Thiago Branquinho | Marcelo Branquinho

SEGURANÇA CIBERNÉTICA INDUSTRIAL

As infraestruturas críticas mundiais correm perigo. Aprenda a proteger redes e sistemas de controle com uma metodologia comprovada na prática.

ALTA BOOKS
EDITORA
Rio de Janeiro, 2021

Segurança Cibernética Industrial

ISBN: 978-65-5520-466-7

Impresso no Brasil — 1ª Edição, 2021 — Edição revisada conforme o Acordo Ortográfico da Língua Portuguesa de 2009.

Erratas e arquivos de apoio: No site da editora relatamos, com a devida correção, qualquer erro encontrado em nossos livros, bem como disponibilizamos arquivos de apoio se aplicáveis à obra em questão.

Acesse o site **www.altabooks.com.br** e procure pelo título do livro desejado para ter acesso às erratas, aos arquivos de apoio e/ou a outros conteúdos aplicáveis à obra.

Suporte Técnico: A obra é comercializada na forma em que está, sem direito a suporte técnico ou orientação pessoal/exclusiva ao leitor.

A editora não se responsabiliza pela manutenção, atualização e idioma dos sites referidos pelos autores nesta obra.

Dados Internacionais de Catalogação na Publicação (CIP) de acordo com ISBD

B821s Branquinho, Thiago

Segurança Cibernética Industrial: as infraestruturas críticas mundiais correm perigo. Aprenda a proteger redes e sistemas de controle com uma metodologia comprovada na prática / Thiago Branquinho, Marcelo Branquinho. - Rio de Janeiro, RJ : Alta Books, 2021.
416 p. ; 17cm x 24cm.

Inclui bibliografia e índice.
ISBN: 978-65-5520-466-7

I. Segurança cibernética. 2. Segurança Cibernética Industrial. I. Branquinho, Marcelo. II. Título.

2021-2778 CDD 001.53
CDU 007

Elaborado por Vagner Rodolfo da Silva - CRB-8/9410

ALTA BOOKS EDITORA

Rua Viúva Cláudio, 291 — Bairro Industrial do Jacaré
CEP: 20.970-031 — Rio de Janeiro (RJ)
Tels.: (21) 3278-8069 / 3278-8419
www.altabooks.com.br — altabooks@altabooks.com.br

Produção Editorial
Editora Alta Books

Diretor Editorial
Anderson Vieira

Gerência Comercial
Daniele Fonseca

Coordenação Financeira
Solange Souza

Editor de Aquisição
José Rugeri
acquisition@altabooks.com.br

Produtores Editoriais
Illysabelle Trajano
Larissa Lima
Maria de Lourdes Borges
Paulo Gomes
Thiê Alves
Thales Silva

Equipe Comercial
Adriana Baricelli
Daiana Costa
Kaique Luiz
Victor Hugo Morais

Equipe Ass. Editorial
Brenda Rodrigues
Caroline David
Luana Goulart
Marcelli Ferreira
Mariana Portugal
Raquel Porto

Marketing Editorial
Livia Carvalho
Gabriela Carvalho
Thiago Brito
marketing@altabooks.com.br

Atuaram na edição desta obra:

Revisão Gramatical
Aline Vieira
Alessandro Thomé

Capa
Rita Motta

Diagramação
Catia Soderi

Ouvidoria: ouvidoria@altabooks.com.br

Editora afiliada à:

ASSOCIADO

Dedicamos este livro às inúmeras vítimas da pandemia do COVID-19
e à comunidade de profissionais de segurança cibernética, que travam batalhas
diárias para proteger pessoas, o meio ambiente e negócios ao redor do mundo.

