tema do presente estudo, uma vez que se sabe a incerteza da natureza das ameaças e a dinâmica das vulnerabilidades em ambientes industriais utilizando esse protocolo.

1.2 Objetivos

Tendo em vista a relevância do tema, o presente estudo propõe uma investigação detalhada de ataques cibernéticos em redes OPC UA, visando desenvolver, implementar e validar uma bancada experimental para simulações de intrusões em sistemas de automação e controle industriais. Busca-se compreender as potenciais fragilidades que podem comprometer a segurança destas redes, identificando os principais pontos de risco e explorando possíveis contramedidas para mitigar as ameaças identificadas.

Observa-se um caráter desafiador ao objetivo, uma vez que a complexidade e a diversidade dos dados trafegados pelas camadas do protocolo demandam um alto grau de especialização em segurança cibernética e técnicas avançadas de engenharia de redes.

Dentro desse contexto, os objetivos específicos a serem atingidos pela metodologia proposta são:

- Investigar e compreender os princípios e conceitos fundamentais das redes OPC UA, a fim de identificar os principais desafios e ameaças relacionados à segurança nestas redes;
- Propor e desenvolver uma bancada experimental como ambiente industrial de simulação de ataques cibernéticos;
- Investigar, selecionar e aplicar alguns ataques comuns para IIoT e demonstrar a reação do protocolo OPC UA às intrusões na rede;
- Analisar o cenário de ataque do ponto de vista do invasor, a fim de identificar os desafios da segurança, encontrar possíveis novas vulnerabilidades e propor contramedidas para mitigação.

1.3 Estrutura dos Capítulos

Esta dissertação está estruturada em capítulos que abordam os diferentes aspectos dos trabalhos desenvolvidos. O Capítulo 2 apresenta uma revisão abrangente da literatura relacionada ao tema, incluindo os conceitos teóricos fundamentais das redes OPC UA, os princípios essenciais da segurança cibernética e as técnicas de análise de vulnerabilidades aplicadas a essas redes. Além disso, são discutidos trabalhos anteriores relevantes para o contexto deste estudo. No Capítulo 3, os principais componentes e materiais empregados na montagem da bancada experimental para a realização dos ensaios de intrusão são detalhados. Também são descritos em pormenor os ataques cibernéticos selecionados e a metodologia adotada para sua análise. Os resultados esperados são apresentados no Capítulo 4. Por fim, o Capítulo 6 delinea o cronograma proposto para a conclusão bem-sucedida deste programa de mestrado.

2 REFERENCIAL TEÓRICO

Este capítulo serve como uma base para a compreensão dos fundamentos teóricos e estruturas conceituais que informam a pesquisa, aprofundando-se na literatura relevante e nos conceitos teóricos associados às redes OPC UA, fundamentos da segurança cibernética e a aplicação de técnicas de análise de vulnerabilidades para aprimorar a segurança dessas redes. Ao examinar a base de conhecimento existente, uma estrutura teórica é estabelecida, a fim de formular estratégias eficazes e garantir a implementação bem-sucedida da abordagem proposta. O capítulo é finalizado com alguns estudos correlatos e como se diferem do presente trabalho.

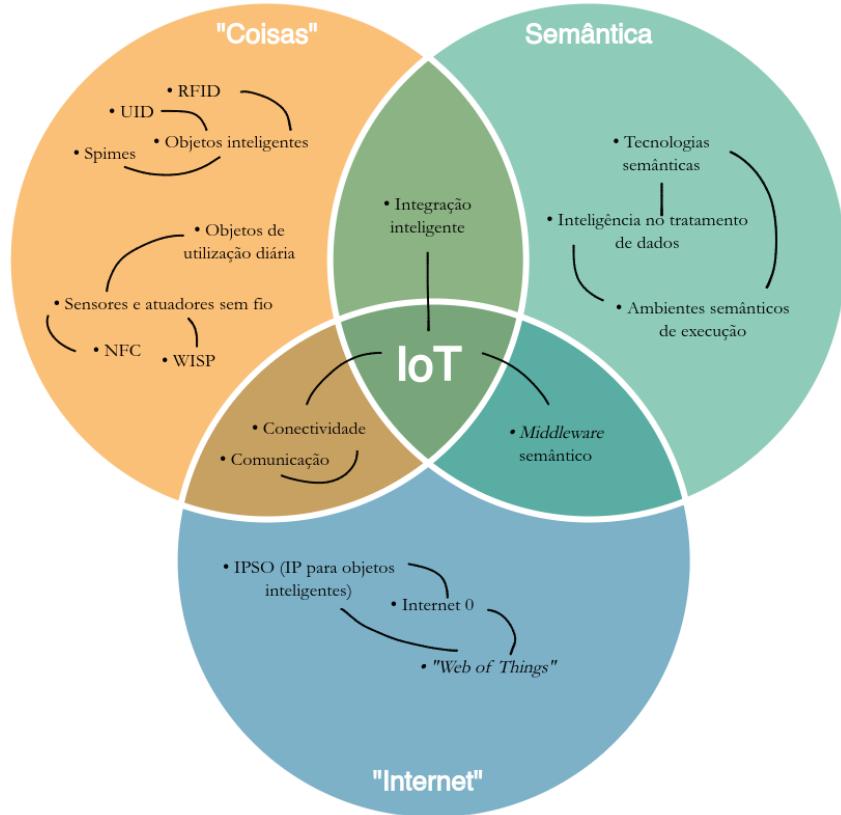
2.1 Protocolos IoT e IIoT

A Indústria 4.0 se materializou em diversas esferas, tratando-se como a integração de inúmeras possibilidades de tecnologias para atender as demandas do mercado, tanto em relação às transformações da forma de como os processos de manufatura e máquinas são feitos, como também em relação às grandes mudanças de modelos de negócios (??). Esta onda de inovação está impulsionando as organizações a investirem em novas tecnologias, incluindo Internet das Coisas e IIoT, transformando-as em realidade diária ao revolucionar como dispositivos, sistemas e aplicativos interagem e colaboram.

De acordo com ??), o termo IoT foi utilizado pela primeira vez em 1999, por Kevin Ashton, que trabalhou em um padrão para marcar objetos em aplicações de logística, utilizando RFID. Desde então, os pesquisadores referem-se à expressão como a interconexão de objetos cotidianos incorporados com sensores, atuadores e capacidades de comunicação. No entanto, devido ao crescimento exponencial dos protocolos de comunicação inteligentes e da conectividade distribuída advindos dessa tecnologia, a quarta revolução incorporou essas características positivas nos processos industriais e no desenvolvimento de produtos, que, consequentemente, começaram a ter seus dados otimizados dinamicamente. A Figura 4 apresenta a convergência de diferentes visões destacadas pela IoT.

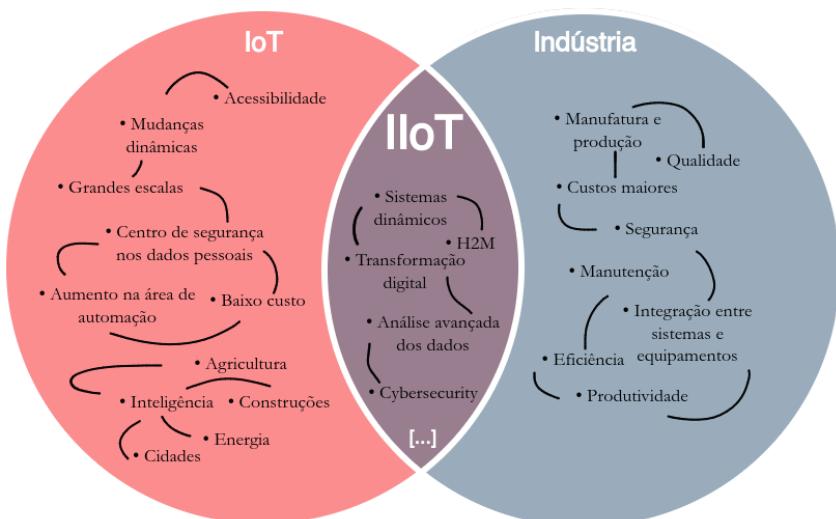
Para fortalecer o desenvolvimento no âmbito industrial, surgiu o IIoT como um novo tipo de ecossistema que envolve todos os domínios de logística, fabricação, gerenciamento e desenvolvimento. Concentra-se especificamente na aplicação da IoT em ambientes industriais, viabilizando aprimoramentos em automação e eficiência e produtividade em variados setores (*e.g.*, manufatura, energia, transporte e saúde). A Internet das Coisas Industrial não apenas envolve elementos de *software* tradicionais, mas também requer controladores e sensores de *hardware*, bem como plataformas de serviços em nuvem, para alcançar o domínio inteligente (??). A Figura 5 ilustra a convergência dos tópicos de formação da IIoT.

Figura 4 – Convergência de diferentes visões destacadas pela IoT



Fonte: adaptada de (??)

Figura 5 – Convergência dos tópicos de formação da IIoT



Fonte: elaborada pelo autor.

Em sua escala, alcance e complexidade, a transformação digital, oriunda da atual revolução tecnológica, apresenta à sociedade desafios singulares ao alterar radicalmente nosso modo de viver e interagir. Intrinsecamente conectada à incessante troca de informações, ela atribui uma alta significância para as formas de transmissão, coleta e tratamento desses dados, que, cada vez mais abundantes, trazem informações mais completas e suficientes.

Para que os dispositivos de transmissão de informações se comuniquem, uma linguagem formal deve ser especificada. De modo análogo à comunicação humana, estabelecer um diálogo compreensível torna-se uma tarefa árdua quando as partes envolvidas não compartilham o mesmo dialeto. Dessa forma, as linguagens especificam um conjunto de regras que asseguram uma comunicação cognoscível e a interoperabilidade entre sistemas, dispositivos e pessoas em diversos contextos.

Tanto a IoT quanto a IIoT dependem de protocolos robustos para estabelecer canais de comunicação confiáveis e seguros. Esses protocolos desempenham um papel crucial ao permitir o monitoramento, controle e gerenciamento em tempo real das implantações. Compreender os conceitos fundamentais e as características desses, é essencial para implementar e aproveitar efetivamente o potencial das tecnologias da (I)IoT.

O termo protocolo, de acordo com (??), caracteriza o conjunto de regras e orientações que redigem a comunicação e interação entre diferentes entidades ou sistemas, estabelecendo o formato, a ordem e o significado das mensagens trocadas. Projetado principalmente para garantir a interoperabilidade entre sistemas de vários fornecedores, um protocolo também simplifica a integração e o comissionamento de redes de comunicação de dados, reduzem os custos de instalação e permitem testes e validações independentes, o que, por sua vez, leva a projetos mais eficientes (??).

Os protocolos de comunicação existentes, tanto os originalmente projetados para ambientes industriais quanto os para a IoT, não oferecem as características necessárias para a quantidade cada vez maior de dispositivos conectados (??). Por essa razão, um novo conjunto de protocolos escaláveis e leves surgiu, dos quais se destacam o OPC UA, MQTT, CoAP, entre outros. No entanto, neste trabalho, o protocolo OPC UA é o único abordado, uma vez que representa o foco central desta investigação.

2.1.1 Principais Aspectos do Protocolo OPC UA

Open Platform Communications (OPC, anteriormente conhecido como *OLE for Process Control*), desenvolvido pela OPC Foundation, é um padrão de comunicação amplamente utilizado por vários anos nos mais diversificados setores da tecnologia da informação e automação industrial. De acordo com ??), o OPC tem sido muito aceito nas últimas décadas como o padrão industrial mais popular entre usuários e desenvolvedores. A maioria dos fornecedores de IHM (Interface Homem-Máquina), SCADA (do inglês *Supervisory Control and Data Acquisition*), e DCS (do inglês *Distributed Control System*)

da área, oferecem a tecnologia OPC como parte integrada de seus produtos.

Duas etapas principais compõem o desenvolvimento desta tecnologia: (I) OPC Classic, e (II) OPC UA. Em suma, o Classic fornece padrões de interface de comunicação neutros (no âmbito de fornecedores) para controle de processo e sistemas de automação de manufatura, incluindo acesso a dados (OPC DA), alarmes e eventos (OPC A&E) e acesso a dados históricos (OPC HDA). Ele resolve a integração perfeita de dispositivos de campo, dispositivos de controle e sistemas de *software* de automação (e.g., SCADA), melhorando a abertura e a interoperabilidade do sistema (??). No entanto, o produto desenvolvido na primeira etapa é limitado em sua capacidade de realizar aplicações integradas e em plataformas distintas e, principalmente, carece de tecnologias que o transformam em um protocolo de comunicação seguro. É por esse, e outros motivos, que a versão *Unified Architecture* do OPC foi criada. Segundo ??):

O OPC UA não foi planejado apenas como uma nova versão da interface padrão OPC, mas sim como uma nova visão de interoperabilidade "global" e troca de dados padronizada entre aplicações de *software* independentes de fornecedores, linguagens de programação, sistemas operacionais e localização [...], ao implementar independência de plataforma, escalabilidade, alta disponibilidade, capacidade de Internet, entre outras características nesse novo protocolo.

