

	DIN EN IEC 62443-3-3 (VDE 0802-3-3)	DIN
	Diese Norm ist zugleich eine VDE-Bestimmung im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation“ bekannt gegeben worden.	VDE
<p>ICS 35.030; 35.240.50</p> <p>Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme – Teil 3-3: Systemanforderungen zur IT-Sicherheit und Security-Level (IEC 62443-3-3:2013 + COR1:2014); Deutsche Fassung EN IEC 62443-3-3:2019 + AC:2019</p> <p>Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels (IEC 62443-3-3:2013 + COR1:2014); German version EN IEC 62443-3-3:2019 + AC:2019</p> <p>Réseaux industriels de communication – Sécurité dans les réseaux et les systèmes – Partie-3: Exigences relatives à la sécurité dans les systèmes et niveaux de sécurité (IEC 62443-3-3:2013 + COR1:2014); Version allemande EN IEC 62443-3-3:2019 + AC:2019</p> <p>Gesamtumfang 91 Seiten</p> <p>DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE</p>		

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2019-04-03 angenommene Europäische Norm als DIN-Norm ist 2020-01-01.

Diese Norm enthält die Berichtigung EN IEC 62443-3-3:2019/AC:2019, die das Corrigendum 1:2014 zu IEC 62443-3-3:2013 übernimmt.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN IEC 62443-3-3 (VDE 0802-3-3):2015-06.

Für dieses Dokument ist das nationale Arbeitsgremium UK 931.1 „IT-Sicherheit in der Automatisierungstechnik“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (www.dke.de) zuständig.

Die enthaltene IEC-Publikation wurde vom TC 65 „Industrial-process measurement, control and automation“ erarbeitet.

Das IEC-Komitee hat entschieden, dass der Inhalt dieses Dokuments bis zu dem Datum (stability date) unverändert bleiben soll, das auf der IEC-Website unter „<http://webstore.iec.ch>“ zu diesem Dokument angegeben ist. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees das Dokument

- bestätigt,
- zurückgezogen,
- durch eine Folgeausgabe ersetzt oder
- geändert.

AC Das IEC-Corrigendum 1, von CENELEC angenommen als AC, wurde eingearbeitet und mit einer senkrechten Linie und „AC“ am linken Textrand gekennzeichnet.

Das Original-Dokument enthält Bilder in Farbe, die in der Papierversion in einer Graustufen-Darstellung wiedergegeben werden. Elektronische Versionen dieses Dokuments enthalten die Bilder in der originalen Farbdarstellung.

Die Deutsche Fassung wurde im [Abschnitt 3](#) an den aktuellen Standardtext angepasst.

Zu den terminologischen Einträgen in [Abschnitt 3](#) hat das Nationale Gremium noch die folgenden Hinweise:

- Zu [3.1.8](#):
Zum Begriff „Verfügbarkeit“ siehe auch „Internationales Elektrotechnisches Wörterbuch – Deutsche Ausgabe“, Online-Zugang: <http://www.dke.de/dke-iev>.
- Zu [3.1.17](#):
Für den Begriff „Maßnahme“ verwendet ISO/IEC 27001:2008 die Benennung „control“ und IEC 62443-3:2013 „countermeasure“. Hierauf macht die Anmerkung in IEC 62443-3:2013 aufmerksam. Der Text dieser Anmerkung wurde nicht übersetzt. Da beide Benennungen in den jeweiligen deutschen Fassungen dieser Normen mit „Maßnahme“ übersetzt wurden, tritt in diesen die beschriebene Schwierigkeit nicht auf.
- Zu [3.1.20](#):
Die Definition des Begriffs „Gerät“ trifft auf „eingebettetes Gerät“ zu.

Nationaler Anhang NA (informativ)

Zusammenhang mit europäischen und internationalen Dokumenten

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf ein Dokument ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils aktuellste Ausgabe des in Bezug genommenen Dokuments.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe des Dokuments.

Eine Information über den Zusammenhang der zitierten Dokumente mit den entsprechenden deutschen Dokumenten ist nachstehend wiedergegeben.

Tabelle NA.1

Europäisches Dokument	Internationales Dokument	Deutsches Dokument	Klassifikation im VDE-Vorschriftenwerk
–	IEC 62443-2-1	–	–
EN IEC 62443-4-1	IEC 62443-4-1	DIN EN IEC 62443-4-1 (VDE 0802-4-1)	VDE 0802-4-1
EN IEC 62443-4-2	IEC 62443-4-2 ^a	DIN EN 62443-4-2 (VDE 0802-4-2)	VDE 0802-4-2
–	IEC/TS 62443-1-1:2009	–	–
–	IEC/TS 62443-1-3	–	–
–	IEC 62443-2-4:2015 + Cor.:2015	DIN IEC 62443-2-4 (VDE 0802-2-4)	VDE 0802-2-4
EN 62443-3-2 ^a	IEC 62443-3-2 ^a	DIN EN 62443-3-2 (VDE 0802-3-2)	VDE 0802-3-2
–	IEC/TR 62443-1-2 ^a	–	–
–	IEC/TR 62443-1-4 ^a	–	–
–	IEC/TR 62443-2-2 ^a	–	–
–	IEC/TR 62443-2-3	–	–
–	IEC/TR 62443-3-1	–	–
–	ISO/IEC 19790	–	–
EN ISO/IEC 27002	ISO/IEC 27002	DIN EN ISO/IEC 27002	–
^a In Vorbereitung.			

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN IEC 62443-2-4 (VDE 0802-2-4), *IT-Sicherheit für industrielle Automatisierungssysteme – Teil 2-4: Anforderungen an das IT-Sicherheitsprogramm von Dienstleistern für industrielle Automatisierungssysteme*

DIN EN 62443-3-2 (VDE 0802-3-2) (in Vorbereitung), *Sicherheit für industrielle Automatisierungssysteme – Teil 3-2: Sicherheitsrisikobeurteilung und Systemgestaltung*

DIN EN 62443-4-2 (VDE 0802-4-2) (in Vorbereitung), *Industrielle Kommunikationsnetze – IT-Sicherheit für industrielle Automatisierungssysteme – Teil 4-2: Anforderungen an Komponenten industrieller Automatisierungssysteme*

DIN EN IEC 62443-4-1 (VDE 0802-4-1), *IT-Sicherheit für industrielle Automatisierungssysteme – Teil 4-1: Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung*

DIN EN ISO/IEC 27002, *Informationstechnik – Sicherheitsverfahren – Leitfaden für Informationssicherheitsmaßnahmen*

**Industrielle Kommunikationsnetze –
IT-Sicherheit für Netze und Systeme –
Teil 3-3: Systemanforderungen zur IT-Sicherheit und Security-Level
(IEC 62443-3-3:2013 + COR1:2014)**

Industrial communication networks –
Network and system security –
Part 3-3: System security requirements and
security levels
(IEC 62443-3-3:2013 + COR1:2014)

Réseaux industriels de communication –
Sécurité dans les réseaux et les systèmes –
Partie-3: Exigences relatives à la sécurité dans
les systèmes et niveaux de sécurité
(IEC 62443-3-3:2013 + COR1:2014)

Diese Europäische Norm wurde von CENELEC am 2019-04-03 angenommen.

Die Berichtigung tritt am 11. Oktober 2019 zur Einarbeitung in die deutsche Fassung der EN in Kraft.

CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist.

Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC Management Centre oder bei jedem CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem CEN-CENELEC Management Centre mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CENELEC-Mitglieder sind die nationalen elektrotechnischen Komitees von Belgien, Bulgarien, Dänemark, Deutschland, der ehemaligen jugoslawischen Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



Europäisches Komitee für Elektrotechnische Normung
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brüssel

© 2019 CENELEC – Alle Rechte der Verwertung, gleich in welcher Form und in welchem Verfahren, sind weltweit den Mitgliedern von CENELEC vorbehalten.

Ref. Nr. EN IEC 62443-3-3:2019 + AC:2019 D

Europäisches Vorwort

Dieses Dokument (EN IEC 62443-3-3:2019) enthält den Text der IEC 62443-3-3:2013, die vom IEC/TC 65 „Industrial-process measurement, control and automation“ erarbeitet wurde.

Nachstehende Daten wurden festgelegt:

- spätestes Datum, zu dem dieses Dokument auf nationaler Ebene durch Veröffentlichung einer identischen nationalen Norm oder durch Anerkennung übernommen werden muss (dop): 2020-04-03
- spätestes Datum, zu dem nationale Normen, die diesem Dokument entgegenstehen, zurückgezogen werden müssen (dow): 2022-04-03

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CENELEC ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Anerkennungsnotiz

Der Text der Internationalen Norm IEC 62443-3-3:2013 wurde von CENELEC ohne irgendeine Abänderung als Europäische Norm angenommen.

