DOI: 10.5748/19CONTECSI/COM/SEC/7108

# CYBER SECURITY IN LEGACY INDUSTRIAL NETWORKS - A STANDARD VALIDATION ENVIRONMENT: SYSTEMATIC REVIEW OF THE LITERATURE

# SEGURANÇA CIBERNÉTICA EM REDES INDUSTRIAIS LEGADAS - UM AMBIENTE DE VALIDAÇÃO DE NORMAS: REVISÃO SISTEMÁTICA DA LITERATURA

**Fabio dos Santos Oliveira** ; https://orcid.org/0000-0003-2442-9736
Instituto de Pesquisa Tecnológicas do Estado de São Paulo

**Anderson Aparecido Alves da Silva** ; https://orcid.org/0000-0001-5426-6478
Instituto de Pesquisa Tecnológicas do Estado de São Paulo - Universidade de São Paulo - Universidade Paulista - Centro Universitário Senac São Paulo

**Marcelo Teixeira de Azevedo** ; https://orcid.org/0000-0002-4636-1878
Universidade de São Paulo

**Adilson Eduardo Guelfi** ; https://orcid.org/0000-0002-1676-7380
Universidade do Oeste Paulista (UNOESTE

# CYBER SECURITY IN LEGACY INDUSTRIAL NETWORKS - A STANDARD VALIDATION ENVIRONMENT: SYSTEMATIC REVIEW OF THE LITERATURE
# SEGURANÇA CIBERNÉTICA EM REDES INDUSTRIAIS LEGADAS - UM AMBIENTE DE VALIDAÇÃO DE NORMAS: REVISÃO SISTEMÁTICA DA LITERATURA


## ABSTRACT

Industrial networks use specific equipment, software and protocols with specific characteristics according to the sector in which industry operates. They have a different life cycle than Information Technology (IT) and consequently were not developed with protection features, from a security point of view, there are cases with equipment using Microsoft Windows 3.11 or older operating systems, these equipment or systems are classified as legacy. Due to that the demand for remote support, connection in the corporate networks and sometimes to the Internet has increased what is called attack surface, that is, industrial networks that were once isolated became exposed, with several exploitable vulnerabilities and the number of incidents, in this case cyber-attacks, began to increase to the point of affecting people lives, whether in factories or daily. Identifying the main vulnerabilities already documented and defining a set of security standards for legacy industrial networks is a possibility to define a standards validation environment for these networks and consequently support operators to identify vulnerabilities and act proactively. A systematic review of articles, annals of events and specialized literature was carried out to identify the state of the art regarding topics involving legacy industrial networks, identification of anomalies and security standards to present gaps and propose a research agenda, critical analysis of the works developed. Finally, recommend conducting further research and conducting experiments to assist academia and market in dealing with these scenarios, something that is very common in Brazilian industry given the high investment cost for updating proprietary systems.

Keywords: ICS; SCADA; Industrial Cyber-Physical Systems; Cyber Security; Legacy; Anomaly Detection


## RESUMO

As redes industriais utilizam equipamentos, *softwares* e protocolos específicos com características pontuais de acordo com o setor de atuação da indústria. Possuem um ciclo de vida diferentes de equipamentos de Tecnologia da Informação (TI), e consequentemente não foram desenvolvidos com funcionalidades de proteção, do ponto de vista cibernético, há casos de equipamentos utilizando Microsoft Windows 3.11 ou sistemas operacionais mais antigos que este, são os equipamentos ou sistemas classificados como legado. Ocorre que a demanda de suporte remoto, interligação com redes corporativas e por vezes à Internet, aumentou o que se chama de superfície de ataque, ou seja, as redes industriais outrora isoladas, passaram a ficar expostas, com várias vulnerabilidades que podem ser exploradas e o número de incidentes, no caso ataques cibernéticos, começaram a aumentar a ponto de afetar a vida das pessoas seja nas fábricas, seja no dia a dia. Identificar as principais vulnerabilidades já documentadas e definir um conjunto de padrões de segurança para redes industriais legadas é uma possibilidade para definir um ambiente de validação de normas para estas redes e consequentemente auxiliar operadores a identificar vulnerabilidades e atuar de forma proativa. Uma revisão sistemática de artigos, anais de eventos e literatura especializada foi conduzida a fim de identificar o estado da arte no que se refere a temas envolvendo redes industriais legadas, identificação de anomalias e normas de segurança visando apresentar lacunas e propor uma agenda de pesquisa, análise crítica dos trabalhos desenvolvidos. Por fim recomendar a condução de outras pesquisas e realização de experimentos a fim de auxiliar a academia e o mercado no tratamento de cenários como este, algo que na indústria brasileira é bastante comum dado o alto custo de investimento para a atualização de sistemas proprietários.

Palavras-chave: ICS; SCADA; Industrial Cyber-Physical Systems; Cyber Security; Legado; Detecção de Anomalias

## 1. INTRODUÇÃO

As redes industriais são caracterizadas pela utilização de equipamentos diferenciados, denominados *Commercial-Off-The-Shelf* (COTS), que desenvolvem e integram subsistemas operacionais em redes industriais. Estes equipamentos têm pouco ou nenhum recurso de segurança cibernética. Os dispositivos COTS adotam recursos de design à prova de falhas mecânica ou eletrônicas denominados *backup safety system* ou *fail-safe* (CONKLIN, 2016) e (IGURE et al., 2006) que podem ser facilmente explorados e desabilitados intencionalmente, como foram desenvolvidos sem a preocupação de proteção, por exemplo autenticação ou criptografia (IGURE et al., 2006).

A evolução tecnológica, impulsionada pela 4ª Revolução Industrial (4RI), conhecida como Indústria 4.0, que se caracteriza pela convergência e pela possibilidade da combinação de diferentes tecnologias, envolve a digitalização da produção, as fábricas inteligentes, a customização em massa, o uso de dados, sensores e equipamentos conectados em rede associados a sistemas ciber-físicos (ANDERL, 2014) e (SCHWAB, 2016).

