

Inhaltsverzeichnis

Grußwort	19
(HENNING BANTHIEN / Plattform Industrie 4.0)	

Vorwort des Herausgebers	21
(THOMAS SCHULZ)	

Resonanzen der Verbände

I Zentrale Enabler einer erfolgreichen digitalen Transformation	29
(HANS-WILHELM DÜNN / Cyber-Sicherheitsrat Deutschland e.V.)	
II Modulares Bausteinsystem der Security	31
(STEFFEN ZIMMERMANN / VDMA Verband Deutscher Maschinen- und Anlagenbau e.V.)	
III Etablierung einer Sicherheitskultur	33
(LUKAS LINKE / ZVEI Zentralverband Elektrotechnik- und Elektronikindustrie e.V.)	
IV Wirtschaftsschutz in der digitalen Welt	35
(LUKAS KLINGHOLZ / Bitkom Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.)	

A Cybersicherheit als Voraussetzung für erfolgreiche Digitalisierung

A.1 Bedrohungen durch die Digitalisierung der Industrie	39
(JENS MEHRFELD)	
A.1.1 Einleitung	39
A.1.2 Cybersicherheit in bestehenden Industrieanlagen	40
A.1.2.1 Vorgehen der Angreifer bei gezielten Angriffen	40
A.1.2.2 Auswirkungen von Angriffen auf Produktionssysteme	42
A.1.2.2.1 Steuerungskontrolle	42
A.1.2.2.2 Anzeige	43
A.1.2.2.3 Safety	43
A.1.2.2.4 Daten	43
A.1.3 Veränderungen durch Industrie 4.0	44
A.1.3.1 Wertschöpfungsnetzwerke	45
A.1.3.1.1 Verbindungen zu Kunden	46
A.1.3.1.2 Cloud-Services	47
A.1.3.1.3 Fernzugriffe	48
A.1.3.1.4 Auftragsfertigung	49

A.1.3.1.5 Benutzer- und Berechtigungsverwaltung	49
A.1.3.2 Blick in Unternehmen	50
A.1.3.2.1 Schwachstellen	51
A.1.3.2.2 Dynamische Konfiguration	52
A.1.3.2.3 Entwicklung	53
A.1.3.2.4 Updates und Änderung der Funktionen	54
A.2 Cybersicherheit als Grundlage für die Digitalisierung der Industrie	57
(HELMUT LEOPOLD; PAUL TROMPISCH)	
A.2.1 Cybersicherheit – ein inhärenter Bestandteil der Digitalisierung	57
A.2.1.1 Umfassende Digitalisierung und Vernetzung	57
A.2.1.2 Veränderung der Geschäftsmodelle und Disruptive Effekte	57
A.2.2 Bedrohungslage	58
A.2.2.1 Grundlegende Technologieabhängigkeit	58
A.2.2.2 Cyberspace – der neue Aktionsraum der internationalen Kriminalität	58
A.2.2.3 Vielfältige Cyber-Security-Angriffsmethoden	59
A.2.2.4 Neue Trends: Cybercrime as a Service	60
A.2.3 Herausforderungen für Unternehmen	60
A.2.3.1 IT-Systeme sind grundsätzlich fehleranfällig	60
A.2.3.2 Die steigende Komplexität verstärkt die Verletzlichkeit unserer IT-Systeme	61
A.2.3.2.1 Externe, aber auch interne Gefahren	61
A.2.3.2.2 Legacy-Systeme	62
A.2.3.3 Digitalisierung und Cybersicherheit brauchen eine neue Kultur des Miteinanders	63
A.2.3.4 Standardisierung	64
A.2.3.5 Cybersicherheit muss neu verstanden werden	65
A.2.4 Herausforderung für die Wirtschaft	65
A.2.4.1 Fachkräftemangel	65
A.2.4.2 Breites Problembewusstsein und internationale Governance fehlen	67
A.2.4.3 Europäische Markttreiber mit Vorbildwirkung	67
A.2.5 Cybersicherheit verlangt neue Schutz- und Verteidigungsstrategien und neue Formen der Kooperation	68