In der offiziellen Fassung sind unter „Literaturhinweise“ zu den aufgelisteten Normen die nachstehenden Anmerkungen einzutragen:

IEC 62443-2-4	ANMERKUNG	Harmonisiert als EN IEC 62443-2-4.
IEC 62443-4-1	ANMERKUNG	Harmonisiert als EN IEC 62443-4-1.
IEC 62443-4-2	ANMERKUNG	Harmonisiert als EN IEC 62443-4-2.
ISO/IEC 27002	ANMERKUNG	Harmonisiert als EN ISO/IEC 27002.

Anerkennungsnotiz zu AC

Der Text der Berichtigung IEC 62443-3-3:2013/COR1:2014 wurde von CENELEC ohne irgendeine Abänderung als EN IEC 62443-3-3:2019/AC:2019-10 angenommen.

Anhang ZA (normativ)

Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ANMERKUNG 1 Ist eine internationale Publikation durch gemeinsame Abänderungen modifiziert worden, gekennzeichnet durch (mod.), dann gilt die entsprechende EN oder das HD.

ANMERKUNG 2 Aktualisierte Informationen über die in diesem Anhang aufgeführten aktuellen Fassungen der Europäischen Normen sind hier verfügbar: www.cenelec.eu.

<u>Publikation</u>	<u>Jahr</u>	<u>Titel</u>	<u>EN/HD</u>	<u>Jahr</u>
IEC 62443-2-1	–	Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program	–	–
IEC/TS 62443-1-1	2009	Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models	–	–

Inhalt

Seite

Europäisches Vorwort.....	2
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen	3
0 Einleitung.....	13
0.1 Überblick.....	13
0.2 Zweck und Anwenderkreis	14
0.3 Verwendung innerhalb anderer Teile der Normenreihe IEC 62443.....	14
1 Anwendungsbereich	16
2 Normative Verweisungen	16
3 Begriffe, Abkürzungen und Erläuterungen	16
3.1 Begriffe	16
3.2 Abkürzungen	24
3.3 Vereinbarungen	26
4 Beschränkungen der IT-Sicherheit aufgrund der Natur des Automatisierungssystems	27
4.1 Überblick.....	27
4.2 Unterstützung wesentlicher Funktionen	27
4.3 Ausgleichsmaßnahmen	28
4.4 Minimal erforderliche Rechte (en: least privilege)	28
5 Grundlegende Anforderung FR 1 – Identifizierung und Authentifizierung	29
5.1 Zweck und Beschreibungen des SL-C(IAC).....	29
5.2 Begründung	29
5.3 SR 1.1 – Identifizierung und Authentifizierung von menschlichen Nutzern	29
5.3.1 Anforderung.....	29
5.3.2 Begründung und zusätzliche Hinweise	29
5.3.3 Weitergehende Anforderungen	30
5.3.4 Security-Level.....	30
5.4 SR 1.2 – Identifizierung und Authentifizierung von Softwareprozessen und Geräten	30
5.4.1 Anforderung.....	30
5.4.2 Begründung und zusätzliche Hinweise	30
5.4.3 Weitergehende Anforderungen	31
5.4.4 Security-Level.....	31
5.5 SR 1.3 – Nutzerkontenverwaltung.....	32
5.5.1 Anforderung.....	32
5.5.2 Begründung und zusätzliche Hinweise	32
5.5.3 Weitergehende Anforderungen	32
5.5.4 Security-Level.....	32
5.6 SR 1.4 – Verwaltung der Bezeichner	32
5.6.1 Anforderung.....	32

5.6.2	Begründung und zusätzliche Hinweise	32
5.6.3	Weitergehende Anforderungen	33
5.6.4	Security-Level	33
5.7	SR 1.5 – Verwaltung der Authentifizierer	33
5.7.1	Anforderung	33
5.7.2	Begründung und zusätzliche Hinweise	33
5.7.3	Weitergehende Anforderungen	34
5.7.4	Security-Level	34
5.8	SR 1.6 – Management drahtloser Zugriffsverfahren	34
5.8.1	Anforderung	34
5.8.2	Begründung und zusätzliche Hinweise	35
5.8.3	Weitergehende Anforderungen	35
5.8.4	Security-Level	35
5.9	SR 1.7 – Stärke der Authentifizierung durch Passwörter	35
5.9.1	Anforderung	35
5.9.2	Begründung und zusätzliche Hinweise	35
5.9.3	Weitergehende Anforderungen	36
5.9.4	Security-Level	36
5.10	SR 1.8 – PKI-Zertifikate	36
5.10.1	Anforderung	36
5.10.2	Begründung und zusätzliche Hinweise	36
5.10.3	Weitergehende Anforderungen	37
5.10.4	Security-Level	37
5.11	SR 1.9 – Stärke der Authentifizierung durch öffentliche Schlüssel	37
5.11.1	Anforderung	37
5.11.2	Begründung und zusätzliche Hinweise	37
5.11.3	Weitergehende Anforderungen	38
5.11.4	Security-Level	38
5.12	SR 1.10 – Rückmeldung vom Authentifizierer	38
5.12.1	Anforderung	38
5.12.2	Begründung und zusätzliche Hinweise	38
5.12.3	Weitergehende Anforderungen	38
5.12.4	Security-Level	38
5.13	SR 1.11 – Erfolgreiche Anmeldeversuche	39
5.13.1	Anforderung	39
5.13.2	Begründung und zusätzliche Hinweise	39
5.13.3	Weitergehende Anforderungen	39
5.13.4	Security-Level	39
5.14	SR 1.12 – Nutzungshinweis	39

5.14.1	Anforderung	39
5.14.2	Begründung und zusätzliche Hinweise	39
5.14.3	Weitergehende Anforderungen	40
5.14.4	Security-Level	40
5.15	SR 1.13 – Zugriff über nicht vertrauenswürdige Netze	40
5.15.1	Anforderung	40
5.15.2	Begründung und zusätzliche Hinweise	40
5.15.3	Weitergehende Anforderungen	40
5.15.4	Security-Level	40
6	Grundlegende Anforderung FR 2 – Nutzungskontrolle	41
6.1	Zweck und Beschreibungen des SL-C(UC)	41
6.2	Begründung	41
6.3	SR 2.1 – Durchsetzung der Autorisierung	41
6.3.1	Anforderung	41
6.3.2	Erläuterung und zusätzliche Hinweise	41
6.3.3	Weitergehende Anforderungen	42
6.3.4	Security-Level	42
6.4	SR 2.2 – Nutzungskontrolle von Funkverbindungen	43
6.4.1	Anforderung	43
6.4.2	Begründung und zusätzliche Hinweise	43
6.4.3	Weitergehende Anforderungen	43
6.4.4	Security-Level	43
6.5	SR 2.3 – Nutzungskontrolle von tragbaren und mobilen Geräten	43
6.5.1	Anforderung	43
6.5.2	Begründung und zusätzliche Hinweise	43
6.5.3	Weitergehende Anforderungen	44
6.5.4	Security-Level	44
6.6	SR 2.4 – Plattformübergreifender Code	44
6.6.1	Anforderung	44
6.6.2	Begründung und zusätzliche Hinweise	44
6.6.3	Weitergehende Anforderungen	44
6.6.4	Security-Level	45
6.7	SR 2.5 – Sitzungssperrung	45
6.7.1	Anforderung	45
6.7.2	Begründung und zusätzliche Hinweise	45
6.7.3	Weitergehende Anforderungen	45
6.7.4	Security-Level	45
6.8	SR 2.6 – Beendigung einer Fernzugriffssitzung	45
6.8.1	Anforderung	45