Este crescimento da demanda para conectar as *Industrial Control Systems* (ICS) às redes corporativas, à Internet ou ainda a possibilidade de acesso remoto a estas redes que eram totalmente isoladas dentro das fábricas, sem manutenção e atualizações de segurança estabelece um problema para os chamados ambientes Operacionais de Tecnologia (OT) quando comparados aos sistemas corporativos de Tecnologia da Informação (TI), que possuem uma estratégia de atualização constante (TANENBAUM, 2003) e (CONKLIN, 2016).

Incidentes como BlackEnergy (CASE, 2016), Stuxnet (FALLIERE et al. 2011) e Irongate (SETOLA et al. 2019) tiveram ampla divulgação na mídia, evidenciando a necessidade de investimento e atenção para questões de ciber segurança em ambientes industriais. Segundo Pliatsios et al. (2020), Igure et al. (2006), Hentea, (2008), Lezzi et al. (2018), avaliar o modelo de implementação da ISC e propor um padrão de monitoramento para identificar anormalidades de forma efetiva, é uma considerável contribuição para a indústria e academia.

Portanto, equipamentos e softwares legados que não possuem funcionalidades de segurança cibernética, justamente por serem específicos (JADIDI et al. 2022), são parte do problema geral das ICS, principalmente aquelas em funcionamento por longos períodos, sem perspectiva de parada para atualização. Além disso, ambientes heterogêneos, com diferentes fabricantes e características, também aumentam o risco das operações das empresas sobre diferentes aspectos (EFSTATHOPOULOS et al. 2019).

Identificar as principais vulnerabilidades de uma ICS com ferramentas específicas e conhecimento técnico, conforme pontuam Stephen et al. (2016) e Efstathopoulos et al. (2019), permite definir um conjunto de padrões de segurança cibernética para redes industriais legadas (KHAN et al. 2020). Definir um ambiente que valide a conformidade destas redes legadas com um padrão pré-definido de tráfego e comportamento (EFSTATHOPOULOS et al. 2019) e (RADOGLOU-GRAMMATIKIS et al. 2021), permite conhecer o comportamento padrão de uma ICS, entendendo quais são os parâmetros esperados, o volume da dados, a identificação de anomalias, as definições de posição de equipamentos e as mensagens de notificação e status dos ativos gerenciados, auxiliam a estabelecer um padrão de conformidade de tráfego e segurança para esta rede.

Levando em conta todo o histórico de falta de padronização em segurança nas ICS relatado nas referências previamente apresentadas, os objetivos deste artigo são desenvolver uma revisão sistemática de artigos, anais de eventos e literatura especializada a fim de identificar o estado da arte no que se refere a temas envolvendo redes industriais legadas, identificação de anomalias e normas de segurança visando apresentar lacunas e propor uma agenda de pesquisa, análise crítica dos trabalhos desenvolvidos e por fim recomendar a condução de outras pesquisas e realização de experimentos a fim de auxiliar a academia e o mercado no tratamento de cenários como este, considerando o cenário atual de indústria de médio e pequeno porte no Brasil.

Este artigo está organizado da seguinte forma: a seção 2 apresenta a fundamentação teórica, enquanto a seção 3 a metodologia utilizada. A seção 4 os resultados encontrados. A seção 5 apresenta as conclusões face as análises executadas e finalmente a seção 6 com as referências bibliográficas.

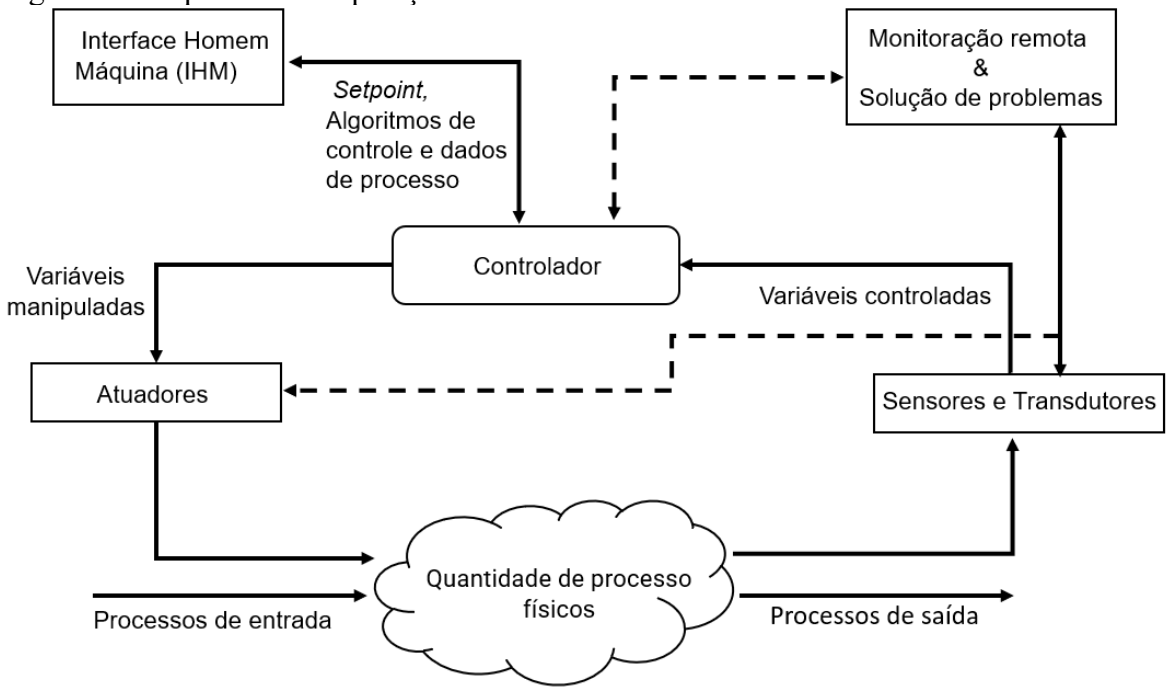
## 2. FUNDAMENTAÇÃO TEÓRICA

Nesta seção conceitos importantes são descritos. Questões envolvendo data da primeira implementação, responsáveis, empresas envolvidas, pessoas ou pesquisadores por criar e desenvolver a tecnologia apresentada não são descritos, o objetivo principal é a explicação detalhada do tema.

