Ficha de identificação da obra elaborada pelo autor, através do Programa de Geração Automática do Sistema Integrado de Bibliotecas do IF Goiano - SIBi

Rodrigues, Rafael
R696c Convergência entre Tecnologia da Informação e Tecnologia de Automação: Protocolos de Integração e Desafios de Segurança Cibernética / Rafael Rodrigues. Catalão 2026.

33f. il.

Orientador: Prof. Esp. Luís Felipe Schons Silva.
Tcc (Bacharel) - Instituto Federal Goiano, curso de 0920203 - Bacharelado em Sistemas de Informação - Catalão - Noturno (Campus Catalão).
I. Título.

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO

PARA DISPONIBILIZAR PRODUÇÕES TÉCNICO-CIENTÍFICAS NO REPOSITÓRIO INSTITUCIONAL DO IF GOIANO

Com base no disposto na Lei Federal nº 9.610, de 19 de fevereiro de 1998, AUTORIZO o Instituto Federal de Educação, Ciência e Tecnologia Goiano a disponibilizar gratuitamente o documento em formato digital no Repositório Institucional do IF Goiano (RIIF Goiano), sem ressarcimento de direitos autorais, conforme permissão assinada abaixo, para fins de leitura, download e impressão, a título de divulgação da produção técnico-científica no IF Goiano.

IDENTIFICAÇÃO DA PRODUÇÃO TÉCNICO-CIENTÍFICA

- ☐ Tese (doutorado)
- ☐ Dissertação (mestrado)
- ☐ Monografia (especialização)
- ☑ TCC (graduação)
- ☐ Artigo científico
- ☐ Capítulo de livro
- ☐ Livro
- ☐ Trabalho apresentado em evento
- ☐ Produto técnico e educacional - Tipo:

Nome completo do autor:
Rafael Rodrigues

Matrícula:
2021109202030253

Título do trabalho:
Convergência entre Tecnologia da Informação e Tecnologia de Automação: Protocolos de Integração e Desafios de Segurança Cibernética

RESTRIÇÕES DE ACESSO AO DOCUMENTO

Documento confidencial: ☑ Não ☐ Sim, justifique:

Informe a data que poderá ser disponibilizado no RIIF Goiano: ☐/☐/☐

O documento está sujeito a registro de patente? ☐ Sim ☑ Não

O documento pode vir a ser publicado como livro? ☐ Sim ☑ Não

DECLARAÇÃO DE DISTRIBUIÇÃO NÃO-EXCLUSIVA

O(a) referido(a) autor(a) declara:

• Que o documento é seu trabalho original, detém os direitos autorais da produção técnico-científica e não infringe os direitos de qualquer outra pessoa ou entidade;

• Que obteve autorização de quaisquer materiais inclusos no documento do qual não detém os direitos de autoria, para conceder ao Instituto Federal de Educação, Ciência e Tecnologia Goiano os direitos requeridos e que este material cujos direitos autorais são de terceiros, estão claramente identificados e reconhecidos no texto ou conteúdo do documento entregue;

• Que cumpriu quaisquer obrigações exigidas por contrato ou acordo, caso o documento entregue seja baseado em trabalho financiado ou apoiado por outra instituição que não o Instituto Federal de Educação, Ciência e Tecnologia Goiano.

gov.br Documento assinado digitalmente
RAFAEL RODRIGUES
Data: 02/08/2026 14:58:15-0300
Verifique em https://validar.iti.gov.br

Catalão — Local
02 / 08 / 2026 — Data

Assinatura do autor e/ou detentor dos direitos autorais

Ciente e de acordo:

gov.br Documento assinado digitalmente
LUIS FELIPE SCHONS SILVA
Data: 02/08/2026 17:14:35-0300
Verifique em https://validar.iti.gov.br

Assinatura do(a) orientador(a)

SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA GOIANO

Ata nº 29/2026 - CC-CAT/GE-CAT/CMPCAT/IFGOIANO

ATA DE DEFESA DE TRABALHO DE CONCLUSÃO CURSO

Aos vinte e oito dias do mês de julho de 2026, às 19 horas, reuniu-se na Sala 211 do IF Goiano Campus Catalão a banca examinadora composta pelos docentes: Luís Felipe Schons Silva (orientador), Eduardo Castilho Rosa (membro) e Jean Tomaz da Silva (membro), para examinar o Trabalho de Conclusão de Curso (TCC) intitulado "*Convergência entre Tecnologia da Informação e Tecnologia de Automação: Protocolos de Integração e Desafios de Segurança Cibernética*" do estudante Rafael Rodrigues, Matrícula nº 2021109202030253 do Curso de Bacharelado em Sistemas de Informação do IF Goiano – Campus Catalão. A palavra foi concedida ao estudante para a apresentação oral do TCC, onde houve posteriormente a arguição do candidato pelos membros da banca examinadora. Após tal etapa, a banca examinadora decidiu pela **APROVAÇÃO** do estudante, tendo este obtido média 6,1. Ao final da sessão pública de defesa foi lavrada a presente ata que segue assinada pelos membros da Banca Examinadora.

(Assinado Eletronicamente)

Luis Felipe Schons Silva

Orientador

(Assinado Eletronicamente)

Dr. Eduardo Castilho Rosa

Membro

(Assinado Eletronicamente)

Me. Jean Tomaz da Silva

Membro

Documento assinado eletronicamente por:

- **Luis Felipe Schons Silva**, **PROF ENS BAS TEC TECNOLOGICO-SUBSTITUTO**, em 28/07/2026 22:12:43.
- **Eduardo Castilho Rosa**, **PROFESSOR ENS BASICO TECN TECNOLOGICO** , em 28/07/2026 22:14:39.
- **Jean Tomaz da Silva**, **PROFESSOR ENS BASICO TECN TECNOLOGICO** , em 28/07/2026 22:49:31.

Este documento foi emitido pelo SUAP em 28/07/2026. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifgoiano.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 842296
Código de Autenticação: 225c4f6358

INSTITUTO FEDERAL GOIANO
Campus Catalão
Rua Salustiano Oliveira da Paz, 1621, Bairro Ipanema, CATALAO / GO, CEP 75.705-040
(64)99212-9907

Convergência entre Tecnologia da Informação e Tecnologia de Automação: Protocolos de Integração e Desafios de Segurança Cibernética

Rafael Rodrigues, Luís Felipe Schons Silva
Instituto Federal Goiano – Catalão, Goiás, Brasil
rafael.rodrigues1@estudante.ifgoiano.edu.br, luis.schons@ifgoiano.edu.br

Resumo.
A convergência entre Tecnologia da Informação (TI) e Tecnologia de Automação (TA) é fundamental para a Indústria 4.0, pois permite integrar dados corporativos e sistemas industriais, favorecendo o monitoramento, a tomada de decisão e a eficiência operacional. No entanto, essa integração também amplia a exposição a ataques cibernéticos, deixando sistemas de controle, sensores, CLPs e redes industriais mais vulneráveis a ataques digitais. Este trabalho analisa os principais protocolos utilizados na convergência TI-TA, com foco em OPC UA, EtherNet/IP, Profinet e Modbus TCP, analisando suas vantagens, limitações e adequação à integração segura. A pesquisa foi conduzida por meio de revisão bibliográfica qualitativa e descritiva, com base em literatura técnica, normas e relatórios de segurança publicados entre 2022 e 2026. Os resultados mostram que o OPC UA é o protocolo mais adequado para a integração segura entre os ambientes industrial e corporativo, sobretudo quando combinado com segmentação de rede, DMZ industrial Zero Trust e as orientações da IEC 62443.

Palavras-chave: Tecnologia da Informação; Tecnologia de Automação; Eficiência Operacional; OPC UA; Segurança Cibernética Industrial.

1. Introdução

A automação industrial tem como finalidade aumentar a eficiência, a precisão, a produtividade e a segurança dos processos produtivos. Desde a Revolução Industrial, os sistemas industriais passaram por sucessivas transformações, incorporando máquinas, sensores, controladores, redes industriais e, mais recentemente, recursos de inteligência artificial e análise de dados. Essa evolução contribuiu para a redução de custos operacionais, a melhoria da qualidade dos produtos e o maior controle sobre os processos produtivos (BRANCO; AHLERT; MOTTA, 2015).

Nesse contexto, a convergência entre Tecnologia da Informação (TI) e Tecnologia de Automação (TA), também associada ao conceito de Tecnologia Operacional (TO), tornou-se um dos elementos centrais da Indústria 4.0. A TI está relacionada ao armazenamento, processamento, transmissão e proteção de dados corporativos. Já a TA compreende os sistemas empregados no monitoramento e no controle de processos físicos, incluindo controladores lógicos programáveis (CLPs), sensores, atuadores, sistemas SCADA e sistemas de controle distribuído.

A integração entre esses ambientes permite que dados oriundos do chão de fábrica sejam compartilhados com sistemas corporativos, bancos de dados, plataformas analíticas, sistemas MES (*Manufacturing Execution System*), ERP (*Enterprise Resource Planning*) e aplicações em nuvem. Essa integração viabiliza o acompanhamento da produção em tempo real, a antecipação de falhas, a otimização de processos, a redução de paradas não programadas e o suporte à tomada de decisões.

