



**FACULDADE PRESIDENTE ANTÔNIO CARLOS DE
CONSELHEIRO LAFAIETE**

ENGENHARIA DE CONTROLE E AUTOMAÇÃO



**INTEGRAÇÃO DE SISTEMAS LEGADOS NA INDÚSTRIA 4.0: UM MAPEAMENTO
SISTEMÁTICO DA LITERATURA**

**LEGACY SYSTEMS INTEGRATION IN INDUSTRY 4.0: A SYSTEMATIC
LITERATURE MAPPING**

Carlos Eduardo Rodrigues Crespo

Alex Vitorino

Rodovia MG 482 - Gigante, Conselheiro Lafaiete - MG, 36400-000 – Brasil

<161-000239@aluno.unipac.br>.

Resumo

As atualizações de sistemas e equipamentos legados nos processos industriais representam desafios para as empresas que desejam modernizar suas operações. A adoção da indústria 4.0 é essencial para transformar as fábricas em ambientes inteligentes e eficientes. No entanto, a substituição completa de equipamentos por versões de última geração pode ser economicamente inviável. Uma solução promissora é a incorporação de componentes de IoT nos equipamentos legados usando soluções desenvolvidas com a finalidade de integração aos sistemas da indústria 4.0. Essa abordagem viabiliza a digitalização dos processos e oferece uma alternativa acessível para modernizar a fabricação, aproveitando os benefícios da digitalização e aumentando a competitividade das empresas no mercado. Neste artigo, é apresentado um mapeamento sistemático sobre a integração de sistemas legados na indústria 4.0. Foram analisados 61 artigos avaliados entre os anos de 2017 a 2023. Os resultados fornecem perspectivas sobre as tecnologias utilizadas nas atualizações, os protocolos de comunicação adequados para alcançar a interoperabilidade e a segurança dos dados trafegados.

Palavras-chave: Indústria 4.0. IoT. Sistemas legados. Segurança de dados.

Abstract

The updates of legacy systems and equipment in industrial processes pose challenges for companies aiming to modernize their operations. The adoption of Industry 4.0 is crucial to transforming factories into intelligent and efficient environments. However, fully replacing equipment with state-of-the-art versions can be economically unfeasible. A promising solution is the incorporation of IoT components into legacy equipment using solutions designed for integration with Industry 4.0 systems. This approach enables process digitalization and provides an affordable alternative to modernize manufacturing, leveraging the benefits of digitalization and enhancing companies' competitiveness in the market. This article presents a systematic mapping on the integration of legacy systems in Industry 4.0. A total of 61 articles published between 2017 and 2023 were analyzed. The results offer insights into the technologies used in updates, the appropriate communication protocols to achieve interoperability and data security.

Keywords: Industry 4.0. IoT. Legacy systems. Data security.

LISTA DE SIGLAS

1:1 - Um para um

AMQP - *Advanced Message Queuing Protocol*

CoAP - *Constrained Application Protocol*

DTLS - *Datagram Transport Layer Security*

HTTPS - *Hypertext Transfer Protocol Secure*

IA - Inteligencia Artificial

IOT - *Internet Of Things*

IIOT - *Internet Industrial Of Things*

MQTT - *Message Queue Telemetry Transport*

OPC-UA - *Open Platform Communications Unified Architecture*

OPEX - *Operational Expenditure*

QoS - *Quality of Service*

PLC - *Programmable Logic Controller*

SCADA - *Supervisory Control and Data Acquisition*

TA - Tecnologia da Automação

TLS - *Transport Layer Security*

TI - Tecnologia da informação

1 INTRODUÇÃO

A Indústria 4.0 representa uma revolução no meio industrial. Impulsionada pela integração de tecnologias avançadas, essa nova fase traz consigo uma série de benefícios, como uma maior eficiência na fabricação, otimização de custos e introdução de novos modelos de negócios. Através da automação, troca de dados, adoção de sistemas ciber-físicos, Internet das Coisas e computação em nuvem, as fábricas se tornaram mais inteligentes e interconectadas, permitindo uma produção mais ágil e adaptável (ALQOUD; SCHAEFER; MILISAVLJEVIC-SYED, 2022).

No entanto, a transição para a Indústria 4.0 nem sempre é fácil, pois muitas empresas ainda possuem equipamentos legados que precisam ser atualizados para acompanhar as demandas tecnológicas. Superar esse desafio é essencial para que as empresas possam se manter competitivas em um cenário cada vez mais digital e inovador.

Frente à necessidade de conectar digitalmente a linha de produção, as indústrias se deparam com alguns desafios: atualizar os ativos existentes ou substituí-los por novos equipamentos e garantir a integridade e a segurança das informações (GIVEHCHI et al., 2017). Substituir os maquinários resulta em benefícios imediatos decorrentes da digitalização da linha de produção. Porém, essa opção implica em altos custos e no descarte de máquinas ainda funcionais. Assim, a atualização dos ativos existentes se apresenta economicamente viável como uma solução para esse problema (ALQOUD; SCHAEFER; MILISAVLJEVIC-SYED, 2022).

A digitalização da indústria aumenta significadamente a quantidade de dados gerados, aumentando a preocupação com a segurança e privacidade deles (CHANAL; KAKKASAGERI, 2020). A coleta e análise das informações sobre os processos produtivos e trabalhadores levantam

questões sobre o armazenamento, compartilhamento e proteção (ABIODUN et al., 2021). Sendo assim, se faz necessário medidas robustas de segurança cibernética para mitigar ataques e garantir que dados sensíveis não sofram vazamentos.

Neste estudo, será realizado um mapeamento sistemático da literatura para reunir os principais aspectos relacionados à transformação digital da manufatura praticada no contexto da indústria 4.0. Nesse sentido, foram definidas duas perguntas de pesquisa correlacionadas: "Quais são as melhores práticas para implementação de sistemas legados na Indústria 4.0?" e "Como essa implementação impacta na segurança da rede e na privacidade dos dados organizacionais?"

Este artigo está organizado da seguinte forma: Na seção 2 será realizada a revisão bibliográfica. A Seção 3 descreve o detalhamento da metodologia utilizada. A seção 4 apresenta os resultados e discussões de pesquisa. A Seção 5 apresenta as considerações finais.

2 REVISÃO BIBLIOGRÁFICA

2.1 Sistemas legados

Sistemas ou equipamentos legados referem-se a ativos industriais que se tornaram obsoletos por apresentarem documentação desatualizada, falta de peças e mão de obra especializada, mas que ainda desempenham funcionalidades importantes na planta industrial (BOANO, 2021).

Em equipamentos legados é comum encontrar problemas de desempenho, estabilidade e disponibilidade. Isso acarreta altos custos de operação e manutenção, também conhecidos como OPEX (SANCHEZ-LONDONO et al., 2023).

Nesses sistemas, a integração com tecnologias mais modernas também é dificultada, isso em virtude das programações e estruturas obsoletas. A atualização desses sistemas legados para uma infraestrutura de produção inteligente é um processo conhecido como *retrofitting*. O *retrofitting* de sistemas legados abrange a instalação de sensores adicionais, a integração de novas tecnologias para permitir a coleta de dados em tempo real e a comunicação com outros sistemas (LIMA; MASSOTE; MAIA, 2019).

Isso propicia que as empresas disponham dos benefícios da Indústria 4.0, como por exemplo a otimização de processos, a tomada de decisões com base nos dados e a manutenção preditiva. Permitindo, dessa forma, que as empresas aproveitem ao máximo seus investimentos anteriores, ao mesmo tempo em que se adaptam às demandas e oportunidades da era digital (JASPERT et al., 2021).

