

Thiago Branquinho | Marcelo Branquinho

SEGURANÇA CIBER NÉTICA INDUSTRIAL

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

Segurança Cibernética Industrial

Copyright © 2021 da Starlin Alta Editora e Consultoria Eireli.
ISBN: 978-65-5520-466-7

Todos os direitos estão reservados e protegidos por Lei. Nenhuma parte deste livro, sem autorização prévia por escrito da editora, poderá ser reproduzida ou transmitida. A violação dos Direitos Autorais é crime estabelecido na Lei nº 9.610/98 e com punição de acordo com o artigo 184 do Código Penal.

A editora não se responsabiliza pelo conteúdo da obra, formulada exclusivamente pelo(s) autor(es).

Marcas Registradas: Todos os termos mencionados e reconhecidos como Marca Registrada e/ou Comercial são de responsabilidade de seus proprietários. A editora informa não estar associada a nenhum produto e/ou fornecedor apresentado no livro.

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.

Accesse 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	
1. Segurança cibernética. 2. Segurança Cibernética Industrial. I. Branquinho, Marcelo. II. Título.	
2021-2778	CDD 001.53 CDU 007

Elaborado por Wagner Rodolfo da Silva - CRB-8/940



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

Gerência Comercial
Daniele Fonseca

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

Produtores Editoriais
Illysbelle Trajano
Larissa Lima
Maria de Lourdes Borges
Paulo Gomes
Thié Alves
Thales Silva

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

Diretor Editorial
Anderson Vieira

Coordenação Financeira
Solange Souza

Equipe Comercial
Adriana Baricelli
Daiana Costa
Kaïque Luiz
Victor Hugo Moraes

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:



alabr
ASSOCIAÇÃO BRASILEIRA DE
DIREITOS REPROGRÁFICOS

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.

Amostra

LISTA DE FIGURAS

A TI SAFE e sua metodologia

FIGURA 1 – Etapas da metodologia <i>ICS.SecurityFramework</i> [®]	35
---	----

MÓDULO 1

CAPÍTULO 1

FIGURA 2 – Visão geral do funcionamento de um Sistema de Controle Industrial	46
---	----

FIGURA 3 – Pirâmide de automação, Modelo <i>Purdue</i>	48
---	----

CAPÍTULO 2

FIGURA 4 – Interdependência das infraestruturas críticas	58
---	----

FIGURA 5 – Relatório Global de Riscos de 2020 (<i>World Economic Forum</i>)	60
--	----

FIGURA 6 – Sofisticação das ferramentas de ataque ao longo dos anos	62
--	----

FIGURA 7 – Crimes cibernéticos são um negócio bilionário	69
---	----

CAPÍTULO 3

FIGURA 8 – Representação gráfica da Web	72
--	----

FIGURA 9 – Anonimato de dados que trafegam na rede TOR	74
---	----

FIGURA 10 – Transações comerciais na Dark Web	75
--	----

CAPÍTULO 4

FIGURA 11 – Arquitetura básica SCADA	81
---	----

FIGURA 12 – Integração das redes de T.I. e T.O.	82
--	----

FIGURA 13 – Convergência entre as redes de T.I. e T.O. ao longo do tempo	83
---	----

FIGURA 14 – Vetores de ataque em uma rede industrial	84, 85
---	--------

FIGURA 15 – Resultado de busca por “PLC” no site <i>Shodan</i>	86
---	----

CAPÍTULO 5

FIGURA 16 – Tela de abertura do TI Safe <i>Incident DB</i>	92
FIGURA 17 – Tela com pedido de resgate do malware WannaCry	98
FIGURA 18 – Cenário de ataques ocorridos durante a pandemia	100
FIGURA 19 – Aumento dos ataques durante a pandemia	101

MÓDULO 2**CAPÍTULO 1**

FIGURA 20 – Impactos derivados de incidentes	113
FIGURA 21 – Composição do risco	114
FIGURA 22 – Níveis de risco a partir do impacto e da probabilidade	116
FIGURA 23 – Cenário de riscos	119
FIGURA 24 – Classificação de sistemas de controle segundo o modelo ANSSI	122
FIGURA 25 – Fluxograma para a classificação de riscos	123
FIGURA 26 – Escala de classificação entre impactos e probabilidades	124