Historicamente, antes da integração massiva dos dados operacionais, diversos ambientes industriais operavam de forma isolada, com pouca ou nenhuma conexão com redes externas. Esse modelo, frequentemente associado ao conceito de *air gap*, reduzia a exposição a ameaças cibernéticas ao limitar os vetores de acesso remoto aos sistemas industriais. Contudo, o avanço da Indústria 4.0 passou a conectar ativos industriais a redes corporativas, sistemas externos e, em alguns casos, à Internet. Esse processo é particularmente sensível porque muitos ativos de TA possuem longos ciclos de vida, projetados originalmente para ambientes isolados e priorizando disponibilidade, segurança operacional e continuidade do processo, não necessariamente mecanismos modernos de cibersegurança.

Essa transição amplia a superfície de ataque dos ambientes industriais e introduz riscos associados à perda de disponibilidade, comprometimento da integridade dos dados, interrupção de processos, danos a equipamentos, prejuízos financeiros e impactos à segurança dos trabalhadores. Relatórios recentes indicam que os ambientes de TA deixaram de ser alvos secundários e passaram a ocupar posição central em ataques cibernéticos, especialmente nos setores industrial e de manufatura (FORTINET, 2025; 3STRUCTURE, 2025; WTSNET, 2026).

Diante desse cenário, a integração entre TI e TA, embora essencial para a modernização industrial, pode ampliar significativamente os riscos cibernéticos quando realizada sem critérios adequados de segmentação, escolha de protocolos, controle de acesso e adoção de boas práticas de segurança. Assim, o objetivo deste artigo é analisar os principais protocolos de comunicação empregados na convergência entre TI e TA, avaliando suas vantagens, limitações e adequação à integração segura. Também são discutidos os riscos cibernéticos associados a essa convergência e as principais estratégias de mitigação, fundamentadas em boas práticas, no modelo Purdue e na norma IEC 62443 (SILVA, 2021; PEREIRA, 2021).

2. Metodologia

A pesquisa foi desenvolvida por meio de uma revisão bibliográfica de caráter qualitativo e descritivo, com abordagem analítica. O objetivo foi examinar os principais protocolos de comunicação utilizados na convergência entre TI e TA, identificar os riscos cibernéticos associados a essa integração e discutir estratégias de mitigação fundamentadas em normas, modelos de referência e boas práticas de segurança industrial.

O material analisado foi composto por literatura técnica especializada, normas internacionais, publicações acadêmicas, relatórios de segurança cibernética e documentos técnicos de fabricantes e organizações vinculadas à automação industrial. Entre as principais referências utilizadas, destacam-se a série IEC 62443, a ABNT IEC TS 624431-1, relatórios da *Fortinet*, publicações sobre convergência TI-TA e materiais técnicos relacionados aos protocolos OPC UA*, EtherNet/IP, Profinet e Modbus TCP*. Ao todo, foram selecionados 22 documentos incluindo normas, documentos técnicos, relatórios recentes de segurança cibernética e publicações acadêmicas clássicas ou complementares sobre automação industrial.

A seleção dos materiais considerou os seguintes critérios de inclusão: relação direta com a convergência entre TI e TA, abordagem de protocolos de comunicação industrial, discussão sobre segurança cibernética em ambientes de automação, controle industrial ou tecnologia operacional, publicação ou atualização recente e disponibilidade de acesso ao conteúdo completo. Foram excluídos trabalhos voltados exclusivamente à segurança em ambientes corporativos de TI, sem relação direta com sistemas industriais, redes de automação, controle de processos ou tecnologia operacional. Além disso, a pesquisa priorizou as publicações entre 2022 e 2026, utilizando as referências anteriores a essas datas como fundamentação conceitual e histórica. Esse recorte temporal foi definido em razão do aumento recente da exposição dos ambientes industriais a ataques cibernéticos, especialmente aqueles envolvendo *ransomware*, exploração de protocolos legados, vulnerabilidades em redes industriais e ameaças direcionadas a sistemas de controle e automação (FORTINET, 2025; WTSNET, 2026).

A análise foi organizada em três etapas como mostra na tabela 1.

Tabela 1 – Etapas de pesquisa, foco de análise e base normativa/técnica.

Etapas	Nome da etapa	Foco da Análise	Base Normativa/ Técnica
1	Característica dos protocolos	OPC UA, EtherNet/IP, Profinet e Modbus TCP	Literatura técnica e documentação de fabricantes
2	Identificação dos riscos	Ransomware industrial, ataques a protocolos legados, SCADA, CLPs e vulnerabilidades de rede	Fortinet (2025), WTSNET (2026) e relatórios setoriais
3	Análise das estratégias de mitigação	Segmentação de rede, DMZ industrial, Zero Trust, controle de acesso e monitoramento contínuo	IEC 62443, ABNT IEC TS 62443-1-1 e modelo Purdue

Fonte: Autoria própria.

Na primeira, os protocolos OPC UA, *EtherNet/IP, Profinet e Modbus TCP* foram caracterizados quanto à segurança nativa, suporte a aplicações em tempo real, interoperabilidade, integração com ambientes de TI e compatibilidade com equipamentos legados. Na segunda etapa, foram identificados os principais riscos cibernéticos relacionados à convergência TI-TA, incluindo ransomware industrial, exploração de protocolos legados, ataques a sistemas SCADA, comprometimento de CLPs e vulnerabilidades de rede. Na terceira etapa, foram analisadas estratégias de mitigação com base na IEC 62443, na ABNT IEC TS 62443-11, no modelo Purdue adaptado à Indústria 4.0 e em recomendações técnicas relacionadas à segmentação de redes, DMZ industrial, controle de acesso, monitoramento contínuo e abordagem Zero Trust. A tabela 1 resume essas etapas com foco da análise e a base normativa e técnica utilizada.

Ao final, os dados obtidos na revisão foram organizados de forma comparativa, permitindo relacionar as características técnicas dos protocolos industriais com os riscos cibernéticos identificados e com as estratégias de mitigação recomendadas. Dessa forma, a metodologia adotada buscou fornecer uma análise técnica e normativa da convergência entre TI e TA, com foco na integração segura de ambientes industriais.

Em alinhamento às discussões recentes sobre transparência, integridade e uso responsável de inteligência artificial na produção científica, registra-se que ferramentas de IA generativa foram utilizadas de forma auxiliar no processo de revisão e aprimoramento da clareza textual, organização das ideias e adequação da linguagem acadêmica. A definição do tema, a seleção das fontes, a análise crítica, a interpretação dos resultados e a responsabilidade pelo conteúdo final são integralmente dos autores.

3. Desenvolvimento

3.1 Redes de TI e TA: diferenças estruturais e necessidade de convergência

A adoção de sistemas inteligentes de produção tem ampliado a comunicação entre máquinas, sensores, controladores e sistemas de gestão. Essa integração melhora a coordenação dos processos, aumenta a precisão operacional e contribui para a redução de erros e custos produtivos (QUINTELLA; ROCHA, 2007).

A TI atua principalmente na gestão de dados corporativos, operando sobre redes Ethernet, protocolos TCP/IP, servidores, bancos de dados e sistemas administrativos. Sua lógica de segurança é tradicionalmente baseada na tríade CIA: confidencialidade, integridade e disponibilidade, com maior ênfase na proteção da informação.

A TA, por outro lado, está voltada ao monitoramento e controle de processos físicos. Inclui CLPs, sensores, atuadores, IHMs, sistemas SCADA, DCS e dispositivos industriais conectados. Nesses ambientes, a disponibilidade operacional costuma ser a prioridade, pois interrupções podem gerar paradas de produção, danos a equipamentos e riscos à integridade humana.

Essa diferença cria um desafio importante. Em ambientes de TI, atualizações, reinicializações e substituições de sistemas são práticas comuns. Em ambientes industriais, essas ações exigem planejamento rigoroso, pois uma parada indevida pode comprometer a produção. Assim, práticas tradicionais de segurança corporativa nem sempre podem ser aplicadas diretamente à automação industrial.

A convergência entre TI e TA surge da necessidade de transformar dados operacionais em informação estratégica. Para isso, é necessário conectar o chão de fábrica a sistemas supervisórios, bancos de dados, plataformas de análise, MES, ERP e ambientes em nuvem. Essa integração exige protocolos adequados, arquitetura de rede segmentada e políticas de segurança compatíveis com as necessidades industriais.

3.2 Protocolos de convergência entre TI e TA

A seleção dos protocolos de comunicação representa uma decisão estratégica para o sucesso da convergência entre TI e TA, pois impacta diretamente o desempenho

operacional, a confiabilidade dos processos e o nível de exposição a riscos cibernéticos. Em ambientes industriais integrados, os profissionais responsáveis pela arquitetura de rede devem garantir simultaneamente a integridade dos dados, funcionalidade dos sistemas, desempenho em tempo real, escalabilidade da infraestrutura e segurança das comunicações, além de assegurar a aquisição confiável de dados e a eficiência no intercâmbio de informações entre os diferentes níveis da automação (LUGLI; SANTOS, 2011).

É importante compreender, no entanto, que os protocolos industriais não foram desenvolvidos para atender os mesmos propósitos. Cada um possui características técnicas próprias que o tornam mais ou menos adequado a determinados contextos de aplicação. Protocolos orientados ao controle de processos, como o *Profinet e o EtherNet/IP,* priorizam o determinismo e a baixa latência, requisitos indispensáveis para automação de máquinas, robótica e sistemas de controle em tempo real. Em contrapartida, protocolos como o OPC UA foram projetados com foco na integração semântica, na interoperabilidade entre fabricantes e na disponibilização estruturada de dados para sistemas corporativos, plataformas de análise e ambientes de nuvem.

