contecc 2025
CONGRESSO TÉCNICO-CIENTÍFICO DA ENGENHARIA E DA AGRONOMIA

CIBERSEGURANÇA EM SISTEMAS *SCADA*

VICTOR CIRIMBELLI CASTILHO[1]

[1]Pós-graduando em Engenharia de Software, USP/Esalq, Taubaté-SP, victorcastilho03@gmail.com

Apresentado no
Congresso Técnico Científico da Engenharia e da Agronomia – CONTECC
06 a 09 de outubro de 2025

RESUMO: O artigo apresenta um estudo teórico voltado à cibersegurança em sistemas *SCADA* (*Supervisory Control And Data Acquisition*), amplamente utilizados para supervisão e controle de processos industriais, focado em identificar os riscos cibernéticos associados a tais sistemas e estratégias de mitigação, protegendo os colaboradores, a informação e os ativos físicos. Com a convergência entre os sistemas de Tecnologia da Informação (TI) e Tecnologia Operacional (TO), os sistemas *SCADA* tendem a sofrer uma maior exposição a vulnerabilidades cibernéticas, apesar dos benefícios quanto à agilidade e tomadas de decisões, sendo necessária a devida gerência nestes cenários. A pesquisa conclui que, para garantir a segurança dos sistemas *SCADA*, é necessário integrar práticas de segurança cibernética, infraestrutura robusta e a capacitação contínua dos profissionais, o fator humano se demonstra como um fator importante, pois é ele quem toma as decisões para implementação dos ambientes e como operá-los, o que pode comprometer ou não todo o sistema. Além disso, uma rede segura e sistemas de monitoramento adequados são fundamentais para a prevenção e resposta a incidentes.
PALAVRAS-CHAVE: *SCADA*, cibersegurança, riscos.

CYBER SECURITY FOR SCADA SYSTEMS

ABSTRACT: The article presents a theoretical study focused on cybersecurity in SCADA (Supervisory Control And Data Acquisition) systems, which are widely used for the supervision and control of industrial processes. It aims to identify the cyber risks associated with such systems and proposes mitigation strategies, to protect personnel, information, and physical assets. With the convergence of Information Technology (IT) and Operational Technology (OT) systems, SCADA systems tend to be more exposed to cyber vulnerabilities, despite the benefits in agility and decision-making. Therefore, proper management in these scenarios is necessary. The research concludes that, in order to ensure the security of SCADA systems, it is essential to integrate cybersecurity practices, robust infrastructure, and continuous training of professionals. The human factor proves to be crucial, as it is the individual who makes decisions regarding the implementation and operation of these environments, which can either compromise or safeguard the entire system. Furthermore, a secure network and appropriate monitoring systems are fundamental for the prevention of and response to incidents.
KEYWORDS: SCADA, cybersecurity, risks.

INTRODUÇÃO

SCADA significa *Supervisory Control And Data Acquisition*, em português Sistema de Supervisão e Aquisição de Dados, o próprio nome reforça seu foco e, portanto, trata-se de um pacote de *softwares* alocados em um hardware, conectado geralmente via controladores lógicos programáveis (*PLCs*) e outros módulos e componentes industriais de mercado (DANEELS; SALTER, 1999).

Com a evolução da indústria, houve a necessidade do desenvolvimento de *softwares* responsáveis pela supervisão e controle de manipulações operacionais, seja para equipamentos específicos, linhas de produção e afins. Os *SCADA* foram desenvolvidos com esta função, possuindo capacidade de customização para atender os mais diversos ambientes e sendo uma parte fundamental

para a agilidade, segurança e disponibilidade, permitindo operações remotas em equipamentos (ZANGHI, 2019).

A tecnologia da informação e a tecnologia operacional, também avançaram suas vantagens competitivas para coleta e envio de dados de produção. Porém, isso leva a desvantagens, principalmente quanto a ciberataques (CIGREF, 2019). Sistemas de controle e automação industrial (*IACS*) começaram a integrar tecnologias desenvolvidas para sistemas de negócio, aumentando assim a possibilidade de sofrerem ciberataques (IEC 62443-2-1, 2010).

Devido sua criticidade, é importante ter atenção à segurança, não somente de infraestrutura e controle de acesso, mas também com a cibersegurança por conta dos avanços tecnológicos, com a necessidade de manter a segurança da informação e barrar acessos indevidos, tanto de pessoas não capacitadas, quanto de invasores que podem não só extrair informações críticas do negócio, como também causar danos patrimoniais e até mesmo colocar em risco a vida de colaboradores (IEC 62443-2-1, 2010). O estudo visa responder à questão: de que maneira as boas práticas no cenário industrial podem mitigar os riscos de ataques na cibersegurança?