CAPÍTULO 2

FIGURA 27 – Análise de riscos na metodologia <i>ICS.SecurityFramework</i> [®]	127
FIGURA 28 – Domínios da metodologia <i>ICS.SecurityFramework</i> [®]	130
FIGURA 29 – Espelhamentos de rede para análise dinâmica	132

CAPÍTULO 3

FIGURA 30 – PSCI na metodologia <i>ICS.SecurityFramework</i> [®]	139
--	-----

MÓDULO 3**CAPÍTULO 1**

FIGURA 31 – Educação e conscientização na <i>ICS.SecurityFramework</i> [®]	148
FIGURA 32 – Tríade de educação e conscientização	149
FIGURA 33 – Etapas do planejamento de educação e conscientização	150
FIGURA 34 – Formação em Segurança de Automação Industrial	152
FIGURA 35 – Tabuleiro do jogo Ciber Suspeito	160

CAPÍTULO 2

FIGURA 36 – Governança na metodologia <i>ICS.SecurityFramework</i> [®]	163
FIGURA 37 – Modelo CSMS da norma ISA/IEC 62443	169
FIGURA 38 – Papéis e responsabilidades estabelecidos pela LGPD	175
FIGURA 39 – Formato diversificado de uma política de segurança	179
FIGURA 40 – Arcabouço das políticas de segurança	180
FIGURA 41 – Detalhes da governança em uma política de segurança	180
FIGURA 42 – Controles em uma política de segurança	182
FIGURA 43 – Linha do tempo de um plano de continuidade	190
FIGURA 44 – Etapas de execução do PCN	191
FIGURA 45 – Custo-benefício do plano de continuidade	193

CAPÍTULO 3

FIGURA 46 – Segurança de borda na <i>ICS.SecurityFramework</i> [®]	199
FIGURA 47 – Ataque por <i>pivot</i> a uma rede industrial	202
FIGURA 48 – Firewall separando as redes de T.I. e T.O.	204
FIGURA 49 – Atuação de uma DMZ	205
FIGURA 50 – Firewall com DMZ entre as redes de T.I. e T.O.	206
FIGURA 51 – Par de firewalls com DMZ entre as redes de T.I. e T.O.	208
FIGURA 52 – Visão geral de uma VPN	213
FIGURA 53 – Bloqueador de sinal Wi-Fi (<i>jammer</i>)	218
FIGURA 54 – Delimitação do sinal Wi-Fi dentro do perímetro da empresa	220

CAPÍTULO 4

FIGURA 55 – Proteção da rede industrial na <i>ICS.SecurityFramework</i> [®]	225
FIGURA 56 – A Muralha da China concretiza o conceito de Bastion Model	226
FIGURA 57 – Conduítes: os caminhos entre as zonas	228
FIGURA 58 – Firewalls utilizados para segregar diferentes zonas	229
FIGURA 59 – Topologia de uma rede de automação	230
FIGURA 60 – Especificação das zonas de segurança	231
FIGURA 61 – Adição dos conduítes entre as zonas de segurança	232
FIGURA 62 – Proteção das zonas de segurança	233
FIGURA 63 – NGFW protegendo o conduíte (norma ISA/IEC 62443)	235

FIGURA 64	– Firewall industrial protegendo uma rede de energia	238
FIGURA 65	– Ataque baseado no princípio da poça d'água	239
FIGURA 66	– Desvio de comportamento registrado por um IDS industrial	242
FIGURA 67	– Arquitetura operacional de uma solução de IDS industrial	244
CAPÍTULO 5		
FIGURA 68	– Controle de malware na metodologia <i>ICS.SecurityFramework</i> [®]	247
FIGURA 69	– Primeiros três passos de um ataque por malware	255
FIGURA 70	– Últimos três passos de um ataque por malware	256
FIGURA 71	– Vulnerabilidades exploradas em relação ao tempo do patch	257
FIGURA 72	– Funcionamento de antimalware industrial de próxima geração	261
FIGURA 73	– Verificação de malware na nuvem	262
FIGURA 74	– Aprendizado de soluções de segurança	262
CAPÍTULO 6		
FIGURA 75	– Segurança de dados na metodologia <i>ICS.SecurityFramework</i> [®]	265
FIGURA 76	– Estratégia de backup	267
FIGURA 77	– Tempo necessário para adivinhar uma senha por software	271
FIGURA 78	– <i>Sniffer Wireshark filtrando mensagens GOOSE (IEC 61850)</i>	272
FIGURA 79	– Teste de humanidade: captcha	277
FIGURA 80	– Teste por fotografia	277
FIGURA 81	– Autenticação por desafio–resposta	278
FIGURA 82	– Tokens USB e smart card	280
FIGURA 83	– Token OTP	280
FIGURA 84	– Autenticação por OTP no smartphone	281
FIGURA 85	– Autenticação por leitura de código QR	282
FIGURA 86	– Funcionamento de um sistema de autenticação por biometria	283
FIGURA 87	– Detalhes da impressão digital	284
FIGURA 88	– Matriz bidimensional dos pontos identificáveis em uma digital	285
FIGURA 89	– Autenticação por reconhecimento da face	286