Os protocolos legados, por sua vez, embora amplamente difundidos e compatíveis com a maioria dos equipamentos industriais existentes, foram desenvolvidos em um contexto em que a segurança cibernética não era uma preocupação central. Como resultado, apresentam limitações estruturais significativas nesse aspecto, tornando-se vetores de vulnerabilidade em redes convergidas quando utilizados sem os devidos controles complementares. A compreensão dessas diferenças é, portanto, fundamental para a definição de uma arquitetura de convergência TI-TA segura, eficiente e alinhada às exigências da Indústria 4.0. A seguir, são analisados os quatro principais protocolos abordados neste trabalho: OPC UA*, EtherNet/IP, Profinet e Modbus TCP.*

3.2.1 OPC UA (*Open Platform Communications Unified Architecture*)

OPC UA é um padrão aberto que independe de plataforma, é orientado a serviços e desenvolvido pela OPC Foundation no ano de 2008, ele viabiliza a troca de dados entre diversos sistemas, incluindo CLPs, sistemas supervisórios, bancos de dados e aplicações corporativas (ALTUS, 2024; FERSILTEC, 2022). Diferentemente de protocolos mais simples, o OPC UA incorpora nativamente mecanismos de segurança baseados em

TLS/SSL, autenticação por certificados digitais, controle de acesso baseado em funções RBAC (*Role-Based Access Control*, traduzido para Controle de Acesso Baseado em Funções) e auditoria de eventos, tornando-o a solução mais robusta para ambientes que exigem conformidade com as normas de segurança cibernética industrial (ALTUS, 2024; GRAÇA, 2024).

Ao contrário de protocolos de comunicação mais simples, que se limitam à transmissão de valores brutos, o OPC UA adota um modelo de informação estruturado e semântico. Isso significa que, além de transportar dados, o protocolo é capaz de associar contexto, significado e relacionamentos às informações transmitidas, permitindo que sistemas superiores como bancos de dados, plataformas de análise preditiva, sistemas de gestão da produção e aplicações de inteligência artificial interpretem e processem os dados de forma autônoma e confiável, sem necessidade de tradução ou reprocessamento intermediário.

Outro diferencial é a presença de recursos nativos de segurança e pode utilizar criptografia, autenticação por certificados digitais, controle de acesso baseado em usuários e funções, além de auditoria de eventos. Esses mecanismos tornam o protocolo mais adequado para ambientes que exigem integração segura entre sistemas industriais e corporativos (ALTUS, 2024; GRAÇA, 2024). Na convergência TI-TA, o OPC UA atua como camada de integração entre o ambiente operacional e os sistemas corporativos, conforme ilustrado pela figura 1.

O protocolo coleta os dados de campo, disponibilizados pelos CLPs, SCADA, sensores e dispositivos industriais, organiza estes dados e disponibiliza para sistemas superiores, na camada corporativa, como planilhas e *dashboards*. Esse comportamento torna o OPC UA uma das principais tecnologias de suporte à Indústria 4.0 e à Internet Industrial das Coisas (CRYPTOID, 2020; WESTCON, 2022).

O OPC UA pode ser considerado a solução mais robusta entre os protocolos industriais analisados quando o critério adotado é a combinação de segurança nativa, interoperabilidade e capacidade de modelagem semântica. Em segurança, o padrão suporta políticas criptográficas configuráveis, com mecanismos de autenticação, assinatura digital, integridade e confidencialidade, permitindo adequação a diferentes requisitos de proteção. Em interoperabilidade, sua independência de plataforma e seu modelo padronizado favorecem a comunicação entre sistemas heterogêneos. Em

semântica, o protocolo estrutura dados e metadados em um modelo de informação que amplia a compreensão do contexto industrial.

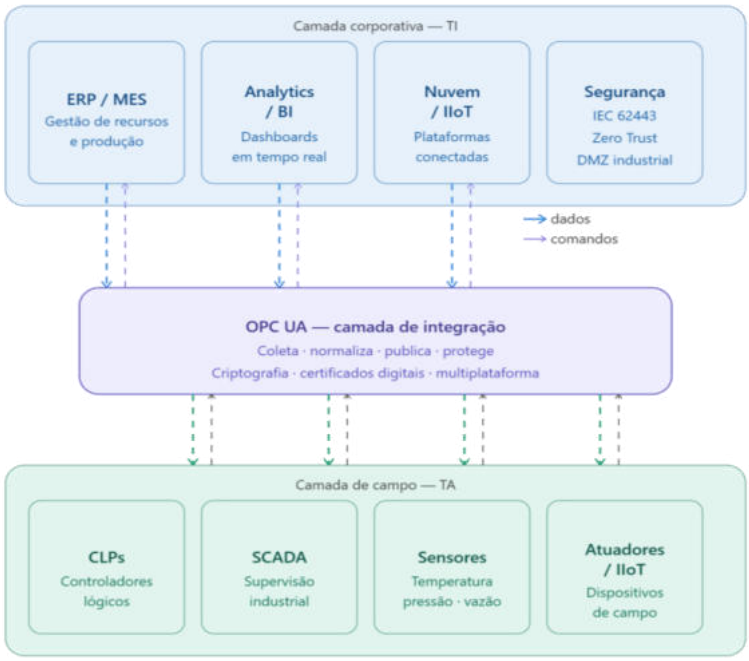

Figura 1 - Arquitetura OPC UA como camada de integração na convergência TI-TA. Fonte: Elaborado pelo autor.

Apesar dessas vantagens, a segurança deste protocolo depende da configuração adequada. Certificados mal gerenciados, permissões amplas ou criptografia desativada podem comprometer o ambiente. Portanto, o uso do OPC UA deve estar associado à segmentação de rede, gestão de identidades, controle de acesso e monitoramento contínuo.

3.2.2 EtherNet/IP

O EtherNet/IP (*Ethernet Industrial Protocol*) é um protocolo industrial baseado em tecnologia de rede com fio padrão, desenvolvido pela ODVA (*Open DeviceNet Vendors Association*) e amplamente adotado em ambientes de automação discreta e de processos para comunicação entre CLPs, I/O distribuídos e supervisórios (FIBERROAD, 2025; COME-STAR, 2026). Opera sobre TCP/IP e UDP/IP, utilizando o protocolo CIP (*Common Industrial Protocol*) como camada de aplicação, o que facilita a integração com infraestruturas de TI existentes. A figura 2 apresenta uma topologia *Ethernet/IP*.

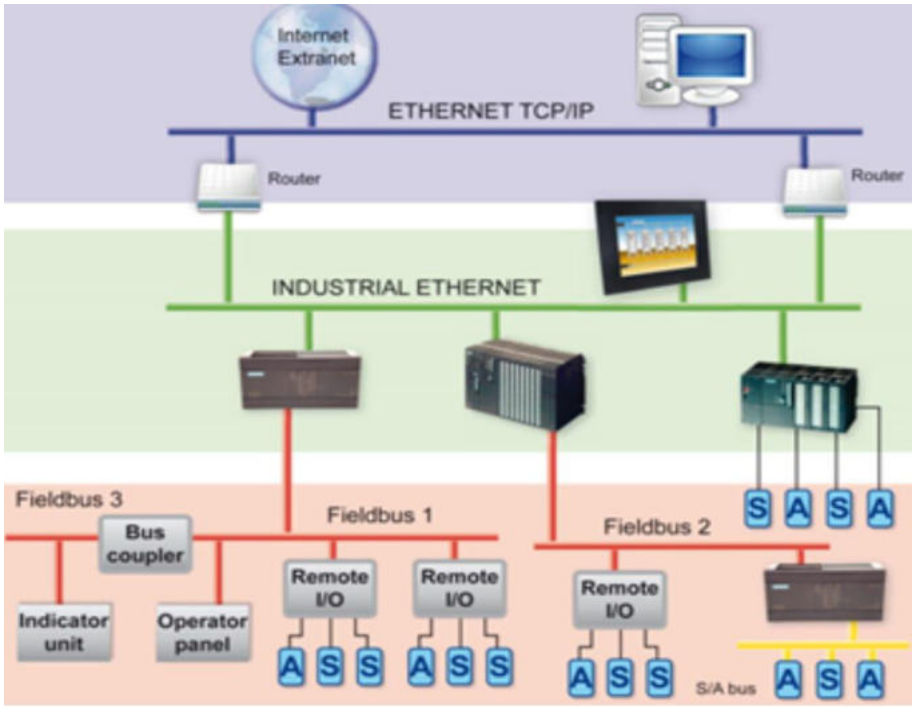

Figura 2 - Topologia de rede utilizando Ethernet/IP. Fonte: Adaptado de IEB Media (2026).

A principal vantagem do *EtherNet/IP* está no fato de ser baseado na Ethernet comercial padrão, o que reduz custos de infraestrutura e facilita sua integração com redes corporativas de TI. Além disso, o protocolo oferece suporte à comunicação em tempo real, com determinismo adequado para aplicações industriais de alta velocidade. Outro aspecto relevante é seu amplo ecossistema, composto por centenas de fabricantes de automação, o que favorece a interoperabilidade entre sistemas e amplia a disponibilidade de dispositivos compatíveis no mercado.

Em contrapartida, suas limitações incluem o custo mais elevado dos equipamentos em comparação a protocolos mais simples, além da necessidade de *switches* gerenciáveis e de uma configuração de rede mais cuidadosa. A implantação e a administração desse tipo de rede tendem a ser mais complexas, exigindo profissionais com conhecimento em redes industriais e domínio técnico mais avançado. Além disso, sob a perspectiva da segurança o protocolo CIP, utilizado pelo *EtherNet/IP*, oferece apenas mecanismos básicos de proteção e não possui criptografia nativa incorporada ao protocolo. Dessa forma, é necessário adotar mecanismos externos de segurança, como *firewalls* industriais, segmentação de rede, controle de acesso e políticas de comunicação, a fim de mitigar vulnerabilidades quando o sistema estiver conectado à rede corporativa ou exposto à Internet.