Desta forma, o presente artigo buscou compreender formas de mitigar riscos voltados a cibersegurança dos sistemas *SCADA*. Para atingir este objetivo geral, os objetivos específicos se dividiram em: a) levantar quais são possíveis riscos de cibersegurança dos sistemas; b) estudar possíveis formas de mitigar e; c) investigar boas práticas no contexto industrial visando redução de riscos.

MATERIAL E MÉTODOS

O artigo se trata de um estudo teórico, elaborado utilizando artigos publicados e materiais de empresas de tecnologia consolidadas no mercado, o que possibilitou o levantamento de riscos cibernéticos e de infraestrutura junto a maneiras de contê-los. O intervalo da pesquisa se inicia em 1999 devido a alguns conceitos sólidos e se estende até 2025, graças a contemporaneidade do assunto (GIL, 2017).

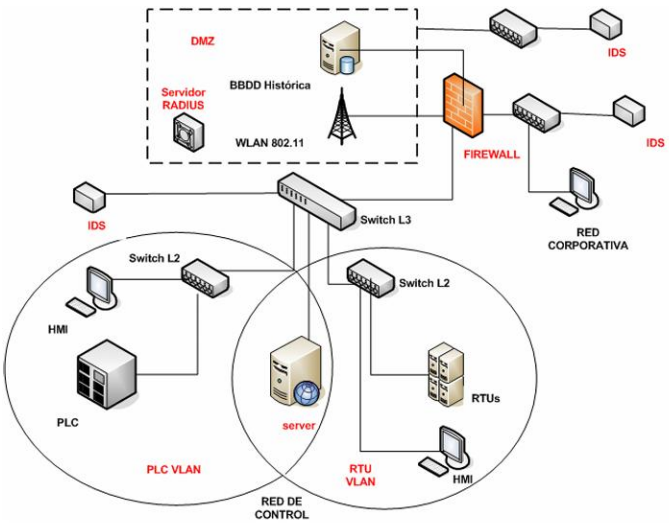
Pilares essenciais para a implementação de sistemas *SCADA* de uma forma generalista, foram apresentados, focado em pontos para a cibersegurança e indicando os riscos mais comuns, além de formas de mitigação e boas práticas que podem evitar ataques, desde os fatores tecnológicos aos comportamentais.

RESULTADOS E DISCUSSÃO

De início, deve-se considerar uma infraestrutura sólida e bem mapeada, a *COMMSCOPE* (2023), companhia provedora de serviços de infraestrutura, reforça esta exigência para atender a coleta e transformação de dados de forma eficiente e segura, com os avanços industriais, os requisitos de conectividade necessitam acompanhar a mesma tendência. Uma infraestrutura precária pode gerar situações de riscos, na qual uma parada indevida ou uma perda de comunicação podem causar acidentes.

Em infraestruturas para sistemas *SCADA* é comum contemplar dispositivos conectados a uma rede local, desde componentes de chão de fábrica eletromecânicos até o supervisório e servidores. A *NISSC* (*National Infrastructure Security Co-ordination Centre*) (figura 1) propõe uma arquitetura de rede robusta para atender as necessidades de comunicação e segurança de tais sistemas, requerendo processos de gestão de rede segura, que devem identificar e gerenciar todas as conexões da *Internet* em direção à rede *SCADA* e vice-versa, e da rede corporativa para a rede de controle. Esses processos estão sob mecanismos especializados e restritivos, como: *firewalls*, *IDS* (Sistema de Detecção de Intrusões), *IPS* (Sistema de Prevenção de Intrusões), antivírus, servidores *RADIUS* ou protocolos *VPN* (Redes Privadas Virtuais) (ALCARAZ et al., 2008).

Figura 1. Topologia de rede proposta pela *NISSC*



Fonte: *Secure Management of SCADA Networks*, 2008

Com uma infraestrutura bem elaborada e aplicada, os riscos referentes a acessos externos indevidos e disponibilidade são mapeados e mitigados. Com isso, o controle de acesso é o próximo tópico que se deve ter atenção, pois pode ser considerado um dos fatores decisivos para a segurança de um sistema *SCADA*, evitando operações indevidas onde o supervisório estiver localizado.

De acordo com a *CISCO* (2021), empresa de tecnologia focada em soluções de rede**,** o maior risco para a segurança da informação é o fator humano, tanto por questões de *ransomware* quanto a própria complexidade dos ataques. Isto reforça a necessidade de um controle rigoroso de usuário, tanto em capacitações quanto em alocações nos devidos grupos. O controle de acesso é o método utilizado para garantir que os usuários tenham as devidas responsabilidades. Além disso, é de extrema importância que a organização tenha políticas de controle de acesso rigorosas, pois a operação de sistemas *SCADA* podem colocar em risco não só ativos, mas a integridade física de colaboradores (IEC 62443-2-1, 2010).