MÓDULO 4

CAPÍTULO 1

- FIGURA 90** – IIoT (*Industrial Internet of Things*) 303
- FIGURA 91** – Ciclo de um sistema ciberfísico 304
- FIGURA 92** – Arquitetura da Indústria 4.0 306
- FIGURA 93** – Novos riscos trazidos com a Indústria 4.0 307

CAPÍTULO 2

- FIGURA 94** – Ataque na comunicação entre o programador e o robô 313

CAPÍTULO 3

- FIGURA 95** – Tempo de transmissão e ataque em GOOSE 324
- FIGURA 96** – Anatomia do ataque Black Energy 325
- FIGURA 97** – Potenciais contramedidas contra o ataque Black Energy 326

CAPÍTULO 4

- FIGURA 98** – A evolução das redes de comunicação ao longo do tempo 332
- FIGURA 99** – Conexão segura entre chão de fábrica e nuvem 337

CAPÍTULO 5

- FIGURA 100** – Principais vetores de ataques às cidades inteligentes 341
- FIGURA 101** – Desafios de segurança cibernética para as cidades inteligentes 345

MÓDULO 5

CAPÍTULO 1

- FIGURA 102** – O Monitoramento na *ICS.SecurityFramework*[®] 353
- FIGURA 103** – Arquitetura operacional de um SIEM 356
- FIGURA 104** – Interface de operação de firewall de próxima geração 360
- FIGURA 105** – NGFW e IDS industrial atuando em conjunto 361
- FIGURA 106** – Relatório gerencial fornecido por um SOC industrial 363
- FIGURA 107** – O Ciclo do *threat hunting* 364
- FIGURA 108** – Passos realizados durante a resposta a um incidente 365
- FIGURA 109** – Arquitetura simplificada de um *honeypot* industrial 368
- FIGURA 110** – Pilares de operação do ICS–SOC 370

FIGURA 111	– Processo de início das atividades do ICS–SOC	371
CAPÍTULO 2		
FIGURA 112	– Tela com pedido de resgate em ataque por <i>ransomware</i>	383

Amostra

LISTA DE TABELAS

MÓDULO 2

CAPÍTULO 2

TABELA 1 – Normas utilizadas em análises de riscos de plantas industriais	128, 129
--	----------

MÓDULO 3

CAPÍTULO 2

TABELA 2 – Diferenças entre requisitos de performance de T.O. e T.I.	166
TABELA 3 – Diferenças entre os requisitos de confiabilidade de T.O. e T.I.	166
TABELA 4 – Diferenças entre os objetivos de gerência de riscos de T.O. e T.I.	166
TABELA 5 – Diferenças entre as práticas de governança de T.O. e T.I.	167
TABELA 6 – Sugestão de cronograma para implantação da LGPD	177

MÓDULO 5

CAPÍTULO 2

TABELA 7 – Exemplos de correlação entre crimes do Código Penal e ataques	374
---	-----

Amostra

SUMÁRIO

Introdução ao livro	29
Autores	31
Autores Principais	31
Autores Colaboradores	32
Revisor	33
A TI SAFE e sua metodologia	35
Objetivos do livro	37
Conecte-se!	39

MÓDULO 1

AUTOMAÇÃO INDUSTRIAL E TERRORISMO CIBERNÉTICO

CAPÍTULO 1

Automação Industrial	43
1.0 Introdução	43
1.1 O que é automação industrial?	44
1.2 Sistema de controle industrial	45

1.3 Nível 0: aquisição de dados	49
1.4 Nível 1: autômatos programáveis	49
1.5 Nível 2: supervisão e controle	51
1.6 Principais ferramentas de desenvolvimento	52