B Regelkonformität mit Normen und Richtlinien

B.1 Normenreihe ISO/IEC 27 000: IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme	73
(Prof. Dr. OLIVER WEISSMANN)	
B.1.1 Hintergrund	73
B.1.2 Gliederung, Inhalte und Abschnitte	76
B.1.2.1 Kontext der Organisation	76
B.1.2.2 Leadership / Organisationsleitung	77
B.1.2.3 Planung	78
B.1.2.4 Unterstützung	79
B.1.2.5 Betrieb	80

B.1.2.6 Performance-Bewertung	80
B.1.2.7 Kontinuierliche Verbesserung	81
B.1.3 Möglicher Anwendungsbereich und Kontext	81
B.1.4 Umsetzungen mit hohem Anwendernutzen	83
B.2 Normenreihe IEC 62 443: Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme	87
(DAVID FUHR)	
B.2.1 Hintergrund	87
B.2.2 Aufbau	87
B.2.2.1 Anwendungsbereiche	89
B.2.2.1.1 Betreiber	89
B.2.2.1.2 Dienstleister	89
B.2.2.1.3 Integrator	89
B.2.2.1.4 Hersteller	89
B.2.2.1.5 Zertifizierungen	90
B.2.2.2 Umsetzungen	90
B.2.2.2.1 Grundkonzepte	90
B.2.2.2.2 IEC 62 443-2-1	91
B.2.2.2.3 IEC 62 443-2-4	92
B.2.2.2.4 IEC 62 443-3-3	92
B.2.2.2.5 IEC 62 443-4-1 und IEC 62 443-4-2	93
B.2.2.3 Der Weg durch die IEC 62 443	93
B.3 Richtlinienreihe VDI/VDE 2182: Informationssicherheit in der industriellen Automatisierung	97
(HEIKO ADAMCZYK; MICHAEL KRAMMEL)	
B.3.1 Hintergrund und Anwendungsbereich	97
B.3.2 Aufbau und inhaltliche Gliederung	98
B.3.3 Umsetzungen mit hohem Anwendernutzen	100
B.4 NAMUR-Arbeitsblatt NA 163: IT-Risikobeurteilung von PLT-Sicherheitseinrichtungen	109
(THOMAS LEIFELD; ERWIN KRUSCHITZ)	
B.4.1 Einführung	109
B.4.2 Allgemeine Beschreibung der Vorgehensweise	110
B.4.3 Identifikation des betrachteten Systems	111
B.4.4 Definition der Schutzziele	111
B.4.5 Verfahren zur detaillierten Risikoanalyse	112
B.4.6 Betrachtung möglicher Auswirkungen	113
B.4.7 Einteilung des betrachteten Systems in Zonen und Übergänge	113
B.4.8 Detaillierte Risikobetrachtung	114
B.4.9 Anwendung des Verfahrens	114