As redes industriais, aqui definidas como *Industrial Control Systems* (ICS) são estruturas complexas e requerem um amplo detalhamento, conforme explica Alcaraz et al. (2012) há uma estrutura de funcionamento quase que hierárquica que consiste no *Process Control Systems* (PCS) que é um sistema específico que executa tarefas pré-definidas em ambientes industriais dos mais diversos tipos. Sua função é monitorar o funcionamento da solução como um todo, supervisionando sensores, entre outros tipos de dispositivos, instalados em diferentes locais, em geral no chão de fábrica, coletando dados captados por estes dispositivos. O PCS pode ser identificado como *Supervisory Control and Data Acquisition* (SCADA), como comumente se encontra na literatura. Um sistema SCADA, pode estar posicionado em uma planta industrial, mas também pode operar e monitorar uma planta remotamente. Deve controlar performance, operação contínua de sistemas industriais em tempo real. Há também o *Distributed Control Systems* (DCS) que também executa as funções de um sistema SCADA, porém sempre próximo dos equipamentos que deverá monitorar. Utilizando a expressão SCADA equaliza-se o conceito.

Babu et al. (2017) descreve a Figura 1 como a arquitetura de funcionamento da ICS, onde os componentes responsáveis pela monitoração remota e solução de problemas, por vezes até a prevenção ou recuperação de um processo. A intersecção entre o operador e os demais componentes da ICS, funcionam de acordo com uma tarefa específica, ou seja, cada dispositivo tem um campo de atuação dentro dos níveis específicos da ICS. O operador pode inserir dados definidos como variáveis controladas que são transferidas para os sensores, controladores lógicos programáveis e atuadores. Cabe aos sensores medir grandezas físicas (elétricas ou não elétricas) de entrada e fornecer as respectivas saídas. Estes dados são enviados como variáveis de controle para o controlador que utiliza algoritmos de processo e *setpoints* para gerar as variáveis manipuladas. A operação de controle, pode ser feita pela Interface Homem Máquina (IHM), tanto para monitorar e ajustar *setpoints* ou outros parâmetros, mas também registrar eventos e apresentar como estão os demais processos em andamento.

Figura 1 – Arquitetura de operação da ICS




Fonte: Babu et al. (2017)

O campo de aplicação das ICS é vasto, contemplando das linhas de produção de alimentos, medicamento, veículos, mas também de operações de refinarias, sistemas de distribuição, geração e distribuição de energia, tratamento de água e esgoto, sistemas de telecomunicação, mineração, transporte ferroviário e em vários destes cenários contando com ambientes hostis, variando de poeira, ruídos, trepidação, calor, produtos químicos além de risco de vida para os operadores envolvidos (IGURE et al. 2006).

Por fim um conceito importante é o sistema de detecção de anomalias. Conforme descreve Kreimel et al. (2020) é um sistema amplamente utilizado na área de tecnologia da informação, como uma estratégia de defesa contra ações que visam comprometer a segurança de uma rede ou um equipamento. O ataque, que gera a anomalia, pode ser executado por alguém que faz parte da própria infraestrutura da rede, no caso um *insider* ou um agente externo, no caso um *outsider*. Sua função, portanto, é utilizar mecanismos para coletar, analisar e reportar eventos anormais, ou que pareçam anormais em um ambiente computacional. Este modelo de proteção pode ser aplicado em redes ICS, considerando as características de operação.

## 3. METODOLOGIA

Este artigo é uma revisão sistemática da literatura, conforme descreve Galvão, et al. (2019) a RSL pode ser classificada como uma modalidade de pesquisa, em função de padrões determinados trata um grande volume de informações de forma a trazer compreensão sobre temas escolhidos e avaliar com base em um contexto específico, o que pode ser utilizado para reproduzir um experimento, descrever um assunto ou ainda conduzir uma pesquisa considerando dados bibliográficos consultados. Ao se definir uma estratégia de busca, alinhada a uma base de pesquisa selecionada, além da definição de critérios de inclusão e exclusão de artigos científicos. A partir deste ponto deve-se analisar uma massa de informações, sem esquecer da necessidade de delimitar e determinar os escopos necessários.

A seguir o planejamento, a forma de condução e controle da revisão são detalhados.

O planejamento consiste no desenvolvimento da RSL, deve cobrir estudos relacionados à segurança cibernética, detecção de anomalias em redes, redes industriais de médio e pequeno porte classificadas como legadas, visando executar a validação e comparação de comportamentos destas redes tendo como referência normas de segurança cibernética. Para tanto, utilizar as principais bases de pesquisa e respectivos estudos disponíveis.

A condução desta etapa deve considerar expressões relacionadas ao tema e um problema de pesquisa definido, uma string de busca aplicada a uma base de artigos resultou em uma determinada quantidade de estudos correlatos. Estes estudos requerem avaliação de seu conteúdo visando identificar, de acordo com critérios de inclusão e exclusão quais estudos podem ser selecionados para a RSL aqui proposta. A utilização de ferramentas como Microsoft Excel e bases específicas de busca, fornecem suporte para avaliação dos trabalhos selecionados.

A análise dos dados deve auxiliar na identificação de características de cada estudo, como por exemplo técnicas utilizadas, relevância do assunto, contribuição para compreensão do estágio atual e trabalhos correlatos. Uma eventual exclusão por conta de similaridades, permitindo também a definição de parâmetros entre os estudos. A apresentação desta análise por meio de visualização gráfica auxilia na compreensão das escolhas e tópicos relevantes, além de identificar qual base pode fornecer mais insumos para a pesquisa.

### 3.1. Planejamento da Revisão Sistemática

Esta etapa tem como objetivo, definir um ambiente que valide normas e padrões de segurança cibernética em redes industriais formadas por equipamentos legados conforme já apresentado. A revisão sistemática procura identificar estudos que possam auxiliar na resposta à questão principal da pesquisa: Como definir um ambiente que valide a conformidade de padrões de segurança cibernética em redes industriais legadas?

A questão de pesquisa será decomposta e organizada utilizando a estratégia PICO. PICO representa um acrônimo para *Population, Intervention, Comparison e Outcome*. Neste sentido podemos considerar:

- População: Redes industriais legadas de pequeno e médio porte;
- Intervenção: O desenvolvimento de monitoração de redes industriais legadas utilizando a conformidade dessa rede com um conjunto de padrões de segurança proposto;
- Comparação: Considerar a bibliografia exploratória;
- Resultados (O – Output): O sistema de monitoração para identificar anomalias na rede.