3.2.3 Profinet

O *Profinet* é um protocolo de comunicação industrial baseado em *Ethernet,* desenvolvido pela Siemens e padronizado pela *PROFIBUS & PROFINET International* (PI). Destaca-se pela alta velocidade de comunicação, até 100 Mbit/s e recursos avançados como redundância de sistema, segurança funcional (*PROFIsafe*) e gerenciamento de energia (*PROFIenergy*). Esse protocolo é amplamente utilizado em sistemas de automação integrada, especialmente em linhas de produção com requisitos rigorosos de sincronismo. A arquitetura deste protocolo é representada pela figura 3.

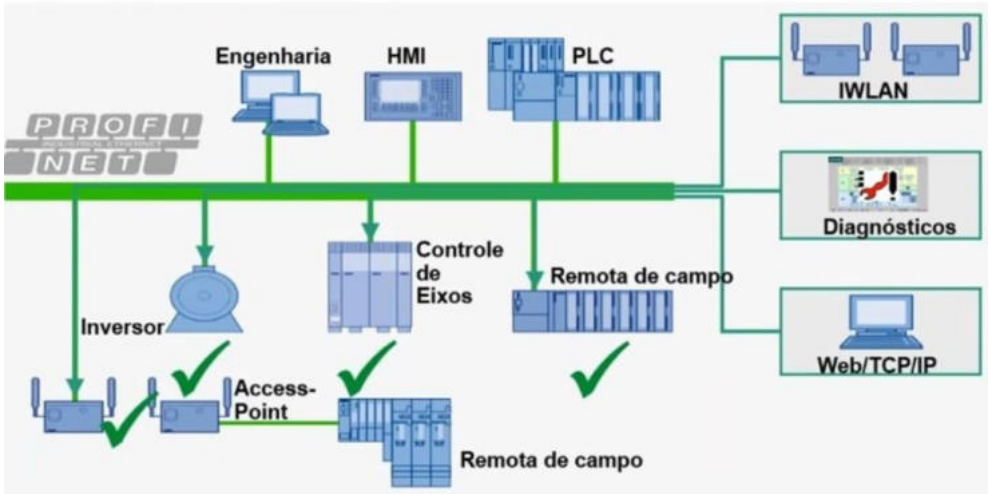

Figura 3 - Arquitetura de rede PROFINET em ambiente industrial. Fonte: Fertron (2023).

Dentre suas principais vantagens, está a capacidade de atender demandas de controle e supervisão com baixa latência, o que torna esse protocolo adequado para linhas de produção e processos que dependem de sincronismo. Além disso, ele é padronizado em normas IEC 62443, o que reforça sua consolidação como solução de referência para automação industrial (YANG; LI, 2014).

Apesar dessas vantagens, o *Profinet* também apresenta desafios de segurança. Ao depender de Ethernet industrial, o protocolo se torna sensível a riscos comuns de rede, exigindo medidas adicionais de proteção, como segmentação, autenticação e planejamento seguro da arquitetura. Documentos técnicos recentes da *PROFIBUS & PROFINET International* reforçam a necessidade de diretrizes específicas para segurança do protocolo (PROFIBUS & PROFINET INTERNATIONAL, 2025).

Do ponto de vista da integração entre TI e TA, o protocolo contribui para conectar controladores, sensores, atuadores e sistemas de supervisão a plataformas corporativas e analíticas. Essa característica o aproxima dos objetivos da Indústria 4.0, pois favorece a circulação estruturada de dados entre os diferentes níveis da arquitetura industrial (PI NORTH AMERICA, 2010; NXP, 2024).

3.2.4 Modbus TCP

O *Modbus TCP* representa a extensão para redes Ethernet do protocolo *serial Modbus*, criado em 1979. Devido à sua simplicidade, ampla compatibilidade e facilidade de implementação, permanece sendo um dos protocolos mais utilizados na integração de dispositivos legados, instrumentos de campo, medidores e CLPs de gerações anteriores a redes IP, permitindo sua comunicação com sistemas SCADA e plataformas de supervisão (FIBERROAD, 2025; COME-STAR, 2026). A figura 4 apresenta a topologia da rede *Modbus TCP*.

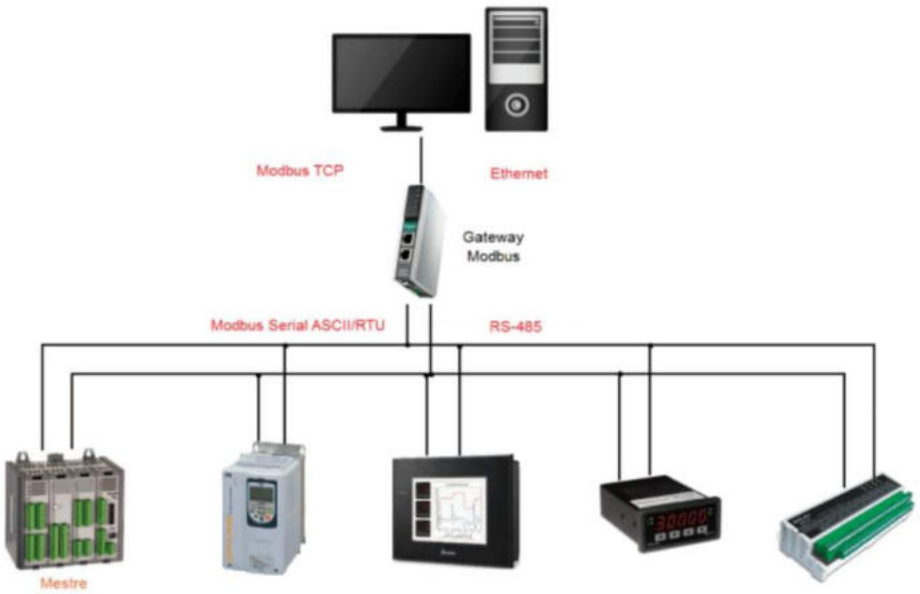

Figura 4 - Topologia de rede Modbus TCP . Fonte: Freitas (2014).

Entre suas principais vantagens, destacam-se a implementação simples, o baixo custo e o amplo suporte em equipamentos industriais, incluindo dispositivos modernos e legados. Essas características tornam o *Modbus TCP* uma alternativa prática para integrar ativos já existentes a sistemas mais recentes, muitas vezes por meio de *gateways* que

possibilitam a modernização da infraestrutura sem a substituição completa dos instrumentos instalados.

Entretanto, o protocolo apresenta limitações importantes, especialmente do ponto de vista de segurança. O *Modbus TCP* não possui mecanismos nativos de criptografia, autenticação ou controle de acesso, o que pode permitir que qualquer dispositivo conectado à rede envie comandos de leitura ou escrita, aumentando o risco de manipulação indevida de dados e operações. Além disso, o protocolo transmite apenas valores brutos, sem informações semânticas ou contexto associado, exigindo que sistemas superiores interpretem os dados recebidos. Essas fragilidades contribuem para sua exposição a ataques quando utilizado sem proteção adequada, reforçando a necessidade de empregá-lo em redes bem segmentadas e protegidas por camadas adicionais de segurança, como *firewalls* industriais, *gateways*, controle de acesso e, quando necessário, conversão para protocolos mais robustos.

3.2.5 Análise comparativa entre os protocolos

A análise comparativa dos protocolos evidencia que nenhuma solução única é suficiente para atender à totalidade dos requisitos de uma arquitetura de convergência TI-TA. A abordagem mais recomendada pela literatura técnica e normas internacionais IEC 62443 é o uso de protocolos em camadas hierárquicas (COME-STAR, 2026; WESTCON, 2022).

A *EtherNet/IP* e o *Profinet* são utilizados para garantir uma comunicação determinística com CLPs, I/O distribuídos e atuadores, onde a menor latência possível e a maior disponibilidade são requisitos críticos para o controle de processos industriais. No nível de supervisão e integração, o OPC UA atua como protocolo de convergência, reunindo os dados operacionais, organizando-os semanticamente e disponibilizando-os para sistemas corporativos, bancos de dados e plataformas de análise. Para a integração de equipamentos legados, recomenda-se o uso de *gateways* para conversão e mapeamento de dados do protocolo *Modbus TCP* para OPC UA, permitindo integrar ativos antigos ao ecossistema convergente sem necessidade de substituição imediata, preservando os investimentos existentes e ampliando de forma progressiva e segura a integração entre as redes.

Essa arquitetura em camadas está alinhada ao modelo *Purdue Reference Model*, adaptado para a Indústria 4.0, no qual o OPC UA atua como camada de integração no nível 3 MES, conectando-se ao nível 2 SCADA/DCS via *gateways* seguros e ao nível 4 ERP/*Cloud* por meio de interfaces padronizadas (GRAÇA, 2024; ALTUS, 2024). A análise comparativa dos protocolos de convergência analisados é ilustrada na tabela 2.

Tabela 2 – Comparativo dos protocolos de convergência TI-TA

Protocolo	Segurança Nativa	Interoperabilidade	Integração TI-TA	Suporte a Legados
OPC UA	Alta	Alta	Alta	Alta
EtherNet/IP	Básica	Boa	Alta	Boa
Profinet	Básica	Boa	Boa	Nenhum
Modbus TCP	Nenhum	Básica	Básica	Nenhum

Fonte: elaborado pelos autores com base em ALTUS (2024), FIBERROAD (2025), COME-STAR (2026) & WTSNET (2026).