No entanto, poder ser complicado aplicar esse *retrofitting*, em virtude desse sistema demandar a consideração de fatores como a compatibilidade de sistemas existentes, segurança da informação e a viabilidade econômica (JASPERT et al., 2021).

2.2 Indústria 4.0

A quarta revolução industrial é marcada pelo conjunto de tecnologias digitais avançadas que se integram ao ambiente industrial. Termos como IoT, IIoT, IA, *big data*, computação em nuvem, realidade aumentada e robótica avançada são intrínsecas à também chamada de Indústria 4.0 (OZTEMEL; GURSEV, 2020).

Seus princípios abrangem a digitalização do processo de produção, tornando as fábricas ambientes inteligentes, onde a automação e a associação entre humanos e máquinas são necessárias (AINSWORTH et al., 2021).

As coletas e análises em tempo real obtidas diretamente da planta auxiliam em *insights* valiosos que ajudam na tomada de decisão em todo processo. Isso viabiliza a personalização dos produtos de acordo com as necessidades individuais do cliente, além de reduzir desperdícios e promover a sustentabilidade nas operações industriais (LASS; GRONAU, 2020).

Descrita como uma confluência entre o setor de manufatura e as tecnologias de informação e comunicação, a Indústria 4.0 busca capacitar os fabricantes com flexibilidade nos processos produtivos, permitindo-os lidar com as mudanças imprevistas mediante a conectividade entre os ativos de produção envolvidos em cada processo produtivo (KANNOTH; SCHNICKE; ANTONINO, 2021).

Portanto, a comunicação e interoperabilidade entre máquinas e sistemas são fundamentais para realizar os processos de produção de forma flexível e adaptável, com o objetivo de lidar com mudanças do mercado. (ETZ; BRANTNER; KASTNER, 2020).

2.3 Interoperabilidade

Um dos principais obstáculos enfrentados na modernização digital das indústrias está relacionado à diversidade das tecnologias de comunicação entre equipamentos de chão de fábrica e demais sistemas da empresa (KANNOTH; SCHNICKE; ANTONINO, 2021).

No passado, as fábricas eram obrigadas a usar um tipo de protocolo de comunicação de acordo com o fabricante do equipamento. Esse tipo de protocolo proprietário não permitia a comunicação com ativos de fabricantes diferentes, forçando a empresa adquirir a solução completa do fornecedor para montar sua rede industrial. Porém ao passar do tempo foi ficando inviável devido ao alto custo, já que necessitaria a troca total dos equipamentos se a fabricante parasse de produzir certa peça ou saísse do mercado.

Diante dessa situação foram desenvolvidos protocolos padrões e as redes de comunicação foram construídas com base em uma variedade de interfaces sequenciais, o que resultou em uma ampla gama de padrões e protocolos, criando um cenário no qual várias empresas adotaram diferentes protocolos em seus sistemas de manufatura (HAZRA et al., 2021).

No entanto, a incompatibilidade desses protocolos herdados com os protocolos de IOT tem gerado uma alta demanda por adaptadores, switches e gateways capazes de facilitar a

integração desses sistemas heterogêneos(GIVEHCHI et al., 2017).

Dessa forma, foram desenvolvidos protocolos para atender aos requisitos da indústria em relação aos sistemas legados, o que é um dos objetos desse estudo.

2.4 Segurança cibernética

A segurança cibernética desempenha um papel crucial na era da Indústria 4.0, garantindo a proteção e a integridade dos sistemas conectados. Ela abrange um conjunto de técnicas e ferramentas implementadas em ambientes residenciais ou industriais para monitorar, mitigar ou bloquear ameaças externas e internas que possam surgir por meio da conexão com a internet (ABIODUN et al., 2021).

Com a interconexão dos equipamentos industriais ao ambiente online, proporcionada pela Indústria 4.0, surgem desafios e preocupações adicionais com a segurança. Anteriormente, a separação entre as redes de Tecnologia da Automação e Tecnologia da Informação mantinham um controle sobre as vulnerabilidades, porém essa conexão ampla com a internet abria portas para possíveis explorações (SCARFò, 2018).

Nesse contexto, as soluções de proteção como *firewalls*, criptografias e autenticação multifator passam a desempenhar um papel fundamental na rede de automação industrial. Essas medidas visam promover a segurança dos processos de produção e preservar a integridade dos dados, protegendo contra acessos não autorizados, vazamento de informações sensíveis e ataques cibernéticos(COLELLI; PANZIERI; PASCUCCI, 2019).

Além disso, a segurança cibernética da Indústria 4.0 inclui a melhoria dos métodos de conscientização e treinamento dos funcionários, por intermédio de políticas de segurança e atualizações contínuas de defesa para acompanhar o cenário de ameaças cibernéticas em constante mudança. Sendo assim, proteger os sistemas conectados é essencial para garantir a continuidade dos processos industriais, a confiabilidade dos dados e proteger a reputação de uma empresa no ambiente digital(KAYAN et al., 2022).

3 METODOLOGIA

O mapeamento sistemático de literatura é uma metodologia de pesquisa utilizada para identificar, analisar e sintetizar estudos relevantes existentes sobre um determinado tópico de pesquisa. É uma abordagem rigorosa e estruturada que permite obter uma visão abrangente do estado atual do conhecimento em uma área específica, conhecido na literatura como "Estado da Arte".

Ao contrário de uma revisão bibliográfica tradicional, que pode ser mais subjetiva e menos transparente em relação aos critérios de inclusão e exclusão de estudos, o mapeamento sistemático segue um protocolo pré-definido e utiliza critérios claros para a seleção de estudos. O processo de mapeamento sistemático envolve as seguintes etapas:

1. **Formulação da pergunta de pesquisa:** Define-se claramente a pergunta de pesquisa que orientará todo o mapeamento sistemático.
2. **Desenvolvimento do protocolo:** Elabora-se um protocolo detalhado que estabelece os critérios de inclusão e exclusão, as fontes de busca, as estratégias de busca, os procedimentos de seleção e extração de dados, e os métodos de análise dos estudos.
3. **Busca e seleção de estudos:** Realiza-se uma busca sistemática em bases de dados, periódicos, conferências e outros recursos relevantes para identificar estudos que atendam aos critérios de inclusão estabelecidos no protocolo. Os estudos encontrados passam por uma seleção inicial com base em critérios de relevância.
4. **Extração e análise de dados:** Os dados relevantes dos estudos selecionados são extraídos de forma sistemática, como informações sobre os autores, ano de publicação, metodologia utilizada, resultados obtidos, entre outros. Em seguida, os dados são analisados e sintetizados, buscando identificar padrões, tendências e lacunas no conhecimento.
5. **Relato dos resultados:** Os resultados do mapeamento sistemático são apresentados em um relatório que descreve de forma clara e transparente o processo de pesquisa, os estudos incluídos, as principais descobertas e as limitações do estudo.

o mapeamento sistemático de literatura é fundamental para a realização de revisões sistemáticas e meta-análises. Essas técnicas de pesquisa dependem de uma busca completa e sistemática da literatura existente. Ao realizar um mapeamento sistemático prévio, os pesquisadores estabelecem uma base sólida de estudos relevantes e confiáveis que servem como ponto de partida para análises mais aprofundadas. Isso ajuda a garantir que as revisões sistemáticas e meta-análises sejam abrangentes, objetivas e representativas do conhecimento atual.