C Fabrik als Anwendungsdomäne / Industrial Control Systems

C.1 Einführung und Grundlagen Cybersicherheit für Industrielle Steuerungssysteme (ICS)	119
(Dr.-Ing. CHRISTIAN HAAS; THOMAS SCHULZ)	
C.1.1 Die Fabrik als Anwendungsdomäne	119
C.1.1.1 Der Unterschied zwischen Information Technology (IT) und Operational Technology (OT)	119
C.1.1.2 Bedrohungen der Digitalisierung in der Industrie	121
C.1.1.3 Grundbegriffe der Cybersicherheit in der Industrie	123
C.1.2 Systemsicherheit für industrielle Steuerungssysteme	124
C.1.2.1 Sicherheitsmaßnahmen	126
C.1.2.1.1 Relevante Standards	126
C.1.2.1.2 Organisatorische Maßnahmen	127
C.1.2.1.3 Technische Maßnahmen	128
C.1.2.2 Grundkonzepte technischer Maßnahmen	129
C.1.2.2.1 Trennung von Unternehmensnetz und Produktion (Demilitarized Zone – DMZ)	130
C.1.2.2.2 Segmentierung in Anlagen-Subnetze	130
C.1.2.2.3 Netzwerkzugangskontrolle (Network Access Control – NAC)	131
C.1.2.2.4 Überwachungstechniken (Deep Packet Inspection – DPI) ..	132
C.2 Grundlegende Sicherheitsbedrohungen und Lösungsmöglichkeiten im ICS-Umfeld: Probleme – Lösung – Beispiele	135
(Dr. rer. nat. KEMAL AKMAN; PETER REHÄUBER)	
C.2.1 Einleitung	135
C.2.2 Schwachstellen und veränderte Bedrohungslage	135
C.2.2.1 Angriffe auf industrielle Kontrollsysteme	136
C.2.2.2 Advanced Persistent Threats	139
C.2.3 Standards und Richtlinien als Grundlage für erste Orientierungen	140
C.2.4 Strategien zum Schutz	141
C.2.4.1 Netzwerksicherheit	141
C.2.4.2 Netzwerkarchitektur	141
C.2.4.3 Übersicht einiger relevanter Netzwerkprotokolle unter Sicherheitsaspekten	144
C.2.4.3.1 OLEPC, Modbus, ICCP, DNP3	144
C.2.4.3.2 Spezialisierte Feldbusprotokolle	147
C.2.4.4 Angriffserkennung und Anomalieerkennung	148
C.2.4.5 Sicherheit der Maschinen und Anlagen	149
C.2.4.5.1 SPS / PLC	149
C.2.4.5.2 HMI	149
C.2.4.5.3 IEDs	149
C.2.4.5.4 RTUs	150
C.2.4.5.5 Anzeigesysteme	150
C.2.4.5.6 Weitere Komponenten	150
C.2.5 Bedrohungsszenarien der Maschinen und Anlagen	151

C.2.6	Sicherheitsmaßnahmen für Maschinen und Anlagen	151
C.2.7	Sicherheit im und durch den Prozess	152
C.2.7.1	Security by Design	152
C.2.7.2	Erkennung und Management von Schwachstellen	153
C.2.7.3	Patch Management	154
C.2.7.4	Konfigurationsmanagement	154
C.2.7.5	Netzwerksegmentierung	154
C.2.7.6	Detect	155
C.2.7.7	Respond & Recover	156
C.2.7.8	Lifecycle Management	156

C.3 Monitoring der Kommunikation im ICS – Transparenz und Anomalieerkennung

(Dr. rer. pol. FRANK STUMMER)		
C.3.1	Einleitung: Einbindung des Monitoring in die Gesamtsicherheitsstrategie	159
C.3.2	Spezifika im industriellen Umfeld	160
C.3.2.1	Aktion vs. Rückwirkungsfreiheit und Safety	161
C.3.2.2	Verallgemeinerungen vs. Domänenbesonderheiten	161
C.3.2.3	Organisatorische Einbindung	162
C.3.3	Typen von Anomalien	163
C.3.3.1	Angriffe	163
C.3.3.2	Fehlkonfigurationen	165
C.3.3.3	Netzwerküberwachung	167
C.3.4	Kommunikationsmonitoring als Datenquelle für SIEM und Co.	168
C.3.4.1	Datentypen und Nutzungsmöglichkeiten	168
C.3.4.2	Normierung und Vollständigkeit	169