6.8.2	Begründung und zusätzliche Hinweise	45
6.8.3	Weitergehende Anforderungen	46
6.8.4	Security-Level	46
6.9	SR 2.7 – Begrenzung der Anzahl gleichzeitiger Sitzungen	46
6.9.1	Anforderung	46
6.9.2	Begründung und zusätzliche Hinweise	46
6.9.3	Weitergehende Anforderungen	46
6.9.4	Security-Level	46
6.10	SR 2.8 – Prüfbare Ereignisse und deren Aufzeichnung	46
6.10.1	Anforderung	46
6.10.2	Begründung und zusätzliche Hinweise	47
6.10.3	Weitergehende Anforderungen	47
6.10.4	Security-Level	47
6.11	SR 2.9 – Speicherkapazität für Aufzeichnungen	47
6.11.1	Anforderung	47
6.11.2	Begründung und zusätzliche Hinweise	47
6.11.3	Weitergehende Anforderungen	48
6.11.4	Security-Level	48
6.12	SR 2.10 – Reaktion auf ausgefallene Verarbeitung von Ereignisdaten	48
6.12.1	Anforderung	48
6.12.2	Begründung und zusätzliche Hinweise	48
6.12.3	Weitergehende Anforderungen	48
6.12.4	Security-Level	48
6.13	SR 2.11 – Zeitstempel	49
6.13.1	Anforderung	49
6.13.2	Begründung und zusätzliche Hinweise	49
6.13.3	Weitergehende Anforderungen	49
6.13.4	Security-Level	49
6.14	SR 2.12 – Nichtabstreitbarkeit	49
6.14.1	Anforderung	49
6.14.2	Begründung und zusätzliche Hinweise	49
6.14.3	Weitergehende Anforderungen	50
6.14.4	Security-Level	50
7	Grundlegende Anforderung FR 3 – Systemintegrität	50
7.1	Zweck und Beschreibungen des SL-C(SI)	50
7.2	Begründung	50
7.3	SR 3.1 – Kommunikationsintegrität	50
7.3.1	Anforderung	50
7.3.2	Begründung und zusätzliche Hinweise	50

7.3.3	Weitergehende Anforderungen	51
7.3.4	Security-Level.....	51
7.4	SR 3.2 – Schutz vor Schadcode	52
7.4.1	Anforderung.....	52
7.4.2	Begründung und zusätzliche Hinweise	52
7.4.3	Weitergehende Anforderungen	52
7.4.4	Security-Level.....	52
7.5	SR 3.3 – Verifikation der IT-Sicherheitsfunktionalität.....	53
7.5.1	Anforderung.....	53
7.5.2	Begründung und zusätzliche Hinweise	53
7.5.3	Weitergehende Anforderungen	53
7.5.4	Security-Level.....	53
7.6	SR 3.4 – Software- und Informationsintegrität	54
7.6.1	Anforderung.....	54
7.6.2	Begründung und zusätzliche Hinweise	54
7.6.3	Weitergehende Anforderungen	54
7.6.4	Security-Level.....	54
7.7	SR 3.5 – Eingabevalidierung.....	54
7.7.1	Anforderung.....	54
7.7.2	Begründung und zusätzliche Hinweise	54
7.7.3	Weitergehende Anforderungen	55
7.7.4	Security-Level.....	55
7.8	SR 3.6 – Vorbestimmte Zustände der Ausgänge.....	55
7.8.1	Anforderung.....	55
7.8.2	Begründung und zusätzliche Hinweise	55
7.8.3	Weitergehende Anforderungen	55
7.8.4	Security-Level.....	55
7.9	SR 3.7 – Fehlerbehandlung	55
7.9.1	Anforderung.....	55
7.9.2	Begründung und zusätzliche Hinweise	56
7.9.3	Weitergehende Anforderungen	56
7.9.4	Security-Level.....	56
7.10	SR 3.8 – Sitzungsintegrität.....	56
7.10.1	Anforderung.....	56
7.10.2	Begründung und zusätzliche Hinweise	56
7.10.3	Weitergehende Anforderungen	56
7.10.4	Security-Level.....	57
7.11	SR 3.9 – Schutz von Prüfinformationen	57
7.11.1	Anforderung.....	57

7.11.2	Begründung und zusätzliche Hinweise	57
7.11.3	Weitergehende Anforderungen	57
7.11.4	Security-Level	57
8	Grundlegende Anforderung FR 4 – Vertraulichkeit der Daten	57
8.1	Zweck und Beschreibungen des SL-C(DC)	57
8.2	Begründung	58
8.3	SR 4.1 – Vertraulichkeit von Informationen	58
8.3.1	Anforderung	58
8.3.2	Begründung und zusätzliche Hinweise	58
8.3.3	Weitergehende Anforderungen	59
8.3.4	Security-Level	59
8.4	SR 4.2 – Dauerhaftigkeit von Informationen	59
8.4.1	Anforderung	59
8.4.2	Begründung und zusätzliche Hinweise	59
8.4.3	Weitergehende Anforderungen	59
8.4.4	Security-Level	60
8.5	SR 4.3 – Verwendung von Verschlüsselung	60
8.5.1	Anforderung	60
8.5.2	Begründung und zusätzliche Hinweise	60
8.5.3	Weitergehende Anforderungen	60
8.5.4	Security-Level	60
9	Grundlegende Anforderung FR 5 – Eingeschränkter Datenfluss	61
9.1	Zweck und Beschreibungen des SL-C(RDF)	61
9.2	Begründung	61
9.3	SR 5.1 – Netzaufteilung	61
9.3.1	Anforderung	61
9.3.2	Begründung und zusätzliche Hinweise	61
9.3.3	Weitergehende Anforderungen	62
9.3.4	Security-Level	62
9.4	SR 5.2 – Schutz der Zonengrenze	62
9.4.1	Anforderung	62
9.4.2	Begründung und zusätzliche Hinweise	62
9.4.3	Weitergehende Anforderungen	63
9.4.4	Security-Level	63
9.5	SR 5.3 – Beschränkung der Mensch-zu-Mensch-Kommunikation	63
9.5.1	Anforderung	63
9.5.2	Begründung und zusätzliche Hinweise	63
9.5.3	Weitergehende Anforderungen	64
9.5.4	Security-Level	64

9.6	SR 5.4 – Aufteilung von Anwendungen.....	64
9.6.1	Anforderung.....	64
9.6.2	Begründung und zusätzliche Hinweise	64
9.6.3	Weitergehende Anforderungen	64
9.6.4	Security-Level.....	64
10	Grundlegende Anforderung FR 6 – Rechtzeitige Reaktion auf Ereignisse.....	65
10.1	Zweck und Beschreibungen des SL-C(TRE)	65
10.2	Begründung	65
10.3	SR 6.1 – Zugriffsmöglichkeit auf Ereignisprotokolle.....	65
10.3.1	Anforderung.....	65
10.3.2	Begründung und zusätzliche Hinweise	65
10.3.3	Weitergehende Anforderungen	65
10.3.4	Security-Level.....	66
10.4	SR 6.2 – Kontinuierliche Überwachung.....	66
10.4.1	Anforderung.....	66
10.4.2	Begründung und zusätzliche Hinweise	66
10.4.3	Weitergehende Anforderungen	66
10.4.4	Security-Level.....	66
11	Grundlegende Anforderung FR 7 – Ressourcenverfügbarkeit.....	67
11.1	Zweck und Beschreibungen des SL-C(RA).....	67
11.2	Begründung	67
11.3	SR 7.1 – Schutz gegen DoS-Ereignisse	67
11.3.1	Anforderung.....	67
11.3.2	Begründung und zusätzliche Hinweise	67
11.3.3	Weitergehende Anforderungen	67
11.3.4	Security-Level.....	68
11.4	SR 7.2 – Ressourcenmanagement	68
11.4.1	Anforderung.....	68
11.4.2	Begründung und zusätzliche Hinweise	68
11.4.3	Weitergehende Anforderungen	68
11.4.4	Security-Level.....	68
11.5	SR 7.3 – Datensicherung im Automatisierungssystem (Backup).....	68
11.5.1	Anforderung.....	68
11.5.2	Begründung und zusätzliche Hinweise	68
11.5.3	Weitergehende Anforderungen	69
11.5.4	Security-Level.....	69
11.6	SR 7.4 – Wiederherstellung des Automatisierungssystems	69
11.6.1	Anforderung.....	69
11.6.2	Begründung und zusätzliche Hinweise	69

11.6.3	Weitergehende Anforderungen	69
11.6.4	Security-Level	69
11.7	SR 7.5 – Notstromversorgung.....	69
11.7.1	Anforderung	69
11.7.2	Begründung und zusätzliche Hinweise	70
11.7.3	Weitergehende Anforderungen.....	70
11.7.4	Security-Level	70
11.8	SR 7.6 – Netz- und IT-Sicherheitseinstellungen	70
11.8.1	Anforderung	70
11.8.2	Begründung und zusätzliche Hinweise	70
11.8.3	Weitergehende Anforderungen.....	70
11.8.4	Security-Level	70
11.9	SR 7.7 – Geringste Funktionalität	71
11.9.1	Anforderung	71
11.9.2	Begründung und zusätzliche Hinweise	71
11.9.3	Weitergehende Anforderungen.....	71
11.9.4	Security-Level	71
11.10	SR 7.8 – Verzeichnis der Komponenten eines Automatisierungssystems	71
11.10.1	Anforderung	71
11.10.2	Begründung und zusätzliche Hinweise	71
11.10.3	Weitergehende Anforderungen.....	71
11.10.4	Security-Level	71
Anhang A (informativ) Diskussion des SL-Vektors		72
A.1	Überblick	72
A.2	Security-Level.....	72
A.2.1	Definition	72
A.2.2	SL-Arten	73
A.2.3	Anwendung der Security-Level	73
A.3	SL-Vektor	77
A.3.1	Grundlegende Anforderungen.....	77
A.3.2	SL-Festlegung	78
A.3.2.1	Überblick	78
A.3.2.2	SL 0: Keine besonderen Anforderungen oder Schutzmaßnahmen notwendig	78
A.3.2.3	SL 1: Schutz gegen gelegentlichen oder zufälligen Missbrauch	78
A.3.2.4	SL 2: Schutz gegen einen absichtlichen Missbrauch mit einfachen Mitteln und geringem Aufwand, allgemeinen Fertigkeiten und geringer Motivation	79
A.3.2.5	SL 3: Schutz gegen einen absichtlichen Missbrauch mit raffinierten Mitteln und mittlerem Aufwand, IACS-spezifische Fertigkeiten und mittlerer Motivation	79
A.3.2.6	SL 4: Schutz gegen einen absichtlichen Missbrauch mit raffinierten Mitteln und erheblichem Aufwand, IACS-spezifische Fertigkeiten und hoher Motivation	79