LISTA DE FIGURAS

Capítulo 5

MÓDULO 2

Capítulo1

Capítulo 2

Capítulo 3

MÓDULO 3

Capítulo 1

Capítulo 2

Capítulo 3

Capítulo 4

Capítulo 5

Capítulo 6

MÓDULO 4

MÓDULO 5

LISTA DE TABELAS

MÓDULO 2

Capítulo 2

MÓDULO 3

Capítulo 2

MÓDULO 5

Capítulo 2

SUMÁRIO

MÓDULO 1

AUTOMAÇÃO INDUSTRIAL E TERRORISMO CIBERNÉTICO

MÓDULO 2

ANÁLISE DE RISCOS E PLANEJAMENTO

MÓDULO 3

CONTROLES DE SEGURANÇA CIBERNÉTICA INDUSTRIAL

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

CAPÍTULO 5

Controle de Malware **247**

CAPÍTULO 6

Segurança de Dados **265**

MÓDULO 4

SEGURANÇA CIBERNÉTICA PARA A TRANSFORMAÇÃO DIGITAL

MÓDULO 5

MONITORAMENTO CONTÍNUO E FORENSE INDUSTRIAL

CAPÍTULO 2

MÓDULO

1

AUTOMAÇÃO INDUSTRIAL E TERRORISMO CIBERNÉTICO

Conceitos apresentados neste capítulo

A automação industrial está amplamente presente nas sociedades contemporâneas, embora, em muitos casos, não seja percebida pela população.

Para projetar soluções de segurança cibernética eficientes, é necessário, antes de tudo, aprender como a automação é implementada e de que forma ela é operada.

Este capítulo aborda as quatro etapas que compõem o funcionamento de um Sistema de Controle Industrial (do inglês ICS, Industrial Control Systems): a aquisição de dados, a conversão de dados, a comunicação em rede e a supervisão e controle.

O conceito de redes industriais é estudado por meio da hierarquia de sistemas, conhecida como a "pirâmide de automação" (Modelo Purdue, da norma ISA-95), e as principais ferramentas utilizadas para o desenvolvimento de sistemas de supervisão e controle são brevemente apresentadas.

CAPÍTULO 1

AUTOMAÇÃO INDUSTRIAL

1.0 INTRODUÇÃO

Uma rede é composta por fios entrelaçados com espaços regulares e feita conforme objetivos específicos (caça, descanso, práticas esportivas etc.). As redes de computadores e a automação seguem uma lógica parecida. Diversos equipamentos ligam-se entre si, compartilhando informações, realizando serviços, protegendo o próprio sistema, entre outras funções. Elas se estendem e se potencializam cada vez mais, assumindo tarefas antigas e criando novas.

Nessas redes, existe ainda um elemento que se encontra no limiar, ora como uma parte dependentemente integrada, ora como uma parte individualmente autônoma: o ser humano. A liberdade permite que as pessoas transitem entre máquinas e equipamentos que elas mesmas construíram. Essa diferença lhes dá uma sensação de autonomia e poder que não é plenamente independente. Ao contrário, a tendência das sociedades contemporâneas demonstra que a relação com suas redes materiais e virtuais é tão estreita e intensa, que, sem elas, a vida humana retroagiria décadas, talvez séculos.

Isso torna bastante complexa a reflexão sobre a condição humana em relação às redes de informação e automação. Os objetivos individuais são peculiares, as funções de cada pessoa são diversificadas, e os usos variam conforme interesses e períodos. No entanto, uma coisa é certa: a maioria dos seres humanos compõe hoje, direta ou indiretamente, tais redes. A maioria das pessoas as usufrui, seja enquanto um profissional de tecnologia que garante a normalidade dos sistemas

industriais, seja enquanto alguém que acabou de abastecer seu carro com combustível e pagou com o cartão de crédito.

Na verdade, são tais usos que interligam as pessoas às suas máquinas e aos seus equipamentos. Afinal, as redes de informação e de automação foram criadas exatamente para satisfazer as necessidades e os interesses humanos. Assim, uma rede industrial é mais do que um conjunto de máquinas reunido em um mesmo lugar. Ela se constitui fundamentalmente pela troca de informações entre equipamentos a partir de determinados protocolos. Protocolos são, basicamente, as formas de regulamento sobre o modo como a informação será regida material e virtualmente; ou melhor, o modo como ela será gerada, regrada, compartilhada e sincronizada.

Uma rede industrial é baseada em uma série de protocolos de comunicação e tarefas relacionadas tanto à produção e à segurança de uma indústria quanto à distribuição de seus produtos aos consumidores. Como essas redes estão diretamente ligadas ao bom funcionamento de uma empresa e, em muitos casos, compõem infraestruturas críticas, elas precisam ser supervisionadas permanentemente.

Para isso, são utilizados sistemas de controles específicos que coordenam as informações cibernéticas de uma empresa, monitorando e supervisionando as variáveis evidenciadas pelos processos industriais. Desse modo, cria-se uma atmosfera de segurança eficiente e sofisticada para garantir a normalidade das operações das redes de automação industrial.