O controle dos estudos e a base de apoio à revisão sistemática tem origem na pesquisa exploratória, realizada por meio de consulta bibliográfica de artigos publicados em conferências, periódicos e revistas nas bases de buscas bem como com os critérios descritos nas sessões seguintes.

Os critérios de seleção das bases de busca foram:

- Conter material acadêmico como por exemplo artigos, anais de eventos revistas cientificas, publicações e experimentos;
- Possuir capacidade de pesquisa detalhada, permitindo diferentes seleções como data de publicação, tipo de estudo, pesquisa por sinônimos, data de publicação, exportação, indicação de número de citações e acesso aos artigos completos;
- Ser reconhecida como fonte de consulta confiável na comunidade acadêmica.

Com base nos critérios definidos, as bases descritas no Quadro 1 foram selecionadas, em função da qualidade dos artigos e por incluir as principais revistas literárias e eventos científicos e técnicos.

Quadro 1 – Fontes de Busca da Revisão Sistemática

| Fonte de Busca | Endereço Online |
|---|---|
| Web of Science | https://access.clarivate.com/ |
| Scopus | https://www.elsevier.com/pt-br/solutions/scopus |
| ACM Digital Library | https://dl.acm.org |

Fonte: Elaborado pelo autor

Durante a pesquisa exploratória percebeu-se que o idioma dos trabalhos em sua totalidade foi o inglês. As palavras-chave, foram estabelecidas considerando somente dois dos seguintes idiomas:

- Língua inglesa: ICS, SCADA, Industrial Cyber-Physical Systems, Legacy, Anomaly detection.
- Língua portuguesa: ICS, SCADA, Sistemas Industriais Cyber-Físicos, Legado, Detecção de anomalia.

Recorreu-se aos operadores lógicos “AND” e “OR” para combinação das palavras-chave. A *string* de busca, utilizada foi definida desta forma: ((((TS=(ICS)) OR TS=(scada)) OR TS=(Industrial Cyber-Physical System*)) AND TS=(legacy)) AND TS=("Anomaly Detection")

A estratégia de busca para a identificação dos trabalhos utilizou-se de busca avançada nos sites das bases de busca por meio da aplicação da *string* de busca e suas variações, quando necessário, no período entre 12 de junho de 2022 a 07 de novembro de 2022.

Nesta etapa da revisão sistemática, os critérios de inclusão e exclusão, limitam a seleção dos trabalhos conforme sua relevância para o objetivo da pesquisa. Portanto, com base em avaliações qualitativas foram definidos os seguintes critérios de inclusão:

1. O estudo descreve características de redes industriais;
2. O estudo aborda vulnerabilidades de redes industriais;
3. O estudo aborda redes industriais antigas, ou sistemas legados;
4. O estudo aborda segurança da informação aplicada para redes industriais;
5. O estudo descreve padrões e nomas de segurança da informação.

Ao mesmo tempo que foram definidos os seguintes critérios de exclusão:

a. O estudo apresenta o mesmo tópico e citações de outros estudos;
b. O estudo não está disponível digitalmente;
c. O estudo aborda novas implementações de redes industriais;
d. Resultados apresentados não são aplicáveis;
e. O estudo aborda redes industriais *stand alone* (não estão conectadas à outras redes/Internet);
f. O estudo utiliza idiomas diferentes do português, inglês e espanhol.

Não foram considerados artigos levantados na pesquisa exploratória, que serviram por exemplo para referenciar e justificar o problema de pesquisa, portanto, não compõem o processo proposto acima.

Uma vez definidos os critérios de seleção de artigos, a estratégia para seleção propriamente dita dos trabalhos, deve considerar os trabalhos retornados na pesquisa nas bases selecionadas.

A primeira revisão executada, considerando os tópicos pertinentes, deve levar em consideração o título do trabalho, visando eliminar algum artigo que não tenha relação com os temas pesquisados. Neste ponto elimina-se estes materiais, bem como remove-se os artigos duplicados. Em função dos títulos, inicia-se a leitura do *abstract* que permite uma avaliação inicial da proposta do trabalho, partindo da premissa que foi desenvolvido de acordo com os critérios mínimos de confecção de um *abstract*. Esta etapa deve eliminar mais artigos. A próxima etapa consiste na leitura da introdução dos trabalhos relacionados, considerando a mesma premissa já utilizada com relação ao abstract. Estas etapas visam sempre identificar a relação do material proposto e os critérios de inclusão e exclusão definidos. Nesta fase já existe como resultado a exclusão de trabalhos que não atendam os critérios.

A fase final da seleção deve considerar a leitura integral dos artigos classificados como incluídos, mais uma vez considerando os critérios de inclusão e exclusão e nesta etapa a possibilidade de identificar os artigos mais adequados, ou seja, os artigos que possuem a maior quantidade de critérios de inclusão, logo, os mais alinhados ao objetivo de responder à pergunta de pesquisa. Há também a possibilidade de excluir artigos por conta da possibilidade de apresentar um ou mais critérios de exclusão. Ao final será possível identificar os artigos que efetivamente são classificados como incluídos, considerando os possuem todos os critérios de inclusão.