No que se refere a pergunta de pesquisa, foram criadas duas perguntas complementares:

- **Questão 1:** Quais são as melhores práticas para a implementação de sistemas legados na Indústria 4.0?
- **Questão 2:** Como a implementação dos sistemas legados na Indústria 4.0 impacta na segurança da rede e na privacidade de dados?

Na seção de Desenvolvimento será detalhado todo o processo desenvolvido neste trabalho desde a busca de seleção dos artigos até a fase de extração e análise de dados.

4 DESENVOLVIMENTO

O processo de mapeamento sistemático foi conduzido com o objetivo de coletar, examinar e sintetizar as principais publicações científicas acerca do impacto da Indústria 4.0 nos sistemas legados, tendo como foco a melhor forma para tal realização. A metodologia consistiu em uma

busca de artigos nos principais repositórios científicos, conforme pode ser observado na Tabela 1.

Tabela 1 – Base de dados utilizado na revisão da literatura

Base de dados	Endereço Eletrônico
ACM Digital Library	https://dl.acm.org/
IEEEExplore	https://ieeexplore.ieee.org
Science Direct	https://www.sciencedirect.com/
Springer Link	https://link.springer.com/

Após o levantamento bibliográfico inicial, foi realizada uma leitura aberta sobre o tema do presente artigo, encontrando as palavras chaves que contribuíssem para definir a *string* de busca.

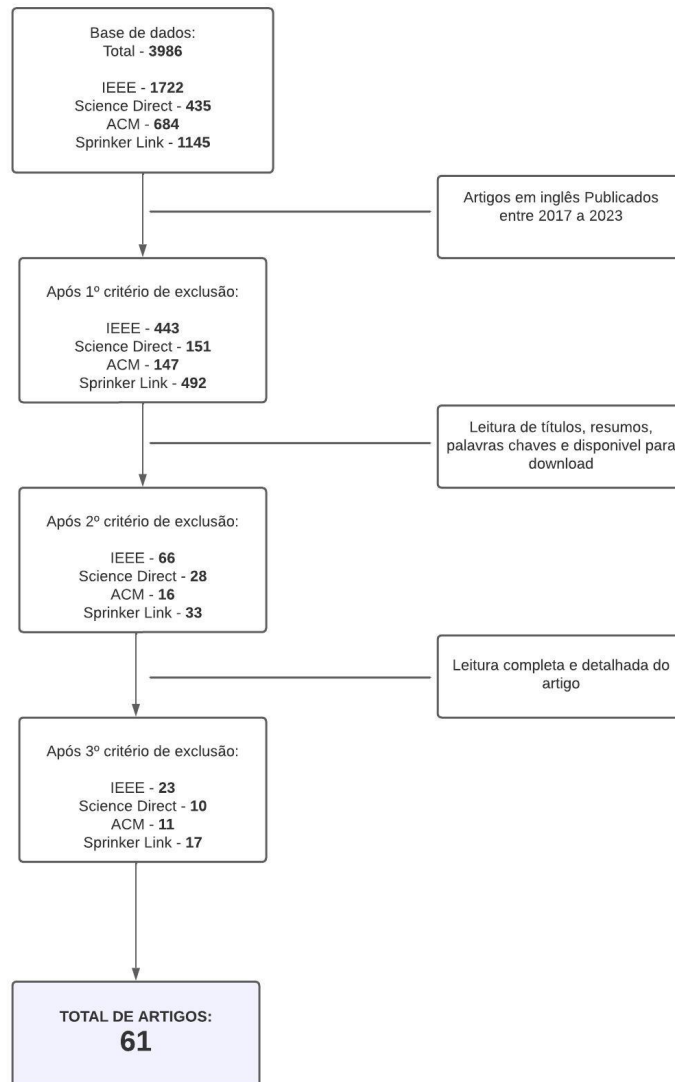
Definida a *string* de busca foram utilizadas as expressões em inglês "*legacy systems*", "*Legacy equipment*", "*legacy devices*", "*legacy machines*", "*Upgrade*", "*migration*", "*integration*" e "*interoperability*" respeitando a lógica de concatenação de cada base de dados.

Em seguida, foi realizado o primeiro filtro de pesquisa, resultando em 3986 artigos. Feito isso, o segundo filtro foi separar aqueles que tivessem sido publicados em inglês e entre os anos de 2017 e 2023, resultando em 1233 artigos.

O terceiro filtro foi separar os artigos que tivessem títulos, resumos e palavras chaves conforme a *string* definida e que estivessem disponíveis para *download*, resultando em 143 artigos.

O quarto e último filtro foi uma leitura abrangente de forma a compreender se eles respondiam as perguntas de pesquisa definidas para este mapeamento sistemático. Chegando, dessa forma, nos 61 artigos discutidos, conforme apresenta o fluxograma da Figura 1.

Figura 1 – Critérios de inclusão e exclusão de artigos.



Fonte: Elaborada pelo autor

Os artigos selecionados após a aplicação dos critérios de exclusão, de qualidade e de relevância, foram agrupados em repositório científico e estão listados por título com seus respectivos autores, método e aspecto principal (temática). As Tabelas 2, 3, 4 e 5, respectivamente, apresentam o resultado da pesquisa. A coluna “Método” utiliza a seguinte legenda: Revisão da Literatura (RL), Estudo de Caso (EC) e Estudos Experimentais (EX).

Na primeira base de dados, a ACM Digital Library, pode-se observar que foram selecionados 11 artigos científicos, em sua maioria o método científico utilizado foi a Revisão de Literatura.

Na base de dados Science Direct, foram filtrados 10 artigos científicos, entre os métodos utilizados destacam-se o revisão de literatura e estudo de caso com grande relevância para a temática de “Retrofit”.

Tabela 2 – Artigos selecionados da ACM Digital Library

Título	Autores	Método	Aspecto Principal
A Comprehensive Survey on Interoperability for IIoT: Taxonomy, Standards, and Future Directions	(HAZRA et al., 2021)	RL	IoT
A service-oriented middleware framework for manufacturing industry 4.0	(AL-JAROUDI; MOHAMMED; JAWHAR, 2018)	RL	Indústria 4.0
Blueprints for architecture drivers and architecture solutions for Industry 4.0 shopfloor applications	(ANTONINO et al., 2019)	RL	Indústria 4.0
Cybersecurity of Industrial Cyber-Physical Systems: A Review	(KAYAN et al., 2022)	RL	Segurança de rede
Decentralized Integration Approach of Disjoint Modules in Factory Environments	(MATHIAS et al., 2022)	RL	Protocolo OPC UA
Development of a Smart Sensor System using OPC UA	(LEE; KIM; LEE, 2017)	EX	Protocolo OPC UA
Emerging Cybersecurity Capability Gaps in the Industrial	(AXON et al., 2022)	RL	Segurança de Rede
Enabling Industry 4.0 Communication Protocol Interoperability: An OPC UA Case Study	(KANNOTH; SCHNICKE; ANTONINO, 2021)	EC	Protocolo OPC UA
Enabling Support of Legacy Devices for a more Sustainable Internet of Things	(BOANO, 2021)	RL	Retrofit
Service Computing for Industry 4.0: State of the Art, Challenges, and Research Opportunities	(SIQUEIRA; DAVIS, 2021)	RL	Indústria 4.0
Towards designing open and secure IoT systems: insights for practitioners	(VOGEL; VARSHNEY, 2018)	RL	Segurança de rede