A escolha dos protocolos não se resume ao desempenho de transmissão, envolve uma avaliação multidimensional que considera segurança nativa, interoperabilidade entre fabricantes, capacidade de integração com sistemas corporativos e compatibilidade com ativos legados. Os quatro protocolos centrais desta pesquisa: OPC UA, *EtherNet/IP, Profinet e Modbus TCP*, apresentam perfis distintos em cada uma dessas dimensões, razão pela qual nenhum deles, isoladamente, constitui solução universal para ambientes de convergência TI-TA (FIBERROAD, 2025; COME-STAR, 2026).

A divergência mais significativa entre os protocolos analisados está na forma como a segurança é tratada. As versões tradicionais de protocolos industriais como *Modbus TCP* e *EtherNet/IP* foram concebidas em um contexto no qual as redes de automação eram consideradas isoladas e confiáveis, razão pela qual não incorporavam, nativamente, mecanismos de autenticação, criptografia e verificação de integridade. O OPC UA, por sua vez, foi projetado considerando que os dados industriais poderiam atravessar diferentes redes e domínios de segurança, integrando esses mecanismos à própria arquitetura do protocolo. Sua comunicação segura baseia-se na criação de canais

protegidos, na autenticação das aplicações por meio de certificados digitais X.509 e na negociação de modos e políticas de segurança que determinam a assinatura e a criptografia das mensagens. Entretanto, a proteção efetiva depende da configuração adequada desses recursos, uma vez que o OPC UA também permite modos de comunicação sem assinatura ou criptografia.

Especificamente, o OPC UA opera em três modos de segurança configuráveis: *None* (sem proteção), *Sign* (assinatura digital sem criptografia) e *SignAndEncrypt* (assinatura e criptografia plena com TLS 1.2/1.3 e certificados X.509). Esse último fornece proteção completa, impedindo adulteração e interceptação. Por este motivo a norma IEC 62541 recomenda esse modo de segurança para todos os ambientes industriais.

Na tabela comparativa, o *EtherNet/IP* e o *Profinet* foram classificados como básicos, no quesito segurança nativa. Para o *EtherNet/IP*, a classificação decorre da possibilidade de qualquer dispositivo poder estabelecer conexões com um adaptador *EtherNet/IP* e executar operações, incluindo a reinicialização do equipamento. Esse protocolo depende de controles externos, *VLANs* e segmentação de rede para mitigação dos riscos. Já o *Profinet* foi projetado para operar em redes isoladas e, portanto, oferece pouca ou nenhuma funcionalidade de segurança. O protocolo dispõe de segurança funcional consolidada por meio do perfil *PROFIsafe* (IEC 61784-3), voltado à proteção física de máquinas e operadores, mas não incorpora criptografia de dados nem autenticação de rede por padrão, o que o mantém na classificação de segurança nativa básica (PROFIBUS & PROFINET INTERNATIONAL, 2025).

O *Modbus TCP* apresentou a pior classificação. Embora amplamente utilizado pela sua simplicidade, interoperabilidade e desempenho em tempo real, esse protocolo foi originalmente projetado sem quaisquer considerações de segurança, carecendo de recursos essenciais como criptografia, proteção de integridade e autenticação. Isso expõe os sistemas de controle industrial a ameaças graves, incluindo interceptação, injeção de comandos e ataques de repetição, especialmente quando operam sobre redes não seguras. A classificação ocorre, portanto, a partir de uma limitação estrutural e histórica: o protocolo foi criado em 1979, décadas antes de a segurança cibernética tornar-se uma preocupação central em ambientes industriais.

O desempenho de transmissão também é contrastante entre os protocolos. O *Profinet* apresenta o maior desempenho entre os protocolos analisados: opera a velocidades de transmissão de 100 Mbit/s ou 1 Gbit/s e define três classes de comunicação em tempo real: Classe 1 (*RT*, *Real Time*) para ciclos na ordem de dezenas de milissegundos; e Classes 2 e 3 (*IRT*, *Isochronous Real Time*) para sistemas que requerem ciclos na ordem de centenas de microssegundos e variações de tempo de ciclo inferiores a 1 µs. Essa característica torna o protocolo uma referência para aplicações que exigem sincronismo, como a robótica.

O *EtherNet/IP* opera a 100 Mbit/s e oferece comunicação em tempo real adequada à maioria das aplicações industriais de controle, com tempos de ciclo típicos de 1 a 10 ms em redes bem dimensionadas (FIBERROAD, 2025). O OPC UA, por sua vez, não foi originalmente concebido para sistemas com controle em tempo real. Dessa forma, o protocolo suporta dois modelos de comunicação: cliente-servidor (baseado em TCP/IP ponto a ponto) e publicador-assinante (um para muitos, por meio da extensão *PubSub*), sem capacidade de tempo real nativa. Apesar disso, iniciativas como o OPC UA sobre TSN (*Time-Sensitive Networking*) buscam superar essa limitação para aplicações de controle determinístico. O *Modbus TCP* opera sobre TCP/IP padrão a 100 Mbit/s e apresenta latências típicas de 50 a 200 ms em modo de *polling*, aceitáveis para supervisão e aquisição de dados, mas insuficientes para controle de movimento ou sincronismo (INDUSTRIALMONITORDIRECT, 2026).

Outro fator relevante é a interoperabilidade, que define a capacidade de um protocolo comunicar-se de forma transparente com dispositivos, sistemas e fabricantes diferentes. O OPC UA se destaca nessa dimensão porque, além da comunicação, provê modelagem semântica de informações: fornece modelos de informação unificados para a descrição semântica compatível com múltiplos fornecedores de máquinas, plantas e empresas inteiras, sendo projetado como arquitetura orientada a serviços. Isso significa que os dados trafegam acompanhados de contexto e metadados, permitindo que sistemas de ERP, plataformas analíticas e aplicações de inteligência artificial os interpretem sem conversões intermediárias.

Em seguida, o *EtherNet/IP* ocupa a segunda posição por suportar centenas de fabricantes no ecossistema e permitir integração com outros protocolos da família CIP (*DeviceNet, ControlNet*). No entanto, sua interoperabilidade é circunscrita a esse

ecossistema e não oferece modelagem semântica nativa (LRI AUTOMAÇÃO, 2024). O *Profinet*, por sua vez, é o padrão dominante em ambientes Siemens e possui ampla adoção na Europa, mas sua interoperabilidade entre diferentes fabricantes exige arquivos GSD e configurações específicas, o que reduz a sua flexibilidade em ambientes heterogêneos (PROFIBUS & PROFINET INTERNATIONAL, 2025). Por fim, o *Modbus TCP* apresentou a pior interoperabilidade. Apesar da sua simplicidade garantir a ele suporte em praticamente qualquer dispositivo industrial, a ausência de modelagem semântica faz com que os dados sejam transmitidos como valores brutos em registradores de 16 bits, sem contexto, limitando severamente sua utilidade em arquiteturas de Indústria 4.0 (COME-STAR, 2026).

A integração TI-TA corresponde ao grau de facilidade com que cada protocolo conecta os dispositivos do chão de fábrica a sistemas corporativos, plataformas em nuvem e ferramentas analíticas. Nesse aspecto, o OPC UA apresenta elevada capacidade de integração e escalabilidade, podendo ser empregado desde a comunicação com uma única máquina até arquiteturas industriais compostas por milhares de nós, desde que adequadamente dimensionadas. O protocolo também oferece mecanismos como redundância, reconexão de sessões, assinaturas de dados e armazenamento temporário de mensagens, os quais aumentam a disponibilidade da comunicação e reduzem o risco de perda de informações diante de instabilidades na rede. Essas características atendem às demandas da Indústria 4.0 e da Internet Industrial das Coisas, que exigem um fluxo contínuo, seguro e contextualizado de dados entre sensores, sistemas industriais e aplicações analíticas. No Modelo *Purdue*, o protocolo pode estabelecer comunicação entre diferentes níveis da arquitetura, especialmente ao integrar sistemas de controle e supervisão aos sistemas MES, localizados no nível 3, e destes com sistemas corporativos, como o ERP, e plataformas em nuvem.

O *EtherNet/IP* também apresenta elevada capacidade de integração entre TI e TA, pois utiliza tecnologias *Ethernet* e TCP/IP, amplamente empregadas nas redes corporativas. Contudo, a ausência de segurança nativa exige camadas adicionais de proteção (ODVA, 2023). O *Profinet*, por sua vez, apresenta boa capacidade de integração e, embora seja amplamente associado a sistemas MES e SCADA no contexto Siemens, sua integração com ambientes de nuvem e ERP de terceiros requer tecnologias complementares, como OPC UA, MQTT e *gateways*. O *Modbus TCP* recebe

classificação básica: ainda que onipresente no chão de fábrica, sua integração com sistemas TI é sempre mediada por *gateways* ou servidores OPC UA que traduzem seus registradores brutos em dados estruturados (FIBERROAD, 2025).

Em relação ao suporte a sistemas legados, o *Modbus TCP* se destacou, evidenciando um desafio recorrente nos ambientes industriais convergidos: o protocolo mais antigo e com menos mecanismos nativos de segurança permanece amplamente utilizado devido à compatibilidade com a base instalada. Criado originalmente em 1979, com apenas o nome de *Modbus*, adquiriu o sufixo *TCP* posteriormente, ao ser adaptado para operar sobre redes TCP/IP. Sua simplicidade o torna suportado por praticamente toda a base instalada de CLPs, IHMs e sensores industriais das últimas quatro décadas. Dessa forma, sua substituição pode ser tecnicamente inviável em muitos contextos sem a troca completa dos equipamentos.