A seguir um resumo das configurações utilizadas em cada base de dados de pesquisa:

**Fonte 1 – Web of Science**
Data de busca: 17 de junho de 2022
Amplitude da busca: “All Metadata”
Campos pesquisados: Tópicos
Período considerado: Não foi definido
String executada: ((((TS=(ICS)) OR TS=(scada)) OR TS=(Industrial Cyber-Physical System*)) AND TS=(legacy)) AND TS=("Anomaly Detection")

**Fonte 2 – Scopus**
Data de busca: 17 de junho de 2022
Amplitude da busca: “All Metadata”
Campos pesquisados: Tópicos
Período considerado: Desde 2015
String executada: (ALL (ICS) OR ALL (scada) OR ALL (Industrial AND Cyber-Physical AND System) AND ALL (cyber*security) AND ALL (legacy) AND ALL (anomaly AND detection)) AND PUBYEAR > 2015 AND PUBYEAR >2015

**Fonte 3 – ACM Digital Library**
Data de busca: 24 de agosto de 2022
Amplitude da busca: “All Metadata”
Campos pesquisados: Full Text Collection
Período considerado: Não foi definido
String executada: [All: scada] AND [All: “cyber security”] AND {All:”anomaly tedection”] AND [All:legacy]

Nas próximas subseções serão apresentados os 5 principais trabalhos retornados da aplicação da string de busca em cada uma das bases consultadas, assim como o resultado de cada etapa das três avaliações, por meio de um quadro, com as seguintes informações:

- ID: contém o número sequencial do estudo;
- Título: contém o título completo do estudo;
- Autor: nome do ou dos autores e autoras;
- Critérios da 3ª fase: indicação do total de critérios de inclusão que o artigo atendeu;
- Resultado da 3ª fase: indicação de artigos incluídos.

Após aplicar os critérios de inclusão e exclusão estabelecidos nos 157 trabalhos encontrados, foram aceitos 5 trabalhos ao final da seleção. O Quadro 2 apresenta os detalhes.

Quadro 2 – Trabalhos selecionados na Síntese da Revisão Sistemática

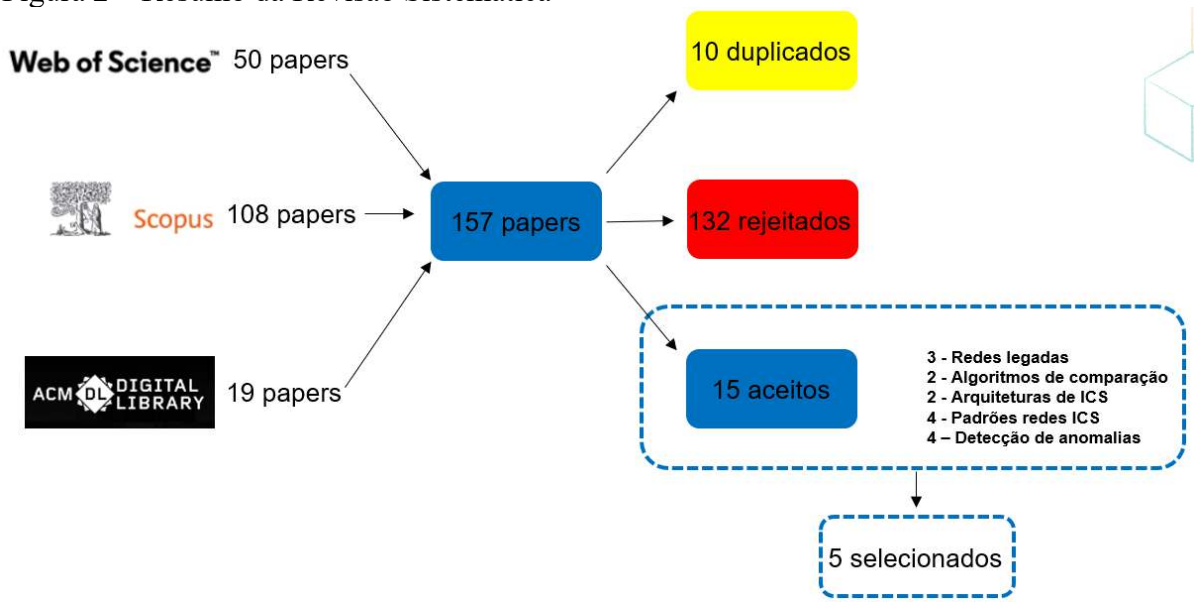
| ID | Título | Autor | Critério 3ª fase | Resultado 3ª fase |
|---|---|---|---|---|
| **5** | **A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics** | **Pliatsios, D; Sarigiannidis, P; Lagkas, T; Sarigiannidis, AG** | **1, 2, 3, 4, 5** | **Incluído** |
| **19** | **SPEAR SIEM: A Security Information and Event Management system for the Smart Grid** | **Radoglou-Grammatikis, P; Sarigiannidis, P; Iturbe, E; Rios, E; Martinez, S; Sarigiannidis, A; Eftathopoulos, G; Spyridis, Y; Sesis, A; Vakakis, N; Tzovaras, D; Kafetzakis, E; Giannoulakis, I; Tzifas, M; Giannakoulias, A; Angelopoulos, M; Ramos, F** | **1, 2, 3, 4, 5** | **Incluído** |
| **24** | **Operational Data Based Intrusion Detection System for Smart Grid** | **Efstathopoulos, G; Grammatikis, PR; Sarigiannidis, P; Sarigiannidis, VAA; Stamatakis, K; Angelopoulos, MK; Athanasopoulos, SK** | **1, 2, 3, 4, 5** | **Incluído** |
| **29** | **A COMPARISON OF UNSUPERVISED LEARNING ALGORITHMS FOR INTRUSION DETECTION IN IEC 104 SCADA PROTOCOL** | **Anwar, M; Borg, A; Lundberg, L** | **1, 2, 3, 4, 5** | **Incluído** |
| **149** | **Using Temporal and Topological Features for Intrusion Detection in Operational Networks** | **Anton, Simon D. Duque and Fraunholz, Daniel and Schotten, Hans Dieter** | **1, 2, 3, 4, 5** | **Incluído** |

Fonte: Elaborado pelo autor

## 4. RESULTADOS

Com a condução da RSL, no decorrer dos meses de junho a novembro de 2022 a Figura 2 apresenta um resumo da avaliação dos artigos identificados nas 3 bases selecionadas. Foram encontrados e avaliados 157 trabalhos, aqui definidos como *papers* (50 da base Web of Science, 108 da base Scopus e 19 da base ACM Library). Após a remoção de artigos duplicados e a rejeição de artigos em função dos critérios de exclusão, mas também por não atender critérios mínimos de inclusão até por conta da impossibilidade de agregar insumos ou apresentar o estado da arte no assunto em avaliação. Dos 15 artigos aceitos, 5 foram selecionados para síntese e definição de campos de extração que auxiliam a revisão sistemática e na resposta para a pergunta de pesquisa.