Tabela 3 – Artigos selecionados da Science Direct

Título	Autores	Métodos	Aspecto Principal
A factory operating system for extending existing factories to Industry 4.0	(LASS; GRONAU, 2020)	EC	Industria 4.0
Adapting an agile manufacturing concept to the reference architecture model industry 4.0: A survey and case study	(YLI-OJANPERÄ et al., 2019)	EC	Retrofit
Big data analytics architecture design—An application in manufacturing systems	(FAHMIDEH; BEYDOUN, 2019)	RL	Industria 4.0
Cyber-physical systems architectures for industrial internet of things applications in Industry 4.0: A literature review	(PIVOTO et al., 2020)	RL	IoT
FutureFit: a strategy for getting a production asset to an industry 4.0 component – a human-centered approach	(BIRTEL et al., 2019)	RL	Retrofit
Interoperability, Flexibility, and Industrial Design Requirements in the IoT	(MACAULAY, 2017)	RL	IOT
Smart Manufacturing Retrofit for Brownfield Systems	(ETZ; BRANTNER; KASTNER, 2020)	EC	Retrofit
Smart retrofitting in manufacturing: A systematic review	(TRIPATHI; DE, 2019)	RL	Retrofit
The Cyber Security Challenges in the IoT Era	(SCARFÒ, 2018)	EC	Segurança de Rede
Toward a Science of Resilience, Supportability 4.0 and Agility	(BERNUS; NORAN; GORANSON, 2020)	RL	Retrofit

Já base de dados Springer Link, foram filtrados 17 artigos científicos. Entre os artigos filtrados nesta base, dois pontos ficaram bastante evidentes, todos os trabalhos referem-se a revisão de literatura e a maioria dos trabalhos duplicados foram identificados nesta fase, o que pode determinar que este repositório pode se tratar também de um indexador de outras base científicas.

Tabela 4 – Artigos selecionados da Springer Link

Título	Autores	Métodos	Aspecto Principal
A Review on the Security of the Internet of Things: Challenges and Solutions	(ABIODUN et al., 2021)	RL	Segurança de rede
A smart process controller framework for Industry 4.0 settings	(COHEN; SINGER, 2021)	RL	Indústria 4.0
Analysis of CoAP implementations for industrial Internet of Things: a survey	(IGLESIAS-URKIA et al., 2019)	RL	Protocolo CoAP
Automation platform independent multi-agent system for robust networks of production resources in industry 4.0	(SEITZ et al., 2021)	RL	Indústria 4.0
Automation technology as a key component of the Industry 4.0 production development path	(BRECHER et al., 2021)	RL	Indústria 4.0
Converging IoT protocols for the data integration of automation systems in the electrical industry	(GIL et al., 2022)	RL	Protocolos (OPC UA, MQTT, HTTPS)
Cyber-Physical Systems in the Context of Industry 4.0: A Review, Categorization and Outlook	(OKS et al., 2022)	RL	Indústria 4.0
Data-driven optimizations in IoT: a new frontier of challenges and opportunities	(TRIPATHI; DE, 2019)	RL	IoT
Internet of Things (IoT), Applications and Challenges: A Comprehensive Review	(KHANNA; KAUR, 2020)	RL	IoT
IoT Eco-system, Layered Architectures, Security and Advancing Technologies: A Comprehensive Survey	(RAJ; SHETTY, 2021)	RL	Segurança de rede
Literature review of Industry 4.0 and related technologies	(OZTEMEL; GURSEV, 2020)	RL	Indústria 4.0
Multi-Modal Industrial IoT Networks: Recent Advances and Future Challenges	(ELSAS; LEEMPUT; HOEBEKE, 2023)	RL	IoT
Security and Privacy in IoT: A Survey	(CHANAL; KAKKASAGERI, 2020)	RL	Segurança de rede
Smart retrofitting in maintenance: a systematic literature review	(SANCHEZ-LONDONO et al., 2023)	RL	Retrofit
SmartPipe: Towards interoperability of industrial applications via computational reflection	(ZHANG et al., 2020)	RL	Interoperabilidade
System architectures for Industrie 4.0 applications	(TRUNZER et al., 2019)	RL	Indústria 4.0
The implementation of virtual reality in digital factory—a comprehensive review	(SEKARAN et al., 2021)	RL	Retrofit

E por fim, na base de dados IEEEExplore, foram filtrados 23 artigos científicos com métodos bastante variados. Devido a volumetria de trabalhos publicados, pode-se inferir que esta base reuni os principais grupos de pesquisa da área tema deste trabalho, além de possuir trabalhos com o maior número de citações, uma média de 8 citações por trabalho publicado.

Tabela 5 – Artigos selecionados da IEEEExplore

Título	Autores	Métodos	Aspecto Principal
A Comprehensive Survey of Industry 4.0 IIoT and Areas of Implementation	(AINSWORTH et al., 2021)	RL	Indústria 4.0
A Seamless Cloud Migration Approach to Secure Distributed Legacy Industrial SCADA Systems	(KHAN et al., 2020a)	EC	Segurança de rede
A Secure Cloud Migration, Monitoring and Analytics Framework for Industrial Internet of Things	(KHAN et al., 2020b)	EX	Segurança da rede
An IoT Gateway for Modbus and MQTT Integration	(SILVA; SILVA, 2019)	EX	Protocolo MQTT
Cyber security primer for legacy process plant operation	(SANDBERG; HUNTER, 2017)	RL	Segurança da Rede
Data Acquisition and Monitoring System for Legacy Injection Machines	(SILVA; SOUSA; ALENYA, 2021)	EC	Protocolo OPC UA
Developing a Security Testbed for Industrial Internet of Things	(AL-HAWAWREH; SITNIKOVA, 2021)	EX	Segurança da Rede
Electromagnetic Interference Analysis of Industrial IoT Networks: From Legacy Systems to 5G	(DIONÍSIO; LOLIĆ; TORRES, 2020)	RL	IoT
Implementation Phases in Modernisation of Legacy Systems	(BAKAR; RAZALI; JAMBARI, 2019)	RL	Retrofit
Implementing an OPC UA interface for legacy PLC-based automation systems using the Azure cloud	(HASKAMP et al., 2018)	EC	Protocolo OPC UA
Implementing OPC-UA services for Industrial Cyber-Physical Systems in Service-Oriented Architecture	(LAM; HAUGEN, 2019)	RL	Protocolo OPC UA
Industry 4.0, How to Integrate Legacy Devices: A Cloud IoT Approach	(PESSOA et al., 2018)	EC	Indústria 4.0
Intelligent operation monitoring IoT tag for factory legacy device	(HAN; KANG; SON, 2017)	EX	IoT
Interoperability for Industrial Cyber-Physical Systems: An Approach for Legacy Systems	(GIVEHCHI et al., 2017)	RL	Retrofit
Inter-Technology Bridging Gateway: A Low Cost Legacy Adaptation Approach to Secure Industrial Systems	(KHAN et al., 2018)	EX	Segurança da rede
IoT Energy Retrofit and the Connection of Legacy Machines Inside the Industry 4.0 Concept	(LIMA; MASSOTE; MAIA, 2019)	RL	Retrofit
Issues in Migrating Legacy Systems to the Cloud	(KHANYE; OPHOFF; JOHNSTON, 2018)	RL	Retrofit
Modbus-OPC UA Wrapper Using Node-RED and IoT-2040 with Application in the Water Industry	(TOC; KORODI, 2018)	EC	Protocolo OPC UA
Native OPC UA Handling and IEC 61499 PLC Integration within the Arrowhead Framework	(CABRAL; DOROFEEV; VARGA, 2020)	EC	Protocolo OPC UA
OPC UA based Universal Edge Gateway for Legacy Equipment	(PARK; JEON, 2019)	RL	Protocolo OPC UA
Securing connection between IT and OT: the Fog Intrusion Detection System prospective	(COLELLI; PANZIERI; PASCUCCI, 2019)	EX	Segurança da rede
Security on the Farm: Safely Communicating with Legacy Agricultural Instrumentation	(BELL et al., 2019)	RL	Segurança da rede
Tool and Technology Independent Function Interfaces by Using a Generic OPC UA Representation	(KASPAR et al., 2018)	EX	Protocolo OPC UA

Após a etapa de seleção, os artigos foram categorizados de acordo com o método de pesquisa escolhido por seus respectivos autores para sua elaboração. Os métodos investigados incluíam revisão da literatura, experimentos baseados em abordagens experimentais e estudos de caso.