O *EtherNet/IP* apresenta suporte moderado por ser compatível com equipamentos das últimas duas décadas no ecossistema ODVA, mas não com dispositivos anteriores que utilizavam protocolos seriais. O *Profinet* tem suporte limitado, embora preveja mecanismos de migração a partir do PROFIBUS, sua adoção exige hardware específico para IRT e é mais restrita a equipamentos Siemens de geração recente. O OPC UA, por sua vez, suporta sistemas legados via *gateway*: não se comunica diretamente com dispositivos *Modbus* ou *Profinet* antigos, mas atua como camada de abstração acima deles, traduzindo os dados brutos desses protocolos em modelos de informação semânticos e seguros para consumo pelos sistemas TI (ALTUS, 2024).

A análise multidimensional evidencia que os protocolos cumprem funções complementares em uma arquitetura de convergência TI-TA estruturada em camadas. *Profinet* e *EtherNet/IP* são adequados ao controle determinístico no chão de fábrica (níveis 0 a 2 do Modelo *Purdue*), desde que acompanhados de controles externos de segurança. O OPC UA é o protocolo de referência para a camada de integração (nível 3), conectando com segurança os ambientes operacional e corporativo. Já o *Modbus TCP* é inevitável para compatibilidade com sistemas legados, mas deve ser confinado a segmentos isolados e convertido para OPC UA por meio de *gateways* seguros antes de qualquer comunicação com redes TI. Conforme sintetizam Fiberroad (2025) e Come-Star (2026), a convergência segura não resulta da escolha de um único protocolo, mas da orquestração deliberada de todos eles dentro de uma arquitetura segmentada e normativa.

3.3 Riscos de segurança cibernética na integração TI-TA

A integração entre redes industriais e redes corporativas amplia expressivamente a superfície de ataque, uma vez que ativos anteriormente isolados passam a se comunicar com sistemas conectados à infraestrutura de TI e, em alguns casos, à Internet. Segundo o relatório *State of Operational Technology and Cybersecurity 2025* (Fortinet, 2025), a manufatura foi, pelo segundo ano consecutivo, o setor mais afetado por ataques de intrusão, superando inclusive o setor financeiro (VDI BRASIL, 2026). No Brasil, 71% dos *malwares* direcionados à indústria correspondem a *ransomware*, enquanto os ataques a protocolos industriais, como *Modbus e EtherNet/IP*, cresceram 84% (WTSNET, 2026). Dessa forma, torna-se necessário adotar estratégias específicas de segurança para ambientes industriais, incluindo segmentação de redes, controle rigoroso de acesso, monitoramento contínuo do tráfego, uso de *firewalls* industriais e atualização das políticas de comunicação entre TI e TA.

Os riscos de segurança associados ao protocolo de convergência entre TI e TA podem ser organizados em cinco dimensões principais. A primeira dimensão refere-se à ampliação da superfície de ataque decorrente da adoção desse protocolo. Com o aumento do número de dispositivos conectados às redes industriais, como CLPs, módulos de I/O, sensores, *gateways* e IHMs (Interface Homem-Máquina), crescem também os possíveis pontos de entrada para agentes maliciosos. A implementação do protocolo de convergência TI/TA reduziu a antiga separação física entre os ambientes corporativo e industrial, conhecida como *air gap*, tornando sistemas antes isolados mais suscetíveis a ataques remotos (INTERNATIONALIT, 2023; 3STRUCTURE, 2025).

A segunda dimensão envolve a presença de dispositivos industriais legados e desprotegidos no contexto de protocolo de convergência. Muitos ativos de TA foram projetados para operar por longos períodos em redes isoladas, sem considerar requisitos modernos de segurança, como autenticação, criptografia ou controle de acesso. Quando esses equipamentos passam a se comunicar com redes corporativas, tornam-se vetores de ataque de difícil mitigação, principalmente por apresentarem limitações técnicas, dependência de fornecedores específicos e baixa compatibilidade com soluções atuais de proteção (INTERNATIONALIT, 2023; CGONE, 2024).

A terceira dimensão está relacionada à dificuldade de aplicação de atualizações e correções de segurança em que utilizam o protocolo . Sistemas de automação industrial geralmente exigem alta disponibilidade, muitas vezes operando em regime contínuo. Essa característica dificulta a criação de janelas de manutenção para aplicação de *patches*, atualização de *firmware* ou substituição de componentes vulneráveis no escopo do protocolo. Como consequência, falhas conhecidas podem permanecer ativas por meses ou até anos, aumentando a exposição dos sistemas industriais a ataques (INTERNATIONALIT, 2023; CG-ONE, 2024).

A quarta dimensão corresponde aos ataques direcionados e às ameaças persistentes avançadas, conhecidas como APTs (*Advanced Persistent Threats*) explorando vulnerabilidades do protocolo de convergencia. De acordo com o Relatório Global de Ameaças da Fortinet 2025, atores maliciosos avançados têm reduzido campanhas genéricas em massa e passado a realizar reconhecimento detalhado de redes industriais. Nesse contexto, protocolos vulneráveis, como o *Modbus,* podem ser explorados como rotas de acesso automatizadas a ambientes críticos (3STRUCTURE, 2025). Nesses casos, o objetivo do ataque não se limita ao roubo de dados, podendo envolver a interrupção de processos produtivos, a manipulação de comandos industriais e o comprometimento de serviços essenciais.

Por fim, a quinta dimensão refere-se à propagação lateral de ameaças facilitadas pelo protocolo de convergência, que seria uma brecha inicial na rede corporativa pode ser utilizada como ponto de partida para alcançar sistemas de controle industrial. Esse movimento lateral permite que invasores avancem progressivamente entre segmentos da rede, até atingir ativos críticos de automação. As consequências podem incluir paradas de produção, danos a equipamentos, perdas financeiras e, em cenários mais graves, riscos físicos aos trabalhadores e à segurança operacional da planta (INTERNATIONALIT, 2023; VDI BRASIL, 2026).

3.4 Implicações regulatórias e organizacionais da convergência TI-TA

Além dos riscos técnicos, a convergência entre TI e TA também produz impactos regulatórios e organizacionais relevantes. No aspecto normativo, uma integração mal planejada pode gerar não conformidades com a série IEC 62443, referência internacional

para a segurança de Sistemas de Controle e Automação Industrial, também denominados IACS (*Industrial Automation and Control Systems*). No contexto brasileiro, destaca-se ainda a ABNT IEC TS 62443-1-1, publicada em agosto de 2023, que estabelece terminologia, conceitos e modelos relacionados à segurança cibernética de sistemas industriais (ABNT, 2023).

A centralização de dados operacionais, registros de eventos, logs de acesso e informações de desempenho em plataformas corporativas também pode gerar obrigações relacionadas à Lei Geral de Proteção de Dados Pessoais (LGPD), especialmente quando esses dados permitem identificar pessoas, operadores, usuários de sistemas ou padrões de comportamento associados à operação industrial (CG-ONE, 2024). Assim, a convergência TI-TA não deve ser analisada apenas como uma questão de conectividade ou desempenho, mas também como um processo que exige governança, rastreabilidade, controle de acesso e responsabilidade sobre o tratamento das informações.

Do ponto de vista organizacional, os impactos de um incidente cibernético em ambientes industriais tendem a ser mais amplos do que em sistemas corporativos tradicionais. Enquanto em redes de TI os efeitos geralmente envolvem indisponibilidade de sistemas, vazamento de dados ou prejuízos administrativos, em ambientes de TA as consequências podem atingir diretamente o processo físico. Entre os principais efeitos estão a interrupção de linhas de produção, perdas financeiras por paradas não programadas, danos a equipamentos, comprometimento da qualidade dos produtos, exposição de trabalhadores a riscos operacionais, danos à imagem institucional, responsabilização civil e penal em caso de acidentes e sanções regulatórias.

Dessa forma, a segurança da convergência TI-TA deve ser tratada como uma responsabilidade estratégica da organização. A proteção dos ambientes industriais não depende apenas da escolha de protocolos mais seguros, mas também da definição de políticas institucionais, da capacitação das equipes, da documentação dos ativos, da gestão de riscos e da adoção de práticas contínuas de auditoria e conformidade.

3.5 Estratégias de mitigação de riscos

Com base na revisão da literatura e nas recomendações associadas à IEC 62443, a mitigação dos riscos na convergência entre TI e TA deve adotar uma abordagem integrada,

envolvendo dimensões técnicas, organizacionais e normativas. Essa visão é necessária porque os riscos identificados não se concentram em um único ponto da arquitetura. Eles podem surgir da exposição de protocolos legados, da ausência de segmentação de rede, da baixa maturidade das equipes, da falta de inventário de ativos, da ausência de políticas de acesso ou da não conformidade com normas de segurança cibernética industrial.

Nesse sentido, a convergência segura não deve ser compreendida apenas como a implantação de um protocolo ou ferramenta específica, mas como a construção de uma arquitetura de proteção em camadas. Essa arquitetura deve combinar segmentação, controle de acesso, monitoramento, escolha adequada de protocolos, gestão contínua de riscos e conformidade normativa. As principais estratégias de mitigação podem ser organizadas em três dimensões: técnica, organizacional e normativa.

