Anwendungsbeginn

Anwendungsbeginn dieser Norm ist ... .

Inhalt

Seite

Nationales Vorwort ... 5
Nationaler Anhang NA (informativ) Zusammenhang mit Europäischen und Internationalen Normen ... 5
Nationaler Anhang NB (informativ) Fachwörterliste ... 6
0 Einleitung ... 16
0.1 Überblick ... 16
0.2 Zweck und Anwenderkreis ... 17
0.3 Verwendung innerhalb anderer Teile der Normenreihe IEC 62443 ... 17
1 Anwendungsbereich ... 19
2 Normative Verweisungen ... 19
3 Begriffe, Abkürzungen und Erläuterungen ... 19
3.1 Begriffe ... 19
3.2 Abkürzungen ... 27
3.3 Erläuterungen ... 29
4 Beschränkungen der IT-Sicherheit aufgrund der Natur des Automatisierungssystems ... 30
4.1 Überblick ... 30
4.2 Unterstützung wesentlicher Funktionen ... 30
4.3 Ausgleichsmaßnahmen ... 31
4.4 Minimal erforderliche Rechte (en: least privilege) ... 31
5 Grundlegende Anforderung FR 1 – Identifizierung und Authentifizierung ... 31
5.1 Zweck und Beschreibungen des SL-C(IAC) ... 31
5.2 Begründung ... 32
5.3 SR 1.1 – Identifizierung und Authentifizierung von menschlichen Nutzern ... 32
5.4 SR 1.2 – Identifizierung und Authentifizierung von Softwareprozessen und Geräten ... 33
5.5 SR 1.3 – Nutzerkontenverwaltung ... 34
5.6 SR 1.4 – Verwaltung der Kennungen ... 35
5.7 SR 1.5 – Verwaltung der Authentifizierern ... 36
5.8 SR 1.6 – Management drahtloser Zugriffsverfahren ... 37
5.9 SR 1.7 – Stärke der Authentifizierung durch Passwörter ... 38
5.10 SR 1.8 – PKI-Zertifikate ... 39
5.11 SR 1.9 – Stärke der Authentifizierung durch öffentliche Schlüssel ... 39
5.12 SR 1.10 – Rückmeldung vom Authentifizierer ... 41
5.13 SR 1.11 – Erfolglose Anmeldeversuche ... 41
5.14 SR 1.12 – Nutzungshinweis ... 42
5.15 SR 1.13 – Zugriff über nicht vertrauenswürdige Netze ... 42
6 Grundlegende Anforderung FR 2 – Nutzungskontrolle ... 43

Seite

6.1 Zweck und Beschreibungen des SL-C(UC) 43
6.2 Begründung 43
6.3 SR 2.1 – Durchsetzung der Autorisierung 44
6.4 SR 2.2 – Nutzungskontrolle von Funkverbindungen 45
6.5 SR 2.3 – Nutzungskontrolle von tragbaren und mobilen Geräten 46
6.6 SR 2.4 – Plattformübergreifender Code 47
6.7 SR 2.5 – Sitzungssperrung 47
6.8 SR 2.6 – Beendigung einer Fernzugriffssitzung 48
6.9 SR 2.7 – Begrenzung der Anzahl gleichzeitiger Sitzungen 48
6.10 SR 2.8 – Prüfbare Ereignisse und deren Aufzeichnung 49
6.11 SR 2.9 – Speicherkapazität für Aufzeichnungen 50
6.12 SR 2.10 – Reaktion auf ausgefallene Verarbeitung von Ereignisdaten 51
6.13 SR 2.11 – Zeitstempel 51
6.14 SR 2.12 – Nicht-Abstreitbarkeit 52
7 Grundlegende Anforderung FR 3 – Systemintegrität 53
7.1 Zweck und Beschreibungen des SL-C(SI) 53
7.2 Begründung 53
7.3 SR 3.1 – Kommunikationsintegrität 53
7.4 SR 3.2 – Schutz vor Schadcode 54
7.5 SR 3.3 – Verifikation der IT-Sicherheitsfunktionalität 55
7.6 SR 3.4 – Software- und Informationsintegrität 56
7.7 SR 3.5 – Eingabevalidierung 57
7.8 SR 3.6 – Vorbestimmte Zustände der Ausgänge 58
7.9 SR 3.7 – Fehlerbehandlung 58
7.10 SR 3.8 – Sitzungsintegrität 59
7.11 SR 3.9 – Schutz von Prüfinformationen 60
8 Grundlegende Anforderung FR 4 – Vertraulichkeit der Daten 60
8.1 Zweck und Beschreibungen des SL-C(DC) 60
8.2 Begründung 60
8.3 SR 4.1 – Vertraulichkeit von Informationen 61
8.4 SR 4.2 –Dauerhaftigkeit von Informationen 62
8.5 SR 4.3 – Verwendung von Verschlüsselung 63
9 Grundlegende Anforderung FR 5 – Eingeschränkter Datenfluss 63
9.1 Zweck und Beschreibungen des SL-C(RDF) 63
9.2 Begründung 64
9.3 SR 5.1 – Netzaufteilung 64
9.4 SR 5.2 – Schutz der Zonengrenze 65
9.5 SR 5.3 – Beschränkung der persönlichen Kommunikation 66
9.6 SR 5.4 – Aufteilung von Anwendungen 67