	Seite
A.3.3 SL-Vektorformat	80
Anhang B (informativ) Abbildung der Systemanforderungen (SR) und weitergehenden Anforderungen (RE) auf die Security-Level (SL) 1 bis 4 der grundlegenden Anforderungen (FR).....	81
B.1 Überblick.....	81
B.2 SL-Abbildungstabelle.....	81
Literaturhinweise.....	86
Bilder	
Bild 1 – Aufbau der Normenreihe IEC 62443	15
Bild A.1 – Beispiel aus der verfahrenstechnischen Industrie mit Zonen und Conduits	75
Bild A.2 – Beispiel aus der Fertigungsindustrie mit Zonen und Conduits.....	76
Bild A.3 – Schematische Darstellung der Wechselbeziehung der Verwendung verschiedener SL-Arten	77
Tabellen	
Tabelle B.1 – Abbildung von SR und RE auf die FR für SL 1– 4 (1 von 5).....	81

0 Einleitung

0.1 Überblick

ANMERKUNG 1 Diese Norm ist Teil einer Reihe zur IT-Sicherheit industrieller Automatisierungssysteme (IACS). Sie wurde von der Arbeitsgruppe 4, Task Group 2 des ISA 99-Komitees in Zusammenarbeit mit IEC TC 65/WG 10 erarbeitet. Dieses Dokument schreibt die IT-Sicherheitsanforderungen an Automatisierungssysteme entsprechend den sieben grundlegenden Anforderungen nach IEC 62443-1-1 vor und weist dem betrachteten System Security-Level (SL) zu.

ANMERKUNG 2 Das Format dieser Norm folgt den Vorgaben von ISO/IEC, wie sie in den ISO/IEC-Direktiven, Teil 2, beschrieben sind [11].¹ Diese legen sowohl das Format einer Norm als auch die Verwendung von Wörtern wie „muss“, „sollte“, und „darf“ fest. Die Anforderungen in den normativen Abschnitten folgen den Vorgaben nach Anhang H der ISO/IEC-Direktiven.

Die auf dem Gebiet der industriellen Automatisierungstechnik (IACS, en: industrial automation and control system) tätigen Organisationen verwenden in zunehmendem Maße handelsübliche netzwerkfähige Geräte (COTS, en: commercial-off-the-shelf), die kostengünstig, effizient und in hohem Maße automatisiert sind. Ebenfalls werden Automatisierungssysteme in zunehmendem Maße aus wirtschaftlichen Gründen mit Netzen, die nicht zur IACS gehören, verbunden. Solche Geräte, offene Netzwerktechnologien und vermehrte Verbindungsfähigkeit bieten eine zunehmende Gelegenheit für Cyberattacken gegen die Hardware und Software von Automatisierungssystemen. Diese Schwächen können bei installierten Automatisierungssystemen Folgen für die Gesundheit, Sicherheit und Umwelt, die wirtschaftliche Situation und das Ansehen haben.

Organisationen, die zur IT-Sicherheit industrieller Automatisierungssysteme Lösungen aus der kommerziellen Informationstechnik (IT) einsetzen, verstehen möglicherweise die Auswirkungen dieser Entscheidung nicht in vollem Umfang. Obwohl viele kommerzielle IT-Anwendungen und IT-Sicherheitslösungen auch auf IACS angewendet werden können, so muss dies doch in geeigneter Weise erfolgen, um negative Folgen zu vermeiden. Aus diesem Grund muss bei der Festlegung der Systemanforderung auf eine Kombination aus funktionalen Anforderungen und Risikobewertung zurückgegriffen werden, häufig auch unter Beachtung betrieblicher Probleme.

Die IT-Sicherheitsmaßnahmen in einem IACS sollten nicht dazu führen, dass wesentliche Dienste und Funktionen oder gar Notfallprozeduren nicht ausgeführt werden können (einige oft installierte IT-Sicherheitsmaßnahmen haben das Vermögen hierzu). Bei den Sicherheitszielen des IACS stehen die Verfügbarkeit eines Automatisierungssystems, der Schutz und der Betrieb (selbst bei eingeschränkter Betriebsart) der Produktionsanlagen und das Antwortverhalten zeitkritischer Systeme im Vordergrund. Reine IT-Sicherheitsziele legen oft nicht dasselbe Gewicht auf diese Faktoren; sie haben eher den Schutz von Informationen als den von Betriebsmitteln im Auge. Diese andersartigen Zielsetzungen müssen klar als Schutzziele formuliert werden, unabhängig vom erreichten Integrationsgrad der Anlage. Ein wesentlicher Arbeitsschritt im Verlauf der Risikobewertung sollte, wie in IEC 62443-2-1² gefordert, die Benennung derjenigen Dienste und Funktionen sein, die für den Betrieb unverzichtbar sind (beispielsweise könnte in einigen Anlagen die technische Betriebsbetreuung als eine nachrangige Funktion eingestuft werden). In manchen Fällen könnte es dagegen hinnehmbar sein, dass eine IT-Sicherheitsmaßnahme zu einem vorübergehenden Ausfall von nachrangigen Diensten oder Funktionen führt, dagegen sollte ein unverzichtbarer Dienst oder eine unverzichtbare Funktion nicht in abträglicher Weise betroffen sein.

In der vorliegenden Norm wird angenommen, dass ein IT-Sicherheitsprogramm nach IEC 62443-2-1 aufgestellt wurde und betrieben wird. Des Weiteren wird davon ausgegangen, dass ein Sicherheitspatch-Management in Übereinstimmung mit den in IEC/TR 62443-2-3 [5] dargelegten Empfehlungen unter Verwendung der in der vorliegenden Norm dargelegten Systemanforderung und weitergehenden Anforderungen stattfindet. Zusätzlich wird in IEC 62443-3-2 [8] beschrieben, wie in einem Projekt risikobasierte IT-Sicherheitsstufen, die sogenannten Security-Level (SLs), festgelegt werden, die dann dazu herangezogen werden, um Produkte mit geeigneten Fähigkeiten entsprechend dieser Norm auszuwählen. Die vorliegende Norm orientiert sich

¹ Zahlen in rechteckigen Klammern verweisen auf die Literaturhinweise.

² Viele Dokumente der Normenreihe IEC 62443 befinden sich zurzeit in Überarbeitung oder in Erarbeitung.

wesentlich an ISO/IEC 27002 [15] und NIST SP800-53, rev 3 [24] (für eine vollständigere Liste der Quellen siehe [Abschnitt 2](#) und die Literaturhinweise).

Hauptziel der Normenreihe IEC 62443 ist die Bereitstellung eines flexiblen Rahmenwerkes zur erleichterten Behandlung gegenwärtiger und zukünftiger Sicherheitslücken eines IACS und die Anwendung von Abhilfemaßnahmen in einer systematischen und vertretbaren Weise. Es ist wichtig zu verstehen, dass es die Absicht der Reihe der Normen IEC 62443 ist, die Unternehmens-Sicherheit mit Erweiterungen zu versehen, die die Anforderungen an die kommerzielle IT aufnehmen und diese mit den besonderen Anforderungen nach strenger Verfügbarkeit, wie sie von IACS benötigt wird, zusammenzuführen.

0.2 Zweck und Anwenderkreis

Diese Norm richtet sich an die auf dem Gebiet der industriellen Automatisierungstechnik tätigen Betreiber, Systemintegratoren, Produktlieferanten, Dienstleister und gegebenenfalls Genehmigungsstellen. Zu letzteren gehören auch Behörden und Regulierer, deren Zuständigkeit es ist, die Einhaltung von Gesetzen und Vorschriften durch Prüfungen zu überwachen.