Com relação aos aspectos mais relevantes utilizados nos estudos primários e secundários filtrados pelo mapeamento sistemático destacam-se as seguintes temáticas: IoT, Indústria 4.0, Segurança de Redes, Protocolo OPC UA, Retrofit, Protocolo CO AP, Protocolo MQTT e Interoperabilidade. Após essa categorização, tornou-se possível realizar uma análise mais detalhada

dos resultados obtidos que será apresentada na Seção 5.

5 RESULTADOS E DISCUSSÃO

Por meio da utilização da ferramenta *online* Free Word Cloud Genator¹, foi construída uma nuvem de palavras (Figura 2). Este gráfico apresenta as palavras mais frequentes encontradas nos artigos filtrados. Essas palavras podem ser visualizadas em fontes de tamanho maior e cor diferente, diminuindo a fonte e alterando a cor conforme a frequência. O objetivo do gráfico de nuvem de palavras é fornecer uma visão geral rápida e intuitiva dos termos mais relevantes e recorrentes no texto analisado. Como é possível verificar, as pesquisas apresentam inúmeros aspectos como o tipo de protocolo frequentemente utilizados nas empresas para integração dos sistemas legados na Indústria 4.0, por exemplo.

Figura 2 – Nuvem de palavras

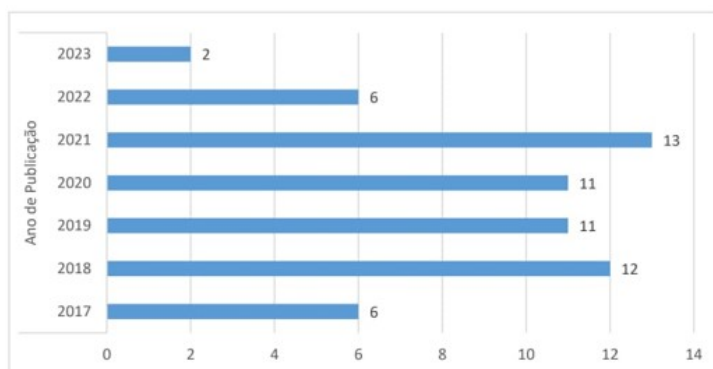


Fonte: Elaborada pelo autor

Como primeira análise, definindo como critério inicial que os artigos estivessem sido publicados entre os anos de 2017 e 2023, dentro dos 61 artigos filtrados conforme explicado no tópico Metodologia deste trabalho encontrados nas bases de dados eletrônicas definidas, fez-se o agrupamento dos artigos tendo como premissa os anos de publicação de cada um deles, conforme apresenta o gráfico da Figura 3.

¹ <https://www.freewordcloudgenerator.com>

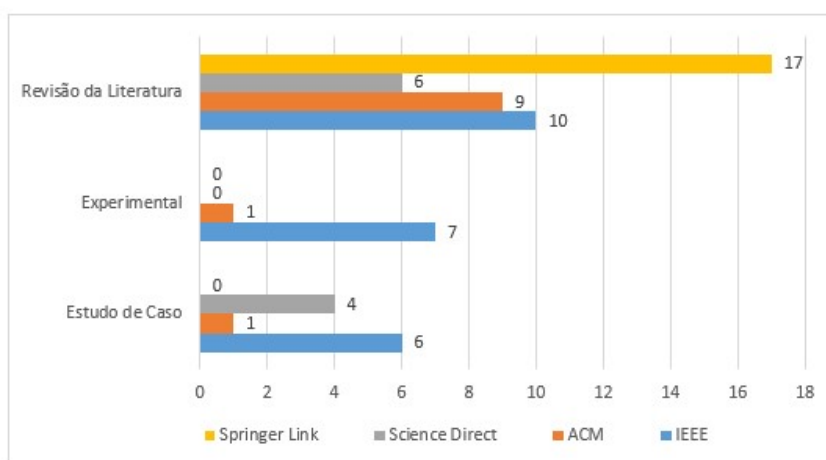
Figura 3 – Ano de publicação dos artigos



Fonte: Elaborada pelo autor

Feito o agrupamento pelo ano de publicação, posteriormente foi realizada a análise de artigos por base de dados utilizada. Dessa forma, observou-se que 17 deles foram encontrados na base de dados *Springer Link*, 10 na *Science Direct*, 11 na ACM e 23 na IEEE, conforme apresenta o gráfico da Figura 4.

Figura 4 – Artigos por base de dados



Fonte: Elaborada pelo autor

A Figura 4 ainda apresenta que 68,85% dos artigos encontrados utilizaram a Revisão de Literatura como método de estudo, correspondendo a 42 artigos dos 61 filtrados, 13,11% (8 artigos) utilizaram Estudos Experimentais em seus desenvolvimentos e 18,03% (11 artigos) realizaram Estudos de Casos para desenvolverem os artigos.

Outra análise realizada foi que, dos 61 artigos definidos no último filtro, 57 deles tem como assunto a IOT e 48 mencionam algum tipo de protocolo. Desses 48 artigos, 24 discorrem a respeito do MQTT, 7 sobre AMQP, 14 sobre CoAP, 7 sobre HTTPS e 29 mencionam o protocolo OPC UA como assunto principal.

A Tabela 6 apresenta os artigos mais relevantes em relação a discussão comparativa quanto a interoperabilidade e segurança dos protocolos mencionados anteriormente para a implementação de sistemas legados na Indústria 4.0.