C.4 Cyber Security im Lebenszyklus von automatisierten Sicherheitseinrichtungen

(Dr.-Ing. TOBIAS KLEINERT; THOMAS LEIFELD)		
C.4.1	Automatisierte Sicherheitseinrichtungen	171
C.4.1.1	Zweck und Funktion	171
C.4.1.2	Functional Safety Management und SIS-Lebenszyklus	172
C.4.2	Cyberisiko für automatisierte Sicherheitseinrichtungen	173
C.4.2.1	Betrachtungsgegenstand und funktionale Trennung der Automatisierung	173
C.4.2.2	Bedrohung durch Cyberangriffe	175
C.4.2.3	Grundsätzliches zur Cybersicherheit von SIS	176
C.4.3	SIS-Cyber-Security-Management	177
C.4.3.1	Grundkonzept und Kernelemente	177
C.4.3.2	SIS-Cyber-Sicherheitskonzept	178
C.4.3.3	SIS-Cyber-Risikoanalyse	178
C.4.3.4	SIS-Cyber-Risikohandhabung	179
C.4.3.5	SIS-Cyber-Sicherungsmaßnahmen	180
C.4.3.6	Organisation, Auditierung und kontinuierliche Verbesserung	181
C.4.3.7	Einbindung in den SIS-Lebenszyklus	181
C.4.3.8	Praktische Anwendbarkeit der Methoden	182

D Mobile und intelligente Komponenten / Smart Devices

D.1 Cybersicherheit für mobile und intelligente Komponenten – Einführung und Grundlagen	185
(Prof. Dr.-Ing. HANS-JOACHIM HOF)	
D.1.1 Einleitung	185
D.1.2 Cybersicherheit in Industrie-4.0-Anwendungen	185
D.1.3 Allgemeine Bedrohungen der Sicherheitsziele in Industrie-4.0-Anwendungen	189
D.1.4 Spezifische Bedrohungen für mobile und intelligente Komponenten in Industrie-4.0-Anwendungen	192
D.1.4.1 Bedrohungen durch unsichere lokale Schnittstellen	192
D.1.4.2 Bedrohungen durch unsichere Wartungs- und Administrationszugänge	193
D.1.4.3 Bedrohungen durch unsichere Zugangskontrolle	194
D.1.4.4 Bedrohungen durch unsichere Datenspeicherung	195
D.1.4.5 Bedrohungen durch unsichere Netzwerkkommunikation	195
D.1.4.6 Bedrohungen des Device-Managements	196
D.1.5 Sicherheitsmaßnahmen	196
D.1.5.1 Schutz vor Manipulation von Software und Firmware	196
D.1.5.2 Schutz kryptographischen Materials	199
D.1.5.3 Schutz der Kommunikation	200
D.1.5.4 Sichere Identitäten	201
D.2 Cyber Security für Industrie-4.0-Komponenten	207
(MICHAEL JOCHEM / Dr.-Ing. LUTZ JÄNICKE)	
D.2.1 Gesichert in die digitale und vernetzte Produktion einsteigen	207
D.2.2 Kommunikations- und Vertrauensbeziehungen	207
D.2.2.1 Sicherheit im Referenzarchitekturmodell Industrie 4.0 (RAMI 4.0)	208
D.2.2.2 Sicherheit in der Verwaltungsschale der Industrie-4.0-Komponente	210
D.2.3 Sichere Kommunikation als Kernthema	212
D.2.3.1 Kommunikationsbeziehungen	213
D.2.3.2 Kommunikationsstrukturen	214
D.3 Wirksamer Schutz von Smart Devices mit Künstlicher Intelligenz (KI)	219
(MARK HARTMANN)	
D.3.1 Einleitung	219
D.3.2 Verbesserung der Cyberabwehr durch Künstliche Intelligenz	219
D.3.3 Künstliche Intelligenz zum Schutz von Smart Devices	219
D.3.3.1 Künstliche Intelligenz (KI)	220
D.3.3.2 Machine Learning (ML)	221
D.3.3.2.1 Klassifizierung und Supervised Learning	221
D.3.3.2.2 Clustering und Non-supervised Learning	222
D.3.3.3 Deep Learning (DL)	223
D.3.3.4 Ersatz regelbasierter Schutzsysteme durch ML-Modelle	224
D.3.3.5 Erkennen von Anomalien	225