CAPÍTULO 2

Infraestruturas Críticas e Terrorismo Cibernético 55

2.0 Introdução	55
2.1 O que são infraestruturas críticas?	56
2.2 A evolução da guerra	58
2.3 O novo panorama do hacking	61
2.4 Tipos de hackers	63
2.5 Perfis dos atacantes cibernéticos.....	64
2.6 O fator humano	66
2.7 Crimes cibernéticos	68

CAPÍTULO 3

A Dark Web 71

3.0 Introdução	71
3.1 The Onion Router (TOR)	73
3.2 O mercado ilícito da dark web	75

CAPÍTULO 4

Desafios em Segurança Cibernética Industrial 79

4.0 Introdução	79
4.1 As ilhas de automação	80
4.2 Evolução dos sistemas de controle industriais	81

4.3 Convergência entre as redes de T.I. e T.O.	83
4.4 As fraquezas das redes integradas	84
4.5 Dispositivos industriais expostos na web	85
4.6 Desafios de segurança das redes industriais	87

CAPÍTULO 5

Histórico de Ataques e Armas Cibernéticas	91
5.0 Introdução	91
5.1 Bancos de dados de incidentes	91
5.2 Histórico de incidentes cibernéticos	92
EXERCÍCIOS DE REVISÃO.....	105

MÓDULO 2

ANÁLISE DE RISCOS E PLANEJAMENTO

CAPÍTULO 1

Introdução ao Risco	111
1.0 Introdução	111
1.1 Causas e consequências	112
1.2 Conceitos	113
1.3 Avaliação de riscos	115
1.4 Cenário de riscos	117
1.5 Classificação de redes industriais	121

CAPÍTULO 2

Análise de Riscos **127**

2.0 Introdução	127
2.1 Análise estática	128
2.2 Análise dinâmica	132
2.3 Elaboração do relatório da análise de riscos	134

CAPÍTULO 3

Planejamento de Segurança Cibernética Industrial **137**

3.0 Introdução	137
3.1 Elaboração do plano	138
EXERCÍCIOS DE REVISÃO.....	141

MÓDULO 3

CONTROLES DE SEGURANÇA CIBERNÉTICA INDUSTRIAL

CAPÍTULO 1

Educação e Conscientização **147**

1.0 Introdução	147
1.1 Organização do plano de treinamento da automação	148
1.2 Ferramentas para educação e conscientização	150
1.3 Treinamentos e certificações	152
1.4 Filmes, documentários e séries	156
1.5 Jogos educacionais	159

CAPÍTULO 2

Governança e Monitoramento 163

2.0 Introdução	163
2.1 Segurança para redes de T.I. e T.O.	164
2.2 Padrões, normas e leis	168
2.3 Política de segurança de automação	177
2.4 Gestão de continuidade de negócios	186

CAPÍTULO 3

Segurança de Borda 199

3.0 Introdução	199
3.1 O conceito de firewall	200
3.2 Arquiteturas de segurança de borda	203
3.3 Princípio do menor privilégio	208
3.4 Firewalls ultrapassados	209
3.5 Firewall de próxima geração (NGFW)	210
3.6 VPN	213
3.7 Gateway de segurança unidirecional	214
3.8 Segurança de wi-fi industrial	216

CAPÍTULO 4

Proteção da Rede Industrial 225

4.0 Introdução	225
4.1 Modelo de zonas e conduítes	228
4.2 Segmentação da rede industrial	235
4.3 VLAN	236
4.4 Firewall industrial de próxima geração	236

4.5 Arquitetura zero trust	239
4.6 IDS industrial	241

CAPÍTULO 5

Controle de Malware **247**

5.0 Introdução	247
5.1 Malware, a principal arma dos hackers	249
5.2 Desenvolvimento de armas cibernéticas	253
5.3 Dinâmica de um malware	255
5.4 A ineficácia dos patches em redes de automação	256
5.5 O uso de antivírus em redes industriais	258
5.6 <i>Whitelisting</i>	259
5.7 Antimalware de próxima geração (EDR)	260

CAPÍTULO 6

Segurança de Dados **265**

6.0 Introdução	265
6.1 Backup	266
6.2 Ameaças à segurança de dados	269
6.3 Roubo de identidades	270
6.4 Autenticação em sistemas	274
6.5 Mecanismos de autenticação	276
6.6 Impressão digital (<i>Minutia</i>)	284
6.7 Quebrando a segurança da impressão digital	285
6.8 Autenticação biométrica em indústrias	286
6.9 Riscos do acesso remoto industrial	287
6.10 Garantindo a segurança no acesso remoto	288
EXERCÍCIOS DE REVISÃO.....	291