Seite
10 Grundlegende Anforderung FR 6 – Rechtzeitige Reaktion auf Ereignisse ... 67
10.1 Zweck und Beschreibungen des SL-C(TRE) ... 67
10.2 Begründung ... 68
10.3 SR 6.1 – Zugriffsmöglichkeit auf Ereignisprotokolle ... 68
10.4 SR 6.2 – Kontinuierliche Überwachung ... 68
11 Grundlegende Anforderung FR 7 – Ressourcenverfügbarkeit ... 69
11.1 Zweck und Beschreibungen des SL-C(RA) ... 69
11.2 Begründung ... 70
11.3 SR 7.1 – Schutz gegen DoS-Ereignisse ... 70
11.4 SR 7.2 – Ressourcenmanagement ... 70
11.5 SR 7.3 – Datensicherung im Automatisierungssystem (Backup) ... 71
11.6 SR 7.4 – Wiederherstellung des Automatisierungssystems ... 72
11.7 SR 7.5 – Notstromversorgung ... 72
11.8 SR 7.6 – Netz- und IT-Sicherheitseinstellungen ... 73
11.9 SR 7.7 – Geringste Funktionalität ... 73
11.10 SR 7.8 – Verzeichnis der Komponenten eines Automatisierungssystems ... 74
Anhang A (informativ) Diskussion des SL-Vektors ... 75
A.1 Überblick ... 75
A.2 Security-Level ... 75
A.2.1 Definition ... 75
A.2.2 SL-Arten ... 76
A.2.3 Anwendung der Security-Level ... 76
A.3 SL-Vektor ... 80
A.3.1 Grundlegende Anforderungen ... 80
A.3.2 SL-Festlegung ... 81
A.3.3 SL-Vektorformat ... 83
Anhang B (informativ) Abbildung der Systemanforderungen (SR) und weitergehenden Anforderungen (RE) auf die Security-Level (SL) 1- 4 der grundlegenden Anforderungen (FR) ... 84
B.1 Überblick ... 84
B.2 SL-Abbildungstabelle ... 84
Literaturhinweise ... 89

Bilder

Bild 1 – Aufbau der Normenreihe IEC 62443 ... 18
Bild A.1 – Beispiel aus der verfahrenstechnischen Industrie mit Zonen und Conduits ... 78
Bild A.2 – Beispiel aus der Fertigungsindustrie mit Zonen und Conduits ... 79
Bild A.3 – Schematische Darstellung der Verwendung verschiedener SL-Arten ... 80

Tabellen

Tabelle B.1 – Abbildung von SR und RE auf die FR für SL 1- 4 ... 84