1.1 O QUE É AUTOMAÇÃO INDUSTRIAL?

Antes do aprofundamento conceitual sobre as redes industriais e sobre os sistemas de supervisão e aquisição de dados, também conhecidos como SCADA (Supervisory Control And Data Acquisition), é importante compreender o que é a automação industrial. A automação é um conjunto complexo de processos entre seres humanos e máquinas que visa aperfeiçoar um processo produtivo. Para isso, utilizam-se máquinas eletromecânicas, software e outros equipamentos tecnológicos específicos para cada segmento do sistema industrial em conformidade com os esforços humanos enquanto forças pensantes e controladoras de tais processos.

O principal objetivo da automação é a maximização dos processos de produção com maior eficiência em relação ao tempo e ao consumo de energia, bem como

melhorar as condições de segurança durante a realização de trabalhos brutos e arriscados (PAULA; SANTOS, 2008, p. 09).

A automação também está relacionada com movimentos mais sofisticados e delicados que exigem precisão cirúrgica, uniformidade e rapidez. Tais cenários demonstram como a automação se tornou complexa atualmente, com um aumento considerável da utilização de protocolos e demais implementações. Entre suas características, podem-se destacar: acionamento, sensoriamento, controle, comparação e programas. Com funções bastante específicas, essas propriedades da automação compõem o funcionamento das infraestruturas contemporâneas.

Desde processos de soldagem e pintura até o agrupamento de produtos, a automação envolve não apenas a robotização, como também transmissores de pressão, temperatura e outros componentes necessários para a existência e normalidade da produção. A partir da coleta e da conversão de dados, da comunicação entre o chão de fábrica e os sistemas de controle e o monitoramento de tais processos, criam-se as condições para a própria segurança cibernética da indústria e, consequentemente, da sociedade. Afinal, a automação está presente na linha de produção de diversos setores produtivos.

1.2 SISTEMA DE CONTROLE INDUSTRIAL

O *Industrial Control System* (ICS), ou, em tradução livre, Sistema de Controle Industrial, é responsável por uma série de processos, entre eles a eficiência e normalidade da produção de uma empresa (YADAV; PAUL, 2020, p. 01). Os ICS estão presentes em usinas de energia, companhias de saneamento básico, entre vários outros setores. Um Sistema de Controle Industrial é estruturado em quatro etapas: a aquisição de dados, a conversão de dados, a comunicação e o monitoramento, e controle. A Figura 2 mostra a visão geral do fluxo de um ICS, desde a coleta de dados na planta até a chegada deles na esfera de monitoramento e controle.

A aquisição dos dados de equipamentos e das máquinas é feita por dispositivos presentes no que se costuma chamar de chão de fábrica, ou, mais especificamente, no Nível 0 da pirâmide de automação. Atualmente, existem instrumentos desse tipo para medir praticamente qualquer parâmetro físico imaginável convertido em algum tipo de grandeza.