Figura 2 – Resumo da Revisão Sistemática




Fonte: Elaborador pelo autor

Após a seleção dos trabalhos conforme indica os Quadros 3, 4, 5, 6 e 7 a leitura completa dos artigos visa elaborar a síntese da revisão sistemática, em função dos critérios de seleção já definidos, descritos nos quadros no campo de extração e um campo adicional que tem como objetivo auxiliar estudos futuros.

Quadro 3 – Síntese do artigo de Pliatsios et al. (2020)

| Artigo | Síntese | Campo de extração |
|---|---|---|
| **Pliatsios et al. (2020)**<br><br>**A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics** | Estudo apresenta a arquitetura recomendada para uma rede industrial, a descrição dos protocolos utilizados, discute os impactos que um incidente de segurança pode gerar e as principais ameaças, as tendências e evoluções envolvendo sistemas SCADA. Adicionalmente apresenta propostas e táticas possíveis para reforçar a segurança destes sistemas. O artigo descreve uma característica dos sistemas Legados que operam em redes isoladas desde sua implementação, mas as necessidades de negócio forçaram a conexão destes produtos à Internet, aumentando as ameaças de segurança. especificamente com relação aos protocolos utilizados, o artigo descreve as características de cada um, detalhando a estrutura de funcionamento o que auxilia a definição da formação da comunicação e suas características técnicas, algo fundamental para a definição de estratégias de monitoração e identificação de anomalias. Por fim o material apresenta um resumo das técnicas que podem ser utilizadas a fim de reforçar a segurança de sistemas SCADA. | **Descreve características de redes industriais**<br>Aborda a arquitetura destas redes, bem como os protocolos utilizados, além das características de conter sistemas legados e por fim relaciona a criticidade destas redes Infraestrutura Crítica e o impacto que um ataque cibernético pode causar.<br>**Descreve vulnerabilidades de redes**<br>Aborda a conexão de redes industriais à Internet e redes corporativas, além das vulnerabilidades mais comuns.<br>**Descreve redes com sistemas legados**<br>Menciona o isolamento das redes com sistemas legados e diferencial de performance entre os novos protocolos frente aos protocolos legados.<br>**Descreve Segurança da Informação aplicada para redes industriais**<br>Além de abordar arquiteturas recomendáveis aborda tendencias de pesquisa e melhorias futuras para sistemas SCADA.<br>**Descreve padrões de Segurança da Informação**<br>Propõe técnicas e táticas para reforçar a segurança de sistemas SCADA.<br><br>**Descreve técnicas, ferramentas e procedimentos utilizados**<br>Por se tratar de um Survey, apresenta requerimentos necessários para redes industriais e principais questões envolvendo Segurança. |

Fonte: Elaborado pelo autor

Quadro 4 – Síntese do artigo de Radoglou-Grammatikis et al. (2021)

| Artigo | Síntese | Campo de extração |
|---|---|---|
| **Radoglou-Grammatikis et al. (2021)**<br><br>**SPEAR SIEM: A Security Information and Event Management system for the Smart Grid** | Artigo propõe um sistema de correlação de eventos tomando como base que os dispositivos e protocolos utilizados nestas redes são antigos e não foram planejados para tratar ameaças cibernéticas. Emprega o Secure And PrivatE smArt gRid (SPEAR SIEM), considerando que um *Security Information Event Management* (SIEM) tem a função de registrar, correlacionar e reportar incidentes de segurança. O objetivo central do artigo é implementar um sistema que detecte, normalize e correlacione eventos que podem ser classificados como ataques cibernéticos em plantas de geração hidroelétrica de energia, subestações, residências e plantas de geração de energia. | **Descreve características de redes industriais**<br>Aborda protocolos e sistemas legados, como ativos característicos em redes *Smart Grid.*<br>**Descreve vulnerabilidades de redes**<br>Aborda o aumento da possibilidade de ataques (*attack surface*) na medida que as redes industriais são conectadas a dispositivos IoT.<br>**Descreve redes com sistemas legados**<br>Menciona que sistemas legados aumentam a superfície de ataque em redes industriais, quando da interconexão com sistemas IoT.<br>**Descreve Segurança da Informação aplicada para redes industriais**<br>Implementação de medidas de Segurança específicas para protocolos industriais.<br>**Descreve padrões de Segurança da Informação**<br>Tem como referência do estudo a aplicação do *Security Information and Event Management* (SIEM) para monitorar, detectar, organizar, agregar, normalizar e correlacionar visando prevenir incidentes.<br>**Descreve técnicas, ferramentas e procedimentos utilizados**<br>Desenvolve um sistema de monitoração específico para redes *Smart Grid* com a capacidade de calcular a reputação de cada ativo conectado à rede, com base em dados operacionais. |

Fonte: Elaborado pelo autor

Quadro 5 – Síntese do artigo de Efstathopoulos et al. (2019)

| Artigo | Síntese | Campo de extração |
|---|---|---|
| **Efstathopoulos et al. (2019)**<br><br>**Operational Data Based Intrusion Detection System for Smart Grid** | O estudo visa utilizar *Intrusion Detection System* (IDS) para notificar operadores do sistema supervisório (uma categoria de sistema SCADA) de forma imediata, quando da ocorrência de ataques cibernéticos ou ainda um comportamento anormal em uma rede específica, utilizando *machine learning* e *deep learning*. Como os sistemas SCADA por vezes integram diferentes fornecedores e protocolos classificados como legados, estes produtos não possuem características básicas de segurança como mecanismos de autenticação e autorização. | **Descreve características de redes industriais**<br>Aborda produtos legados e ambientes heterogêneos encontrados nestas redes.<br>**Descreve vulnerabilidades de redes**<br>Aborda incidentes já ocorridos, bem como as vulnerabilidades mais comuns encontradas nas redes industriais.<br>**Descreve redes com sistemas legados**<br>**Descreve Segurança da Informação aplicada para redes industriais**<br>Aborda arquiteturas necessárias e características relevantes para implementação de uma rede industrial.<br>**Descreve padrões de Segurança da Informação**<br>Especificamente sobre IDS.<br>**Descreve técnicas, ferramentas e procedimentos utilizados**<br>Aborda a utilização de um sistema de *Intrusion Detection System* (IDS) com dados operacionais, aplicável para redes *Smart Grid* usando *machine learning* e modelos *deep learning,* com o objetivo de notificar operadores no caso de incidentes. |