Systemintegratoren, Produktlieferanten und Dienstleister werden mit Hilfe dieser Norm bewerten, in wie weit ihre Produkte und Dienstleistungen die funktionalen IT-Sicherheitsfähigkeiten erbringen können, um die Anforderungen des Betreibers, ausgedrückt als SL-T (en: target security level, zu erreichendes SL), zu erreichen. Ebenso wie die Zuweisung von SL-Ts müssen auch die einzelnen Systemanforderungen (SR, en: system requirements) an das Automatisierungssystem und die weitergehenden Anforderungen (RE, en: requirements enhancements) auf den IT-Sicherheitsleitlinien, den Vorgehensweisen und der Risikobewertung des Betreibers im Zusammenhang mit der jeweiligen Anlage beruhen. Dabei ist zu beachten, dass manche Systemanforderungen Voraussetzungen für zulässige Ausnahmen enthalten, etwa wenn ihr Einhalten zur Verletzung fundamentaler betrieblicher Anforderungen eines Automatisierungssystems führen sollte (was Ausgleichsmaßnahmen notwendig machen könnte).

Beim Entwurf eines Automatisierungssystems, das eine Menge von Systemanforderungen zum jeweiligen SL-T einhalten soll, ist es nicht erforderlich, dass jede Komponente des vorgeschlagenen Automatisierungssystems auch jede Systemanforderung auf der in dieser Norm angegebenen Stufe einhalten muss. So können auch Ausgleichsmaßnahmen ergriffen werden, um die von anderen Subsystemen benötigte Funktionalität bereitzustellen und auf der Ebene des Automatisierungssystems dennoch die SL-T-Anforderungen einzuhalten. Die Einbeziehung von Ausgleichsmaßnahmen während der Entwurfsphase sollte durch eine umfassende Dokumentation begleitet werden, so dass das erreichte SL des Automatisierungssystems, SL-A(Automatisierungssystem), die beabsichtigten, sich aus dem Entwurf ergebenden IT-Sicherheitsfähigkeiten vollständig widerspiegelt. Auf ähnliche Weise können während der Zertifizierungsprüfung und während der nach erfolgter Installation durchgeführten Prüfungen Ausgleichsmaßnahmen eingesetzt und dokumentiert werden, um so den SL des Automatisierungssystems zu erreichen.

Der Detaillierungsgrad dieser Norm reicht nicht aus, um eine integrierte IT-Sicherheitsarchitektur zu entwerfen und aufzubauen. Hierzu sind zusätzliche und tiefergehende Analysen in der Systemebene und die Ausarbeitung abgeleiteter Anforderungen notwendig, die Gegenstand weiterer Normen der Reihe IEC 62443 sind, siehe die Einleitung. Man beachte, dass die Bereitstellung von ausreichend detaillierten Spezifikationen für den Aufbau einer IT-Sicherheitsarchitektur, nicht das Ziel dieser Norm ist. Dieses ist vielmehr die Festlegung einer gemeinsamen kleinsten Menge von Anforderungen, um fortschreitend strengere Security-Levels erreichen zu können. Der Entwurf einer diese Anforderungen einhaltenden Architektur obliegt den Systemintegratoren und Produktlieferanten. Sie sind bei diesen Arbeiten frei, individuelle Auswahlen zu treffen, und können sich somit dem Wettbewerb stellen und Innovationen vorantreiben. Diese Norm beschränkt sich ganz bewusst auf die Festlegung funktionaler Anforderungen und legt nicht fest, wie diese erfüllt werden sollten.

0.3 Verwendung innerhalb anderer Teile der Normenreihe IEC 62443

[Bild 1](#) stellt graphisch die Zusammensetzung der Normenreihe IEC 62443 zum Zeitpunkt der Ausarbeitung der vorliegenden Norm dar.

IEC 62443-3-2 verwendet die Systemanforderungen (SR) und die weitergehenden Anforderungen (RE) als Prüfliste. Nachdem das betrachtete System anhand von Zonen und Conduits beschrieben wurde und diesen individuelle SL-Ts zugewiesen wurden, werden die in dieser Norm beschriebenen Systemanforderungen und

weitergehende Anforderungen und deren Abbildung auf SL-Cs zur Zusammenstellung einer Liste von Anforderungen verwendet, die der Entwurf des Automatisierungssystem einhalten muss. Dieser kann dann auf Vollständigkeit geprüft werden, dabei ergeben sich die SL-A.

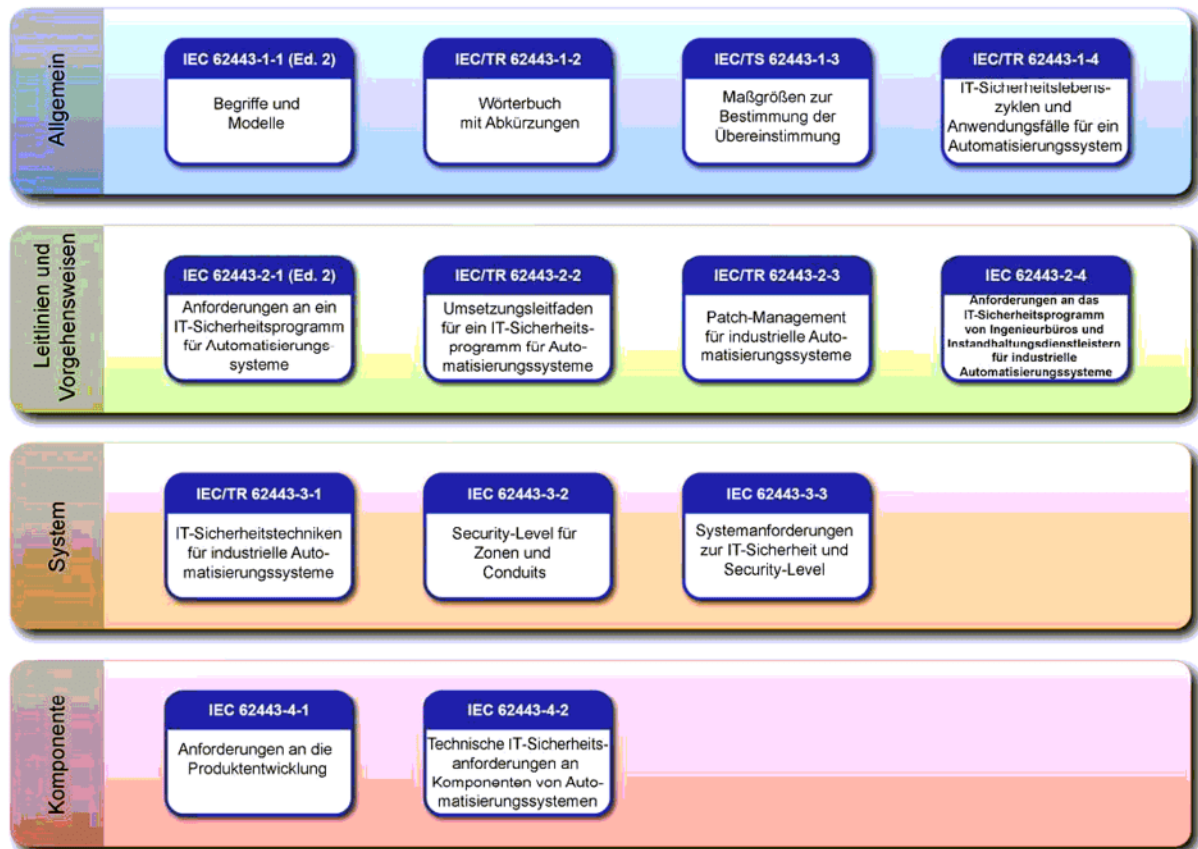


Bild 1 – Aufbau der Normenreihe IEC 62443

IEC/TS 62443-1-3 [2] verwendet die grundlegenden Anforderungen (FR), die Systemanforderungen (SR), die weitergehenden Anforderungen (RE) und deren Abbildung auf die SL-C (SL-C capable, erreichbares SL) als Prüfliste, anhand derer geprüft wird, ob die quantitativen Maßgrößen vollständig spezifiziert sind. Die quantitativen Maßgrößen zur Bestimmung der Übereinstimmung sind abhängig vom Zusammenhang. In Verbindung mit IEC 62443-3-2 werden die vom Betreiber angestrebten SL-T in quantitative Maßgrößen übersetzt; diese können dann bei Systemanalysen und der Abwägung unterschiedlicher Entwürfe zur Entwicklung einer IT-Sicherheitsarchitektur herangezogen werden.