Aproveitando as tecnologias de Serviços Web, XML e .NET, o UA é caracterizado por sua definição de objeto unificado e apresenta uma arquitetura completamente orientada a serviços (SOA, do inglês *Service Oriented Architecture*). Também pode ser integrado com as mais recentes tecnologias, como: *Time Sensitive Networking* (TSN) e 5G (??), e os dados de comunicação podem ser codificados usando diferentes métodos. Dentre as principais vantagens do protocolo, se destacam:

- Independência de plataforma: por oferecer diferentes pilhas de *software* em C/C++, .Net e Java, é possível desenvolvê-lo em vários sistemas e dispositivos embarcados, não limitando apenas à plataforma da Microsoft, como no OPC Classic;
- Mecanismos de segurança aprimorados: inclui um conjunto completo de mecanismos de comunicação segura, na qual requer autenticação de duplo sentido para ambos os certificados e estabelecimento de canais seguros;
- Modo de acesso unificado aos dados: ao integrar os dados atuais, notificações de eventos e histórico no mesmo espaço de endereço na modelagem de informações, o OPC UA unifica as diferentes funções anteriores, por meio de apenas uma chamada;
- Supporte a estruturas de dados complexas: as especificações existentes oferecem apenas uma organização hierárquica simples de itens, enquanto o OPC UA oferece

metamodelos de informações que podem ser facilmente estendidos, sendo possível incluir e excluir as ligações entre esses modelos de dados.

Todas as especificações lançadas pela OPC Foundation para o protocolo OPC UA estão disponibilizadas em 24 partes, pela última versão de lançamento 1.05.02 do documento ‘OPC UA Specification’ (??). As partes 1 a 7 do documento apresentam as principais características da tecnologia, assim como o modo de segurança, espaço de endereçamento, conjunto de serviços, modelo de informação padrão, mapeamentos e perfis de serviço. As partes 8 a 13 estão relacionadas às definições de tipo de acesso a dados gerais padrão, como acesso a dados, alarmes e condições, programas, acesso histórico, descoberta e agregados. Alguns dos principais conceitos teóricos do protocolo concernentes para esta dissertação estão apresentados nas subseções abaixo, como o *Address Space*, o *Information Model*, a transmissão dos dados, a segurança implementada em cada camada e o processo de conexão entre um cliente e servidor OPC UA.

2.1.1.1 Espaço de Endereçamento e Modelo de Informação

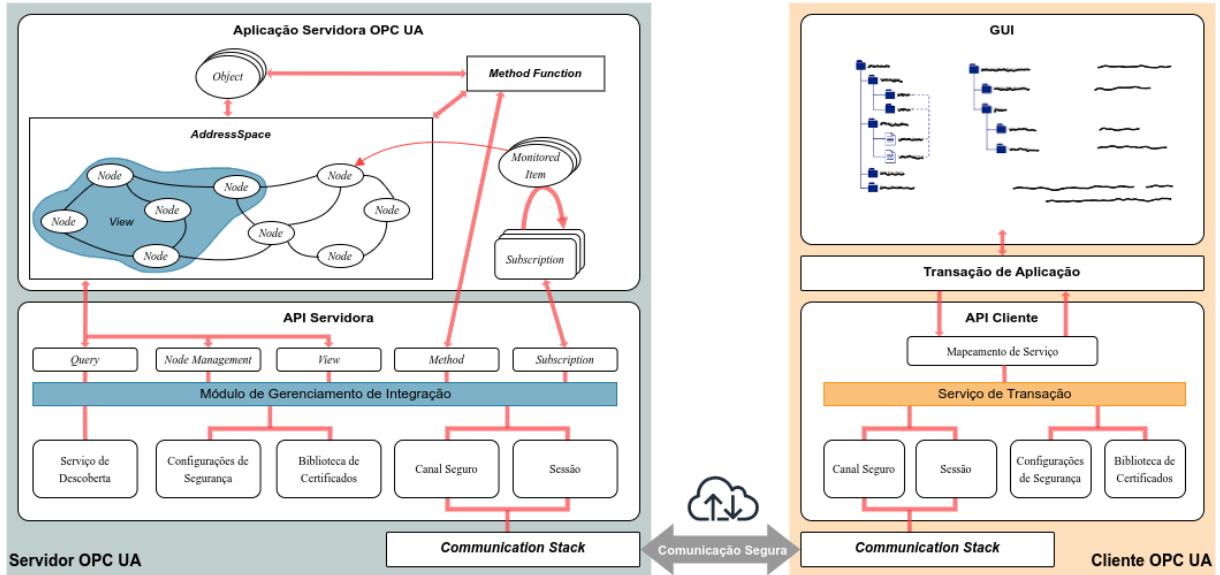
Conceitua-se de forma concisa o Espaço de Endereço e Modelo de Informação (do inglês *Address Space* e *Information Model*) como, respectivamente, a fundação e componente central do OPC UA. Pode-se equiparar esses dois conceitos, analogamente, à estrutura óssea e ao coração no corpo humano, na devida ordem supracitada. O *Address Space* representa uma ampla variedade de informação, incluindo instâncias de objetos, variáveis e tipos (??). O OPC UA propõe um *Address Space* consistente e um modelo de serviço, e isso ajudará a unificar dados, eventos e informações históricas no espaço de endereço do mesmo servidor (??).

Os *Nodes* se caracterizam como os componentes em um Espaço de Endereço, sendo que cada um recebe uma classe correspondente a um elemento específico do modelo de objeto (do inglês *Object Model*), incluindo variáveis, métodos e eventos. Essas classes servem coletivamente como os ‘metadados’ do *Address Space* e cada *Node*, uma instância de uma classe.

A definição de classe contempla atributos e referências. Os Atributos (do inglês *Attributes*) formam os componentes fundamentais de uma classe e cada definição de atributo inclui um ID, nome, descrição, tipo de dados e indicadores de obrigatoriedade. As referências (do inglês *References*), por sua vez, indicam o relacionamento entre dois *Nodes* conhecidos, e uma referência é determinada exclusivamente pelo nó de origem, o de destino, a semântica da referência e a sua direção.

A Figura 6 apresenta a arquitetura cliente-servidor do OPC UA, ilustrando as conexões entre os conceitos supracitados.

Figura 6 – Arquitetura Cliente-Servidor do OPC UA



Fonte: adaptada de (??, Parte 6) e (??).

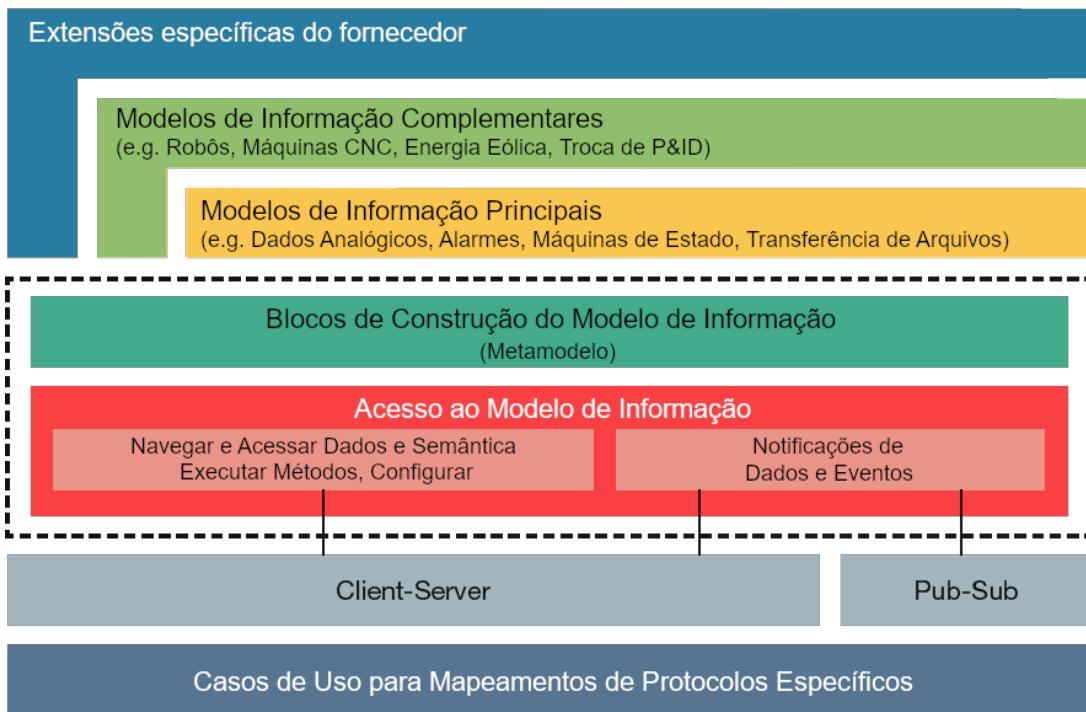
O *Information Model* é composto principalmente de *Nodes* e *References*, possibilitando a representação de diversas informações estruturadas e hierárquicas. Com funcionalidade abrangente orientada a objetos, até estruturas complexas de várias camadas podem ser modeladas e estendidas. O OPC UA oferece uma estrutura de modelo fundamental e a possibilidade de criação de outros complementares para aplicações específicas, a fim de aprimorar ainda mais o sistema.

A relação entre modelos de informação fundamental e específicos do usuário são representados na Figura 7. A aplicação OPC UA apresenta a flexibilidade em seu desenvolvimento por poder ser iniciada a partir de um Modelo de Informação principal ou complementar padronizado que se alinha conforme o domínio específico. Com isso, aproveitando a abordagem de modelagem orientada a objetos do protocolo e utilizando o conjunto predefinido de serviços de acesso e manipulação, a interoperabilidade excepcional pode ser alcançada pelo sistema (??).

2.1.1.2 Métodos de Comunicação

O OPC UA abrange mapeamentos de elementos independentes de protocolo para protocolos de transporte e segurança padronizados. Atualmente, a transmissão de dados pode ser realizada por meio de três métodos distintos: TCP/IP, SOAP/HTTP e HTTPS. Em termos de implementação de segurança, obrigatória para todas as variantes, o OPC UA define *UA Secure Conversation* e *WS Secure Conversation* para TCP/IP e SOAP/HTTP, como os respectivos protocolos (??).

Figura 7 – Infraestrutura de modelos do OPC UA



Fonte: adaptada de (??).

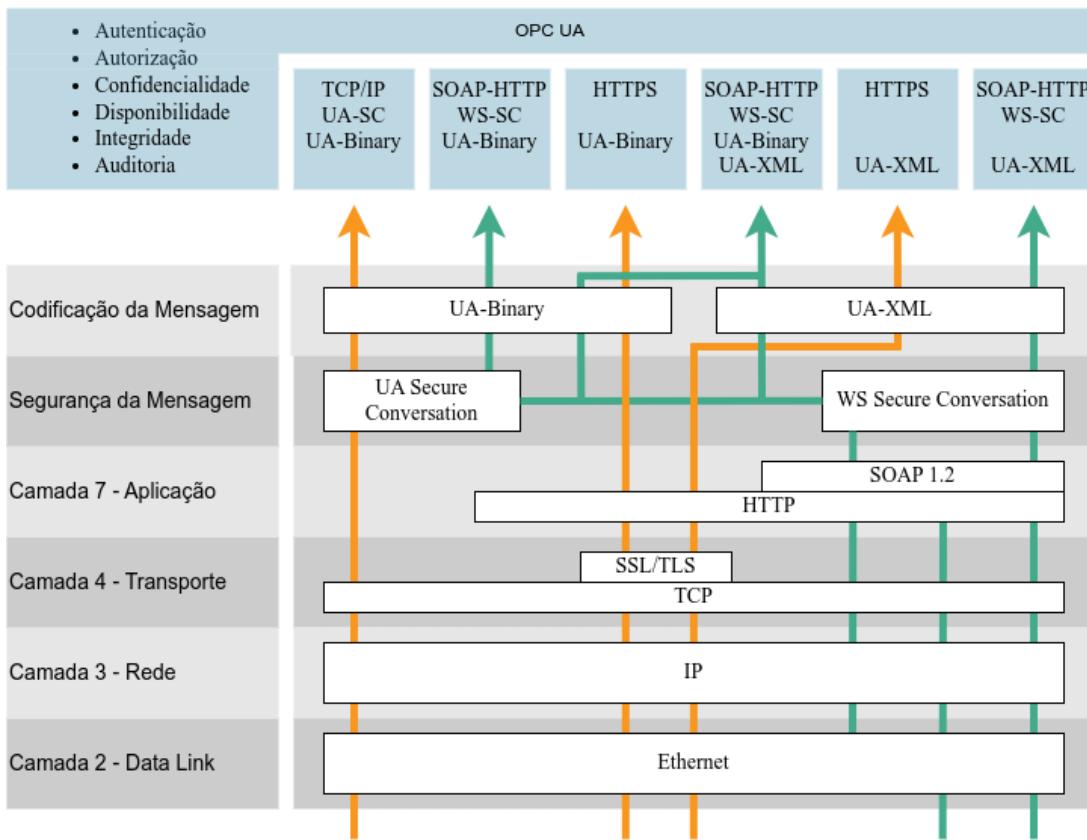
Em relação à codificação de mensagens e apresentações de dados, o OPC UA oferece duas opções principais: UA-XML e UA-*Binary*, nos quais utilizam, respectivamente, esquemas de codificação para Serviços Web e formatos binários, descritos na Parte 6 do documento de especificações (??), para comunicação eficiente em sistemas de alta velocidade ou embarcados. Com isso, permitem flexibilidade na escolha do formato apropriado para transmissão e representação de dados eficientes. A Figura 8 ilustra essas abordagens do UA categorizadas no modelo de referência OSI (do inglês *Open Systems Interconnection*), destacando os componentes de comunicação supracitados.

2.1.1.3 Escopo de Proteção

A segurança por muito tempo foi negligenciada, resultando no reconhecimento tardio de sua gravidade e na adoção vagarosa de medidas protetivas. Esse cenário foi especialmente evidenciado em ambientes industriais, cujas preocupações com segurança foram historicamente abordadas em conjunto com a TI. No entanto, à medida que a interconexão digital avança, a necessidade de proteção contra uma crescente gama de ataques cibernéticos em sistemas ciber-físicos tornou-se inegável, não apenas na camada de aplicação, mas em toda a infraestrutura desses ambientes críticos.

