

Anwendungsbeginn

Anwendungsbeginn dieser Norm ist ...

Inhalt

	Seite
Nationales Vorwort.....	8
Einleitung	9
1 Anwendungsbereich	11
1.1 Allgemeines	11
1.2 Zielstellung	11
1.3 Anwendung.....	12
1.4 Rahmen	13
2 Normative Verweisungen	13
3 Begriffe und Abkürzungen	14
3.1 Begriffe	14
3.2 Abkürzungen	15
4 Kerntechnikspezifische IT-Sicherheitsmaßnahmen für Leittechnik	17
4.1 Zielgruppen und Lebenszyklusaktivitäten für Leittechnik.....	17
4.2 Quelle für die Bestimmung der IT-Sicherheitsmaßnahmen für kerntechnikspezifische Leittechnik	18
4.2.1 Allgemeines	18
4.2.2 IT-Sicherheitsgrade und IT-Basissicherheit	18
4.2.3 Rechnergestützte Leittechniktools für Leittechnik-Engineering, -instandhaltung und -diagnostik	19
4.2.4 Sicherheit und IT-Sicherheit	19
4.2.5 Andere zugehörige Leitlinien und Normen	19
4.3 Katalog der IT-Sicherheitsmaßnahmen.....	19
4.3.1 ISO/IEC 27002 ist die Basis für die IT-Sicherheitsmaßnahmen nach IEC 63096	20
4.3.2 Änderungen/Erweiterungen der Beschreibung von IT-Sicherheitsmaßnahmen nach ISO/IEC 27002	20
4.3.3 Struktur einer jeden Maßnahmenbeschreibung	21
4.4 Auswahlprozess für IT-Sicherheitsmaßnahmen	23
4.4.1 Prozess zur Auswahl und Umsetzung von IT-Sicherheitsmaßnahmen für E-Aktivitäten – Projekt-Engineering für anlagenspezifische Leittechniksysteme	25
4.4.2 Prozess zur Auswahl und Umsetzung von IT-Sicherheitsmaßnahmen für D-Aktivitäten – Leittechnik-Systemplattformentwicklung	28
4.4.3 Prozess zur Auswahl und Umsetzung der IT-Sicherheitsmaßnahmen für O-Aktivitäten – Betrieb und Instandhaltung von Leittechniksystemen.....	30
4.4.4 Zusätzliche Prozessanforderungen, die für D-, E- und O-Aktivitäten gültig sind	31
4.5 Dokumentation und Rückverfolgbarkeit von IT-Sicherheitsmaßnahmen	32
4.5.1 Dokumentation der Auswahl an IT-Sicherheitsmaßnahmen (statement of applicability).....	32
4.5.2 Rückverfolgbarkeit.....	32
5 <i>IT-Sicherheitspolitik</i>	32

	Seite
5.1	Vorgaben der Leitung für <i>IT-Sicherheit</i> 32
5.1.1	<i>IT-Sicherheitsrichtlinien</i> 33
5.1.2	Überprüfung der <i>IT-Sicherheitsrichtlinien</i> 35
6	Organisation der <i>IT-Sicherheit</i> 35
6.1	Interne Organisation..... 35
6.1.1	<i>IT-Sicherheitsrollen</i> und -verantwortlichkeiten..... 36
6.1.2	Aufgabentrennung..... 40
6.1.3	Kontakt mit Behörden..... 40
6.1.4	Kontakt mit speziellen Interessengruppen..... 41
6.1.5	<i>IT-Sicherheit</i> im Projektmanagement..... 42
6.2	Mobilgeräte und Telearbeit 43
6.2.1	Richtlinie zu Mobilgeräten..... 43
6.2.2	Telearbeit 46
7	Personalsicherheit..... 49
7.1	Vor der Beschäftigung..... 49
7.1.1	Sicherheitsüberprüfung..... 49
7.1.2	Beschäftigungs- und Vertragsbedingungen..... 50
7.2	Während der Beschäftigung..... 51
7.2.1	Beschäftigungs- und Vertragsbedingungen..... 51
7.2.2	<i>IT-Sicherheitsbewusstsein</i> , -ausbildung und -schulung..... 52
7.2.3	Maßregelungsprozess..... 53
7.3	Beendigung und Änderung der Beschäftigung 53
7.3.1	Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung 53
8	Verwaltung der Werte 54
8.1	Verantwortlichkeit für Werte 54
8.1.1	Inventarisierung der Werte..... 54
8.1.2	Zuständigkeit für Werte 55
8.1.3	Zulässiger Gebrauch von Werten 56
8.1.4	Rückgabe von Werten..... 56
8.2	Informationsklassifizierung..... 57
8.2.1	Klassifizierung von Information 57
8.2.2	Kennzeichnung von Information 58
8.2.3	Handhabung von Werten 58
8.3	Handhabung von Datenträgern..... 59
8.3.1	Handhabung von Wechseldatenträgern 59
8.3.2	Entfernung von Datenträgern..... 59
8.3.3	Transport von Datenträgern 60
9	Zugangssteuerung 60
9.1	Geschäftsanforderungen an die Zugangssteuerung..... 60