MÓDULO 4

SEGURANÇA CIBERNÉTICA PARA A TRANSFORMAÇÃO DIGITAL

CAPÍTULO 1

A Digitalização das Infraestruturas Críticas 301

1.0 Introdução	301
1.1 IoT – internet das coisas	302
1.2 IIoT – internet das coisas industriais	302
1.3 Sistemas ciberfísicos	304
1.4 Indústria 4.0 – Nova realidade, novos riscos	305

CAPÍTULO 2

IIoT – O IoT na Manufatura 309

2.0 Introdução	309
2.1 Robôs industriais e colaborativos	310
2.2 Uso de robôs na manufatura	310
2.3 Vulnerabilidades em IIoT	311
2.4 Ataques à cadeia de suprimentos das indústrias	314
2.5 Ataques a robôs usados em áreas sensíveis	315
2.6 Segurança cibernética na robótica	316

CAPÍTULO 3

IoE – O IoT em Energia 319

3.0 Introdução	319
3.1 IoE – IoT em redes de energia	320
3.2 Ataques cibernéticos em IoE	323

CAPÍTULO 4

Segurança em Nuvem 329

4.0 Introdução	329
4.1 Big data e <i>analytics</i>	330
4.2 Ameaças às redes de telecom e 5G industrial	331
4.3 Ameaças aos serviços de nuvem	334
4.4 Conexão segura entre a rede industrial e a nuvem	336

CAPÍTULO 5

Desafios de Segurança Cibernética para Cidades Inteligentes 339

5.0 Introdução	339
5.1 Desafios de segurança das cidades inteligentes	340
EXERCÍCIOS DE REVISÃO.....	347

MÓDULO 5**MONITORAMENTO CONTÍNUO
E FORENSE INDUSTRIAL**

CAPÍTULO 1

Monitoramento Contínuo 353

1.0 Introdução	353
1.1 Projeto de um SOC industrial	358
1.2 Mapas de ameaça em tempo real	367
1.3 Honeypot industrial	368
1.4 Estudo de caso de SOC industrial	369

CAPÍTULO 2

Forense Industrial	373
2.0 Introdução	373
2.1 A perícia forense industrial	375
2.2 Trilhas de auditoria para forense	378
2.3 Estudo de caso	380
EXERCÍCIOS DE REVISÃO	387

RESPOSTAS DOS EXERCÍCIOS	391
GLOSSÁRIO	393
REFERÊNCIAS BIBLIOGRÁFICAS	403
ÍNDICE	409

Amostra



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.

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, regrida, 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, conseqüentemente, 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.