O OPC UA foi desenvolvido com foco na resolução desse problema histórico, ao tratar de questões desse tipo em diversas camadas. Seu escopo de proteção é dividido

Figura 8 – Categorização da comunicação OPC UA no modelo de referência OSI



Fonte: adaptada de (??).

na segurança da informação pela tríade CIA (do inglês *Confidentiality, Integrity and Availability*) e pelo *Framework AAA* - autenticação, autorização e auditoria.

Na camada de aplicação, a autenticação e a autorização do usuário são cruciais. Autenticar o acesso envolve a verificação da identidade do cliente usando métodos como: senhas, certificados X.509V3 ou *tokens* de segurança, conforme supracitado. Por outro lado, autorizar esse acesso implica na sua concessão ou negação a serviços específicos. A documentação de especificação do protocolo não alude como os usuários devem autenticar ou autorizar seus direitos, no entanto, fornece os meios para tal implementação. As aplicações OPC UA, tanto cliente quanto servidora, também devem se identificar durante o estabelecimento da comunicação segura usando certificados, permitindo aceite ou não da requisição.

A camada de comunicação fornece um canal seguro através do qual os dados são transmitidos do cliente para o servidor. Essa mensagem secreta é utilizada para derivar as *Symmetric Keys* do processo de criptografia dos dados requeridos e respondidos, garantindo a confidencialidade da comunicação ao impedir acessos não autorizados. Da mesma forma, a integridade é mantida por meio de assinaturas para verificar se as informações recebidas

pelo cliente correspondem ao que foi enviado pelo servidor. A subseção 2.1.1.4 detalha o procedimento envolvido no estabelecimento do canal seguro entre servidor e cliente OPC UA.

Por fim, as aplicações geram registros de auditoria que abrangem vários eventos, como tentativas de conexão, negociações de opções de segurança, alterações de configuração e sistema, interações do usuário e rejeições de sessão. O suporte a essas trilhas de auditoria de segurança é oferecido por meio de dois mecanismos: (I) a garantia da rastreabilidade entre os *logs*, por meio de um identificador local na solicitação; e (II) a definição de parâmetros para inclusão nos registros de auditoria (parâmetros descritos pela Parte 5 das especificações).

Mesmo com toda sua construção voltada para fortificar o sistema contra-ataques, o OPC UA encontra desafios de segurança internos e externos, visto que a diversidade de protocolos na transmissão das mensagens herda os riscos de segurança dos mesmos. Assim, o estabelecimento de tecnologias robustas de segurança de rede é imperativo para lidar efetivamente com esses desafios.

2.1.1.4 Processo de Conexão Segura

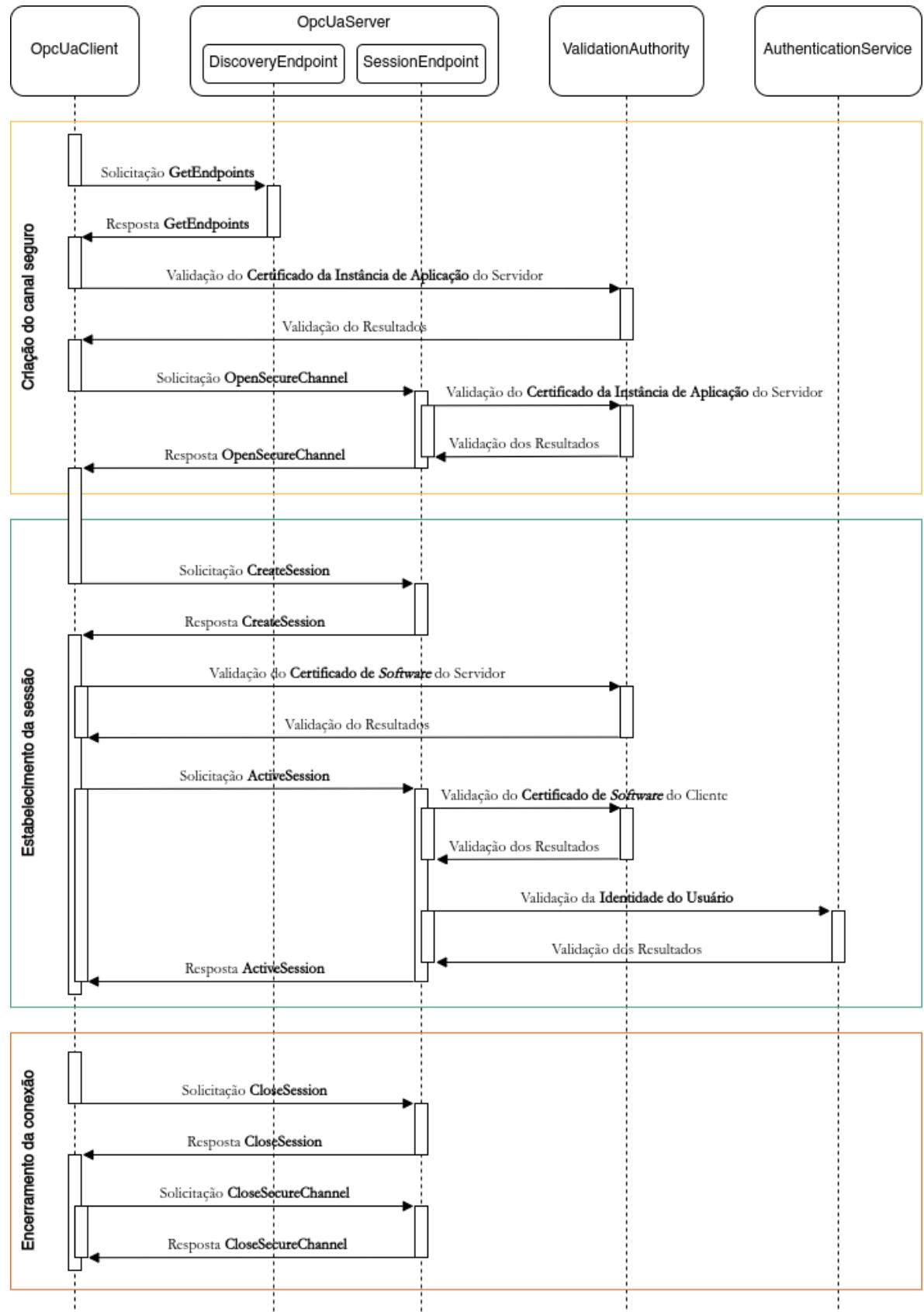
O canal seguro estabelecido em uma comunicação OPC UA deve respeitar uma série de medidas no estabelecimento e no término da conexão, como a negociação de segurança, a decisão do algoritmo criptográfico e as políticas e perfis de segurança utilizados. A Figura 9 apresenta o diagrama de sequências desse processo.

Na etapa da criação da conexão, as diferentes opções de configuração do servidor são coletadas pelo cliente, caso esse não esteja pré-configurado. Uma solicitação **GetEndpoints** não segura é enviada do cliente ao **DiscoveryEndpoint** do servidor, a fim de obter as descrições dos **Endpoints** de sessão existentes, incluindo a configuração de segurança. Uma vez que essas informações são coletadas, o cliente seleciona o **Endpoint** e valida o certificado da instância de aplicação do servidor.

A segunda etapa ocorre caso o certificado seja considerado confiável após a validação. Uma solicitação **OpenSecureChannel** é criada e enviada ao **Endpoint** de sessão do servidor, incluindo a Política de Segurança e Modo de Segurança. O OPC UA incorpora um modelo de segurança flexível que consiste em três modos, descritos pelo Quadro 1.

Para lidar com a ameaça central da permissão de clientes maliciosos à rede, é possível alcançar a disponibilidade e a integridade do conteúdo das mensagens no modo seguro **Sign**, uma vez que as identidades dos servidores e clientes podem ser verificadas através da infraestrutura de chave pública e certificados. Para criptografar o conteúdo da comunicação de rede, utiliza-se o modo **Sign&Encrypt**, garantindo também a confiabilidade desses dados.

Figura 9 – Processo de criação e encerramento de conexão no OPC UA



Fonte: adaptada de (??).

Quadro 1 – Modos de segurança do OPC UA

Modos	Descrição
<i>None</i>	<ul style="list-style-type: none"> • Nenhuma segurança
<i>Sign</i>	<ul style="list-style-type: none"> • Codificado com a chave privada do remetente • Somente o proprietário do certificado possui a chave privada • Qualquer pessoa pode verificar a identidade • Fornece autenticidade
<i>Sign&Encrypt</i>	<ul style="list-style-type: none"> • Adiciona criptografia para assinar • Codificação com chave pública do receptor • Qualquer pessoa pode criptografar • Somente o proprietário do certificado pode ler • Autenticidade, confidencialidade e integridade

Fonte: adaptado de (??).

Assim sendo, uma sessão é instaurada com base no canal seguro criado pela conexão, mediante uma solicitação de **CreateSession** devidamente protegida pelo cliente. Na resposta dos servidores, por sua vez, são fornecidos os certificados de *software*. A fase final do estabelecimento da comunicação é iniciada, então, após a validação bem-sucedida desses certificados por parte do cliente. Essa fase envolve a ativação da sessão criada através da solicitação **ActiveSession** ao servidor, cujas informações adicionais de credenciais do usuário e do *software* estão contidas. A validação dos dados complementares representa o encerramento dessa composição de conexão, permitindo que o cliente acesse e comunique-se com o servidor exitosamente.

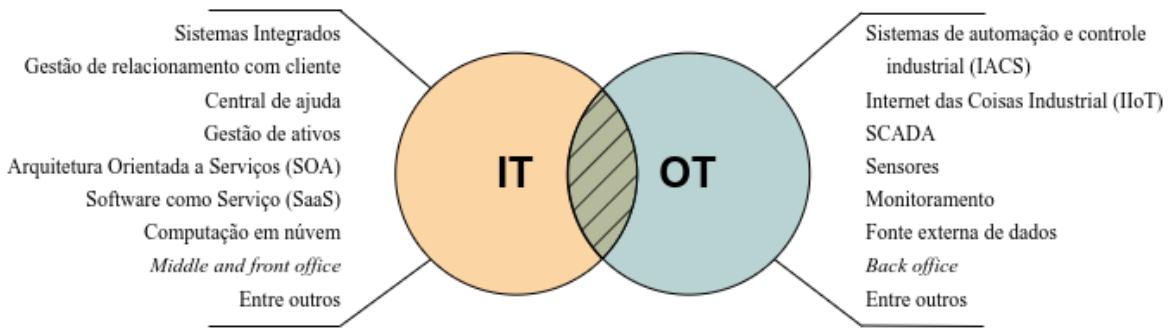
O encerramento de uma conexão OPC UA ocorre por meio das solicitações **CloseSession** e **CloseSecureChannel**. A especificação do OPC UA (??) afirma que as mensagens de encerramento sejam apenas assinadas, pois nenhuma informação secreta é transmitida nessa etapa.

2.2 *Cybersecurity*

No passado, os setores de tecnologia da informação e tecnologia operacional eram organizacionalmente separados. Atualmente, a transformação digital está pressionando a indústria a reconsiderar esse paradigma e implantar projetos de convergência que unam TI e TO em um mesmo conceito. A Figura 10 apresenta os principais tópicos abordados na convergência TI/TO. Essa convergência não está apenas gerando um desafio complexo em termos de comunicação de dados, mas também enfrentando uma classificação de preocupações de segurança cibernética (??).

Os Sistemas de Automação e Controle Industrial abrangem vários tipos de sistemas, incluindo SCADA, DCS (do inglês *Distributed Control System*), CLP (Controlador Lógico

Figura 10 – Tópicos da convergência TI/TO



Fonte: adaptado de (??).

Programável), sistemas de monitoramento, entre outros. A convergência TI/TO tornou os IACS mais complexos, poderosos e produtivos. Por outro lado, introduziu também novas vulnerabilidades a potenciais acidentes e incidentes relacionados com a segurança, aumentando drasticamente seu risco associado. Esses sistemas são alvos cada vez mais frequente de ataques devido ao valor dos dados e à sua importância crítica para a economia. O Quadro 2 resume os resultados da comparação das principais características e objetivos de segurança do IACS com os do sistema de TI.

Em 2022, a equipe de resposta a emergências cibernéticas em sistemas de controle industriais da Kaspersky (Kaspersky ICS CERT) revelou o estado atual e os desafios da segurança cibernética industrial em seu relatório de ameaças para sistemas de automação industrial (??) ao registrar 1.198.532 ataques, representando um aumento de 16,2% em relação ao ano anterior. Os ataques de *ransomware* e as ameaças persistentes avançadas (APT, do inglês *Advanced Persistent Threat*) foram as principais preocupações para os IACS durante o período analisado.

Adicionalmente, um estudo conduzido por ??) destacou a segurança cibernética como mais premente na adoção da IIoT. Isso sublinha a necessidade imperativa de que as empresas da área, juntamente com outros fatores críticos, como *Big Data*, Inteligência Artificial e *Software de Código Aberto*, coloquem a segurança cibernética no centro de suas prioridades, evidenciando a complexidade e a relevância crescente da segurança digital no cenário industrial atual.

De acordo com ??), a avaliação do risco de segurança cibernética de um sistema pode ser derivada como a interseção de três elementos: ativos, vulnerabilidades e ameaças. Na perspectiva de um IACS, ativos são objetos cibernéticos relacionados ao controle industrial – componentes de *hardware* e *software* – e devem ser protegidos pelo sistema. Vulnerabilidades são pontos fracos de ativos que podem ser explorados por ameaças.