Fonte: Elaborado pelo autor

Quadro 6 – Síntese do artigo de Anwar et al. (2021)

| Artigo | Síntese | Campo de extração |
|---|---|---|
| **Anwar et al. (2021)**<br><br>**A Comparison of Unsupervised Learning Algorithms for Intrusion Detection in IEC 104 SCADA Protocol** | Em função das vulnerabilidades de sistemas SCADA e eventos comprovadamente danosos que afetaram até países, uma solução para tratar eventos de segurança nas redes industriais, no caso a detecção de anomalias ou acessos indevidos em sistemas SCADA é proposta, com a aplicação de técnicas de *machine learning* para detecção de intrusão. O estudo procura comparar diferentes algoritmos de *machine learning* não supervisionados a partir de *datasets* disponíveis visando comprovar se tais algoritmos podem identificar ataques em um protocolo específico para redes industriais. | **Descreve características de redes industriais**<br>Aborda ambientes modernos e legados funcionando ao mesmo tempo e os riscos envolvidos.<br>**Descreve vulnerabilidades de redes**<br>Aborda ações necessárias para lidar com ataques de Denial of Service (DoS).<br>**Descreve redes com sistemas legados**<br>Aborda a heterogeneidade das redes com produtos legados e modernos e o impacto que este cenário pode trazer para a Segurança, bem como a deficiência de protocolo antigos que não possuem funcionalidades de segurança como autenticação e criptografia.<br>**Descreve Segurança da Informação aplicada para redes industriais**<br>Aborda a aplicação dos algoritmos para tratar pontos de intrusão, vetores de ataques, isolamento de segmentos de rede e definição de perfis em função das estatísticas de tráfego.<br>**Descreve padrões de Segurança da Informação**<br>Aborda funcionalidades como criptografia, autenticação e integridade de comunicações em novos, ou ainda modernos protocolos de comunicação industrial.<br><br>**Descreve técnicas, ferramentas e procedimentos utilizados**<br>Utilização de algoritmos de *machine learning* para identificar vetores de ataques cibernéticos para um protocolo industrial específico. |

Fonte: Elaborado pelo autor

Quadro 7 – Síntese do artigo de Anton et al. (2019)

| Artigo | Síntese | Campo de extração |
|---|---|---|
| **Anton et al. (2019)**<br><br>**Using Temporal and Topological Features for Intrusion Detection in Operational Networks** | Estudo apresenta dois tipos de sistemas de detecção de intrusão em redes industriais. Faz uma avaliação de ambos e sua implementação de forma agregada utilizando *datasets* específicos, ou seja, um conjunto de dados que possui o compartimento histórico de um determinado equipamento ou sistema por um determinado período de tempo. Utilizando um processo industrial para tratamento de água, ataques cibernéticos foram simulados a fim de detectar a intrusão na rede. Com um determinando período de monitoração, diferentes processos da rede foram cobertos, propiciando a utilização de uma matriz para identificar o comportamento anormal na rede por conta de variações fora de um padrão pré-estabelecido, que pode ser um ataque ou um problema de configuração em um PLC. | **Descreve características de redes industriais**<br>Aborda o isolamento destas redes no passado e a complexidade técnica e financeira de implementar atualizações.<br>**Descreve vulnerabilidades de redes industriais**<br>Descreve a falta de atualização que propicia ataques e as mutações que ataques podem apresentar.<br>**Descreve redes com sistemas legados**<br>Descreve a relevância da proteção de redes com sistemas legados e a atenção dispensada para o tema envolvendo fornecedores e empresas.<br>**Descreve Segurança da Informação aplicada para redes industriais**<br>Aborda as diferenças no tratamento de redes de IT e OT.<br>**Descreve padrões de Segurança da Informação**<br>Aborda questões como autenticação, atualização e criptografia e análise de tráfego.<br><br>**Descreve técnicas, ferramentas e procedimentos utilizados**<br>Descreve técnicas de avaliação de comportamento de rede. |

Fonte: Elaborado pelo autor

### 4.1. Análise

Todos os estudos descrevem as vulnerabilidades das redes industriais quando da interconexão com redes corporativas e Internet, partindo da premissa que a Internet não é segura em função do volume de ameaças cibernéticas que são desenvolvidas diariamente. Os resultados são homogêneos, porém, como a maioria dos artigos está relacionada a redes Smart Grid (artigos de Radoglou-Grammatikis et al. (2021), Efstathopoulos et al. (2019) e Anwar et al. (2021), ou seja, ambientes relacionados a energia elétrica, novas pesquisas, por exemplo a inclusão de outras palavras-chave na *string* de busca, devem identificar material de outros setores da economia. Por outro lado, demonstra que o setor energético tem maior exposição a riscos cibernéticos, utiliza amplamente ICS e consequentemente existem mais pesquisas relacionadas à Segurança Cibernética.

O artigo de Anwar et al. (2021), tem um resultado pouco consistente em função do volume da dados utilizados, mas é um referencial importante para a compreensão dos riscos e soluções possíveis para aplicação em redes industriais. A arquitetura proposta para a utilização de um IDS descrita no artigo de Efstathopoulos et al. (2019) é a mais adequada para redes industriais e pôde ser identificada também em outros artigos. A revisão sistemática da literatura suporta a afirmação que é possível desenvolver um ambiente de validação de normas de segurança para redes industriais legadas.

A utilização de *datasets* para o estudo de comportamento de uma ICS ou para a simulação de eventos conforme Anton et al. (2019) utiliza em seu artigo, é positivo sob a ótica de permitir a simulação de eventos, mas requer atenção para o tipo de dado coletado, qual o contexto de utilização e que equipamentos foram utilizados. Em ambientes ICS as variações de tipo de equipamento, no caso uma característica pontuada em diversos artigos, que descreve ambientes heterogêneos e que, portanto, podem não produzir as mesmas sérias históricas de eventos e comprometer a solução para um determinado problema e o entendimento do comportamento de uma ICS.