IEC 62443-4-1 [9] beschreibt die Gesamtanforderungen während der Entwicklung von Produkten. Daher wendet sie sich an Produktlieferanten. Die Anforderungen an die IT-Sicherheit der Produkte werden aus der Liste der grundlegenden Anforderungen und der weitergehenden Anforderungen abgeleitet, wie sie in der vorliegenden Norm festgelegt sind. Bei der Entwicklung der Produktfähigkeiten werden die normativen Qualitätsfestlegungen nach IEC 62443-4-1 verwendet werden.

IEC 62443-4-2 [10] enthält Zusammenstellungen abgeleiteter Anforderungen, die eine detaillierte Abbildung der in dieser Norm festgelegten Systemanforderungen auf Subsysteme und Komponenten des betrachteten Systems darstellen. Zum Zeitpunkt der Ausarbeitung der vorliegenden Norm waren in IEC 62443-4-2 folgende Arten von Komponenten aufgeführt: eingebettete Geräte, Host-Geräte, Infrastrukturkomponenten und Anwendungen. So gesehen wendet sich die IEC 62443-4-2 an Verkäufer (Produktlieferant und Dienstleister). Die Anforderungen an die IT-Sicherheit der Produkte werden zunächst aus der Liste der grundlegenden Anforderungen und der weitergehenden Anforderungen (RE) spezifiziert in der vorliegenden Norm, abgeleitet. Zu ihrer Verfeinerung werden IT-Sicherheitsanforderung und -maßgrößen nach IEC 62443-3-2 und IEC/TS 62443-1-3 verwendet.

1 Anwendungsbereich

Diese Norm der Reihe IEC 62443 legt anhand der sieben grundlegenden Anforderungen (FR) nach IEC 62443-1-1 detaillierte technische Systemanforderungen (SR) an IACS fest, einschließlich der Festlegung der Anforderungen zu erreichbaren Security-Level, SL-C(Automatisierungssystem). Diese Anforderungen werden von verschiedene Personen im Bereich der industriellen Automatisierungstechnik angewendet, in dem sie, anhand der festgelegten Zonen und Conduits eines betrachteten Systems, einen angemessenen, zu erreichender Security-Level SL-T(Automatisierungssystem) für ein Schutzobjekt entwickeln.

Nach IEC 62443-1-1 gibt es insgesamt sieben grundlegende Anforderungen:

- a) Identifizierung und Authentifizierung (IAC),
- b) Nutzungskontrolle (UC),
- c) Systemintegrität (SI),
- d) Vertraulichkeit der Daten (DC),
- e) eingeschränkter Datenfluss (RDF),
- f) rechtzeitige Reaktion auf Ereignisse (TRE),
- g) Verfügbarkeit der Ressourcen (RA),

Diese sieben Anforderungen bilden die Grundlage für die erreichbaren SLs eines Automatisierungssystems, die SL-C(Automatisierungssystem). Auf der Ebene des Automatisierungssystems ist die Festlegung der erreichbaren IT-Sicherheit das Ziel dieser Norm und nicht die der erreichten SLs (SL-A) oder zu erreichenden SLs (SL-T), welche außerhalb des Anwendungsbereichs dieser Norm liegen.

Für einen äquivalenten Satz von nicht-technischen, programmbezogenen, erreichbaren Systemanforderungen, die für das vollständige Erreichen eines SL-T eines Automatisierungssystems erforderlich sind, wird auf IEC 62443-2-1 verwiesen.

2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

IEC 62443-1-1:2009, *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*

IEC 62443-2-1, *Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program*

3 Begriffe, Abkürzungen und Erläuterungen

3.1 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach IEC 62443-1-1 und IEC 62443-2-1 und die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- IEC Electropedia: verfügbar unter <http://www.electropedia.org/>
- ISO Online Browsing Platform: verfügbar unter <http://www.iso.org/obp>

ANMERKUNG Viele der nachfolgenden Begriffe entstammen ursprünglich Quellen der International Organization for Standardization (ISO), der International Electrotechnical Commission (IEC) oder des U.S. National Institute of Standards

and Technology (NIST), manchmal mit geringfügigen Änderungen, um die Eignung bei der Festlegung der Sicherheitsanforderungen für Automatisierungssysteme zu verbessern.

3.1.1

Schutzobjekt **Betriebsmittel**

(en: asset)

physikalisches oder logisches Objekt, das für das IACS entweder einen wahrgenommenen oder einen tatsächlichen Wert hat

Anmerkung 1 zum Begriff: In dieser Norm werden unter einem Schutzobjekt alle diejenigen Betrachtungseinheiten verstanden, die im Rahmen des IT-Sicherheitsmanagementsystems des IACS geschützt werden sollten.

3.1.2

Betreiber

(en: asset owner)

für ein oder mehrere IACS verantwortliche Person oder Gesellschaft

Anmerkung 1 zum Begriff: Die Benennung „Betreiber“ wird an Stelle der allgemeinen Benennung „Endanwender“ verwendet.

Anmerkung 2 zum Begriff: Diese Definition umfasst auch alle Komponenten, die Teil des IACS sind.

Anmerkung 3 zum Begriff: Im Zusammenhang mit dieser Norm wird ein Eigner von Anlagevermögen mit dem Betreiber eines IACS gleichgesetzt.

3.1.3

Angriff

(en: attack)

Übergriff auf ein System, der sich aus einer intelligenten Bedrohung herleitet

Anmerkung 1 zum Begriff: Beispielsweise ist eine intelligente Tat der vorsätzlicher Versuch (besonders im Sinne einer Methode oder einer Technik), Dienste zur IT-Sicherheit eines Systems zu umgehen und dessen Sicherheitsvorschriften zu verletzen.

Anmerkung 2 zum Begriff: Es gibt verschiedene allgemein erkannte Angriffsarten:

- Ein „aktiver Angriff“ versucht, die Systemressourcen zu verändern oder ihren Betrieb zu beeinträchtigen.
- Ein „passiver Angriff“ versucht zu lernen oder Informationen aus dem System zu nutzen, er beeinträchtigt aber keine Systemressourcen.
- Ein „Angriff von innen“ ist ein von einer innerhalb der IT-Sicherheitszone liegender Person oder Stelle veranlasster Angriff (von einem Innentäter), beispielsweise von einer Person oder Stelle, der es gestattet ist, auf Systemressourcen zuzugreifen, die diese jedoch in einer Art und Weise nutzt, wie es von den Autorisieren nicht vorgesehen war
- Ein „Angriff von außen“ ist ein von außerhalb der IT-Sicherheitszone veranlasster Angriff, durch einen nicht autorisierten oder illegalen Nutzer (einschließlich eines Innentäters, der von außerhalb der IT-Sicherheitszone aus angreift). Mögliche außenstehende Angreifer reichen von amateurhaften Witzbolden bis zu organisierten Kriminellen, internationalen Terroristen und feindlich gesinnten Regierungen.

3.1.4

Authentifizierung

(en: authentication)

Sicherstellung, dass die von einer Einheit behauptete Eigenschaft korrekt ist

Anmerkung 1 zum Begriff: Authentifizierung ist üblicherweise eine Voraussetzung für die Gewährung des Zugangs zu den Ressourcen eines Automatisierungssystems.

3.1.5

Authentifizierer

(en: authenticator)

Mittel zur Bestätigung der Identität eines Nutzers (menschlicher Nutzer, Softwareprozess oder Gerät)

Anmerkung 1 zum Begriff: Beispielsweise kann ein Passwort oder ein Token als Authentifizierer eingesetzt werden.

3.1.6

Authentizität

(en: authenticity)

Eigenschaft einer Einheit, das zu sein, was sie zu sein vorgibt

Anmerkung 1 zum Begriff: Authentizität wird typischerweise im Zusammenhang mit Vertrauen in die Identität einer Stelle oder die Gültigkeit einer Übertragung, in die Identität einer Nachricht oder des Absenders der Nachricht verwendet.

3.1.7

Automatik

(en: automatic)

Prozess oder Gerät, das bei vorgegebenen Bedingungen ohne menschliches Zutun funktioniert

3.1.8

Verfügbarkeit

(en: availability)

Fähigkeit, einen rechtzeitigen und zuverlässigen Zugang zu den Informationen und zur Funktionalität eines Automatisierungssystems sicherstellen zu können

3.1.9

Kommunikationskanal

(en: communication channel)

bestimmtes logisches oder physikalisches Kommunikationsglied zwischen Schutzobjekten

Anmerkung 1 zum Begriff: Ein Kanal ermöglicht die Herstellung einer Verbindung.