Quadro 2 – Diferenças dos sistemas de TI e o IACS

	TI	IACS
Ambiente de configuração	<ul style="list-style-type: none"> • Equipamento padronizado • Ciclo curto de reposição de equipamentos • Fácil de corrigir e reparar • Use um sistema operacional universal • Velocidade e desempenho da rede 	<ul style="list-style-type: none"> • Equipamentos especializados conforme o processo • Poucos ciclos de substituição de equipamentos • Difícil de corrigir e reparar devido à disponibilidade do equipamento • SO de uso geral personalizado ou operação de SO autodesenvolvido • A comunicação de rede em tempo real é importante
Objetivos Críticos de segurança	<ul style="list-style-type: none"> • Bloqueio o vazamento de dados importantes e a interrupção do serviço 	<ul style="list-style-type: none"> • Bloqueio da possibilidade de interrupção da produção e do processo • Prevenção de acidentes pessoais em caso de acidentes
Efeito nas ameaças à segurança	<ul style="list-style-type: none"> • Danos causados pelo vazamento de dados importantes • Questões legais e danos à confiança da empresa 	<ul style="list-style-type: none"> • Danos diretos causados pela produção e vítimas humanas • Danos à confiabilidade do produto

Fonte: adaptado de (??).

Por sua vez, ameaças são potenciais ações intencionais negativas ou eventos accidentais facilitados por vulnerabilidades, que resultam em impactos indesejáveis. Os IACSSs apresentam vulnerabilidades específicas que precisam ser abordadas para garantir a segurança cibernética, das quais se destacam:

- Rede: a composição obrigatória de redes de comunicação nos sistemas IACSSs os tornam suscetíveis às várias ameaças, uma vez que, devido à interconectividade, as vulnerabilidades também são herdadas. Devido à dificuldade de atacarem diretamente o destino, os invasores encontram, na maioria das vezes, vulnerabilidades na rede IACS como ponto de partida, alcançando assim o host de destino por meio dessa conectividade (??).
- Software e Firmware: a maioria dos sistemas de automação e controle industriais personalizam esses componentes em suas instalações. O desenvolvimento e gerenciamento incorreto desses, como falhas de codificação, inserção de código malicioso ou falta de atualizações de segurança, introduzem vulnerabilidades de segurança no sistema. Além disso, organizações desse meio enfrentam desafios na aplicação de

atualizações de *softwares* e *firmwares* devido à necessidade de minimizar as interrupções operacionais. No entanto, os sistemas que executam um *software* afetado estão mais sujeitos a ataques e explorações, que são geralmente expostas mais rapidamente (??).

- Falta de profissionais qualificados: os engenheiros e especialistas que projetam um IACSs dominam normalmente o *hardware* e *software* de controle no aspecto de aplicação. Há uma lacuna no treinamento com relação à implementação de segurança eficaz usando os recursos existentes dos componentes de uma IACS, sem mencionar os últimos aprimoramentos de segurança cibernética (??). Devido a esta falta de qualificação, as configurações desenvolvidas podem incluir senhas fracas, permissões excessivas, configurações de rede inseguras ou falta de segregação de redes.

Apesar disso, existem diversas normas que oferecem suporte para focar e mitigar vulnerabilidades de segurança atuais e futuras, como as séries ISA/IEC 62443 - definida como a estrutura internacional de padrões de segurança cibernética para TO. A estrutura compreende uma coleção de padrões, relatórios técnicos e informações relacionadas para a proteção de um IACS, além de defender todas as partes relacionadas à segurança cibernética desses sistemas com orientação e uma base comum para medidas técnicas e organizacionais, a fim de aumentar a resiliência digital (??).

Adicionalmente, diversas medidas de proteção desempenham um papel fundamental no aprimoramento da segurança de um IACS, como a segmentação da rede, autenticação e controle de acesso, SDI, SIEM, UTM, entre outras. Entretanto, os Sistemas de Detecção de Intrusão (SDI) se destacam como uma das mais eficazes. Essa tecnologia consegue monitorar comunicações anormais e melhorar o gerenciamento de segurança de uma determinada rede (??).

Diante desse cenário, proteger esses sistemas contra ameaças cibernéticas torna-se uma prioridade essencial para garantir a continuidade das operações, a disponibilidade dos dados, a segurança dos envolvidos, a proteção do meio ambiente e a confiabilidade dos produtos e serviços oferecidos pelas indústrias. A implementação de medidas robustas de segurança cibernética, juntamente com a adoção de práticas recomendadas e a conformidade com as normas e regulamentações pertinentes são fundamentais para mitigar os riscos e fortalecer a resiliência dos sistemas industriais.

2.2.1 Ataques em Redes Industriais

A utilização das redes de comunicação em IACS acrescenta novas vulnerabilidades a ataques ciber-físicos, podendo até prejudicar os processos físicos desses sistemas. Segundo (??), os ataques são também considerados anomalias na rede e podem ser identificados principalmente por meio do fluxo do tráfego de dados. Esses ataques compreendem um

“conjunto de ações ilícitas que tentam comprometer a integridade, confidencialidade, ou disponibilidade de recursos na rede”.

No entanto, para um correto compreendimento acerca dos ataques em redes industriais, é necessário apresentar inicialmente o contexto desse termo. Os ataques cibernéticos causam anomalias no comportamento dos processos observados (na dinâmica das séries temporais de dados) durante a operação do IACS. Essas anomalias podem ser definidas pelo comportamento diferente da operação normal do tráfego da rede.

As anomalias podem ser maliciosas ou não intencionais, mas o conhecimento e análise delas deve ocorrer em todos os casos, pois possibilitam o congestionamento da rede e até um impacto ao processo industrial. Vale ressaltar que nem toda anomalia pode ser considerada um ataque cibernético, mas o contrário é correto. De acordo com (??), as anomalias podem ser classificadas em quatro categorias:

- Anomalias na operação: ocorrem a partir de uma falha ou problema de funcionamento da rede, por exemplo, a interrupção na operação normal, congestionamentos, indisponibilidade de dispositivos, configuração inadequada de um componente ou adição não programada de um mesmo;
- Anomalias *flash-crowd*: representam um aumento repentino no tráfego da rede devido a eventos ou circunstâncias excepcionais, como uma abundância de pacotes oriundos de uma estação para um CLP;
- Anomalias na medição: surgem com a presença de erros ou falhas nos métodos de medição utilizados para monitorar o desempenho da rede, gerando assim, uma análise imprecisa ou distorcida das informações;
- Ataques: anomalia resultante de atividades maliciosa direcionada à rede.

Por compreenderem um conjunto de ações ilícitas efetuadas visando comprometer algum dos pilares de uma comunicação segura (CIA), os ataques em redes de comunicação podem adulterar as informações, não respeitar alguma regra de privacidade e tornar indisponível e não confiável a infraestrutura da rede. O sucesso desses ocorre devido às vulnerabilidades ou possíveis falhas nos elementos da rede, como configurações inadequadas ou erros no desenvolvimento.

Inúmeros ataques cibernéticos foram testemunhados nos últimos anos contra IACS. Alguns desses ataques estão listados no Quadro 3. Tais incidentes históricos destacam as terríveis consequências que uma violação de segurança ou comprometimento do IACS pode ter na economia e na segurança pública, assim como a correlação desses com a falta de segurança dos protocolos de comunicação. Embora esse cenário esteja mudando, com vários protocolos industriais sendo redesenhados, esse assunto continua sendo um problema,

pois os protocolos legados ainda são amplamente utilizados. Além disso, uma das lições aprendidas com os ataques históricos é que, com tempo suficiente, invasores determinados e com bons recursos provavelmente podem obter acesso a quase todo sistema.

Quadro 3 – Principais ataques cibernéticos industriais dos últimos anos

Ano	Alvo	Local	Descrição
2000	Instalação de tratamento de água 'Maroochy Shire'	Austrália	Um dos primeiros relatórios de danos às instalações IACS devido a ataques cibernéticos, no qual causou a liberação de mais de 265.000 galões de esgoto não tratado (??).
2010	Instalações nucleares	Irã	Conhecido como "a primeira arma digital publicamente conhecida do mundo", o STUXNET foi um <i>worm</i> de computador altamente sofisticado e malicioso desenvolvido para atacar um IACS (??).
2012	Instalações de energia	Oriente médio	O <i>malware</i> Shamoon costumava atingir grandes empresas de energia no Oriente Médio, incluindo a Saudi Aramco e a RasGas (??).
2016	Sistema elétrico	Ucrânia	Com esse ataque, 30 subestações de energia foram derrubadas por seis horas, afetando cerca de 80000 pessoas (??).
2021	Sistema de oleoduto	Estados Unidos	Colonial Pipeline, empresa que comporta um dos maiores oleodutos dos Estados Unidos, foi forçada a fechar seu oleoduto após ser atingida por um ataque de <i>ransomware</i> (??).
2021	Sistema de abastecimento de água	Estados Unidos	Um hacker tentou envenenar o abastecimento de água em uma comunidade da Flórida que atende 15.000 pessoas (??).

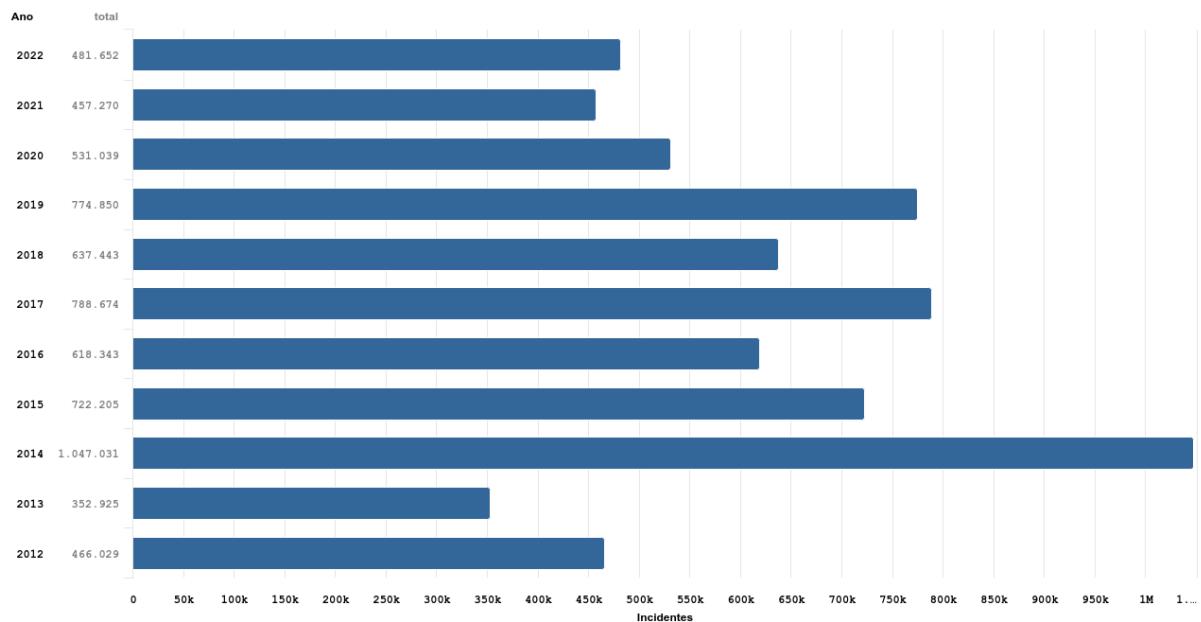
Fonte: elaborado pelo autor.

??) complementam documentando uma ampla gama de ataques ao IACSSs, a fim de descobrir como o sistema e diversos protocolos respondem a diversos tipos de ataques (e.g., negação de serviço (DoS)), assim como avaliar o grau de proteção e vulnerabilidades desses.

Uma taxonomia de ataques ciber-físicos é proposta por ??), baseando-se em três dimensões: (I) conhecimento do adversário sobre o sistema – representa ataques poderosos que permitem a evasão dos adversários –, (II) grau de perturbação – a capacidade de um adversário em afetar o sistema de destino violando sua integridade ou disponibilidade – e (III) grau de divulgação – a capacidade do adversário de obter informações confidenciais durante o ataque, por exemplo, violando dados ou controlando a confidencialidade.

Segundo estatísticas do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (??), o número de ataques aumenta significativamente com o passar dos anos. A Figura 11 apresenta, graficamente, os incidentes notificados ao CERT.br nos últimos 10 anos.

Figura 11 – Notificações de Incidentes recebidos pelo CERT.br nos últimos 10 anos



Fonte: (??)

Os ataques podem ser classificados de diversas formas. A classificação base pode ser observada no glossário proposto por ??), cujos critérios são a origem, o destino ou alvo e objetivos do ataque. Todavia, algumas taxonomias foram propostas a fim de aprimorar essa classificação, como o modelo AVOIDIT (??) – classificando um ataque pelo seu vetor, impacto operacional, defesa, impacto informativo e alvo – e o modelo TAVI (??) – no qual divide a classificação pela ameaça, objetivo, vulnerabilidade e impacto do ataque.

Quanto à origem, os ataques podem ser externos ou internos. Os externos são aqueles disparados por um atacante de fora da rede, enquanto os internos são aqueles provenientes de usuários internos à rede que abusam de seus direitos e privilégios para realizar atividades não autorizadas (??).

Já para a classificação com base no alvo, o ataque é realizado à rede, afetando a camada de comunicação ao impedir a utilização de alguns recursos da rede, ou ao sistema na totalidade, alterando senhas e configurações críticas dos equipamentos.

No ponto de vista da classificação pelo objetivo, existem dois tipos principais de ataques que um invasor pode realizar:

- Passivo: o intruso apenas ‘escuta’ a comunicação, silenciosamente, sem qualquer alteração na comunicação. Tal espionagem ou análise de tráfego pode ocasionar a quebra da confidencialidade da informação, consistindo assim em crime contra a privacidade;
- Ativo: refere-se à modificação de mensagens e fluxo de dados reais ou geração de dados falsos na comunicação. Afeta a integridade e confidencialidade dos dados, uma vez que o intruso pode repetir fluxos de dados antigos, alterando as mensagens de comunicação ou removendo alguma parte selecionada de mensagens importantes de comunicação. Os ataques ativos mais frequentes a redes podem ser classificados como: R2L (*Remote to Local*) e U2R (*User to Root*).