Com as implementações citadas anteriormente, o ambiente que receberá um novo sistema *SCADA* ou até mesmo uma atualização para atender as necessidades da melhor forma possível está apto para tal. Porém, as ações anteriores não anulam 100% outros riscos comuns. Amo (2025) os listam junto a certas maneiras de mitigação:

Mecanismos de autenticação inadequados: Como muitos sistemas *SCADAS* foram desenvolvidos considerando ambientes isolados, há uma deficiência de protocolos de autenticação.

Comunicações sem criptografia: A transmissão de dados pode ser suscetível a interceptações e adulterações, devido a sistemas *SCADA* frequentemente utilizarem comunicações sem criptografia.

Sistemas legados: Componentes *SCADA* mais antigos podem operar em softwares e sistemas desatualizados, o que possibilita ataques e falta de suporte.

Falta de segmentação de rede: Uma rede plana permite que invasores acessem sistemas com maior facilidade.

Acesso remoto sem controle de segurança adequado: Embora conveniente, pode introduzir vulnerabilidades que invasores cibernéticos podem explorar para acessar redes *SCADA*.

Fornecedores: A dependência de terceiros para *software, hardware* e manutenção destes sistemas é comum e práticas inadequadas de fornecedores podem comprometer a segurança introduzindo vulnerabilidades.

Falta de monitoramento em tempo real: Monitoramento em tempo real permite maior agilidade na tomada de decisões em caso de incidentes detecção antecipada e respostas rápidas são essenciais para os sistemas. Sua falta pode causar violações prolongadas e atrasos no tempo de recuperação.

Segurança física: O acesso de pessoal não autorizado aos locais que contenham sistemas *SCADA* pode resultar em manipulações diretas no sistema e sabotagens.

Falta de capacitação de funcionários: Erros humanos podem comprometer até mesmo as proteções técnicas mais avançadas.

A seguir pode-se avaliar de forma geral os riscos comuns citados e maneiras de mitigá-los (tabela 1).

Tabela 1. Sintetização dos riscos de cibersegurança para sistemas *SCADA*

Tabela de riscos	
Riscos	**Formas de Mitigar**
Formas de autenticação inadequados	Implementação de autenticação multifatorial, controle de usuários conforme funções, políticas de senhas rigorosas e acessos temporários.
Comunicações sem criptografia	Adoção de protocolos com criptografia integrada, implementação de *virtual private network (DMZs)* — rede virtual privada —, criptografia ponta a ponta e avaliações periódicas de vulnerabilidades.
Sistemas legados	Gerenciamento de *patches*, atualizações constantes, modernização ou substituição de componentes desatualizados e aplicação de *patches* virtuais em cenários impraticáveis para *patches* tradicionais.
Falta de segmentação de rede	Implementação de segmentação de redes, *firewalls*, sistemas *IDS/IPS* para monitorar e controlar o tráfego, *demilitarized zones (DMZs)* — zonas desmilitarizadas —, e micro segmentação.
Acesso remoto sem controle de segurança	Limitar e monitorar acessos, autenticação multifatorial, isolar sessões remotas com *jumpservers* ou sistemas específicos e aplicar limite de tempo para as credenciais.
Fornecedores e terceirização inadequada	Auditorias regulares, restrição de acessos, comunicação criptografada e cláusulas de cibersegurança em contratos com fornecedores.
Falta de monitoramento em tempo real	Implementação *de Security Information and Event Management (SIEM)* — Gerenciamento de Informações e Eventos de Segurança —, ferramentas de detecção de anomalias, planos de resposta a incidentes e buscas proativas de ameaça, para não depender somente de tratativas reativas.
Segurança física inadequada	Controle rigoroso de acesso físico, alojar o *hardware* em locais seguros, sistemas de vigilância, monitoramento e sensores de violação de segurança.
Falta de capacitação de funcionários	Realização de treinamentos regulares de cibersegurança, conscientização sobre boas práticas e integração de segurança cibernética no cotidiano dos profissionais.

CONCLUSÃO

A análise teórica conduzida neste estudo evidencia que a implementação eficaz de sistemas *SCADA* exige uma abordagem multidisciplinar que integre tecnologia da informação (TI), tecnologia operacional (TO), boas práticas de engenharia, segurança cibernética e capacitação contínua dos profissionais envolvidos. Mesmo com o avanço significativo das tecnologias implementadas, ainda há desafios quanto a segurança, tanto da informação quanto patrimonial.