	Seite
9.1.1	Richtlinie zur Zugangssteuerung..... 60
9.1.2	Zugang zu Netzwerken und Netzwerkdiensten..... 70
9.2	Benutzerzugangsverwaltung 74
9.2.1	Registrierung und Deregistrierung von Benutzern 74
9.2.3	Verwaltung privilegierter Zugangsrechte..... 75
9.2.4	Verwaltung geheimer Authentisierungsinformationen von Benutzern 76
9.2.5	Überprüfung von Benutzerzugangsrechten 77
9.2.6	Entzug oder Anpassung von Zugangsrechten 77
9.3	Benutzerverantwortlichkeiten 78
9.3.1	Gebrauch geheimer Authentisierungsinformationen..... 78
9.4	Zugangssteuerung für Systeme und Anwendungen 79
9.4.1	Informationszugangsbeschränkung 79
9.4.2	Sichere Anmeldeverfahren..... 79
9.4.3	System zur Verwaltung von Kennwörtern 80
9.4.4	Gebrauch von Hilfsprogrammen mit privilegierten Rechten 80
9.4.5	Zugangssteuerung für Quellcode von Programmen 81
10	Kryptographie 82
10.1	Kryptographische Maßnahmen 82
10.1.1	Richtlinie zum Gebrauch von kryptographischen Maßnahmen 82
10.1.2	Schlüsselverwaltung..... 87
11	Physische und umgebungsbezogene Sicherheit 91
11.1	Sicherheitsbereiche 91
11.1.1	Physische Sicherheitsparameter..... 91
11.1.2	Physische Zutrittssteuerung 93
11.1.4	Schutz vor externen und umweltbedingten Bedrohungen..... 94
11.1.5	Arbeiten in Sicherheitsbereichen..... 95
11.1.6	Anlieferungs- und Ladebereiche sowie Lagerhäuser 95
11.2	Geräte und Betriebsmittel..... 96
11.2.1	Platzierung und Schutz von Geräten und Betriebsmitteln 96
11.2.2	Versorgungseinrichtungen 99
11.2.3	Sicherheit der Verkabelung 100
11.2.4	Instandhaltung von Geräten und Betriebsmitteln 100
11.2.5	Entfernen von Werten 101
11.2.6	Sicherheit von Geräten, Betriebsmitteln und Werten außerhalb der Räumlichkeiten..... 102
11.2.7	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln 104
11.2.8	Unbeaufsichtigte Benutzergeräte 105
11.2.9	Richtlinien für eine aufgeräumte Arbeitsumgebung und Bildschirmschoner sperren 106
12	Betriebssicherheit 107
12.1	Betriebsabläufe und -verantwortlichkeiten 107