O *Sniffing* de pacotes representa um ataque passivo em relação ao objetivo, uma vez que não envolve a modificação ou interrupção direta do tráfego de rede. Consiste em uma técnica aplicada para a captura e inspeção minuciosa dos pacotes em uma conexão estabelecida, sem que os agentes da comunicação estejam cientes da interceptação. Vale ressaltar que, enquanto o *Sniffing* em si não causa alterações no tráfego ou nos dados, as informações obtidas podem ser posteriormente exploradas em ataques subsequentes. Por outro lado, o ataque *Probing* é realizado de forma ativa, apesar de não comprometer o sistema. Envolve uma varredura do mesmo por parte do invasor pelo envio de requisições ao alvo, visando identificar entradas do sistema ou vulnerabilidades para posteriormente explorar as fraquezas encontradas.

No ataque DoS, uma sobrecarga do sistema ou rede é ocasionada por meio de solicitações excessivas do invasor, resultando em um esgotamento dos recursos computacionais ou de memória dos equipamentos. Com isso, os componentes da rede ficam impossibilitados de executarem suas tarefas devido ao envio de uma quantidade de informações superior ao que o sistema possa manipular (*flooding*), assim como algumas vulnerabilidades podem ser expostas a partir desse tipo de ataque ativo (exploração de falhas). Há a possibilidade desse ataque ser realizado em série, cujos invasores utilizam de vários locais para lançar o ataque, classificando-o assim como DDoS (do inglês *Distributed DoS*). Um exemplo de DoS no âmbito industrial é um cujo invasor envia um comando para desligar a CPU de um CLP, exigindo a execução de um *hard-reset* do dispositivo para retorno. Uma vez desligada, o CLP não pode se comunicar ou processar qualquer informação, resultando em uma ‘negação de serviço’.

Quando ocorre a obtenção não autorizada de dados confidenciais de comunicação, caracteriza-se um ataque do tipo *Man-In-The-Middle* (MITM), também conhecido como “Espionagem” (do inglês *Eavesdropping*). Essa ação maliciosa pode resultar em uma significativa violação de segurança ou no comprometimento das informações, o que, por sua vez, pode abrir caminho para ataques subsequentes. Em um cenário Cliente-Servidor, caso o

invasor já tenha comprometido o canal de comunicação, ele tem a capacidade de gravar e capturar as mensagens, afetando assim a confidencialidade dos dados. Além disso, uma vez estabelecida a sessão, tanto a autorização quanto a autenticação podem ser impactadas.

Nos ataques de penetração, conhecidos como R2L e U2R, aquisições ou alteração não autorizada dos privilégios, recursos ou dados do sistema, violando as propriedades de integridade e controle dos recursos e dados. Com esses ataques, pode-se ganhar controle de um sistema ao explorar uma variedade de falhas de *software* (??). A categoria R2L se destaca pelo envio de pacotes por uma rede externa, a fim de explorar privilégios de um usuário local. Já na U2R, os invasores conseguem acesso na rede local, e nesse cenário, tenta explorar as vulnerabilidades para obter privilégios adicionais.

De acordo com (??), o ataque MITM e DoS são os tipos mais comuns de ataque que a IIoT enfrenta, sendo responsáveis por quase 64% dos ataques. Com o aumento da interconectividade entre sistemas nas indústrias, o ataque MITM está se tornando um desafio maior, pois é mais fácil para o invasor obter acesso a informações confidenciais através dele. Quando se trata de DoS, além de ser também comumente empregado, pode agir de maneira ativa no sistema, gerando perdas consideráveis para as indústrias. Neste projeto, três ataques são aplicados em uma rede industrial OPC UA: *sniffing* de pacotes, MITM e DoS.

2.2.2 Análise e Descoberta de Vulnerabilidades

Inúmeros empreendimentos de pesquisa têm sido dedicados à análise das origens de erros presentes em sistemas computacionais e *softwares* (popularmente denominados *bugs*). Visando a minimização das ocorrências desses erros nos sistemas e o desenvolvimento de métodos para avaliar a existência, esses estudos apresentam, ordinariamente, ferramentas para a identificação de *bugs* específicos.

Apesar da implementação de várias técnicas e tecnologias, esses erros intrínsecos ao desenvolvimento persistem. As vulnerabilidades surgem quando os *bugs* comprometem a integridade do sistema ou políticas de segurança, podendo ser mensurada pelo grau em que um sistema, subsistema ou componente do sistema tem probabilidade de sofrer danos devido à exposição a um perigo.

As vulnerabilidades podem ser amplamente difundidas e consistentes em vários sistemas. Erros de desenvolvimento, equívocos de configuração e falhas operacionais, frequentemente, servem como porta de entrada para usuários não autorizados, permitindo que efetuem ações maliciosas: expor/alterar informações confidenciais, interromper/destruir um sistema ou assumir o controle de um sistema/*software* (??). Um estudo realizado por ?? revela que 92% dos sistemas que utilizam o protocolo OPC UA estão inadequadamente configurados devido a diversas falhas, como a ausência de controle de acesso, a desativação de funcionalidades de segurança, a utilização de políticas criptográficas obsoletas e a reuti-

lização de certificados. Essa alta porcentagem de inadequações é atribuída principalmente à complexidade das configurações de segurança intrínsecas ao protocolo.

A análise de vulnerabilidades engloba a formulação de uma categorização, ou conjunto destas, que viabiliza a extração das informações pertinentes de um conjunto de vulnerabilidades. De acordo com ??), essas informações podem abranger um conjunto de assinaturas, visando a detecção de intrusões; um conjunto de condições ambientais necessárias para que um invasor explore a vulnerabilidade; um conjunto de características de codificação que facilitem a interpretação do código; ou outras formas de dados. Logo, os dados específicos utilizados para classificar as vulnerabilidades variam conforme os objetivos particulares da categorização, sustentando, assim, a existência de diversos esquemas de classificação.

Com base na indecidibilidade do Problema da Parada de Turing e no Teorema de Rice, é possível demonstrar que muitos problemas relacionados à análise de vulnerabilidades também são indecidíveis em um contexto amplo (??). Isso resulta na falta de uma solução abrangente e definitiva para esses problemas práticos.

Na matemática, um sistema de prova é considerado válido quando não aceita argumentos inválidos e é completo quando aceita todos os argumentos válidos. Da mesma forma, na segurança de *software*, um método de análise de vulnerabilidades é apontado sólido se não aprova sistemas vulneráveis. Caso consiga aprovar todos os programas seguros, sem detectar vulnerabilidades falsas, considera-o completo. Comparativamente, a descoberta de vulnerabilidades de programas oferece informações mais detalhadas sobre cada vulnerabilidade em um programa específico.

Embora o problema da análise e descoberta de vulnerabilidades seja indecidível, a comunidade acadêmica e a indústria de *software* têm proposto várias abordagens devido à sua importância crítica. Essas abordagens, no entanto, são aproximações que freqüentemente carecem de solidez ou completude. Assim, a pesquisa busca melhorias específicas em várias áreas, como cobertura de vulnerabilidades, precisão de descoberta e eficiência de execução.

No entanto, apesar dos desafios inerentes à classificação de vulnerabilidades, as abordagens de análise de vulnerabilidade no âmbito de *software* podem ser categorizadas em três principais vertentes, segundo ??):

- Análise Estática: a análise é realizada com base no código-fonte do *software*, sem a necessidade de execução. Uma abstração generalizada é necessária para avaliar as propriedades do mesmo, concedendo a essa abordagem a capacidade de ser sólida. Porém, caso não haja precisão na generalização, a análise pode resultar em falsas vulnerabilidades. Por isso, deve-se encontrar um equilíbrio entre a precisão e a eficiência computacional;

- Análise Dinâmica: um programa é avaliado enquanto é executado com dados de entrada específicos, monitorando seu comportamento em estados. No entanto, devido à natureza das entradas e esses estados de tempo de execução, sistemas de análise dinâmica não conseguem conceituar completamente o comportamento do *software*. Assim, podem ser completos, aprovando todos os programas seguros e não reportando vulnerabilidades falsas, mas não podem ser sólidos, pois existe a possibilidade de negligenciar vulnerabilidades em estados invisíveis. Limitações práticas incluem a necessidade de um ambiente de tempo de execução funcional e o processamento demorado para casos de teste em *software* complexo;
- Análise Híbrida: combina técnicas de análise estática e dinâmica. Embora possa parecer que a abordagem híbrida une as vantagens de ambas, sendo sólida e completa, isso não é verdade, pois enfrentam também suas limitações. Pode ser uma análise estática com análise dinâmica para identificar vulnerabilidades falsas ou uma análise dinâmica que utiliza técnicas estáticas para orientar a seleção e análise de casos de teste.

Vale ressaltar que nem todos os sistemas de análise estática são sólidos e nem todos os sistemas de análise dinâmica são completos.

De acordo com ??), entre as diversas abordagens de descoberta de vulnerabilidades, algumas já estão bem estabelecidas na indústria de *software*; a saber:

- Teste de Penetração: envolve um teste manual de segurança realizado por uma equipe de especialistas em segurança, que exploram as vulnerabilidades em busca de possíveis pontos de entrada para invasões;
- Fuzz-Testing: também conhecido como teste aleatório, os dados de entrada válidos são aleatoriamente alterados e inseridos na execução em teste, enquanto as falhas são monitoradas para identificar possíveis vulnerabilidades;
- Análise Estática de Fluxo de Dados: também referida como "Análise de Fluxo de Dados Contaminado", é uma abordagem de análise estática em que dados de entradas de fontes não confiáveis são classificados como contaminados. Seu fluxo em direção a instruções confidenciais do *software* é rastreado como um possível indicador de vulnerabilidade.

2.3 Trabalhos Correlatos

O crescente dinamismo dos sistemas industriais e o aumento significativo dos ataques aos IACSSs demandam estudos aprofundados para compreender como as mudanças na arquitetura desses sistemas afetam o desempenho dos mecanismos de segurança. Além disso,

é fundamental manter constantemente atualizada a base de conhecimento, particularmente no que diz respeito aos principais aspectos de segurança cibernética relacionados ao protocolo OPC UA, amplamente utilizado por esses sistemas industriais.

??) destacam a crescente importância de estabelecer uma segurança sólida entre a TI e TO à medida que a digitalização se expande. Embora ambas tecnologias busquem uma comunicação segura, ressalta-se que suas abordagens são distintas. Enquanto a TO prioriza eficiência, consistência e continuidade, a TI se concentra em segurança e flexibilidade. Logo, a solução do protocolo OPC UA é proposta, originalmente introduzido pelo setor de TO, mas visando abranger todos os parâmetros de segurança da TI. Além disso, destaca-se o foco do OPC UA na proteção do canal de comunicação, fundamental para a transformação segura de informações confidenciais, concentrando-se no conceito de *Data In Motion*. Adicionalmente, a segurança das implantações OPC UA foi avaliada por ??) e ??), cujo relato garante um alto nível de segurança do protocolo, desde que sejam realizadas as configurações de segurança corretas.

A extensa análise bibliográfica realizada no trabalho sobre o protocolo OPC UA, resultou em uma gama de publicações concernentes à segurança do protocolo. Em (??), é discutida a importância da segurança na automação industrial e as vulnerabilidades das redes de comunicação OPC UA e proposto um método de criptografia de segurança baseado no algoritmo *Advanced Encryption Standard* (AES). ??) complementam a discussão acima mencionada com a importância do provisionamento seguro em IIoT, bem como (??) para os dispositivos IIoT usando OPC UA. ??) projetam uma implementação de código aberto do OPC UA para melhorar a segurança e a escalabilidade na automação industrial.

O estudo sobre a segurança do OPC UA realizado pelo Escritório Federal Alemão para Segurança da Informação (??) analisa as principais vulnerabilidades e possíveis ameaças dessas redes, baseando-se no tipo de mensagem e modo de segurança escolhido. No entanto, a maioria dos ataques são somente efetuados nos modos de segurança **None** e **Sign**, diferentemente do presente trabalho, nas quais as conexões são também estabelecidas no modo **Sign&Encrypt**.

Uma análise detalhada sobre ataques de negação de serviço em redes OPC UA é realizada por ??). Nesse contexto, uma abordagem para detectar tais ataques nesse tipo de rede é implementada, apresentando como esses ataques podem afetar o consumo de CPU do servidor e podem ser muito poderosos quando inúmeros dispositivos é comprometido.

O estudo (??) aponta que a maioria das vulnerabilidades de segurança do protocolo OPC UA, identificadas por meio de testes de *fuzzing*, decorre de produtos e bibliotecas que não estão em conformidade com as especificações. Nessa circunstância, foram identificadas 17 vulnerabilidades de segurança em produtos relacionados à OPC UA. Por sua vez, ??) revisam as propriedades de confidencialidade e autenticação por meio do uso da ferramenta de verificação de protocolos de criptografia ProVerif. Constatou-se que esses requisitos da

segurança são atendidos quando se utiliza o modo de assinatura e criptografia.

Em (??), três principais ciberataques que ocorrem na IIoT são efetuados em redes OPC UA: *packet sniffing*, *Man-in-the-Middle* (MITM) e negação de serviço (DoS). Um cenário de ataque foi construído e testes de penetração foram realizados por meio de simulações de ataque cibernético que podem ocorrer em uma configuração de segurança inadequada.

Além disso, ??) demonstraram que um ataque de injeção de comando por meio de um canal oculto pode ser realizado em um pacote transmitido de um servidor para um cliente em um ambiente de comunicação baseado no protocolo OPC UA, representando uma potencial ameaça à cadeia de suprimentos.