Considerando a pesquisa realizada, o fator humano se demonstrou o mais crítico em todo o processo, pois toda concepção do sistema *SCADA*, sua arquitetura e operação é realizada por pessoas, as quais devem estar preparadas e capacitadas para tomarem as melhores decisões possíveis, considerando soluções de mercado e desenvolvimentos necessários. Mesmo com os recursos mais avançados e sofisticados, tudo é possível de ser burlado.

A infraestrutura também é um fator fundamental que deve ser elaborado e aplicado com atenção, é devido a ela que os dispositivos serão interligados e realizarão as comunicações entre si. Ela, portanto, deve ser robusta, seguindo as recomendações das normas (normas citadas), afim de

garantir a segurança e controlar as origens, os destinos e acessos as informações, que devem ser monitorados de forma proativa, possibilitando tomadas de decisões ágeis, tanto para melhorias e modificações do sistema quanto para possíveis tratativas e respostas a ataques.

Os sistemas *SCADA* são amplamente utilizados em diversos setores industriais e atualmente indispensáveis pela sua praticidade para operar equipamentos de maneira segura, ágil e remota, mesmo que dentro da empresa. Os avanços tecnológicos e a convergência de tecnologias operacionais e da informação geraram novas vulnerabilidades junto a praticidade da transferência de dados entre os dispositivos.

AGRADECIMENTOS

Gostaria de agradecer a minha esposa Aline Cirimbelli Castilho, pelo apoio ao longo desta pesquisa.

REFERÊNCIAS

DANEELS, A.; SALTER, W. What is SCADA? In: International Conference on Accelerator and Large Experimental Physics Control Systems, Trieste, 1999. Anais... Trieste: International Conference on Accelerator and Large Experimental Physics Control Systems, 1999. p. 339–343. Disponível em: ⟨https://cds.cern.ch/record/532624/files/mc1i01.pdf⟩. Acesso em: 17 jul. 2025.

Zanghi, E. Proteção e Comunicação de Sistemas Elétricos de Potência: Sistemas SCADA: Conceitos. Porto: INESC TEC, [s.d.]. Eric Zanghi (PhD, pesquisador, INESC TEC) disponibilizou o material via ResearchGate. Disponível em: https://www.researchgate.net/profile/Eric-Zanghi2/publication/352156761_Sistemas_SCADA_Conceitos/links/60bb74b3458515218f9245ab/Sisteas-SCADA-Conceitos.pdf. Acesso em: 15 jul. 2025.

CIGREF. IT/OT Convergence: A fruitful integration of information systems and operational systems. In: Relatório técnico Cigref, [s.l.], dez. 2019. Anais... [s.l.]: Cigref, 2019. Disponível em: https://www.cigref.fr/wp/wp-content/uploads/2020/02/Cigref-IT-OT-Convergence-Fruitful-integration-information-operational-systems-December-2019-EN.pdf. Acesso em: 17 jul. 2025.

IEC. Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program. In: Technical standard IEC 62443-2-1, [s.l.], 2010. Anais... [s.l.]: International Electrotechnical Commission – IEC, 2010.

GIL, A. C. Como elaborar projetos de pesquisa. 6. ed. São Paulo: Atlas, 2017.

COMMSCOPE**.** Infraestrutura para redes em Ambientes Industriais. In: Relatório técnico CommScope, [s.l.], 2023. Anais... [s.l.]: CommScope, 2023. Disponível em: https://connectlan.com.br/wp-content/uploads/2023/09/Industria-4.0-Infraestrutura-para-redes-em-Ambientes-Industriais-1.pdf. Acesso em: 16 jul. 2025.

ALCARAZ, C.; FERNÁNDEZ, G.; ROMÁN, R.; BALASTEGUI, A.; LÓPEZ, J. Secure Management of SCADA Networks. In: *Novática, New Trends in Network Management*, vol. 9, Málaga, 2008. Anais... Málaga: Universidad de Málaga, 2008.

CISCO SYSTEMS. Desafios da Cibersegurança no Brasil. In: *inside REPORT • CYBERTECH*, [s.l.], jul. 2021. Anais... [s.l.]: Cisco Systems, 2021. Disponível em: ⟨https://www.cisco.com/c/dam/global/pt_br/solutions/pdfs/report1-distrito.pdf⟩. Acesso em: 17 jul. 2025.

AMO, Z. 9 SCADA system vulnerabilities and how to secure them. In: *ISA Global Cybersecurity Alliance (ISAGCA)*, [s.l.], 21 mar. 2025. Anais... [s.l.]: ISAGCA, 2025. Disponível em: ⟨https://gca.isa.org/blog/9-scada-system-vulnerabilities-and-how-to-secure-them⟩. Acesso em: 17 jul. 2025.