	Seite	
12.1.1	Dokumentierte Betriebsabläufe.....	107
12.1.2	Änderungssteuerung.....	109
12.1.3	Kapazitätssteuerung	110
12.1.4	Trennung von Entwicklungs-, Test- und Betriebsumgebungen	111
12.2	Schutz vor Schadsoftware	112
12.2.1	Maßnahmen gegen Schadsoftware	112
12.3	Datensicherung	114
12.3.1	Sicherung von Informationen	114
12.4	Protokollierung und Überwachung.....	115
12.4.1	Ereignisprotokollierung.....	115
12.4.2	Schutz der Protokollinformation	118
12.4.3	Administratoren- und Bedienerprotokolle.....	119
12.4.4	Uhrensynchronisation	120
12.4.5	<i>NUC – Zentralisierung gesammelter IT-Sicherheitsereignisse</i>	121
12.4.6	<i>NUC – Protokoll-Korrelation und Erkennung von Angriffsszenarien</i>	122
12.5	Steuerung von Software im Betrieb	123
12.5.1	Installation von Software auf Systemen im Betrieb	123
12.6	Handhabung technischer Schwachstellen	126
12.6.1	Handhabung von technischen Schwachstellen	126
12.6.2	Einschränkungen von Softwareinstallation	128
12.6.3	<i>NUC – Steuerungsprozess für technische Verwundbarkeiten</i>	129
12.6.4	<i>NUC – Informationsquellen und Kanäle für technische Verwundbarkeiten</i>	130
12.6.5	<i>NUC – Handhabung von Wechseldatenträger</i>	131
12.6.6	<i>NUC – Einschränkungen zur Ausführung von Software</i>	132
12.7	Audits von Informationssystemen	132
12.7.1	Maßnahmen für Audits von Informationssystemen	132
13	Kommunikationssicherheit	133
13.1	Netzwerksicherheitsmanagement	133
13.1.1	Netzwerksteuerungsmaßnahmen	133
13.1.2	Sicherheit von Netzwerkdiensten.....	140
13.1.3	Trennung in Netzwerken	142
13.2	Informationsübertragung	146
13.2.1	Richtlinien und Verfahren für die Informationsübertragung	146
13.2.2	Vereinbarungen zur Informationsübertragung	148
13.2.3	Elektronische Nachrichtenübermittlung	149
13.2.4	Vertraulichkeits- oder Geheimhaltungsvereinbarungen.....	149
14	Anschaffung, Entwicklung und Instandhaltung von Systemen	151
14.1	Sicherheitsanforderungen an Informationssysteme.....	151
14.1.1	Analyse und Spezifikation von Informationssicherheitsanforderungen	151

	Seite
14.2 Sicherheit in Entwicklungs- und Unterstützungsprozessen	152
14.2.1 Richtlinie für sichere Entwicklung.....	153
14.2.2 Verfahren zur Verwaltung von Systemänderungen	154
14.2.3 Technische Überprüfung von Anwendungen nach Änderungen an der Betriebsplattform.....	155
14.2.4 Beschränkung von Änderungen an Softwarepaketen.....	156
14.2.5 Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme	157
14.2.6 Sichere Entwicklungsumgebung	157
14.2.7 Ausgegliederte Entwicklung	158
14.2.8 Testen der Systemsicherheit.....	159
14.2.9 Systemabnahmetest.....	160
14.3 Testdaten.....	160
14.3.1 Schutz von Testdaten.....	161
15 Lieferantenbeziehungen	161
15.1 Informationssicherheit in Lieferantenbeziehungen.....	161
15.1.1 Informationssicherheitsrichtlinie für Lieferantenbeziehungen	161
15.1.2 Behandlung von Sicherheit in Lieferantenvereinbarungen	164
15.1.3 Lieferkette für Informations- und Kommunikationstechnologie	165
15.2 Steuerung der Dienstleistungserbringung von Lieferanten	167
15.2.1 Überwachung und Überprüfung von Lieferantendienstleistungen	167
15.2.2 Handhabung der Änderungen von Lieferantendienstleistungen	169
16 Handhabung von Informationssicherheitsvorfällen	170
16.1 Handhabung von Informationssicherheitsvorfällen und -verbesserungen	170
16.1.1 Verantwortlichkeiten und Verfahren	170
16.1.2 Meldung von Informationssicherheitsereignissen	176
16.1.3 Meldung von Schwächen in der <i>IT-Sicherheit</i>	177
16.1.4 Beurteilung von und Entscheidung über <i>IT-Sicherheitsereignisse</i>	178
16.1.5 Reaktion auf <i>IT-Sicherheitsvorfälle</i>	179
16.1.6 Erkenntnisse aus <i>IT-Sicherheitsvorfällen</i>	180
16.1.7 Sammeln von Beweismaterial	181
17 <i>IT-Sicherheitsaspekte</i> beim Business Continuity Management.....	183
17.1 Aufrechterhalten der <i>IT-Sicherheit</i>	183
17.1.1 Planung zur Aufrechterhaltung der Informationssicherheit	183
17.1.2 Umsetzung der Aufrechterhaltung der <i>IT-Sicherheit</i>	184
17.1.3 Überprüfen und Bewerten der Aufrechterhaltung der <i>IT-Sicherheit</i>	187
17.2 Redundanzen	188
17.2.1 Verfügbarkeit von informationsverarbeitenden Einrichtungen	188
18 Compliance.....	189
18.1 Einhaltung gesetzlicher und vertraglicher Anforderungen	189
18.1.1 Bestimmung der anwendbaren Gesetzgebung und der vertraglichen Anforderungen.....	189