??) identificaram novas ameaças que podem ocorrer usando o protocolo OPC UA com base em um modelo de ameaças de segurança IoT. O ataque identificado a partir de seu modelo de ameaças OPC UA proposto verificou a possibilidade de dois tipos de ataques de negação de serviço (DoS), utilizando MITM e ataques de inundação.

??) propõem um framework para a descoberta de vulnerabilidades e contramedidas, utilizando o protocolo OPC UA, mas que pode ser aplicado a qualquer alvo de análise. Um teste de conceito é conduzido para derivar e verificar ameaças que podem efetivamente ocorrer por meio da modelagem de ameaças abordadas neste trabalho. Com base no framework proposto, foram identificadas 30 ameaças significativas e quatro vulnerabilidades. Como resultado, a validade de ataques de clientes maliciosos usando certificados e cenários de ataque de negação de serviço (DoS) por inundação foi comprovada, e contramedidas foram desenvolvidas para essas vulnerabilidades.

3 DESENVOLVIMENTO

Devido à importância do tema e ao raciocínio apresentado, um método para análise de vulnerabilidades em redes industriais OPC UA foi desenvolvido. O presente capítulo oferece os principais aspectos da bancada experimental utilizada e o conjunto de estratégias adotados para a realização e desenvolvimento do mesmo, assim como o cronograma proposto para o cumprimento das metas estabelecidas.

3.1 Aspectos da Bancada Experimental para Ensaios de Intrusão em Redes OPC UA

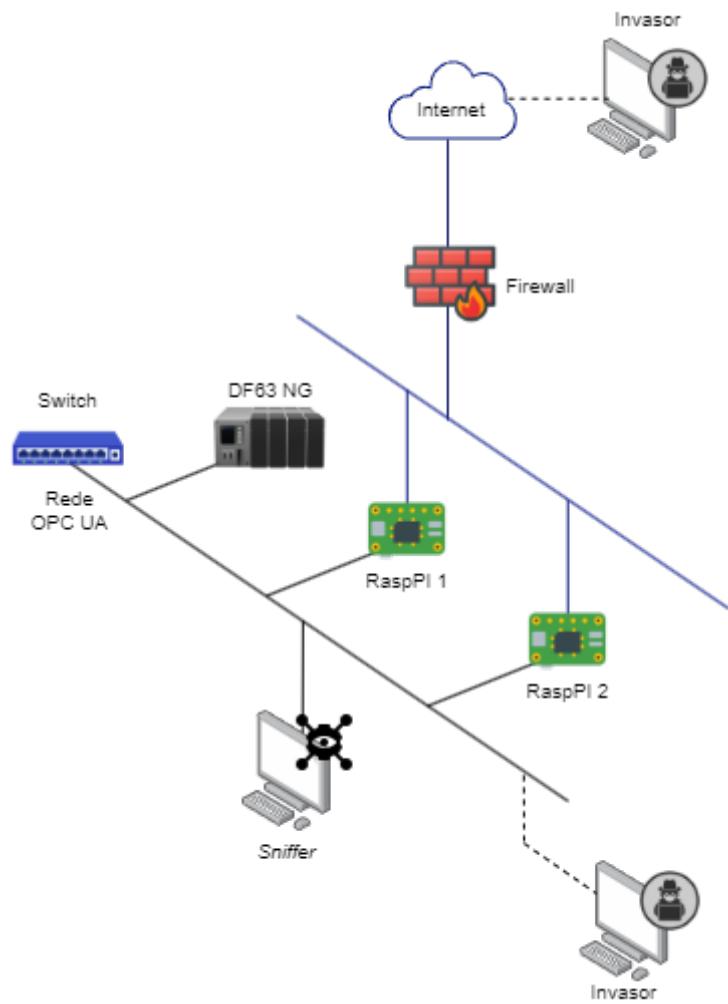
Nesta seção, toda a estrutura responsável pela aquisição de dados experimentais gerados para auxiliar no desenvolvimento do presente trabalho é descrita. A Figura 12 ilustra a composição da estrutura da bancada experimental utilizada, cujos principais componentes são detalhados a seguir:

3.1.1 *Hardware*

Para simular os ataques cibernéticos, são necessários um conjunto de componentes de *hardware* combinados com ferramentas de *software* específicas. A lista a seguir detalha cada equipamento utilizado.

- DF63 NG: representa a nova geração dos controladores multifuncionais da plataforma DFI302 da Nova Smar S/A funcionando como um ‘*linking device*’ para conectar redes H1 independentes e redes Ethernet HSE, especialmente projetado para soluções de controle distribuído em redes industriais. Além de suportar comunicação Modbus, oferece recursos avançados, incluindo redundância ‘*Hot standby*’, comunicação OPC UA nativa, estampa de tempo e configuração por meio da linguagem Ladder conforme IEC 61131. A DF63 NG é altamente versátil, permitindo a instanciação de centenas de blocos funcionais, incluindo blocos flexíveis, e possui um servidor Web integrado para diagnóstico e parametrização;
- Raspberry Pi 4 Modelo B: são utilizados dois mini-computadores de placa única multiplataforma, configuradas com o sistema operacional Kali Linux, hospedando um cliente e um servidor OPC UA cada. A Raspberry Pi 4 Modelo B representa uma evolução significativa em relação às gerações anteriores, incorporando um processador ARM Cortex-A72 quad-core de 64 bits rodando a 1,5 GHz, suporte a Wi-Fi 802.11ac, Bluetooth 5.0 e maior capacidade de memória. Estes aprimoramentos garantem um ambiente experimental mais robusto e capacidade de processamento aprimorada para a condução de testes de intrusão em redes OPC UA. Todas as Raspberry Pi’s

Figura 12 – Esquema geral da bancada experimental para ensaios de segurança cibernética



Fonte: elaborada pelo autor.

existentes na bancada experimental são configuradas como cliente e servidor OPC UA;

- Ethernet Switch: Trata-se de um dos dispositivos de rede mais ubíquos, empregado para centralizar a comunicação entre múltiplos dispositivos. Utiliza a técnica de comutação de pacotes para receber e encaminhar dados de um dispositivo para outro. Neste projeto, faz-se uso de um *Switch* Ethernet da marca TP-Link para estabelecer uma conexão entre os clientes OPC UA e os servidores. O componente de rede que atuar como hospedeiro do servidor OPC UA, encontra-se conectado ao comutador Ethernet por meio de um cabo LAN, da mesma maneira que outro responsável por hospedar o cliente também está conectado ao *Switch*. Cumpre destacar que os comutadores Ethernet da TP-Link incorporam tecnologia Ethernet verde, que resulta em economia de consumo energético, enquanto o controle de fluxo IEEE 802.3x

proporciona uma transferência de dados confiável.

- Elemento Invasor: desempenha um papel fundamental na condução dos testes de intrusão propostos neste estudo. Representa uma simulação de ataque por meio de um computador que pode ser configurado de maneira flexível para atender a cenários específicos de teste. Os ataques são realizados utilizando uma variedade de ferramentas de software, como Hping3 e Nmap (veja subseção 3.1.2). Vale ressaltar que o Elemento Invasor é empregado com extrema cautela em um ambiente controlado, a fim de evitar qualquer impacto adverso e garantir a segurança contínua. Assim, respeitando rigorosamente as considerações éticas, os ataques efetuados neste trabalho pelo elemento invasor não implicam em nenhuma violação das regulamentações estabelecidas pela Lei Geral de Proteção de Dados (LGPD) por não ser aplicado em nenhuma rede ou implementação real.

3.1.2 *Software*

Um conjunto de ferramentas de *software* é necessário para conduzir os ataques às redes OPC UA, das quais se destacam:

- Smar OPC UA server: servidor OPC UA proprietário da Nova Smar S/A, é amplamente aplicado no setor industrial juntamente com a linha de produtos compatíveis com o novo padrão O-PAS (do inglês, *Open Process Automation™ Standards*), desenvolvido pelo OPAF (do inglês, *Open Process Automation™ Forum*), oferecendo um ambiente altamente seguro e eficiente para a comunicação e troca de dados em sistemas de automação industrial. A Nova Smar S/A continua aprimorando seu servidor OPC UA para atender às crescentes demandas do mercado, proporcionando uma solução de conectividade sólida e confiável;
- opcua-asyncio: implementação de código aberto do OPC UA, escrito em Python com suporte para asyncio. O opcua-asyncio opera sob a GNU Lesser General Public License v3.0, permitindo sua integração e distribuição com *software* proprietário. Essa biblioteca é versátil, compatível com vários ambientes Python, e oferece informações detalhadas sobre a implementação de clientes e servidores OPC UA. O opcua-asyncio implementa o conjunto de protocolos binários OPC UA, SDK de cliente e servidor, e é uma opção flexível para desenvolvedores que preferem Python como sua linguagem de programação;
- OPC UA Exploit Framework: projeto *open-source*, desenvolvido e mantido pela Claroaty Team82, que fornece um framework avançado de ferramentas para pesquisa e exploração de vulnerabilidades em redes OPC UA. O intuito deste projeto é facilitar e auxiliar empresas desenvolvedoras de software e fornecedoras de OPC UA na fase

de teste e aprimoramento dos seus produtos, além de suportar pesquisadores da área na análise de novas vulnerabilidades e *bugs* sistêmicos;

- Ettercap: ferramenta de *software* utilizada principalmente para implementar ataques do tipo MITM. Possui recursos extras de captura de conexões *real-time*, filtragem de conteúdo e análise de *hosts* de destino. O Ettercap é utilizado neste projeto para implementar o primeiro cenário de ataque, capturando a conexão entre cliente e servidor OPC UA;
- Hping3: ferramenta de linha de comando que serve como montadora e analisadora de pacotes TCP/IP. Inicialmente concebida para executar ataques de negação de serviço (DoS), o hping3 é agora amplamente empregado em testes de segurança de rede. Oferece suporte a protocolos TCP, UDP e ICMP, bem como um modo de rastreamento de rota;
- Wireshark: software de código aberto usado para capturar e analisar pacotes e protocolos de rede. É principalmente aplicado para solução de problemas de rede, desenvolvimento e análise de protocolos de software e comunicação. Neste trabalho, é utilizado juntamente com um computador *sniffer*;
- Nmap: ferramenta gratuita de código aberto amplamente utilizada para varredura de rede e portas. Através dela, pode-se descobrir os *hosts* e serviços em uma rede dada, bem como detalhes como qual serviço está em execução em qual porta e se a porta está aberta ou fechada, entre outros. Esse resultado é alcançado ao enviar pacotes para o alvo e analisar posteriormente sua resposta.

A Figura 13 apresenta a bancada experimental para ensaios de segurança cibernética.

3.2 Ataques Cibernéticos em Redes Industriais OPC UA

Nesta seção, uma análise detalhada dos cenários de ataque implementados minuciosamente no âmbito do presente projeto é apresentada. A exposição abrangente engloba uma descrição passo a passo das metodologias empregadas para orquestrar três formas distintas de ciberataques: *sniffing* de pacotes (do inglês *Packet Sniffing*), ataques do tipo MITM e de negação de serviço. Ao elucidar as complexidades destes vetores de ataque, objetiva-se proporcionar uma compreensão profunda do cenário em evolução das ameaças à cibersegurança em redes OPC UA.

3.2.1 *Packet Sniffing*

Uma vez que a rede OPC UA esteja instalada e funcionando em seus respectivos dispositivos, o Elemento Invasor inicia o *software* Ettercap e o utiliza como um *sniffer*

Figura 13 – Bancada experimental para ensaios de segurança cibernética



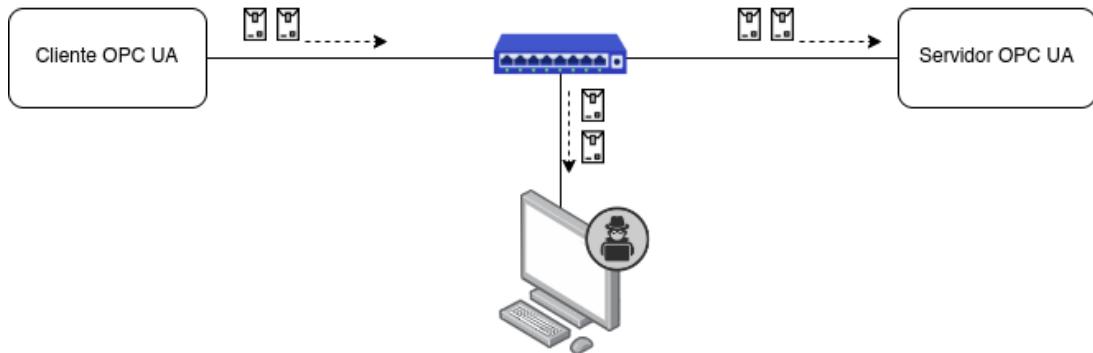
Fonte: elaborada pelo autor.

unificado para obter informações detalhadas sobre os alvos disponíveis na rede. O modo unificado do Ettercap permite a execução do ataque por uma única interface de rede. É importante observar que o Elemento Invasor deve estar configurado na mesma rede de comunicação OPC UA e conectado a uma porta do *switch* gerenciável, que por sua vez, replica o tráfego de dados das outras portas (do componente cliente e servidor OPC UA), conforme ilustrado na Figura 14.

Com o *sniffing* de rede iniciado pelo Ettercap, utiliza-se o Wireshark para analisar mais detalhes sobre os endereços obtidos. A Figura 15 apresenta a série de pacotes que o *software* disponibiliza quando a operação de *sniffing* do tráfego de rede é bem-sucedida. Maiores detalhes da análise aplicada nos dados obtidos nesse processo são apresentados no Capítulo 4.