D.3.3.6	Berücksichtigung der gesetzlichen Anforderungen zum Datenschutz beim Einsatz von ML	225
D.3.3.6.1	Einwilligung der betroffenen Person	225
D.3.3.6.2	Zweckbindung	226
D.3.3.6.3	Automatisierte Entscheidung	226
D.3.3.6.4	Verarbeitung von Daten in einem anderen Land	226
D.3.3.6.5	Weitere rechtliche Aspekte	227
D.3.4	Schlussfolgerungen und Ausblick	227
D.3.4.1	Wo gibt es heute schon effektive Lösungen?	227
D.3.4.2	Was ist Stand heute noch nicht vollständig gelöst?	227
D.3.4.3	Wie könnte die zukünftige Entwicklung aussehen?	228

D.4	Eine Analyse von Angriffen auf Smart Devices und der richtige Umgang mit Sicherheitslücken	229
	(SEBASTIAN NEEF)	
D.4.1	Einleitung	229
D.4.2	Praktische Angriffe auf Smart Devices an ausgewählten Beispielen	229
D.4.2.1	Smarte Bluetooth(Tür-)Schlösser	230
D.4.2.1.1	Funktionsweise	230
D.4.2.1.2	Angriffe	231
D.4.2.2	Smarte Glühbirnen	232
D.4.2.2.1	Funktionsweise	233
D.4.2.2.2	Angriffe	233
D.4.2.3	Human Machine Interfaces	236
D.4.2.3.1	Funktionsweise	236
D.4.2.3.2	Angriffe	236
D.4.2.4	Gemeinsamkeiten und Erkenntnisse	238
D.4.3	Der richtige Umgang mit Sicherheitslücken	239
D.4.3.1	Perspektive eines Hackers	239
D.4.3.2	Perspektive eines Herstellers	240

E Plattformen mit gehosteten Anwendungen / Cloud Computing

E.1	Einführung und Grundlagen der Cloud-Sicherheit	245
	(CHRISTIAN A. GORKE; Prof. Dr. rer. nat. FREDERIK ARMKNECHT)	
E.1.1	Cloud Computing	245
E.1.1.1	Vor- und Nachteile	245
E.1.1.2	Technologie	246
E.1.1.3	Servicemodelle	247
E.1.1.4	Cloud-Modelle	248
E.1.2	Interoperabilität und Datenaustausch	249
E.1.2.1	OSI-Modell und TCP/IP-Modell	249
E.1.2.1.1	Das OSI-Modell	250
E.1.2.1.2	Das TCP/IP-Modell	250
E.1.2.2	Datentransport via HTTP	253
E.1.2.3	Schnittstellen und Datendarstellung	254

E.1.2.3.1	Standardisierte Datenformate	254
E.1.2.3.2	Schnittstellen	255
E.1.3	Bedrohungsszenarien	257
E.1.3.1	Die CIA-Sicherheitsziele	258
E.1.3.2	Die wichtigsten Sicherheitsrisiken	258
E.1.3.3	Seitenkanalangriffe	260
E.1.4	Datenschutz und Compliance	261
E.1.4.1	Geschichte und Entwicklung des Datenschutzes	261
E.1.4.2	Der Wert von Privatsphäre und Daten	263
E.1.4.3	Grundprinzipien des Datenschutzes	265
E.1.4.4	Bundesdatenschutzgesetz (BDSG)	265
E.1.4.5	Datenschutz-Grundverordnung (DSGVO)	266
E.1.4.5.1	Praktische Schritte zur DSGVO-Compliance	266
E.1.4.6	Standards für Sicherheit und Datenschutz in der Cloud	267
E.1.4.7	Cloud-Auditierung	268
E.1.5	Sicherheitsmaßnahmen und Implementierungen	270
E.1.5.1	Data in Transit	270
E.1.5.2	Data at Rest	271
E.1.5.3	Implementierungen bei Cloud-Anbietern	272
E.1.5.4	Ausblick: Verfügbarkeit und Anonymität in der Cloud	272
E.2	Bedrohungsszenarien und Lösungsansätze für Industrie-4.0-Plattformen	275
	(RAPHAEL VALLAZZA)	
E.2.1	Plattformen als Voraussetzung für Industrie 4.0	275
E.2.2	Funktionen und Aufgaben einer IoT-Plattform	276
E.2.3	Risiken und Bedrohungsszenarien	277
E.2.3.1	Datenschutz	278
E.2.3.2	Hacking-Angriffe	279
E.2.3.3	Organisation	279
E.2.3.4	Risikofaktor Mensch	280
E.2.4	Ganzheitliches Sicherheitskonzept – Security by Design	280
E.2.4.1	Maschinen, Geräte und Anwender sicher vernetzen	282
E.2.4.2	Netzwerksegmentierung und Verschlüsselung	284
E.2.4.3	Mandantenfähigkeit, Berechtigungsmanagement, Protokollierung	285
E.2.4.4	OpenSource und Skalierbarkeit	287
E.2.4.5	Usability für mehr Sicherheit	288
E.3	Cybersicherheit am Beispiel einer Entwicklungsplattform für industrielle IoT-Anwendungen	291
	(THOMAS SCHULZ)	
E.3.1	Die Schlüssel zur Plattform-Sicherheit	291
E.3.2	Hohe Sicherheitsstandards von Plattformen	292
E.3.2.1	Sicherheitsnormen	292
E.3.2.1.1	ISO/IEC 27 001	293
E.3.2.1.2	ISO/IEC 27 017	293
E.3.2.1.3	ISO 27 018	293
E.3.2.1.4	ISO 9001	293
E.3.2.1.5	AICPA SOC 2	293