Tabela 6 – Artigos comparativos quanto ao uso dos protocolos

Título	Autores	Resumo
A Comprehensive Survey on Interoperability for IIoT: Taxonomy, Standards, and Future Directions	(HAZRA et al., 2021)	O artigo é uma revisão sistemática da literatura sobre interoperabilidade no contexto do IIoT e da Indústria 4.0.
Analysis of CoAP implementations for industrial Internet of Things: a survey	(IGLESIAS-URKIA et al., 2019)	O artigo analisa e compara implementações do Protocolo CoAP para a IIoT, incluindo suas características, conceitos de segurança e desempenho.
Converging IoT protocols for the data integration of automation systems in the electrical industry	(GIL et al., 2022)	O artigo propõe a implementação de IIoT na indústria elétrica, utilizando uma plataforma que integra protocolos analisando a interoperabilidade entre diferentes dispositivos e sistemas.
Developing a Security Testbed for Industrial Internet of Things	(AL-HAWAWREH; SITNIKOVA, 2021)	O artigo discute sobre modelos de referência e tecnologias emergentes em sistemas IIoT
Industry 4.0, How to Integrate Legacy Devices: A Cloud IIoT Approach	(PESSOA et al., 2018)	O artigo propõe uma abordagem baseada em MQTT e OPC UA para a integração de dispositivos legados na nuvem.
IIoT Eco-system, Layered Architectures, Security and Advancing Technologies: A Comprehensive Survey	(RAJ; SHETTY, 2021)	O artigo fornece uma revisão detalhada de várias arquiteturas, tecnologias, segurança e protocolos usados em um ecossistema IIoT.
Service Computing for Industry 4.0: State of the Art, Challenges, and Research	(SIQUEIRA; DAVIS, 2021)	O artigo aborda tópicos como arquiteturas de sistemas, tecnologias de comunicação, segurança e privacidade de dados.
Smart Manufacturing Retrofit for Brownfield Systems	(ETZ; BRANTNER; KASTNER, 2020)	O artigo aborda tópicos relacionados a arquiteturas de sistemas e tecnologias de comunicação, comparando protocolos e destacando a importância de tecnologias na troca de informações entre máquinas.
Smart retrofitting in maintenance: a systematic literature review	(SANCHEZ-LONDONO et al., 2023)	O artigo menciona a importância dos protocolos de comunicação na coleta e transmissão de dados de sensores em tempo real, da eficiência e confiabilidade nos processos de produção.

Assim sendo, Hazra et al. (2021) apresentam que o protocolo HTTPS é adequado para aplicações de alta segurança, já o MQTT é apropriado para aplicações de baixa largura de banda e baixa latência, enquanto o CoAP é mais adequado para aplicações de baixa energia. Desse modo, eles não são tão eficientes quanto o CoAP em termos de recursos e eficiência energética (IGLESIAS-URKIA et al., 2019).

Gil et al. (2022) descrevem as características dos protocolos HTTPS, MQTT e OPC UA quanto a aplicabilidade de cada um na integração dos sistemas legados abordando o domínio do OPC UA em relação aos demais quando analisado a interoperabilidade, segurança e confiabilidade na comunicação de dados. Concordando com o apresentado pelos autores, Pessoa et al. (2018) e Siqueira e Davis (2021) mencionam que o OPC UA é uma solução segura e confiável para a interoperabilidade de sistemas na Indústria 4.0, enquanto Al-Hawawreh e Sitnikova (2021)

apontam que o MQTT é um protocolo de comunicação importante para a IoT e para a integração de dispositivos legados na nuvem.

Raj e Shetty (2021) elucidam que o AMQP é um protocolo semelhante ao MQTT, mas com uma característica adicional de armazenar e encaminhar dados. No entanto o MQTT suporta comunicações leves de máquina para máquina, conforme também concordam Etz, Brantner e Kastner (2020). Para tanto o AMQP é frequentemente empregado por serviços de software em sistemas industriais avançados e o MQTT é empregado para comunicação entre dispositivos de borda em sistemas industriais avançados (SIQUEIRA; DAVIS, 2021).

Apesar da boa performance do MQTT, Etz, Brantner e Kastner (2020) indicam que o OPC UA tem vantagens sobre os outros protocolos em quase todos os critérios a serem avaliados na integração dos sistemas legados, primordialmente quanto a interoperabilidade, escalabilidade, segurança, modelagem, extensibilidade, descoberta e conformidade. Sendo com isso, importantes para a coleta e transmissão de dados de sensores em tempo real, permitindo a implementação de sistemas de manutenção preditiva e a melhoria da eficiência e confiabilidade dos processos de produção (SANCHEZ-LONDONO et al., 2023).

Dos protocolos filtrados nos artigos, as tecnologias utilizadas por eles para garantir a segurança da rede durante a configuração de dados, são:

OPC UA – Criptografia, certificados digitais, autenticação, controle de acesso granular e assinaturas digitais.

AMQP – TLS, certificados digitais, controle de acesso, autenticação e assinaturas digitais;

MQTT - TLS, certificados digitais, autenticação, controle de acesso e QoS.

CoAP – DTLS, certificados digitais e controle de acesso.

HTTPS - TLS, certificados digitais, criptografia simétrica e assimétrica, algoritmos, controle de acesso e autenticação.

Dessa forma, observou-se que algumas dessas tecnologias possuem utilização comum entre os protocolos listados, conforme apresenta a Figura 5.

Figura 5 – Tecnologia de segurança comuns entre os protocolos

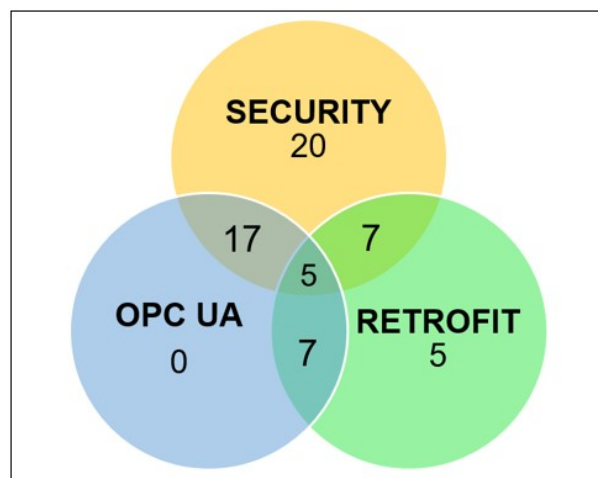


Fonte: Elaborada pelo autor

Essas técnicas visam proteger os dados das empresas, em virtude de, com a atualização dos sistemas legados, estes passam a estar diretamente conectados a internet aumentando, com isso, sua vulnerabilidade e exposição a atitudes criminosas por parte de internos e/ou terceiros.

Após análise detalhada do conteúdo apresentado nos artigos filtrados, foi possível perceber que, 29 deles falam sobre o protocolo OPC UA, 49 falam de segurança de rede e 24 falam de *retrofit*. Observou-se, todos os artigos que falavam sobre OPC UA analisavam segurança de rede e/ou *retrofit* em conjunto ao protocolo. Sendo que 5 dos artigos trataram dos 3 assuntos de simultaneamente, conforme apresenta o Diagrama de Venn da Figura 6.

Figura 6 – Diagrama de Venn



Fonte: Elaborada pelo autor

Levando em consideração que o protocolo OPC UA foi o mais citado entre os protocolos utilizados nos artigos para aplicação no mercado, observou-se que isso se deu primordialmente por esse protocolo ser uma das tecnologias mais recomendadas para implementar camadas de comunicação e informação que garantem a conectividade e interoperabilidade de ativos digitalizados, integrando os sistemas legados em ambientes industriais que exigem conformidade com o Indústria 4.0 (HASKAMP et al., 2018).

6 CONSIDERAÇÕES FINAIS

A implementação da indústria 4.0 e digitalizações de sistemas legados são essenciais para impulsionar a manufatura inteligente e alcançar maior eficiência e produtividade no mercado. Ao integrar tecnologias como IoT, computação em nuvem e análise de dados em tempo real, as empresas têm a oportunidade de gerar novas receitas e serem cada vez mais competitivas.

O foco deste trabalho foi encontrar na literatura estudos que fornecessem *insights* relacionados às questões de pesquisa definidas anteriormente, avaliando, por intermédio de um mapeamento sistemático de literatura, a melhor prática de implementação da indústria 4.0 e o quanto isso afeta na segurança da rede e na privacidade de dados.