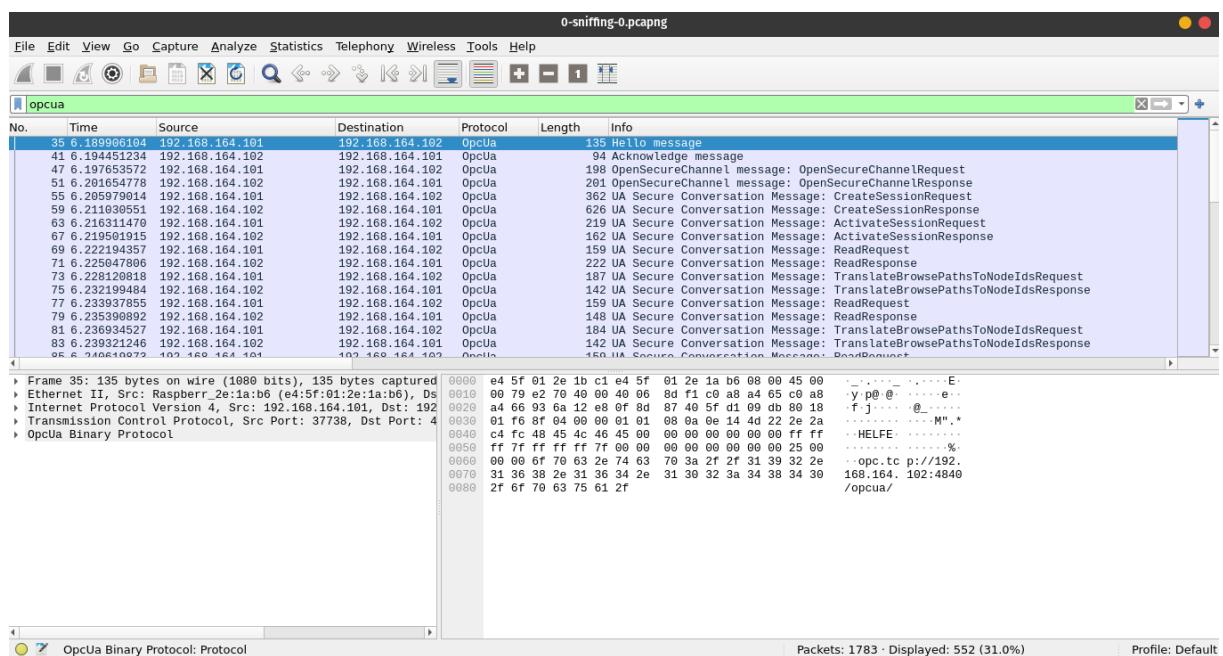
Os detalhes dos pacotes capturados pelo Wireshark são analisados e descritos detalhadamente no Capítulo 4.

Figura 14 – Esquemático do ataque *Packet Sniffing*



Fonte: elaborada pelo autor.

Figura 15 – Resultados de captura do Wireshark durante o *sniffing* de pacotes

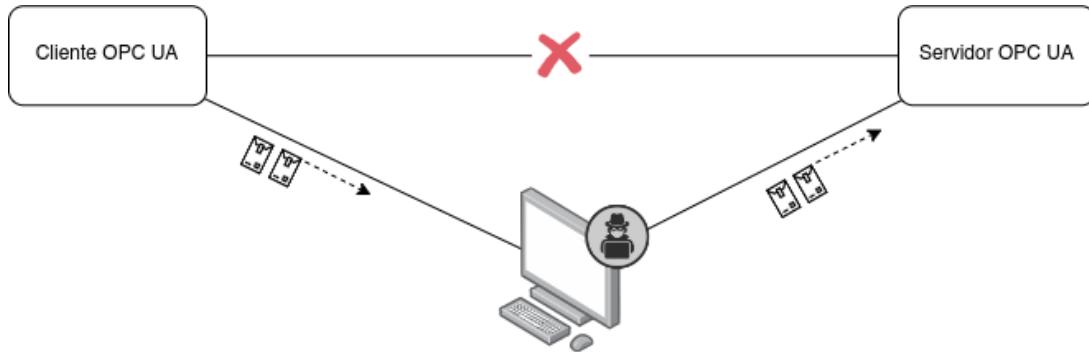


Fonte: elaborada pelo autor.

3.2.2 *Man in The Middle (MITM)*

Ao efetuar esse ataque, o Elemento Invasor pode interceptar as informações do **SecureChannel** entre o cliente e servidor OPC UA, como mostra a Figura 16.

Figura 16 – Esquemático do ataque MITM



Fonte: elaborada pelo autor.

A primeira ferramenta de software utilizada nesse processo é a Ettercap, utilizada para realizar uma varredura da rede. Ao iniciar a busca direta por *hosts* ativos, todos os endereços da máscara de rede são verificados a fim de identificar quais deles estão em funcionamento. Como exemplo, caso a máscara de rede configurada seja 255.255.255.0 (24), um total de 256 endereços são varridos.

Após o término dessa operação de varredura, o Elemento Invasor pode selecionar o(s) alvo(s) nos quais receberam o ataque MITM e então, prosseguir com o ‘envenenamento’ da rede por ARP (do inglês *ARP Spoofing*), um dos tipos mais comuns de efetuar esse ataque. O ARP (do inglês *Address Resolution Protocol*) é um dos protocolos de comunicação mais importantes da camada de rede do modelo OSI, utilizado para determinar o endereço MAC (do inglês *Media Access Control*) de um dispositivo com base no seu endereço IP. Com o *ARP Spoofing*, o invasor é capaz de anunciar à rede que o seu endereço MAC é o correto para os endereços IP pertencentes ao roteador e à estação de trabalho. Assim, estes dois dispositivos atualizam as suas entradas de cache ARP, e, a partir desse ponto, comunicam-se com o invasor, em vez de diretamente entre si.

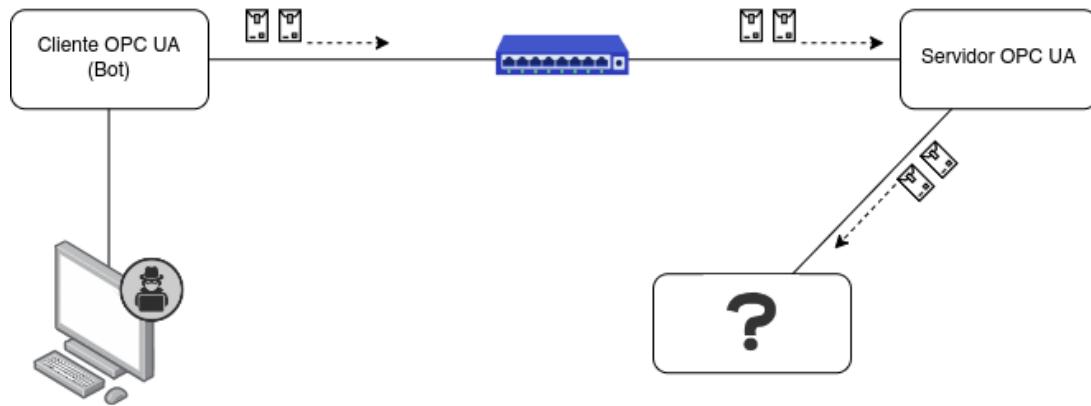
Enquanto o *ARP Spoofing* é realizado pela ferramenta Ettercap, inicia-se a captura de pacotes pelo Wireshark. Para facilitar a visualização e a análise realizada neste estudo, o Wireshark é configurado para o protocolo OPC UA, permitindo um exame detalhado da comunicação entre os dispositivos na rede.

3.2.3 *Denial of Service (DoS)*

Esse tipo de ataque possibilita a inserção de clientes não confiáveis na rede OPC UA pelo Elemento Invasor, assim como uma inundação da rede e do servidor ao enviar

mensagens específicas continuamente. A Figura 17 apresenta um esquemático básico de um funcionamento de DoS, nas quais as solicitações advindas de um cliente OPC UA não confiável são interpretadas pelo servidor, mas não são aceitas pelo remetente devido à sua falsificação de endereço.

Figura 17 – Esquemático do ataque DoS



Fonte: elaborada pelo autor.

Existem diversos cenários possíveis para a efetuação do ataque de negação de serviço. Além do impacto da inundação na rede, ressaltam-se os efeitos no processamento do componente ao sofrer ataques intensivos, nos quais os servidores precisam avaliar as certificações para responderem solicitações. Segundo ??), os principais cenários são:

1. SYN Flooding: o cliente sobrecarrega o servidor enviando mensagens SYN de forma contínua, e o servidor responde com ACK a cada uma dessas mensagens. Embora essa ação possa inundar a rede com tráfego sobrecarregado com estas mensagens, seu impacto no consumo de recursos do servidor é limitado;
2. ACK ou ERR Flooding: nesse cenário, o cliente inunda o servidor com mensagens ACK e/ou ERR, às quais o servidor responde com mensagens ERR. Da mesma forma do anterior, pode haver sobrecarga na rede, mas possui impacto moderado nos recursos do servidor;
3. Inundação com Mensagens Incorretas: são enviadas continuamente mensagens incorretas pelo Elemento Invasor, forçando respostas ERR pelo servidor. Também cria-se sobrecarga na rede, mas apresenta impacto relativamente baixo no processamento do servidor;
4. CLO Flooding: enviam-se, repetidamente, mensagens de solicitação de fechamento de canal (CLO) ao servidor, que responde com mensagens ERR, sobrecarregando a rede com o tráfego destas mensagens.

5. **Inundação com `FindServers` ou `GetEndpoints`:** O cliente estabelece um canal no modo de segurança **None** e, em seguida, envia continuamente mensagens `FindServers()` ou `GetEndpoints()` para o servidor, que, por sua vez, responde com as mesmas mensagens por meio do OPC UA MSG. Apesar de apresentar impacto na rede, não altera os recursos do servidor;
6. **Inundação com Solicitações SYN e OPN:** um cliente não confiável realiza um ataque de negação de serviço enviando continuamente solicitações SYN e OPN ao servidor. O servidor responde com mensagens ACK e ERR. Nesse ataque, o servidor consome recursos substanciais durante a validação do certificado, na solicitação e no processo de criptografia da mensagem. Esse ataque pode ser ainda mais eficaz quando a Autoridade de Certificação está localizada em um sistema diferente, aumentando consideravelmente o tempo de validação do certificado, e, consequentemente, o processamento do componente onde se encontra o servidor.

Duas ferramentas são utilizadas para efetuar a inundação da rede e, assim, alcançar o DoS: OPC UA Exploit Framework e Hping3, além de aplicar o Nmap para efetuar uma varredura da rede a fim de encontrar portas abertas e endereços IP disponíveis.

Uma vez que o Elemento Invasor obteve acesso a algum dos componentes da rede do alvo, o Nmap é utilizado para mapeamento da rede em questão. O comando abaixo executa um *scan* SYN em um range de IPs, relativamente não-obstrusivo e camuflado, uma vez que ele nunca completa uma conexão TCP. Também chamado de escaneamento de portas entreabertas (*half-open scanning*), um pacote SYN é enviado como se fosse abrir uma conexão real, cuja espera-se uma resposta. Um SYN/ACK indica que a porta está ouvindo (aberta), enquanto um RST (*reset*) é indicativo de uma não-ouvinte. Se nenhuma resposta é recebida após diversas retransmissões, a porta é marcada como filtrada. A porta também é marcada como filtrada se um erro ICMP de inalcançável é recebido.

```
Nmap -sS 192.168.164.*
```

A correta execução desse mapeamento resulta em uma lista de IPs disponíveis e portas abertas, que servirão de entrada para os próximos passos. O Hping3 é utilizado para realizar o SYN *Flooding* na rede. Para isso, o *script* de configuração abaixo deve ser implementado pelo Elemento Invasor, customizando-o de acordo com cada cenário.

```
# CONFIGURAÇÃO
set TARGET "192.168.164.101"  # O alvo do ataque
set FAKEIP "192.168.164.201"  # Endereço falso
set BROADCAST "192.168.164.254" # Endereço de broadcast da rede
```

```

set PORTS {{4840}{4192}} # Utilizar as portas abertas encontradas no Nmap
set PORTUDP 123 # Utilizar uma porta UDP ativa

set commandRunTime 180

# EXECUÇÃO
foreach port $PORTS {
    lappend commands "hping3 -S -a $FAKEIP -p $port --flood -V $TARGET"
}

```

Com isso, o Hping3 está preparado para iniciar o ataque direcionado ao endereço e portas especificados, com uma frequência predefinida (neste caso, 180 segundos). A interpretação dos parâmetros utilizados na execução é a seguinte: o argumento **-S** define o tipo de ataque, **-p** identifica a porta de destino, **-V** indica o endereço IP do alvo, enquanto **-a** determina o endereço IP falsificado utilizado no ataque, uma estratégia que pode contornar *firewalls* de forma eficaz.