## 5. CONCLUSÕES

Esta revisão sistemática da literatura identificou uma gama de artigos e eventos, que demonstram a dificuldade de manter sistemas legados frente os riscos cibernéticos, nos ambientes industriais, por outro lado, as referências e possibilidades de implementação de soluções de proteção de acordo com o porte das empresas, merece atenção na medida que novas tecnológicas requerem envolvimento de fornecedores e estes não estão dispostos a investir em bases instaladas legadas, há um campo de pesquisa para identificar estas lacunas, tanto na academia como na indústria. No Brasil a pequena e média indústria terá que encontrar soluções de baixo custo para fazer frente a estes desafios.

Setores da economia, principalmente de alta tecnologia, não estão sujeitos a problemas relacionados a redes legadas, na medida que a produção de produtos de alta tecnologia não permite a utilização de tecnologias antigas. Dados os incidentes reportados e vastamente descritos nos artigos, mostra-se importante que no caso de sistemas que mantenham infraestrutura crítica, ou seja, setores da economia que mantém serviços de alta relevância para a sociedade, se desenvolva uma política nacional para adequação e melhora de aspectos de segurança cibernética, bem como a criação de planos de contingência, gestão de crise e notificação de incidentes. Há que se destacar que os estudos e experimentos já desenvolvidos, não são aplicados em ambientes reais. Esta foi uma limitação dos trabalhos revisados. A aplicação em ambientes efetivamente produtivos, apresenta riscos para a operação das organizações, há, portanto, um paradoxo no sentido de planejar de forma rigorosa a implementação de ações que visem aumentar o nível de segurança das redes industriais,

detectar vulnerabilidades e garantir a operação das fábricas e a segurança física dos operadores.

Por fim, este artigo com a revisão sistemática da literatura, viabiliza o desenvolvimento de trabalhos futuros como a definição de um ambiente para validação de normas de segurança em redes industriais legadas, montagem de protótipos que possam correlacionar eventos existentes a bases da dados de incidentes e propor soluções ou ainda pesquisas relacionadas a países e seu estágio de evolução com relação a proteção cibernética, tanto em pesquisas como na efetiva implementação de soluções.

## 6. REFERÊNCIAS BIBLIOGRÁFICAS

ANDERL, R. (2014). **Industrie 4.0: advanced engineering of smart products and smart production**. Conference: 19th International Seminar on High Technology, Piracicaba, Brazil, pp. 1-14.

ANTON, Simon D. Duque; FRAUNHOLZ, Daniel; SCHOTTEN, Hans Dieter. Using temporal and topological features for intrusion detection in operational networks. In: **Proceedings of the 14th International Conference on Availability, Reliability and Security**. 2019. p. 1-9.

ALCARAZ, Cristina; FERNANDEZ, Gerardo; CARVAJAL, Fernando. **Security aspects of SCADA and DCS environments**. In: Critical Infrastructure Protection. Springer, Berlin, Heidelberg, 2012. p. 120-149

BABU, Bijoy et al. Security issues in SCADA based industrial control systems. In: **2017 2nd International Conference on Anti-Cyber Crimes (ICACC)**. IEEE, 2017. p. 47-51.

CASE, Defense Use. Analysis of the cyber attack on the Ukrainian power grid. **Electricity Information Sharing and Analysis Center (E-ISAC)**, v. 388, p. 1-29, 2016.

CONKLIN, Wm Arthur. IT vs. OT security: A time to consider a change in CIA to include resilienc. In: **2016 49th Hawaii International Conference on System Sciences (HICSS)**. IEEE, 2016. p. 2642-2647.

CORALLO, A., LAZO,i M., & LEZZI, M. (2020). **Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts**.

EFSTATHOPOULOS, Georgios et al. Operational data based intrusion detection system for smart grid. In: **2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)**. IEEE, 2019. p. 1-6.

FALLIERE, Nicolas; MURCHU, Liam O.; CHIEN, Eric. W32. stuxnet dossier. **White paper, symantec corp., security response**, v. 5, n. 6, p. 29, 2011.

GALVÃO, M. C. B.; RICARTE, I. L. M. REVISÃO SISTEMÁTICA DA LITERATURA: CONCEITUAÇÃO, PRODUÇÃO E PUBLICAÇÃO. **Logeion: Filosofia da Informação**, *[S. l.]*, v. 6, n. 1, p. 57–73, 2019. DOI: 10.21728/logeion.2019v6n1.p57-73. Disponível em: https://revista.ibict.br/fiinf/article/view/4835. Acesso em: 01 set. 2022.

HENTEA, Mariana. Improving security for SCADA control systems. **Interdisciplinary Journal of Information, Knowledge, and Management**, v. 3, p. 73, 2008.

IGURE, Vinay M.; LAUGHTER, Sean A.; WILLIAMS, Ronald D. Security issues in SCADA networks. **computers & security**, v. 25, n. 7, p. 498-506, 2006.

JADIDI, Zahra et al. Automated detection-in-depth in industrial control systems. **The International Journal of Advanced Manufacturing Technology**, v. 118, n. 7, p. 2467-2479, 2022.

KHAN, Rafiullah et al. A seamless cloud migration approach to secure distributed legacy industrial SCADA systems. In: **2020 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)**. IEEE, 2020. p. 1-5.

KREIMEL, Philipp et al. Anomaly detection in substation networks. **Journal of Information Security and Applications**, v. 54, p. 102527, 2020.

PLIATSIOS, Dimitrios et al. A survey on SCADA systems: secure protocols, incidents, threats and tactics. **IEEE Communications Surveys & Tutorials**, v. 22, n. 3, p. 1942-1976, 2020

RADOGLOU-GRAMMATIKIS, Panagiotis et al. Spear siem: A security information and event management system for the smart grid. **Computer Networks**, v. 193, p. 108008, 2021.

SCHWAB, K. (2016). **A Quarta Revolução Industrial**. Tradução: Daniel Moreira Miranda, EDIPR

SETOLA, Roberto et al. An overview of cyber attack to industrial control system. **Chemical Engineering Transactions**, v. 77, p. 907-912, 2019.

Tanenbaum, A. S. (2003). Redes de computadores. Brasil: Elsevier.