É visivelmente observado entre os artigos analisados um consenso sobre as diversas vantagens que o protocolo OPC UA oferece quanto a extensibilidade, estruturação de grandes quantidades de dados e aspectos de segurança padronizados em relação aos outros protocolos de comunicação analisados.

Isso é observado, primordialmente, em virtude de entre os 61 artigos mapeados, 29 deles abordarem diretamente o uso do protocolo OPC UA como um protocolo assertivo para a migração dos sistemas legados para a indústria 4.0.

Nesse sentido, o presente artigo identificou que o protocolo OPC UA tem um papel importante quanto a padronização, sendo considerado superior a outras tecnologias em diversos critérios. Sendo também, uma solução quando se leva em consideração a segurança de rede, isso devido às suas funções de criptografia, autenticação, controle de acesso granular, dentre outras medidas de segurança.

Com isso, observa-se que o protocolo incorpora recursos avançados de segurança que visam proteger a comunicação e dados transmitidos entre os sistemas, principalmente, em razão de o OPC UA estar se firmando cada vez mais como um dos protocolos referenciados quando o assunto é a Indústria 4.0.

REFERÊNCIAS

- ABIODUN, O. et al. A review on the security of the internet of things: Challenges and solutions. **Wireless Pers Commun**, v. 119, p. 2603–2637, 2021.
- AINSWORTH, T. et al. A comprehensive survey of industry 4.0, iiot and areas of implementation. In: IEEE. **SoutheastCon 2021**. Atlanta, GA, USA, 2021. p. 1–6.
- AL-HAWAWREH, M.; SITNIKOVA, E. Developing a security testbed for industrial internet of things. **IEEE Internet of Things Journal**, v. 8, n. 7, p. 5558–5573, April 2021.
- AL-JAROUDI, J.; MOHAMED, N.; JAWHAR, I. A service-oriented middleware framework for manufacturing industry 4.0. **SIGBED Rev.**, v. 15, n. 5, p. 29–36, October 2018.
- ALQOUD, A.; SCHAEFER, D.; MILISAVLJEVIC-SYED, J. Industry 4.0: A systematic review of legacy manufacturing system digital retrofitting. **Manufacturing Rev.**, v. 9, n. 32, 2022.
- ANTONINO, P. O. et al. Blueprints for architecture drivers and architecture solutions for industry 4.0 shopfloor applications. In: **Proceedings of the 13th European Conference on Software Architecture - Volume 2**. [S.l.: s.n.], 2019.
- AXON, L. et al. Emerging cybersecurity capability gaps in the industrial internet of things: Overview and research agenda. **Digital Threats**, v. 3, n. 4, p. Article 34, December 2022.
- BAKAR, H. K. A.; RAZALI, R.; JAMBARI, D. I. Implementation phases in modernisation of legacy systems. In: IEEE. **2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS)**. [S.l.], 2019. p. 1–6.
- BELL, T. et al. Security on the farm: Safely communicating with legacy agricultural instrumentation. In: IEEE. **2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)**. [S.l.], 2019. p. 192–194.
- BERNUS, P.; NORAN, O.; GORANSON, T. Toward a science of resilience, supportability 4.0 and agility. **IFAC-PapersOnLine**, v. 53, p. 11199–11206, 2020.
- BIRTEL, M. et al. Futurefit: a strategy for getting a production asset to an industry 4.0 component – a human-centered approach. **Procedia Manufacturing**, v. 38, p. 1000–1007, 2019.
- BOANO, C. A. Enabling support of legacy devices for a more sustainable internet of things: A position paper on the need to proactively avoid an "internet of trash". In: ASSOCIATION FOR COMPUTING MACHINERY. **Proceedings of the Conference on Information Technology for Social Good (GoodIT '21)**. New York, NY, USA, 2021. p. 97–102.
- BRECHER, C. et al. Automation technology as a key component of the industry 4.0 production development path. **Int J Adv Manuf Technol**, v. 117, p. 2287–2295, 2021.
- CABRAL, J.; DOROFEEV, K.; VARGA, P. Native opc ua handling and iec 61499 plc integration within the arrowhead framework. In: IEEE. **2020 IEEE Conference on Industrial Cyberphysical Systems (ICPS)**. [S.l.], 2020. p. 596–601.
- CHANAL, P.; KAKKASAGERI, M. Security and privacy in iot: A survey. **Wireless Pers Commun**, v. 115, p. 1667–1693, 2020.
- COHEN, Y.; SINGER, G. A smart process controller framework for industry 4.0 settings. **J Intell Manuf**, v. 32, p. 1975–1995, 2021.

- COLELLI, R.; PANZIERI, S.; PASCUCCI, F. Securing connection between it and ot: the fog intrusion detection system prospective. In: IEEE. **2019 II Workshop on Metrology for Industry 4.0 and IoT (MetroInd4.0&IoT)**. [S.l.], 2019. p. 444–448.
- DIONÍSIO, R.; LÓPEZ, T.; TORRES, P. Electromagnetic interference analysis of industrial iot networks: From legacy systems to 5g. In: IEEE. **2020 IEEE Microwave Theory and Techniques in Wireless Communications (MTTW)**. [S.l.], 2020. p. 41–46.
- ELSAS, R.; LEEMPUT, D. V.; HOEBEKE, J. e. a. Multi-modal industrial iot networks: Recent advances and future challenges. **Wireless Pers Commun**, 2023.
- ETZ, D.; BRANTNER, H.; KASTNER, W. Smart manufacturing retrofit for brownfield systems. **Procedia Manufacturing**, v. 42, p. 327–332, 2020.
- FAHMIDEH, M.; BEYDOUN, G. Big data analytics architecture design—an application in manufacturing systems. **Computers Industrial Engineering**, v. 128, p. 948–963, 2019. ISSN 0360-8352.
- GIL, S. et al. Converging iot protocols for the data integration of automation systems in the electrical industry. **Journal of Electrical Systems and Information Technology**, Springer, v. 9, n. 1, p. 1, 2022.
- GIVEHCHI, O. et al. Interoperability for industrial cyber-physical systems: An approach for legacy systems. **IEEE Transactions on Industrial Informatics**, v. 13, n. 6, p. 3370–3378, December 2017.
- HAN, H.; KANG, H.; SON, J. Intelligent operation monitoring iot tag for factory legacy device. In: IEEE. **2017 International Conference on Information and Communication Technology Convergence (ICTC)**. [S.l.], 2017. p. 781–783.
- HASKAMP, H. et al. Implementing an opc ua interface for legacy plc-based automation systems using the azure cloud: An icps-architecture with a retrofitted rfid system. In: **2018 IEEE Industrial Cyber-Physical Systems (ICPS)**. St. Petersburg, Russia: [s.n.], 2018. p. 115–121.
- HAZRA, A. et al. A comprehensive survey on interoperability for iiot: Taxonomy, standards, and future directions. **ACM Comput. Surv.**, v. 55, n. 1, p. 9:1–9:35, January 2021.
- IGLESIAS-URKIA, M. et al. Analysis of coap implementations for industrial internet of things: a survey. **J Ambient Intell Human Comput**, v. 10, p. 2505–2518, 2019.
- JASPERT, D. et al. Smart retrofitting in manufacturing: A systematic review. **Journal of Cleaner Production**, v. 312, p. 127555, 2021.
- KANNOTH, S.; SCHNICKE, F.; ANTONINO, P. O. Enabling industry 4.0 communication protocol interoperability: An opc ua case study. In: ASSOCIATION FOR COMPUTING MACHINERY. **7th Conference on the Engineering of Computer Based Systems (ECBS 2021)**. New York, NY, USA, 2021. p. Article 14, 1–9.
- KASPAR, M. et al. Tool and technology independent function interfaces by using a generic opc ua representation. In: IEEE. **2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA)**. [S.l.], 2018. p. 1183–1186.
- KAYAN, H. et al. Cybersecurity of industrial cyber-physical systems: A review. **ACM Comput. Surv.**, Association for Computing Machinery, v. 54, n. 11s, p. 229, January 2022.