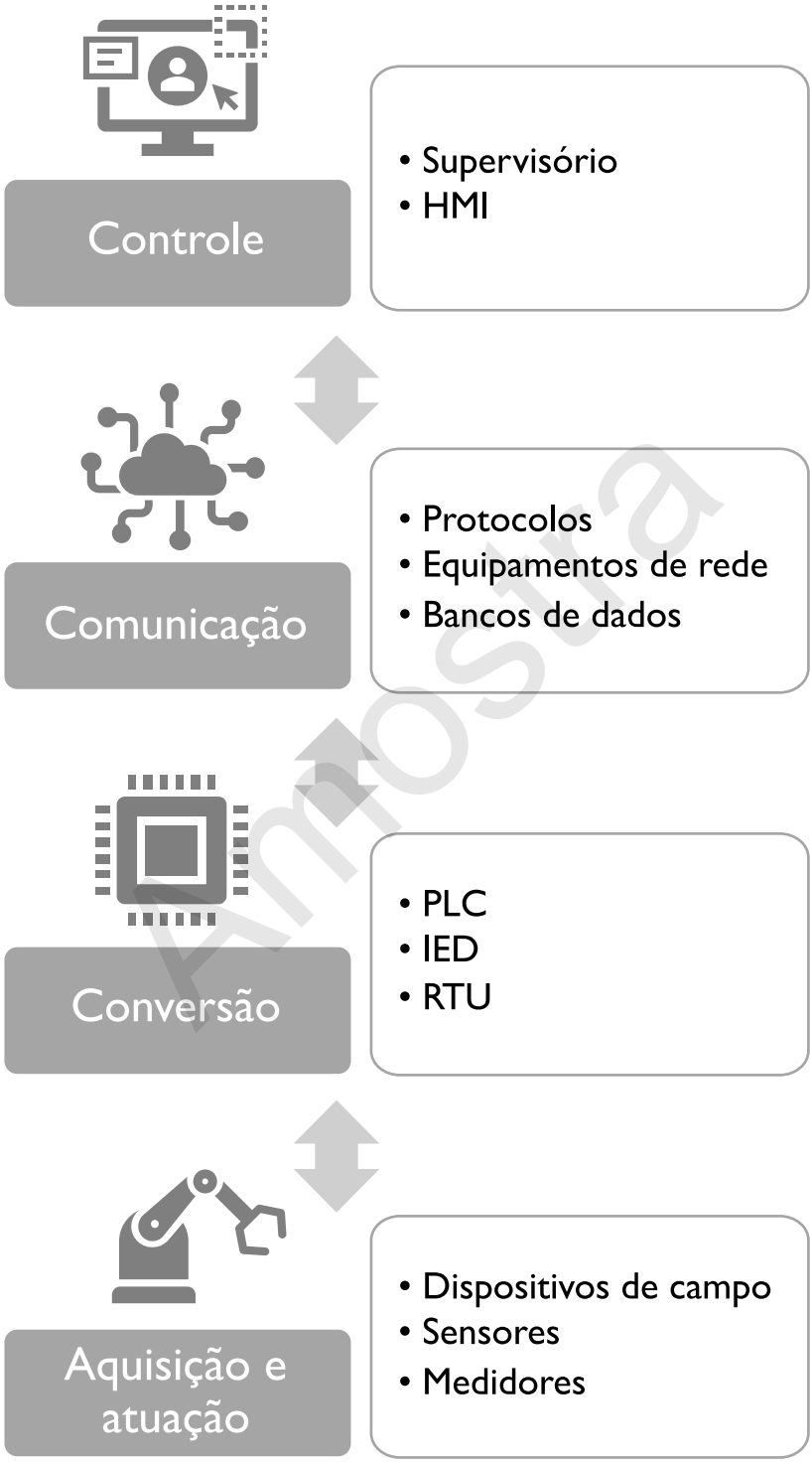

Figura 2 — Visão geral do funcionamento de um Sistema de Controle Industrial

As informações provenientes dos equipamentos de chão de fábrica precisam ser convertidas para que os demais equipamentos possam compreendê-las e utilizá-las. Por isso, os dados adquiridos passam pela etapa de conversão. Apesar de a medição ser feita geralmente já no formato digital, tais dados são, muitas vezes, coletados em formato analógico e enviados aos conversores. Quando os dados são, no entanto, coletados já digitalmente, apenas se utiliza esse formato.

Em seguida, os conversores recebem e transformam esses dados. Eles são conectados por meio de cabos entre os equipamentos de chão de fábrica e os sistemas industriais, transformando os sinais analógicos em sinais digitais e enviando seus bits e bytes para trafegar nas redes de automação. Devido à sua flexibilidade e boa capacidade de programação, são frequentemente utilizados em Sistemas de Controle Industriais.

Para as informações serem transmitidas às redes, usam-se protocolos não usuais chamados de protocolos industriais. No início da automação, as empresas fabricantes como Siemens, ABB, Schneider, Rockwell, Yokogawa, entre outras, desenvolveram seus sistemas utilizando plataformas de desenvolvimento e protocolos de comunicação próprios, e somente essas empresas faziam a manutenção dos sistemas, ficando vedada qualquer alteração ao cliente final, sob o risco da perda da garantia do sistema e prejuízos financeiros subsequentes com uma nova certificação (GARCÍA *et al.*, 2018, p. 03–04).

Pode-se, aqui, fazer uma analogia com a compra de um carro. Ao ir a uma concessionária e adquirir um automóvel, o consumidor recebe as chaves e pode ir embora dirigindo seu novo veículo. Eles podem se locomover para onde quiserem. Mas, se esse carro quebrar, o usuário deverá retorná-lo à concessionária para consertá-lo e não perder sua garantia de fábrica.