3.1.10

Ausgleichsmaßnahme

(en: compensating countermeasure)

Gegenmaßnahme, die anstelle von oder zusätzlich zu inhärenten IT-Sicherheitsfähigkeiten eingesetzt wird, um einer oder mehreren IT-Sicherheitsanforderungen zu genügen

Anmerkung 1 zum Begriff: Beispiele hierfür sind:

- (Komponenten-Ebene) abschließbarer Schaltschrank, in dem sich eine Steuerung befindet, die für sich alleine nicht ausreichend geschützt wäre;
- (Ebene des Automatisierungssystems/der Zonen) physikalische Zugangskontrolle (Wachpersonal, Tore und Schusswaffen) zum Schutz einer Schaltwarte, um den Zugang auf eine Gruppe bekannter Mitarbeiter zu beschränken; um der technischen Anforderung zu entsprechen, dass das Personal durch das IACS eindeutig identifiziert wird; und
- (Komponenten-Ebene) Eine speicherprogrammierbare Steuerung (SPS) erfüllt die vom Betreiber geforderten Fähigkeiten der Zugangskontrolle nicht, daher stellt der Zulieferer der SPS vor diese einen Firewall und verkauft dies zusammen als ein System.

3.1.11

Genehmigungsbehörde

(en: compliance authority)

rechtlich zuständige Stelle, die über die Angemessenheit einer Beurteilung der IT-Sicherheit, ihrer Umsetzung oder Wirksamkeit entsprechend eines Leitdokumentes zu entscheiden hat

3.1.12

Conduit

(en: conduit)

logische Gruppierung von Kommunikationskanälen, die zwei oder mehr Zonen verbindet, für die gemeinsame IT-Sicherheitsanforderungen gelten

Anmerkung 1 zum Begriff: Ein Conduit (ein Leitungsschutzrohr) darf eine Zone durchqueren, solange die IT-Sicherheit der im Conduit verlaufenden Kanäle durch die Zone nicht beeinträchtigt wird.

3.1.13

Vertraulichkeit

(en: confidentiality)

Bewahrung autorisierter Beschränkungen des Zugangs zu Informationen und deren Offenlegung, dies schließt auch Mittel zum Datenschutz und Schutz eigener Informationen ein

Anmerkung 1 zum Begriff: Wird dieser Begriff im Zusammenhang mit einem IACS verwendet, so bezieht er sich auf den Schutz der in diesem vorhandenen Daten und Informationen vor nicht autorisiertem Zugang.

3.1.14

Verbindung

(en: connection)

zwischen zwei oder mehr Endpunkten hergestellter Zusammenschluss, der den Aufbau einer Sitzung unterstützt

3.1.15

Folge

(en: consequence)

Bedingung oder Zustand, der logischerweise oder natürlicherweise auf ein Ereignis folgt

3.1.16

Automatisierungssystem

(en: control system)

Hardware- und Softwarekomponenten eines IACS

3.1.17

Maßnahme

(en: countermeasure)

Tätigkeit, Gerät, Prozedur oder Technik, durch die eine Bedrohung, eine Sicherheitslücke oder ein Angriff verringert wird, und zwar durch Beseitigen, Verhindern, Verringern des möglichen Schadens oder durch Entdeckung und Bericht, so dass Korrekturmaßnahmen eingeleitet werden können

Anmerkung 1 zum Begriff: Für die deutsche Sprachfassung ohne Belang.

3.1.18

eingeschränkter Betrieb

(en: degraded mode)

durch das Vorhandensein möglicher Fehlzustände, die beim Entwurf des Automatisierungssystems bereits berücksichtigt wurden, gekennzeichneten Betriebszustand

Anmerkung 1 zum Begriff: In einem eingeschränkten Betriebszustand kann das Automatisierungssystem trotz des Versagens eines oder mehrerer Systemelemente weiterhin wesentliche Funktionen erbringen, wie beispielsweise bei Fehlfunktion oder Ausfall von Betriebsmitteln, bei einer durch einen Ausfall verursachten Kommunikationsunterbrechung oder bei absichtlicher Abtrennung des Systems, weil erkannt oder vermutet wird, dass Subsysteme kompromittiert worden sind.

3.1.19

demilitarisierte Zone

(en: demilitarized zone)

gemeinsames, begrenztes Netz von Servern, das zwei oder mehr Zonen miteinander verbindet, um den Datenfluss zwischen diesen kontrollieren zu können

Anmerkung 1 zum Begriff: Demilitarisierte Zonen (DMZs) werden typischerweise eingesetzt, um direkte Verbindungen zwischen verschiedenen Zonen zu vermeiden.

3.1.20

Gerät

(en: device)

Betriebsmittel, das einen oder mehrere Prozessoren enthält und über die Fähigkeit verfügt, zu oder von einem anderen Betriebsmittel Daten und Steuerbefehle zu senden oder zu empfangen

Anmerkung 1 zum Begriff: Beispiele hierfür sind Steuerungen, Mensch-Maschine-Schnittstellen, SPSs, abgesetzte Bediengeräte, Messumformer, Aktoren, Ventile, Switches in Netzwerken.

3.1.21

Umgebung

(en: environment)

umgebende Objekte, Gebiete oder Umstände, die das Verhalten des IACS beeinflussen können und/oder durch dieses beeinflusst werden können

3.1.22

wesentliche Funktion

(en: essential function)

zur Erhaltung der Gesundheit, der Sicherheit, der Umwelt sowie der Verfügbarkeit der zu überwachenden Einrichtung erforderliche Funktion oder Fähigkeit

Anmerkung 1 zum Begriff: Zu den wesentlichen Funktionen gehören unter anderem die sicherheitstechnischen Funktionen (SIF), die Steuerungs- und Regelfunktionen sowie die Fähigkeit des Bedieners, die zu überwachende Einrichtung zu beobachten und zu bedienen. Der Verlust wesentlicher Funktionen kann auch als Verlust der Schutz-, bzw. Steuerungsfunktion, der Regelfunktion und der Überwachungsfunktion bezeichnet werden. In einigen Industriebereichen werden noch weitere Funktionen, wie z. B. die Dokumentation des Produktionsgeschehens als wesentlich eingestuft.

3.1.23

Ereignis

Vorfall

(en: event)

Auftreten von oder Änderung zu einer besonderen Menge von Umständen

Anmerkung 1 zum Begriff: In einem IACS kann dies eine von einer Person (berechtigt oder nicht berechtigt) vorgenommene Handlung, eine in dem Automatisierungssystem festgestellte Veränderung (normal oder anormal) oder eine automatische Reaktion des Automatisierungssystems selbst (normal oder anormal) sein.

3.1.24

Firecall

(en: firecall)

Verfahren der Bereitstellung eines Notzugangs zu einem gesicherten Automatisierungssystem

Anmerkung 1 zum Begriff: In einer Notsituation können nicht berechtigte Nutzer zur Problembeseitigung Zugang zu Schlüsselsystemen erlangen. Mit einem Firecall ist üblicherweise eine Nachschau verbunden, durch die sichergestellt wird, dass der Zugang zur Beseitigung eines Problems korrekt genutzt wurde. Bei diesem Verfahren wird im Allgemeinen eine einmalige Benutzerkennung oder ein Einmalpasswort erteilt.

3.1.25

Bezeichner

(en: identifier)

in einem IT-Sicherheitsbereich eindeutiges Symbol, das eine Einheit, die eine Identität vorgibt oder geltend macht, identifiziert, anzeigt oder benennt

3.1.26

identifizieren

(en: identify)

Zusicherung einer Identität

3.1.27

Auswirkung

(en: impact)

bewertete Auswirkung eines bestimmten Ereignisses

3.1.28

Vorfall

(en: incident)

Ereignis, welches nicht Teil des erwarteten Betriebsverhaltens eines Systems oder Dienstes ist und das zu einer Unterbrechung des vom Automatisierungssystem erbrachten Dienstes oder einer Verminderung von dessen Qualität führt oder führen kann

3.1.29

industrielles Automatisierungssystem

(en: industrial automation and control system)

Zusammenstellung von Personal, Hardware, Software und Vorgehensweisen, die eingebunden sind in den Betrieb eines industriellen Prozesses und dessen sicheren und zuverlässigen Betrieb beeinträchtigen oder beeinflussen kann

3.1.30

Integrität

(en: integrity)

Eigenschaft der Absicherung von Genauigkeit und Vollständigkeit von Schutzobjekten

3.1.31

minimal erforderliche Rechte

(en: least privilege)

Grundprinzip, demgemäß Nutzern (Menschen, Softwareprozesse oder Geräte) die entsprechend ihren Pflichten und Funktionen minimal erforderlichen Rechte zugewiesen werden sollten

Anmerkung 1 zum Begriff: Dieses Prinzip wird in einem IACS üblicherweise mittels einer Menge von Rollen realisiert.