Por fim, alguns ataques mais robustos são efetuados com o auxílio da ferramenta OPC UA Exploit Framework. Os ataques de negação de serviço disponibilizados pelo *framework* e escolhidos para execução no ambiente de simulação industrial proposto, são apresentados abaixo, seguidos de suas respectivas categorias, conforme os cenários supracitados e apresentados por ??), e suas descrições:

N/A Loop infinito na cadeia de certificados: refere-se a uma situação em que alguns servidores implementam a verificação da cadeia de certificados por conta própria, sem proteção contra um loop de cadeia infinita. Isso pode ocorrer quando um certificado A, por exemplo, é assinado por outro certificado B, que por sua vez é assinado pelo A. Cria-se uma dependência circular entre os certificados A e B, resultando em um loop infinito durante o processo de verificação da cadeia de certificados;

- (3) Inundação por *Chunk*: envolve o envio de uma quantidade abundante de fragmentos de dados ao servidor sem o envio do fragmento final correspondente. O OPC UA permite a divisão dos dados em fragmentos, comumente chamados como *Message-Chunks* ou *Chunks*, que são enviados à medida que são codificados, a fim de facilitar a transmissão e o processamento. Caso ocorra um erro na criação de um destes fragmentos, um *Chunk* final deve ser enviado ao destinatário para notificar o erro, que por sua vez, é marcado com um sinalizador ‘A’ (abortar) para indicar o erro. O receptor deve verificar a segurança do *MessageChunk* abortado antes de processá-lo e, caso esteja tudo certo, ignorar a mensagem, mas sem encerrar o **SecureChannel**;

- (6) Abertura de múltiplos canais seguros: tentativa de inundaçāo do servidor com uma quantidade abundante de solicitações **OpenSecureChannels**;
- (5) Tradução do caminho de navegação: são enviadas ao servidor requisições de traduções de *browse path* complexas que exploram a falta de limites adequados na resolução destes caminhos, podendo causar também um *call stack overflow*;

Sabendo disso, os ataques acima podem ser efetuados através da seguinte linha de comando base, substituindo SERVER_TYPE pelo tipo de servidor utilizado (*e.g.*, softing, unified, prosys, kepware, triangle, dotnetstd, open62541, ignition, rust, node-opcua, opcua-python, milo e s2opc), IP_ADDR pelo endereço de IP do alvo, PORT pela porta aberta para a comunicação UA, ENDPOINT_ADDRESS pelo endpoint do servidor, FUNC_TYPE pelo tipo de ataque escolhido (verificar na documentação oficial do framework (??), quais os nomes das funções disponíveis) e DIR, necessário para algumas funções:

```
python main.py [SERVER_TYPE] [IP_ADDR] [PORT] [ENDPOINT_ADDRESS] [FUNC_TYPE]
↪ [DIR*]
```

3.3 Metodologia

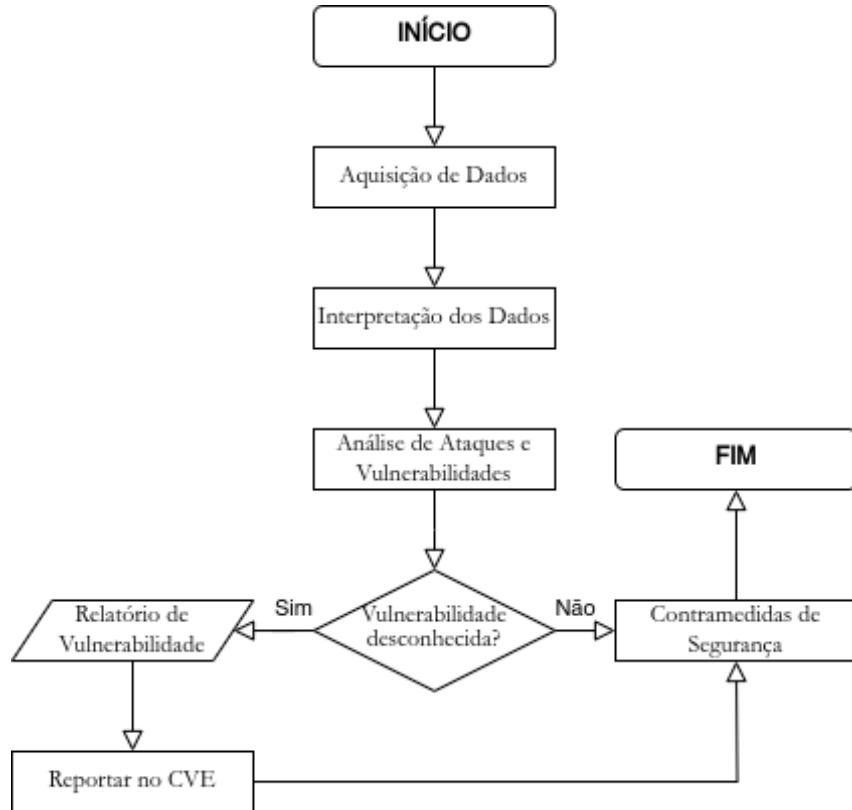
O fluxograma apresentado na Figura 18 explicita a sequência e estrutura de atividades, os passos que compõem a metodologia, posteriormente explicados nas subseções.

Para a realização adequada do experimento proposto neste estudo, a infraestrutura de rede do protocolo OPC UA foi configurada conforme os seguintes parâmetros: um dos Raspberry Pi e a DF63 NG atuaram como servidores, enquanto a outro Raspberry Pi desempenhou o papel de cliente. Além disso, um elemento de rede chamado ‘Sniffer’ (conforme ilustrado na Figura 13) foi inserido na configuração para monitorar e registrar a comunicação da rede. Com o propósito de fornecer uma visão clara dos componentes envolvidos e facilitar a análise dos dados coletados durante o experimento, os endereços IP e MAC de cada elemento do sistema estão resumidos na Tabela 2. Importante mencionar que os servidores OPC UA foram configurados para utilizar a porta padrão 4840, e os endpoints correspondentes também são apresentados ao lado de seus respectivos elementos. Essa estrutura de configuração foi essencial para a condução eficaz do experimento e a subsequente análise dos resultados.

3.3.1 Aquisição de Dados

A fase de aquisição de dados fundamenta-se na captura do tráfego de pacotes transmitidos pela rede OPC UA durante a comunicação entre a aplicação servidora e o cliente da rede, durante a execução dos ataques. Esse processo se baseia na utilização do

Figura 18 – Fluxograma da metodologia proposta



Fonte: elaborada pelo autor.

Tabela 2 – Endereços IP e MAC dos equipamentos da rede OPC UA

Equipamento	IP	MAC	OPC UA Endpoint
DF63 NG	192.168.164.100		
RaspPi 1	192.168.164.101	E4:5F:01:2E:1A:B6	
RaspPi 2	192.168.164.102	E4:5F:01:2E:1B:C1	
Sniffer	192.168.164.201	C8:3A:35:49:FD:58	
Invasor	192.168.164.200		

Fonte: elaborada pelo autor.

software Wireshark, no qual permite a coleta de informações cruciais sobre a comunicação, incluindo detalhes como o tipo de protocolo empregado e a origem e o destino dos dados. As informações capturadas são armazenadas em ordem cronológica com a capacidade de serem salvas em arquivos no formato ‘.pcapng’. O software Wireshark está configurado para atualizar a captura a cada segundo.

Os alvos dos ataques são os servidores OPC UA, e em cada cenário, o elemento *Sniffer* é configurado para realizar a captura do tráfego gerado por estes ataques. Para organizar os pacotes capturados, foi adotada a seguinte nomenclatura de arquivos: ‘[Modo de Segurança]-[Tipo do Ataque]-[Número da Captura].pcapng’. Aqui, o modo de segurança pode assumir os valores 0 (None), 1 (Sign) e 2 (Sign&Encrypt). Os tipos de ataques correspondem àqueles detalhados na seção 3.2 (‘sniffing’, ‘mitm’ e ‘dos-[função]’), e o número da captura é representado por um dígito de 0 a 9. Por exemplo, para salvar a terceira captura obtida durante uma negação de serviço pelo ataque *Chunk Flooding*, com a rede configurada no modo de segurança **Sign**, o arquivo seria nomeado como: ‘1-dos-chunkflood-3.pcapng’.

Além disso, é importante salientar que durante o processo de coleta de dados com o Wireshark, simultaneamente, obtêm-se informações sobre a carga de processamento da CPU nos hospedeiros do servidor OPC UA. Essa abordagem complementa significativamente a análise dos efeitos do ataque sobre o desempenho do sistema. Para viabilizar esse monitoramento, desenvolveu-se um *script* que deve ser ativado pelo elemento *Sniffer* no início da captura de dados. Essa avaliação detalhada contribui para uma compreensão mais completa e precisa dos efeitos das ameaças cibernéticas na infraestrutura OPC UA em análise.

```
#!/bin/bash

output_file="0-dos-chunkflood-3.csv"

if [ ! -e "$output_file" ]; then
    echo "Timestamp (s),RAM (%),CPU (%),Disco (%)" > "$output_file"
fi

# Obter diagnóstico por 1 minuto
duration=60
start_time=$(date +%s)

while true; do
    timestamp=$(date +"%Y-%m-%d %H:%M:%S")

    # Porcentagem de uso da RAM
```

```
ram_usage=$(free | awk '/Mem/ {print $3/$2 * 100.0}')

# Porcentagem de uso do CPU
cpu_usage=$(top -bn1 | grep "Cpu(s)" | awk '{print $2}' | awk -F. '{print
↪  $1}')

# Porcentagem de uso do disco para o sistema de arquivos do root ("/")
disk_usage=$(df -h / | awk 'NR==2 {print $5}' | sed 's/%//')

echo "$timestamp,$ram_usage,$cpu_usage,$disk_usage" >> "$output_file"

current_time=$(date +%s)

if [ $((current_time - start_time)) -ge $duration ]; then
    break
fi

# Escala de 1 segundo
sleep 1

done

echo "Diagnóstico finalizado. Dados salvos no arquivo $output_file"
```

4 RESULTADOS E DISCUSSÕES

4.1 Resultados Esperados

Na busca por aprimorar a cibersegurança dos sistemas de controle e automação industrial por meio de uma análise meticulosa das vulnerabilidades em redes OPC UA, é imperativo delinear os resultados esperados da metodologia aplicada no presente trabalho. As expectativas de resultados estão fundamentadas em uma avaliação abrangente da robustez da rede e variações no desempenho dos controladores ao serem submetidos aos cenários de ataque cibernético apresentados na seção 3.2.

Primeiramente, no que se refere à simulação de ataques de *Packet Sniffing*, espera-se que as redes OPC UA demonstrem um alto nível de resistência à interceptação não autorizada de pacotes, decorrente do modo de segurança inerente ao protocolo utilizado. O maior nível de proteção é apresentado pelo modo **Sign&Encrypt**, no qual inclui recursos de criptografia e autenticação. Consequentemente, as informações trocadas entre cliente e servidor OPC UA permanecem confidenciais, íntegras e disponíveis (CIA), garantindo assim a segurança da rede.

Em segundo lugar, no contexto de ataques do tipo *Man-in-the-Middle* (MITM), é imperativo considerar a detecção e prevenção destas intrusões, também com uma dependência significativa do modo de segurança selecionado. Semelhante ao cenário de ataque anterior, uma configuração que priorize o mais alto nível de segurança e a seleção adequada de políticas de criptografia devem, a princípio, proteger a rede OPC UA contra ataques MITM perpetrados por um possível Elemento Invasor. Entretanto, em situações que existam vulnerabilidades conhecidas na rede e em sua configuração, como a utilização do modo **None**, um elemento não confiável pode explorar tais fragilidades para corromper a tabela ARP (*ARP Spoofing*), permitindo a interceptação das informações transmitidas entre o cliente e o servidor. Além disso, esse invasor pode modificar potencialmente dados por meio da inserção de algum *malware*.

Por fim, no que diz respeito a ataques de negação de serviço (DoS), é importante considerar que os resultados esperados podem diferir dos observados nos ataques mencionados anteriormente, dependendo da capacidade da rede e de processamentos dos componentes *hosts* do servidor OPC UA. Antecipa-se que, embora o ambiente experimental desenvolvido compreenda apenas alguns dispositivos de redes e não incorpore preocupações com a capacidade de comunicação, a correta avaliação dos dados capturados nos cenários simulados deverá evidenciar que esse ataque pode prejudicar a troca de mensagens ao esgotar os recursos de uma rede com grande composição. Estima-se, ainda, que os danos sejam mais significativos quando se utiliza o modo de segurança **Sign&Encrypt** e quando

o inunda com os pacotes referentes a validações de certificado e ao processo de criptografia.

Além disso, a pesquisa se esforça para fornecer informações valiosas sobre vulnerabilidades potenciais que podem ser expostas durante o processo de experimentação. Estas prospecções, caso confirmadas, auxiliam em avanços futuros do protocolo OPC UA e de sistemas IACSs, fortalecendo ainda mais a robustez destes e resistência contra ameaças cibernéticas em constante evolução.

5 CONSIDERAÇÕES PARCIAIS

5.1 Conclusões

5.2 Trabalhos Futuros

6 CRONOGRAMA PROPOSTO

Para auxiliar no planejamento e execução dos objetivos do presente trabalho, as atividades elaboradas para cumprimento são dispostas no Quadro 4 e o cronograma proposto para o cumprimento destas metas, no Quadro 5, permitindo antecipar e mitigar eventuais desvios ou atrasos.

Quadro 4 – Metas estabelecidas para a pesquisa

Metas	Descrição
1	Pesquisa bibliográfica
2	Projeto e implementação do ambiente de teste para coleta de dados
3	Análise e escolha dos ataques cibernéticos
4	Implementação dos ataques na bancada experimental
5	Dissertação para exame de qualificação
6	Coleta e interpretação dos dados
7	Análise dos ataques e vulnerabilidades em redes industriais OPC UA
8	Verificação de desempenho e validação dos resultados
9	Escrita e submissão de artigo científico
10	Entrega final e defesa da dissertação

Fonte: elaborado pelo autor.

Quadro 5 – Cronograma proposto para cumprimento das metas

Metas	2022	2023												2024					
		03	04	05	06	07	08	09	10	11	12	01	02	03	04	05	06		
1	Disciplinas da pós-graduação	■	■	■															
2			■	■	■	■	■												
3					■	■	■	■											
4								■	■	■	■								
5						■	■	■											
6									■	■	■								
7												■	■						
8													■	■	■				
9		■	■																
10															■	■	■		

■ Itens realizados ■ Itens propostos

Fonte: elaborado pelo autor.