Hoje em dia, a maioria das comunicações de redes é realizada por meio do protocolo TCP/IP (GARCÍA *et al.*, 2018, p. 161). Com o passar do tempo, os protocolos industriais foram encapsulados no TCP/IP para que pudessem estabelecer uma comunicação com os equipamentos de diversos fabricantes. Se, por um lado, isso facilitou a troca de informações, por outro, tornou as redes mais vulneráveis.

A partir dos protocolos de comunicação, os dados chegam aos sistemas de monitoramento e controle, que se dividem em dois tipos básicos. O primeiro é o controle supervisório, que é basicamente uma interface desenvolvida especificamente para um Sistema de Controle Industrial (ICS) por empresas especializadas e/ou pela equipe interna do cliente. O segundo tipo é a Interface Homem-Máquina

(IHM). Nesse sistema de controle, monitores touchscreen são instalados na planta para que os operadores possam controlar os equipamentos diretamente.

Mas qual a diferença entre um supervisório e uma IHM? As IHMs são bastante restritas e não permitem alterações por parte do usuário. Já os controles supervisórios permitem, ao contrário, a realização de ajustes e monitoramentos mais avançados e personalizados. Com um sistema supervisório, pode-se coletar dados de formas diferentes e registrá-los em bancos de dados, entre inúmeras outras vantagens. Por meio dele, tem-se um conjunto de controle mais maleável e sofisticado para a automação industrial.

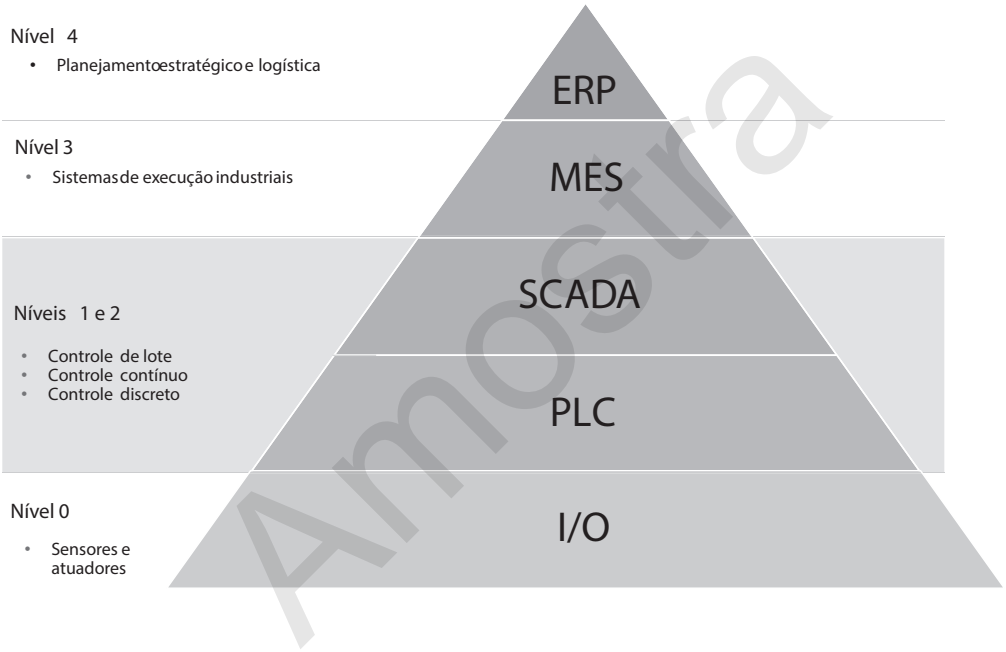

Figura 3 — Pirâmide de automação, Modelo Purdue

Os sistemas de controle obedecem à pirâmide de automação (Figura 3). De forma mais técnica, esse é o Modelo Purdue descrito pela norma ISA-95.

Nele, existem cinco camadas enumeradas de baixo para cima (0, 1, 2, 3 e 4). A primeira camada (I/O) engloba os sensores, medidores e atuadores. A segunda se refere aos autômatos programáveis (PLC), e a terceira, aos sistemas SCADA. Em seguida, está a quarta camada (*Manufacturing Execution Systems*, conhecida pela sigla MES). Ela estabelece a interface entre o chão de fábrica e os sistemas de controle de dispositivos. Por fim, a quinta camada (*Enterprise Resource Planning*, conhecida pela sigla ERP) integra diversos sistemas para planejamento estratégico e logística da organização (GROOVER, 2015, p. 118).