3.1.32

plattformübergreifender Code

(en: mobile code)

von einem abgesetzten, möglicherweise nicht vertrauenswürdigen System, über ein Netz oder mittels mobiler Datenträger übertragenes Programm, welches unverändert in einem lokalen System durch den Empfänger ohne explizite Installation oder Nutzerbestätigung ausgeführt werden kann

Anmerkung 1 zum Begriff: Beispiele plattformübergreifenden Codes sind JavaScript, VBScript, Java Applets, ActiveX-Controls, Flash-Animationen, Shockwave-Movies und Microsoft Office-Makros.

3.1.33

Nichtabstreitbarkeit

(en: non-repudiation)

Fähigkeit, das Auftreten eines behaupteten Ereignisses oder einer Handlung und die verursachende Person oder Stelle nachzuweisen

Anmerkung 1 zum Begriff: Ziel der Nichtabstreitbarkeit ist es, Streitigkeiten über das Auftreten oder Nichtauftreten des Ereignisses oder der Handlung und die Beteiligung von betroffenen Stellen an diesem Ereignis beizulegen.

3.1.34

Produktlieferant

(en: product supplier)

Hersteller eines Hardware- und/oder Softwareprodukts

Anmerkung 1 zum Begriff: Zur besseren Unterscheidung wird diese Benennung anstelle des allgemeinen Wortes „Verkäufer“ verwendet.

3.1.35

Fernzugang

(en: remote access)

Zugriff auf ein Automatisierungssystem durch beliebige Nutzer (Mensch, Softwareprozess oder Gerät), die von außerhalb der angesprochenen IT-Sicherheitszone kommunizieren

3.1.36

Rolle

(en: role)

Menge von zusammenhängenden Verhaltensweisen, Berechtigungen und Verpflichtungen, die allen Nutzern (Menschen, Softwareprozesse oder Geräte) eines IACS zugeordnet sind

Anmerkung 1 zum Begriff: Die Berechtigungen, bestimmte Handlungen vorzunehmen, sind bestimmten Rollen zugeordnet.

3.1.37

sicherheitstechnisches System

(en: safety instrumented system)

System zur Ausführung einer oder mehrerer sicherheitstechnischer Funktionen

3.1.38

Security-Level

(en: security level)

Maß des Vertrauens, dass das IACS von Sicherheitslücken frei ist und in der beabsichtigten Weise funktioniert

Anmerkung 1 zum Begriff: Sicherheitslücken können entweder bei der Entwicklung des IACS entstehen, während seines Lebenszyklus zu irgendeinem Zeitpunkt in dieses hingebacht werden oder sich aus verändernden Bedrohungen ergeben. Bei der Entwicklung entstandene Sicherheitslücken können erst lange nach der Inbetriebnahme erkannt werden, beispielsweise wurde eine Verschlüsselungstechnik ungenügend umgesetzt oder die Leitlinien zur Verwaltung von Nutzerkonten waren ungenügend, wie z. B. das Nicht-Entfernen alter Benutzerkonten. Eingebachte Sicherheitslücken können das Ergebnis eines Patches oder geänderter Leitlinien sein, durch die eine neue Sicherheitslücke geöffnet wird.

3.1.39

Dienstleister

(en: service provider)

Organisation (interne oder externe Organisation, Hersteller usw.), die zugesagt hat, entsprechend einer getroffenen Vereinbarung die Verantwortung zur Erbringung eines bestimmten Unterstützungsdienstes zu übernehmen und, falls angegeben, Lieferungen zu erhalten

Anmerkung 1 zum Begriff: Zur besseren Unterscheidung wird diese Benennung anstelle des allgemeinen Wortes „Verkäufer“ verwendet.

3.1.40

Sitzung

(en: session)

semipermanenter, zustandsbehafteter und interaktiver Informationsaustausch zwischen zwei oder mehr miteinander kommunizierenden Geräten

Anmerkung 1 zum Begriff: Üblicherweise hat eine Sitzung klar definierte Einschalt- und Abschaltverfahren.

3.1.41

Sitzungs-ID

(en: session ID)

Bezeichner, der zum Kenntlichmachen eines bestimmten Sitzungseintrags verwendet wird

3.1.42

Sollwert

(en: set point)

in einer Regelung benannter Zielwert, wobei dieser eine oder mehrere Handlungen im Automatisierungssystem führt

3.1.43

Systemintegrator

(en: system integrator)

Person oder Gesellschaft, die sich darauf spezialisiert hat, Teilsysteme zu einem ganzen System zusammenzufügen, und die dafür sorgt, dass diese Teilsysteme sich entsprechend den Projektspezifikationen verhalten

3.1.44

Bedrohung

(en: threat)

Umstand oder Ereignis mit dem Vermögen, sich durch einen nicht autorisierten Zugriff auf Daten, deren Zerstörung, Offenlegung, Veränderung oder durch Denial-of-Service nachteilig auf den Betrieb (einschließlich Aufgabe, Funktion und Ansehen), auf Vermögenswerte, auf Automatisierungssysteme oder auf Personen auszuwirken

3.1.45

Vertrauen

(en: trust)

Vertrauen, dass man gewiss sein kann, dass eine Operation, die Quelle eines Datenverarbeitungsvorgangs, ein Netz oder ein Softwareprozess sich wie erwartet verhält

Anmerkung 1 zum Begriff: Üblicherweise kann man sagen, dass eine Person oder Stelle einer zweiten vertraut, wenn sie die Annahme trifft, dass sich die zweite wie erwartet verhalten wird.

Anmerkung 2 zum Begriff: Das Vertrauen kann auf einige besondere Funktionen beschränkt sein.

3.1.46

nicht vertrauenswürdig

(en: untrusted)

erfüllt vorher festgelegte Anforderungen zum Vertrauen nicht

Anmerkung 1 zum Begriff: Eine Person oder Stelle kann einfach als nicht vertrauenswürdig erklärt werden.

3.1.47

Zone

(en: zone)

Zusammenfassung logischer oder physikalischer Anlagenteile, für die IT-Sicherheitsanforderungen gemeinsam gelten

Anmerkung 1 zum Begriff: Eine Zone ist klar begrenzt. Die IT-Sicherheitsleitlinien einer Zone werden üblicherweise durch eine Kombination von Verfahren sowohl am Zonenrand als auch innerhalb der Zone durchgesetzt.

3.2 Abkürzungen

Abkürzung	Englische Benennung	Deutsche Benennung
AES	Advanced encryption standard	erweiterter Verschlüsselungsstandard
API	Application programming interface	Schnittstelle für ein Anwendungsprogramm
ASLR	Address space layout randomization	Verwürfelung des Adressraums
BPCS	Basic process control system	Betriebs- und Überwachungseinrichtung
CA	Certification authority	Zertifizierungsstelle
CIP	Critical infrastructure protection	Schutz kritischer Infrastruktur(en)
COTS	Commercial off the shelf	handelsüblich
CRL	Certificate revocation list	Zertifikatsperrliste
DC	Data confidentiality	Datenvertraulichkeit
DEP	Data execution prevention	Datenausführungsverhinderung
DHCP	Dynamic host configuration protocol	Kommunikationsprotokoll zur Zuweisung von Konfigurationen
DMZ	Demilitarized zone	demilitarisierte Zone
DNS	Domain name service	Domänennamendienst
DoS	Denial-of-Service	Ablehnung, einer Stelle, einen Dienst zu erbringen
EICAR	European Institute for Computer Antivirus Research	gemeinnütziger Verein mit dem Ziel Computerviren zu erforschen
EMI	Electromagnetic interference	elektromagnetische Störung
FAT	Factory acceptance testing	Prüfung bei der Werksabnahme
FIPS	[US NIST] <i>Federal Information Processing Standard</i>	Bundesstandard für Informationsverarbeitung der Vereinigten Staaten von Amerika
FR	Foundational requirement	grundlegende Anforderung
FS-PLC	Functional safety PLC	Sicherheitsgerichtete SPS
FTP	File transfer protocol	Dateiübertragungsprotokoll
GLONASS	Global Navigation Satellite System	globales Navigationssatellitensystem <der russischen Föderation>
GPS	Global Positioning System	globales Positionierungssystem
HMI	Human-machine interface	Mensch-Maschine-Schnittstelle
HSE	Health, safety and environmental	Gesundheit, Sicherheit und Umwelt
HTTP	Hypertext transfer protocol	Protokoll zur Übertragung von HTML-Seiten im Internet
HTTPS	HTTP secure	Protokoll zur sicheren Übertragung von HTML-Seiten im Internet
IAC	Identification and authentication control	Identifizierung und Authentifizierung
IACS	Industrial automation and control system(s)	industrielles Automatisierungssystem
IAMS	Instrument asset management system	Instandhaltungssystem für Mess- und Stellgeräte