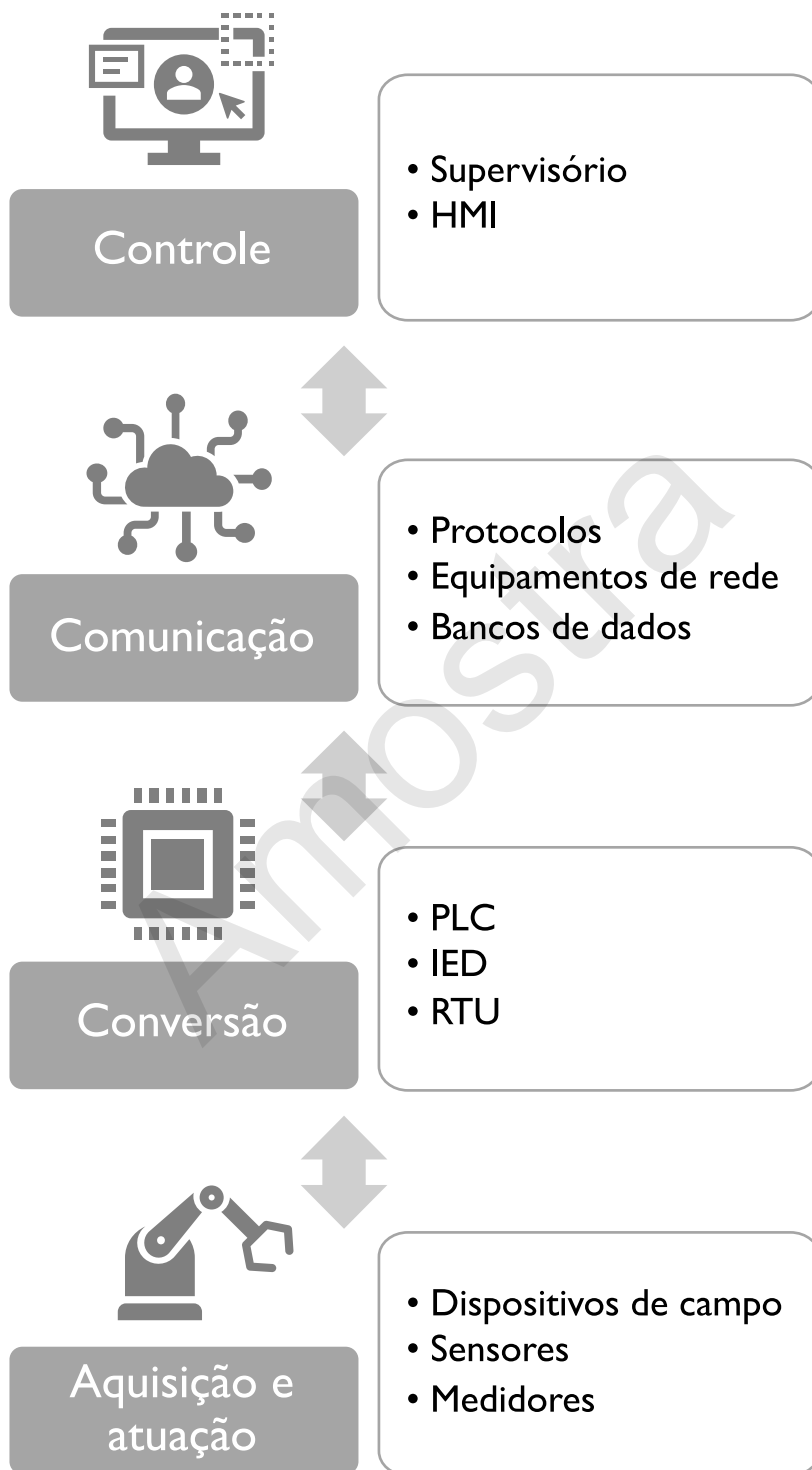


FIGURA 2 — Visão geral do funcionamento de um Sistema de Controle Industrial

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 supervisão, 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 supervisor 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.

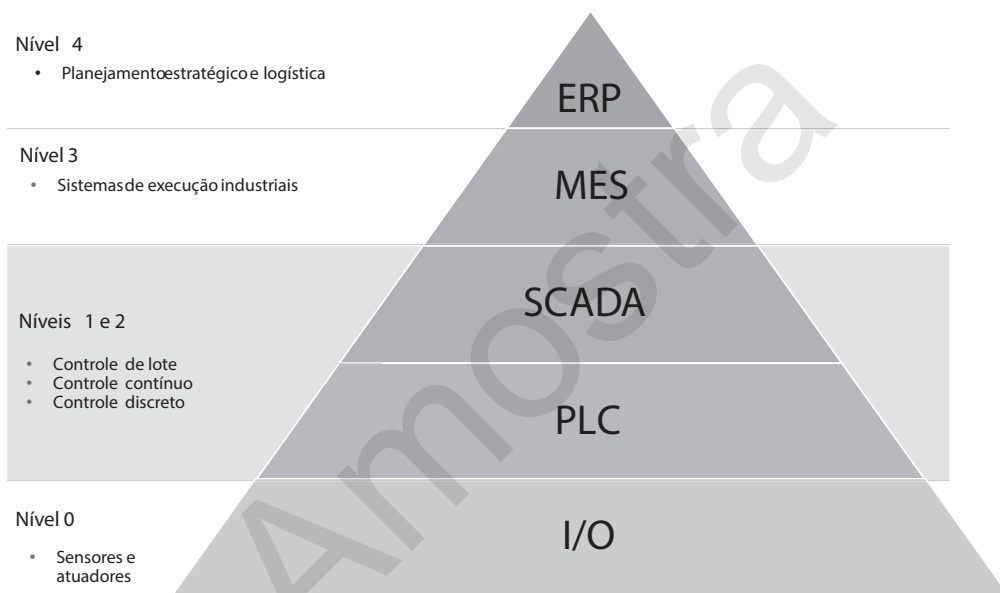


FIGURA 3 — Pirâmide de automação, Modelo Purdue

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 logístico da organização (GROOVER, 2015, p. 118).