E.3.2.1.6	CSA CCM v3.0.1	294
E.3.2.2	Defense in Depth	294
E.3.2.2.1	Schutz der Daten	294
E.3.2.2.2	Security by Design	295
E.3.2.2.3	Schutz von Plattform, Netzwerk und Infrastruktur	295
E.3.2.2.4	Governance und Compliance	296
E.3.2.2.5	Schutz der Edge	296
E.3.2.2.6	Identitäts- und Zugriffsmanagement	296
E.3.2.2.7	Schlüsselmanagement und Verschlüsselung	296
E.3.2.2.8	Kontinuierliche Bewertung	297
E.3.3	Sichere Entwicklungsumgebung von Anwendungen	297
E.3.3.1	Sicherheitsreview-Richtlinien	298
E.3.3.1.1	Phase I: Third Party Risk Management (TPRM)	298
E.3.3.1.2	Phase II: Technical Security Assessment	299
E.3.3.1.3	Phase III: Secure by Design	299
E.3.3.1.4	Phase IV: Penetration Testing	301
E.3.3.1.5	Continuous Risk Management (eGRC)	302
E.3.3.2	Secure Development Lifecycle (SDL)	302
E.3.3.2.1	Sicherheitsschulungen für Entwickler	303
E.3.3.2.2	Design- und Architektur-Review	304
E.3.3.2.3	Security User Stories / Sicherheitsanforderungen	304
E.3.3.2.4	Bedrohungsmodellierung	305
E.3.3.2.5	Automatische statische Anwendungssicherheitstests (SAST)	306
E.3.3.2.6	Automatische dynamische Anwendungssicherheitstests (DAST)	307
E.3.3.2.7	Vulnerability Assessment für Open-Source-Software (OSS)	307
E.3.3.2.8	Penetrationstest	308
E.3.4	Kontinuierliche Überwachung und Reaktion im Betrieb	308
E.3.4.1	Bedrohungsanalyse	309
E.3.4.2	Monitoring	310
E.3.4.3	Inspektion	311
E.3.4.4	Detektion	311
E.3.4.5	Incident Response	312

F Unternehmensorganisation

F.1	Unternehmensorganisation und Informationssicherheit – Einführung und Grundlagen	315
	(Dr. Dipl.-Phys. CHRISTOPH GLOWATZ; PETER HAUFS-BRUSBERG; Prof. Dr.-Ing. HOLGER SCHMIDT)	
F.1.1	Einleitung	315
F.1.2	Der Faktor Mensch in der Informationssicherheit	316
F.1.2.1	Beispiele für Social-Engineering-Angriffe	317
F.1.2.2	Social-Engineering-Angriffsarten	318
F.1.2.3	Sicherheitsmaßnahmen zur Verbesserung von Security Awareness... ..	319
F.1.3	Organisation der Informationssicherheit	320
F.1.3.1	Informationssicherheitsorganisation	321