	Seite
18.1.2 Geistige Eigentumsrechte	190
18.1.3 Schutz von Aufzeichnungen.....	191
18.1.4 Privatsphäre und Schutz von personenbezogener Information.....	192
18.1.5 Regelungen bezüglich kryptographischer Maßnahmen	193
18.2 Überprüfungen der <i>IT-Sicherheit, Audits und Inspektionen</i>	194
18.2.1 Unabhängige Überprüfung der Informationssicherheit.....	195
18.2.2 Einhaltung von Sicherheitsrichtlinien und -standards	196
18.2.3 Überprüfung der Einhaltung von technischen Vorgaben	197
19 <i>NUC – IT-Sicherheit und Architektur</i>	198
19.1 <i>NUC – IT-Sicherheit und Architekturmaßnahmen</i>	198
19.1.1 <i>NUC – IT-Sicherheitsgrade</i>	199
19.1.2 <i>NUC – IT-Sicherungszonen</i>	199
19.1.3 <i>NUC – Administration von IT-Sicherungszonen</i>	200
19.1.4 <i>NUC – Entnahme und Sammlung von Daten</i>	201
19.1.5 <i>NUC – Vorübergehendes Einbringen von Einrichtungen in eine Zone</i>	202
20 <i>NUC – Virtualisierungsumgebung und -infrastruktur</i>	202
20.1 <i>NUC – Maßnahmen für Virtualisierungsumgebung und Infrastruktur</i>	202
20.1.1 <i>NUC – IT-Sicherheitsgrade</i>	202
Anhang A (informativ) <i>IT-Sicherheitsmaßnahmen im Zusammenhang mit IT-Sicherheitsgraden, Aktivitäten, Erhalt von Schutzzielen, Fokus der IT-Sicherheitsmaßnahmen und Änderungen gegenüber ISO/IEC 27002</i>	205
Anhang B (informativ) <i>Zusammenhang mit IEC 62645, Ed. 2</i>	236
Anhang C (informativ) <i>Beispielliste für die Dokumentation zur projektspezifischen Auswahl von IT-Sicherheitsmaßnahmen</i>	240
Anhang D (informativ) <i>Semi-formale Darstellung und Austausch von IT-Sicherheitsmaßnahmen</i>	243
Anhang E (informativ) <i>Kryptographie 10.1</i>	244
Anhang F (informativ) <i>Kryptographie 10.2</i>	245
Anhang G (informativ) <i>Kryptographie 10.3</i>	246
Anhang H (informativ) <i>Kryptographie 10.4</i>	247
Anhang I (informativ) <i>Bild 1 – Übersicht – und Bild 2 – Prozess zur Auswahl von IT-Sicherheitsmaßnahmen</i>	248
Literaturhinweise	251
Bilder	
Bild 1 – Überblick.....	24
Bild 2 – Prozess zur Auswahl von IT-Sicherheitsmaßnahmen	26
Tabellen	
Tabelle A.1 – Übersichtstabelle zu IT-Sicherheitsmaßnahmen	206
Tabelle B.1 – Zusammenhang zwischen IEC 62645, Ed.2-CD2 und IEC 63096:2018-CD1.....	236
Tabelle C.1 – Beispielliste für die Dokumentation zu projektspezifischen Selektierungen von IT-Sicherheitsmaßnahmen	241