3.5.1 Dimensão técnica

Na dimensão técnica, a primeira estratégia consiste na adoção de uma arquitetura de rede segura e segmentada. A norma IEC 62443 recomenda a organização da rede industrial em zonas e condutos, de modo que ativos com funções, criticidade e níveis de risco semelhantes sejam agrupados em zonas protegidas, enquanto os fluxos de comunicação entre elas sejam controlados por condutos específicos. Essa abordagem cria barreiras digitais que reduzem a propagação de ameaças dentro do ambiente industrial. Assim, mesmo que um atacante comprometa inicialmente a rede corporativa ou uma IHM, a segmentação dificulta o avanço até CLPs, sistemas SCADA e demais ativos críticos da automação (VDI BRASIL, 2026).

Uma arquitetura segura deve incluir uma zona desmilitarizada (DMZ) industrial entre os ambientes de TI e TA, evitando conexões diretas entre redes corporativas e sistemas de controle. Essa zona intermediária permite concentrar servidores de integração, historiadores, *gateways*, sistemas de coleta de dados e mecanismos de inspeção de tráfego. Além disso, recomenda-se o uso de *firewalls* industriais, listas de controle de acesso, roteamento restritivo, políticas de microssegmentação e separação lógica entre redes administrativas, supervisórias e de controle.

Outra estratégia relevante é a adoção de princípios de *Zero Trust* em ambientes industriais. A aplicação dessa abordagem à TA, em alinhamento com a IEC 62443, parte do princípio de que nenhuma entidade deve ser considerada confiável por padrão, mesmo

quando localizada dentro da rede interna. Cada acesso deve ser verificado, autenticado e autorizado com base no menor privilégio possível. Assim, operadores, estações de engenharia, servidores, aplicações e dispositivos devem ter permissões estritamente limitadas às funções necessárias para sua operação (MUNIO SECURITY, 2024).

A priorização de protocolos seguros também é essencial. O OPC UA se destaca nesse contexto por oferecer recursos nativos de segurança. Quando configurado adequadamente, com uso de TLS 1.2 ou TLS 1.3, certificados válidos e políticas de acesso bem definidas, o protocolo reduz a exposição de dados sensíveis e evita a transmissão de informações em texto simples (ALTUS, 2024; FERSILTEC, 2022). Já em ambientes que ainda dependem de dispositivos legados baseados em *Modbus TCP*, recomenda-se o uso de *gateways* seguros, encapsulamento controlado, segmentação rígida e listas de controle de acesso restritivas, evitando que esses ativos sejam expostos diretamente à rede corporativa ou à Internet.

3.5.2 Dimensão organizacional

Na dimensão organizacional, a mitigação dos riscos depende da criação de processos contínuos de gestão, monitoramento e capacitação. A gestão contínua de riscos deve seguir uma lógica cíclica, compatível com o modelo PDCA (Planejar, Fazer, Verificar, Agir) previsto em práticas de governança e segurança, envolvendo planejamento, execução, verificação e melhoria contínua. Esse processo deve incluir o inventário de ativos industriais, o mapeamento das ameaças, a classificação da criticidade dos sistemas, a definição de perfis de acesso, a auditoria de logs e a revisão periódica das políticas de segurança (UNIFOA, 2017; IIA BRASIL, 2018).

O inventário de ativos é uma etapa fundamental, pois não é possível proteger adequadamente dispositivos que a organização desconhece. Em ambientes industriais, é comum a presença de CLPs antigos, IHMs desatualizadas, estações de engenharia, *gateways*, sensores inteligentes e servidores de supervisão que permanecem em operação por longos períodos. A ausência de visibilidade sobre esses componentes dificulta a identificação de vulnerabilidades, dependências críticas e pontos de exposição à rede corporativa.

Outro aspecto essencial é a capacitação cruzada entre equipes de TI e TA. A literatura aponta que uma das maiores dificuldades da convergência segura é a lacuna de

profissionais com domínio simultâneo de redes corporativas, segurança da informação, automação industrial e processos produtivos. Equipes de TI geralmente possuem maior familiaridade com proteção de dados, *firewalls*, autenticação e monitoramento de redes. Já equipes de TA conhecem melhor a lógica de funcionamento dos processos físicos, a criticidade dos CLPs, os requisitos de disponibilidade e os impactos de uma parada de produção. A convergência segura exige a aproximação dessas competências por meio de capacitações, equipes multidisciplinares e práticas de comunicação contínua (INTERNATIONALIT, 2023; CG-ONE, 2024).

Nesse contexto, a formação de equipes especializadas, como *Blue Teams* TI-TA, contribui para a defesa ativa dos ambientes industriais. Essas equipes devem ser capazes de interpretar alertas de segurança considerando não apenas indicadores técnicos, mas também o impacto operacional de cada evento. Um comportamento anômalo em uma rede industrial, por exemplo, não deve ser analisado apenas como tráfego incomum, mas também como possível indício de alteração de parâmetros de processo, falha de comunicação com CLPs ou tentativa de manipulação de comandos.

A criação de um Centro de Operações de Segurança (SOC) integrado também representa uma estratégia importante. Esse tipo de estrutura permite correlacionar eventos oriundos de sistemas corporativos e industriais, ampliando a capacidade de detecção e resposta a incidentes. Diferentemente de um centro tradicional, voltado apenas à TI, um SOC integrado deve considerar critérios de segurança, confiabilidade e desempenho operacional. A metodologia SRP (*Safety, Reliability and Performance*) reforça essa perspectiva ao priorizar a confidencialidade dos dados, a segurança física, a continuidade produtiva e a confiabilidade dos processos industriais (MUNIO SECURITY, 2024).

3.5.3 Dimensão normativa

Na dimensão normativa, a adoção da série IEC 62443 fornece uma estrutura de referência para identificar, classificar e mitigar riscos cibernéticos em sistemas de automação e controle industrial. A norma estabelece conceitos como zonas, condutos, níveis de segurança e requisitos técnicos e organizacionais aplicáveis a diferentes componentes da arquitetura industrial. A utilização dos *Security Levels* (SL 1 a SL 4) permite adequar o nível de proteção à criticidade dos ativos e ao perfil de ameaça considerado, evitando tanto a subproteção de sistemas críticos quanto a aplicação

inadequada de controles excessivos em ativos de menor impacto (MUNIO SECURITY, 2024; ABNT, 2023).

A ABNT IEC TS 62443-1-1, ao trazer conceitos e terminologias da IEC 62443 para o contexto brasileiro, contribui para padronizar a compreensão sobre segurança cibernética industrial no país. Essa padronização é relevante porque facilita a comunicação entre gestores, equipes técnicas, fornecedores, integradores e auditores, reduzindo ambiguidades na definição de responsabilidades e requisitos de segurança (ABNT, 2023). Além disso, as atualizações recentes da série ISA/IEC 62443 reforçam a necessidade de alinhar os ambientes industriais aos novos paradigmas de risco, incentivando práticas de certificação e avaliação contínua de conformidade, como a certificação ISA *Secure* (ECHELON CYBER, 2025).

O alinhamento com a LGPD também deve ser considerado quando dados pessoais ou identificáveis circulam por plataformas convergentes. Embora muitos dados industriais sejam essencialmente operacionais, ambientes integrados podem registrar informações associadas a usuários, operadores, turnos, credenciais, eventos de acesso e atividades realizadas em sistemas supervisórios. Nesses casos, a organização deve adotar princípios de privacidade desde a concepção (*Privacy by Design*), minimização de dados, controle de acesso, rastreabilidade e retenção adequada das informações, em conformidade com a Lei nº 13.709/2018.

Portanto, a mitigação dos riscos regulatórios e normativos depende da integração entre governança, documentação, auditoria, políticas de segurança e conformidade legal. A segurança da convergência TI-TA não pode ser tratada apenas como uma ação pontual, mas sim como um processo permanente de gestão de riscos, envolvendo tecnologia, pessoas, processos e normas.

4. Conclusão

A convergência entre TI e TA representa uma tendência estratégica para a modernização industrial. Ao permitir a integração entre dados do chão de fábrica, sistemas supervisórios, plataformas analíticas, MES, ERP e ambientes em nuvem, essa convergência favorece o monitoramento em tempo real, a tomada de decisão baseada em dados, a manutenção preditiva e a otimização dos processos produtivos. Entretanto, os benefícios associados à conectividade também introduzem riscos cibernéticos mais

complexos, especialmente porque incidentes em ambientes industriais podem gerar impactos diretos sobre equipamentos, linhas de produção, trabalhadores e continuidade operacional.

A análise realizada indica que nenhum protocolo, isoladamente, é capaz de atender a todos os requisitos de uma arquitetura segura de convergência entre TI e TA. O OPC UA apresenta maior adequação para cenários de integração entre ambientes industriais e corporativos, principalmente por oferecer interoperabilidade, modelagem semântica dos dados e recursos nativos de segurança, como autenticação, criptografia e controle de acesso. Contudo, sua efetividade depende da configuração adequada desses mecanismos e da adoção de controles complementares. Protocolos como *EtherNet/IP e Profinet* permanecem relevantes em aplicações de controle industrial que exigem desempenho, baixa latência e comunicação com CLPs, I/O distribuídos e atuadores. Já o *Modbus TCP,* embora apresente limitações significativas de segurança, continua importante para a integração de dispositivos legados, desde que utilizado em redes segmentadas, com *gateways* seguros, *firewalls* industriais e políticas restritivas de comunicação.