F.1.3.2	Rollen und Verantwortlichkeiten	322
F.1.3.3	Aufgaben, Kompetenzen, Verantwortlichkeiten und Prozesse	323
F.1.3.4	Organisatorische und technische Maßnahmen	324
F.1.3.5	Fortbildung, Training und Schulung	325
F.1.4	Prozesse in der Informationssicherheit	325
F.1.4.1	Das Asset Management in der Informationssicherheit	326
F.1.4.1.1	Gefahren eines mangelhaften (Information) Asset Managements	327
F.1.4.1.2	Das Asset Management in Standards und Frameworks ...	327
F.1.4.1.3	Das (Information) Asset Management in der Praxis	328
F.1.4.2	Das Incident Management in der Informationssicherheit	329
F.1.4.2.1	Gefahren eines mangelhaften Information Security Incident Managements	329
F.1.4.2.2	Das Incident Management in Standards und Frameworks	330
F.1.4.2.3	Das Security Incident Management in der Praxis	330
F.1.4.3	Das Problem Management in der Informationssicherheit	331
F.1.4.3.1	Gefahren eines mangelhaften Problem Managements	331
F.1.4.3.2	Das Problem Management in Standards und Frameworks	332
F.1.4.3.3	Das Problem Management in der Praxis	332
F.1.4.4	Das Change Management in der Informationssicherheit	332
F.1.4.4.1	Gefahren eines mangelhaften Change Managements	333
F.1.4.4.2	Das Change Management in Standards und Frameworks	333
F.1.4.4.3	Das Change Management in der Praxis	333

F.2 Informationssicherheits-Managementsystem (ISMS) zur Aufrechterhaltung und kontinuierlichen Verbesserung der Informationssicherheit 335
(Prof. Dipl.-El.-Ing. ARMAND PORTMANN)

F.2.1	Managementsysteme	335
F.2.1.1	Informationssicherheits-Managementsystem nach ISO/IEC 27 001	337
F.2.1.2	Zertifizierung des Informationssicherheits-Managementsystems	342
F.2.1.3	Integrierte Managementsysteme	343

F.3 Aufbau eines Identitäts- und Berechtigungsmanagements 345
(DANIEL CONTA)

F.3.1	Einleitung	345
F.3.2	Identitätsmanagement	345
F.3.2.1	Identitätsarten	345
F.3.2.2	Identifizierung von Identitäten	346
F.3.3	Zugriffskontrolle	347
F.3.3.1	Authentifizierung	347
F.3.3.2	Autorisierung	347
F.3.4	Berechtigungssteuerung	348
F.3.4.1	Rollen	348
F.3.4.2	Berechtigungen	348
F.3.4.3	Ressourcen	350

F.3.4.4	Lebenszyklusphasen	351
F.3.5	Role Based Access Control	352
F.3.6	Authentifikationsprozesse	353
F.3.6.1	Verteilung der Verantwortlichkeiten	353
F.3.6.2	Genehmigungsprozess	356
F.3.6.3	Benutzerverwaltung	358
F.3.6.4	Rollenverwaltung	358
F.3.6.5	Ressourcenverwaltung	359
F.3.6.6	Zugriffsverwaltung	360
F.3.6.7	Berechtigungsverwaltung	360
F.3.6.8	Validierung	361
F.3.7	Schrittweiser Aufbau eines Identity Access Managements	361
F.3.7.1	Schritt 1: Analyse der IT-Landschaft	361
F.3.7.2	Schritt 2: Festlegen von Anforderungen und Ziele	362
F.3.7.3	Schritt 3: Definition der Identitätsarten und -träger	364
F.3.7.4	Schritt 4: Bildung eines Rollenmodells	364
F.3.7.5	Schritt 5: Ressourcen überführen und konsolidieren	365
F.3.7.6	Schritt 6: Benutzer und Rollen zuordnen	366
F.3.7.7	Schritt 7: Einführung der Teilprozesse	367
F.3.7.8	Schritt 8: Schaffung von Kontrollmöglichkeiten	367
F.3.7.9	Schritt 9: Inbetriebnahme	368
F.3.7.10	Schritt 10: Kontinuierliche Verbesserung	369