KHAN, R. et al. Inter-technology bridging gateway: A low cost legacy adaptation approach to secure industrial systems. In: IEEE. **2018 IEEE Power & Energy Society General Meeting (PESGM)**. [S.l.], 2018. p. 1–5.

KHAN, R. et al. A seamless cloud migration approach to secure distributed legacy industrial scada systems. In: IEEE. **2020 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)**. [S.l.], 2020. p. 1–5.

KHAN, R. et al. A secure cloud migration, monitoring and analytics framework for industrial internet of things. In: IEEE. **2020 IEEE 6th World Forum on Internet of Things (WF-IoT)**. [S.l.], 2020. p. 1–6.

KHANNA, A.; KAUR, S. Internet of things (iot), applications and challenges: A comprehensive review. **Wireless Pers Commun**, v. 114, p. 1687–1762, 2020.

KHANYE, T.; OPHOFF, J.; JOHNSTON, K. Issues in migrating legacy systems to the cloud. In: IEEE. **2018 8th International Conference on Cloud Computing, Data Science Engineering (Confluence)**. [S.l.], 2018. p. 694–699.

LAM, A. N.; HAUGEN, Implementing opc-ua services for industrial cyber-physical systems in service-oriented architecture. In: IEEE. **IECON 2019-45th Annual Conference of the IEEE Industrial Electronics Society**. [S.l.], 2019. p. 5486–5492.

LASS, S.; GRONAU, N. A factory operating system for extending existing factories to industry 4.0. **Computers in Industry**, v. 115, p. 103128, 2020.

LEE, S.; KIM, C.; LEE, J. Development of a smart sensor system using opc ua. In: ASSOCIATION FOR COMPUTING MACHINERY. **Proceedings of the 15th International Conference on Advances in Mobile Computing & Multimedia (MoMM2017)**. New York, NY, USA, 2017. p. 220–225.

LIMA, F.; MASSOTE, A. A.; MAIA, R. F. Iot energy retrofit and the connection of legacy machines inside the industry 4.0 concept. In: IEEE. **IECON 2019 - 45th Annual Conference of the IEEE Industrial Electronics Society**. [S.l.], 2019. p. 5499–5504.

MACAULAY, T. Interoperability, flexibility, and industrial design requirements in the iot. In: **RIoT Control**. Boston: Morgan Kaufmann, 2017. p. 197–219.

MATHIAS, S. G. et al. Decentralized integration approach of disjoint modules in factory environments. In: ASSOCIATION FOR COMPUTING MACHINERY. **2022 The 3rd International Conference on Industrial Engineering and Industrial Management (IEIM 2022)**. New York, NY, USA, 2022. p. 195–199.

OKS, S. et al. Cyber-physical systems in the context of industry 4.0: A review, categorization and outlook. **Inf Syst Front**, 2022.

OZTEMEL, E.; GURSEV, S. Literature review of industry 4.0 and related technologies. **J Intell Manuf**, v. 31, p. 127–182, 2020.

PARK, H. M.; JEON, J. W. Opc ua based universal edge gateway for legacy equipment. In: IEEE. **2019 IEEE 17th International Conference on Industrial Informatics (INDIN)**. [S.l.], 2019. p. 1002–1007.

PESSOA, M. A. O. et al. Industry 4.0, how to integrate legacy devices: A cloud iot approach. In: **IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society**. [S.l.: s.n.], 2018. p. 2902–2907.

PIVOTO, D. et al. Cyber-physical systems architectures for industrial internet of things applications in industry 4.0: A literature review. **Journal of Manufacturing Systems**, v. 58, p. 176, 12 2020.

RAJ, A.; SHETTY, S. Iot eco-system, layered architectures, security and advancing technologies: A comprehensive survey. **Wireless Pers Commun**, v. 122, p. 1481–1517, 2021.

SANCHEZ-LONDONO, D. et al. Smart retrofitting in maintenance: a systematic literature review. **J Intell Manuf**, v. 34, p. 1–19, 2023.

SANDBERG, C.; HUNTER, B. Cyber security primer for legacy process plant operation. In: IEEE. **2017 Petroleum and Chemical Industry Technical Conference (PCIC)**. [S.l.], 2017. p. 97–102.

SCARFÒ, A. The cyber security challenges in the iot era. In: **Security and Resilience in Intelligent Data-Centric Systems and Communication Networks**. [S.l.]: Academic Press, 2018. p. 53–76.

SEITZ, M. et al. Automation platform independent multi-agent system for robust networks of production resources in industry 4.0. **J Intell Manuf**, v. 32, p. 2023–2041, 2021.

SEKARAN, S. C. et al. The implementation of virtual reality in digital factory—a comprehensive review. **International Journal of Advanced Manufacturing Technology**, v. 115, n. 5-6, p. 1349–1366, 2021.

SILVA, B.; SOUSA, J.; ALENYA, G. Data acquisition and monitoring system for legacy injection machines. In: IEEE. **2021 IEEE International Conference on Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA)**. [S.l.], 2021. p. 1–6.

SILVA, C. R. M.; SILVA, F. A. C. M. An iot gateway for modbus and mqtt integration. In: **2019 SBMO/IEEE MTT-S International Microwave and Optoelectronics Conference (IMOC)**. Aveiro, Portugal: [s.n.], 2019. p. 1–3.

SIQUEIRA, F.; DAVIS, J. G. Service computing for industry 4.0: State of the art, challenges, and research opportunities. **ACM Comput. Surv.**, Association for Computing Machinery, v. 54, n. 9, p. 188, December 2021.

TOC, S.-I.; KORODI, A. Modbus-opc ua wrapper using node-red and iot-2040 with application in the water industry. In: IEEE. **2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY)**. [S.l.], 2018. p. 000099–000104.

TRIPATHI, S.; DE, S. Data-driven optimizations in iot: a new frontier of challenges and opportunities. **Computer Science and Information Technology**, Springer, v. 7, p. 35–43, 2019.

TRUNZER, E. et al. System architectures for industrie 4.0 applications. **Production Engineering Research and Development**, Springer, v. 13, p. 247–257, 2019.

VOGEL, B.; VARSHNEY, R. Towards designing open and secure iot systems: insights for practitioners. In: ASSOCIATION FOR COMPUTING MACHINERY. **Proceedings of the 8th International Conference on the Internet of Things**. New York, NY, USA: Association for Computing Machinery, 2018. p. 36.

YLI-OJANPERÄ, M. et al. Adapting an agile manufacturing concept to the reference architecture model industry 4.0: A survey and case study. **Journal of Industrial Information Integration**, v. 15, p. 147–160, 2019.

ZHANG, S. et al. Smartpipe: Towards interoperability of industrial applications via computational reflection. **Journal of Computer Science and Technology**, v. 35, n. 1, p. 161–178, 2020.