No campo da segurança cibernética, os dados analisados reforçam a criticidade do cenário atual. O crescimento de ataques direcionados a ambientes de Tecnologia Operacional, a exploração de protocolos industriais legados, a ocorrência de *ransomware* industrial e a possibilidade de propagação lateral entre redes corporativas e industriais evidenciam que a convergência TI-TA deve ser conduzida com critérios técnicos, organizacionais e normativos bem definidos. Nesse contexto, estratégias como segmentação por zonas e condutos, adoção de DMZ industrial, controle rigoroso de acesso, aplicação adaptada de princípios de *Zero Trust*, uso de protocolos com recursos nativos de segurança e monitoramento integrado por SOC TI-TA tornam-se essenciais para reduzir a exposição dos ativos industriais.

Conclui-se que a integração segura entre TI e TA exige uma abordagem em camadas, combinando escolha adequada de protocolos, arquitetura de rede segmentada, governança organizacional, capacitação das equipes e conformidade normativa. A adoção da IEC 62443, da ABNT IEC TS 62443-1-1 e de práticas associadas à LGPD contribui para fortalecer a gestão de riscos, a rastreabilidade, a proteção dos ativos industriais e a resposta a incidentes. Dessa forma, a segurança cibernética deve ser compreendida não

como elemento complementar, mas como requisito fundamental para a continuidade, a confiabilidade e a competitividade da indústria conectada.

Como trabalhos futuros, recomenda-se a avaliação experimental de arquiteturas de convergência TI-TA em ambientes industriais reais ou simulados, considerando métricas como latência, disponibilidade, interoperabilidade, segmentação e eficácia dos controles de segurança. Também se sugere investigar o uso de inteligência artificial e aprendizado de máquina na detecção de anomalias em redes industriais convergidas, especialmente em cenários que envolvam protocolos legados, tráfego heterogêneo e integração com plataformas corporativas.

Referências

3STRUCTURE. Cibersegurança industrial: os riscos no ambiente OT na era 4.0. set. 2025. Disponível em: https://3structure.com.br/ciberseguranca-industrial-os-riscos-no-ambiente-ot-na-era-4-0/. Acesso em: 24 maio 2026.

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT IEC TS 62443-1-1: redes de comunicação industrial — Segurança do sistema e da rede — Parte 1-1: terminologia, conceitos e modelos. Rio de Janeiro: ABNT, 2023.

ALTUS. Conectividade na Indústria 4.0: conhecendo os protocolos OPC UA e MQTT. 19 set. 2024. Disponível em: https://www.altus.com.br/post/419/conectividade-na-industria-4-0-3a-conhecendoos-protocolos-opc-ua-e-mqtt. Acesso em: 13 maio 2026.

BRANCO, Gabriela Musse; AHLERT, Hubert; MOTTA, Thiago Stein. Sistemática para integração entre processos e TI. In: WORKSHOP DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DAS IFES, 9., 2015, Belo Horizonte. Anais [...]. Belo Horizonte: WTICIFES, 2015.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2018. Disponível em: planalto.gov.br. Acesso em: 1 ago. 2026.

CENTRO UNIVERSITÁRIO DE VOLTA REDONDA (UniFOA). XI Colóquio Técnico-Científico do UniFOA. Volta Redonda: Editora FOA, 2017. Disponível em: https://editora.unifoa.edu.br/wp-content/uploads/2023/07/exatas.pdf. Acesso em: 1 ago. 2026.

CG-ONE. Convergência TI/TO e os seus impactos na cibersegurança industrial. 10 jul. 2024. Disponível em: https://cg-one.com/blog/convergencia-ti-to-e-os-seus-impactos-na-ciberseguranca-industrial/. Acesso em: 13 maio 2026.

COME-STAR. Protocolos de comunicação PLC: tipos, usos e guia industrial. 2026. Disponível em: https://www.come-star.com/pt/blog/ultimate-guide-to-plccommunication-protocols-types-uses/. Acesso em: 14 maio 2026.

CRYPTOID. Indústria 4.0 depende da convergência entre OT e TI para avançar no Brasil. 2020. Disponível em: https://cryptoid.com.br. Acesso em: 13 maio 2026.

ECHELON CYBER. Navigating the 2024 updates to ISA/IEC 62443. 2025. Disponível em: https://echeloncyber.com/intelligence/entry/navigating-the-2024-updates-to-isaiec-62443. Acesso em: 14 maio 2026.

FERTRON. O que você precisa saber sobre a rede PROFINET? 14 fev. 2023. Disponível em: https://fertron.com.br/2023/02/14/o-que-voce-precisa-saber-sobre-a-rede-profinet/. Acesso em: 1 ago. 2026.

FERSILTEC. OPC UA: o que é e qual é o seu papel na automação industrial? 31 maio 2022. Disponível em: https://fersiltec.com.br/blog/automacao-industrial/opc-uao-que-e-e-qual-e-o-seu-papel-na-automacao-industrial/. Acesso em: 13 maio 2026.

FIBERROAD. O que é convergência TI/TO? 2025. Disponível em: https://fiberroad.com/pt/what-is-it-ot-convergence/. Acesso em: 15 maio 2026.

FORTINET. 2025 State of Operational Technology and Cybersecurity Report. Sunnyvale: Fortinet, 2025. Disponível em: https://www.fortinet.com/resources/reports/state-ot-cybersecurity. Acesso em: 13 maio 2026.

FREITAS, Carlos Márcio. Modbus: fundamentos e aplicações. Embarcados, 2014. Disponível em: https://embarcados.com.br/protocolo-modbus/. Acesso em: 1 ago. 2026.

GRAÇA, V. C. OPC UA na automação, confiabilidade de dados e monitoramento para processo. In: CICTED, 13., 2024, Taubaté. Anais [...]. Taubaté: UNITAU, 2024.

IEB MEDIA. Topologia de rede utilizando Ethernet e TCP/IP. [S. l.], 2026. Disponível em: iebmedia.com. Acesso em: 1 ago. 2026.

INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC). **IEC TR 62541-1**: OPC Unified Architecture Overview and Concepts Guide. Edition 3.0. Geneva: IEC, 2026.

IIA BRASIL. Auditoria interna de cibersegurança: aspectos regulatórios e práticos. São Paulo: IIA Brasil, 2018.

INTERNATIONALIT. Convergência TI/OT: desafios e riscos de segurança cibernética industrial. 2023. Disponível em: https://internationalit.com. Acesso em: 18 maio 2026.

LRI AUTOMAÇÃO INDUSTRIAL. MQTT-SN: Uma variante projetada para redes de sensores. Blog LRI, 5 jan. 2024. Disponível em: https://pt.linkedin.com/pulse/mqtt-sn-uma-variante-projetada-para-redes-29ywf. Acesso em: 1 ago. 2026.

LUGLI, Alexandre Baratella; SANTOS, Max Mauro Dias. Redes industriais para automação industrial: AS-I, PROFIBUS e PROFINET. São Paulo: Érica, 2010.

MUNIO SECURITY. Zero Trust e IEC 62443: fortalecendo a segurança industrial OT. 2024. Disponível em: https://muniosecurity.com/zero-trust-e-iec-62443. Acesso em: 13 maio 2026.

NXP SEMICONDUCTORS. PF5024: Power management integrated circuit (PMIC) for high performance applications. Rev. 1.0. Eindhoven: NXP Semiconductors, 2024. Disponível em: https://www.nxp.com/docs/en/data-sheet/PF5024.pdf. Acesso em: 1 ago. 2026.

ODVA. Device-based firewall profile added to CIP Security to further protect EtherNet/IP networks. Nuremberg: ODVA, 2023. Disponível em: https://www.odva.org/news/device-based-firewall-profile-added-to-cip-security-to-further-protect-ethernet-ip-networks/. Acesso em: 20 maio 2026.

PI NORTH AMERICA. PROFIBUS System Description. [S. l.]: PROFIBUS Nutzerorganisation e.V. (PNO), 2010. Disponível em: https://us.profinet.com/. Acesso em: 1 ago. 2026.

PROFIBUS & PROFINET INTERNATIONAL. PROFINET: industrial Ethernet solution. 2025. Disponível em: https://www.profibus.com. Acesso em: 20 maio 2026.

QUINTELLA, H.; ROCHA, H. Nível de maturidade e comparação dos PDPs de produtos automotivos. Produção, v. 17, n. 1, p. 199–215, 2007.

SIEMENS. PROFINET: comunicação industrial para digitalização. 2026. Disponível em: https://www.siemens.com/pt-br/products/profinet/. Acesso em: 20 maio 2026.

SILVA, João; PEREIRA, Maria. Aplicação do modelo Purdue em arquiteturas de TI/TA. Revista Brasileira de Automação, São Paulo, v. 15, n. 2, p. 45–60, 2021.

UNIFOA. Segurança da informação em ambientes industriais: auditoria e conformidade. Volta Redonda: UniFOA, 2017.

VDI BRASIL. Cibersegurança na Indústria 4.0: como proteger a operação industrial contra ataques e paradas de produção. jan. 2026. Disponível em: https://www.vdibrasil.com/ciberseguranca-industria-4-0/. Acesso em: 24 maio 2026.

WESTCON. Integração OPC UA e automação industrial: conceitos e aplicações. 2022. Disponível em: https://westcon.com.br. Acesso em: 13 maio 2026.

WTSNET. Segurança IoT e OT em 2026: como proteger sua operação. abr. 2026. Disponível em: https://www.wtsnet.com.br/seguranca-iot-ot-2026/. Acesso em: 13 maio 2026.

YANG, Ming-Fu; LI, Guang. Analysis of PROFINET IO communication protocol. In: INTERNATIONAL CONFERENCE ON INSTRUMENTATION AND MEASUREMENT, COMPUTER, COMMUNICATION AND CONTROL, 4., 2014. Proceedings [...]. Harbin: IEEE, 2014. p. 945–949.