G Risikomanagement

G.1	Risikomanagement – Einführung und Grundlagen	373
	(Prof. Dr. STEFAN RUF; Prof. Dr. NILS HERDA)	
G.1.1	Einleitung	373
G.1.2	Grundlegende Begriffe und Definitionen des Risikomanagements	374
G.1.3	Unternehmerisches Risikomanagement	376
G.1.4	Normatives Risikomanagement im Kontext der Cyberrisiken	377
G.1.5	Strategisches Risikomanagement im Kontext der Cyberrisiken	378
G.1.6	Operatives Risikomanagement von Cyberrisiken	379
G.2	Integration der operativen Cybertechnologien in das Risikomanagement des Unternehmens	383
	(JENS HEMPEL)	
G.2.1	Beschreibung des Geltungsbereichs	383
G.2.1.1	Risikomanagement vs. OT-Cyberrisiko	383
G.2.1.2	Wo steht OT mit Bezug auf Cyberrisiken?	384
G.2.2	Lebenszyklus	386
G.2.2.1	Cyberrisiken im Vorfeld der OT-Nutzung	388
G.2.2.2	Souveränes Risikomanagement im OT-Betrieb	390
G.2.2.3	Wie bleibt das Rad am Rollen?	391
G.2.3	Tragende Säulen – mehr als Tools	392
G.2.3.1	Personen im Zentrum	392

G.2.3.2	Gemeinsames Vokabular	392
G.2.3.3	Vom GRC zum IRM	393
G.2.3.4	Standards im Praxisumfeld	394
G.2.3.5	Effizientes Risikomanagement	395
G.2.4	Ausblick	396
G.3	Cybersicherungen als Element eines ganzheitlichen Risikomanagements	397
	(JOHANNES BECKERS; DIRK KALINOWSKI)	
G.3.1	Einführung: Sinn und Zweck einer Cybersicherung	397
G.3.1.1	Schadenbeispiele	397
G.3.1.2	Versicherungsmanagement – Einordnung in das Portfolio	398
G.3.1.3	Lösung: Cybersicherung	399
G.3.2	Cybersicherung	399
G.3.2.1	Inhalt und Aufbau einer Cybersicherung	400
G.3.2.1.1	Drittchadendeckung	400
G.3.2.1.2	Eigenschadendeckung	400
G.3.2.2	Marktüberblick	401
G.3.2.3	Auswahlkriterien	402
G.3.2.4	Nutzenbewertung	404
G.3.3	Der Weg zum Abschluss einer Cybersicherung	405
G.3.3.1	Technisch-organisatorische Voraussetzungen	405
G.3.3.2	Obliegenheiten	407
G.3.4	Ausblick	408
G.3.4.1	Künftige Entwicklung der Cybersicherung	408
G.3.4.2	Silent Cover	408
G.3.4.3	Kumulbetrachtung	409

Resümee

Schlusswort des Herausgebers	411
(THOMAS SCHULZ)	

Management-Statement

Die Bedrohungslage für industrielle Steuerungssysteme wird sich weiter zuspitzen – wirtschaftliche und trotzdem sichere Lösungen zur Gefahrenabwehr sind aber vorhanden	415
(WAGO)	

Abkürzungen	419
--------------------------	------------

Lebensläufe	425
--------------------------	------------

Quellenverzeichnis	432
---------------------------------	------------

Stichwortverzeichnis	469
-----------------------------------	------------