DIN EN IEC 62443-4-1 (VDE 0802-4-1)

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

ICS 25.040.40; 35.030; 35.240.50

IT-Sicherheit für industrielle Automatisierungssysteme – Teil 4-1: Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung (IEC 62443-4-1:2018); Deutsche Fassung EN IEC 62443-4-1:2018

Security for industrial automation and control systems –
Part 4-1: Secure product development lifecycle requirements
(IEC 62443-4-1:2018);
German version EN IEC 62443-4-1:2018

Sécurité des automatismes industriels et des systèmes de commande –
Partie 4-1: Exigences applicables au cycle de vie de développement sécurisé des produits
(IEC 62443-4-1:2018);
Version allemande EN IEC 62443-4-1:2018

Gesamtumfang 63 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

AVA Documents
Document Sharing Hub

Full document details: DIN EN IEC 62443-4-1:2018-10

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2018-02-19 angenommene Europäische Norm als DIN-Norm ist 2018-10-01.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN EN 62443-4-1 (VDE 0802-4-1):2016-11.

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 and control“ erarbeitet.

Das IEC-Komitee hat entschieden, dass der Inhalt dieser Publikation bis zu dem Datum (stability date) unverändert bleiben soll, das auf der IEC-Website unter „http://webstore.iec.ch“ zu dieser Publikation angegeben ist. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees die Publikation
– bestätigt,
– zurückgezogen,
– durch eine Folgeausgabe ersetzt oder
– geändert.

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.

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 (1 von 2)

Europäisches Dokument	Internationales Dokument	Deutsches Dokument	Klassifikation im VDE-Vorschriftenwerk
EN 61508 (alle Teile)	IEC 61508 (alle Teile)	DIN EN 61508 (VDE 0803) (alle Teile)	VDE 0803
EN 62443 (alle Teile)	IEC 62443 (alle Teile)	DIN EN 62443 (VDE 0802) (alle Teile)	VDE 0802

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62443-4-1:2018-10

Tabelle NA.1 (2 von 2)

Europäisches Dokument	Internationales Dokument	Deutsches Dokument	Klassifikation im VDE-Vorschriftenwerk
–	IEC 62443-2-1	–	–
–	IEC 62443-2-4:2015 + Cor.:2015	DIN IEC 62443-2-4 (VDE 0802-2-4)[a]	VDE 0802-2-4
–	IEC 62443-3-2[a]	–	–
–	IEC 62443-3-3	DIN IEC 62443-3-3 (VDE 0802-3-3)[a]	VDE 0802-3-3
EN 62443-4-2[a]	IEC 62443-4-2[a]	DIN EN 62443-4-2 (VDE 0802-4-2)[a]	VDE 0802-4-2
EN 62740	IEC 62740	DIN EN 62740	–
–	IEC/TS 62443-1-1	–	–
–	IEC/TR 62443-1-2[a]	–	–
–	IEC/TS 62443-1-3[a]	–	–
–	IEC/TR 62443-1-4[a]	–	–
–	IEC/TR 62443-2-2[a]	–	–
–	IEC/TR 62443-2-3	–	–
–	IEC/TR 62443-3-1:2009	–	–
EN ISO 9001	ISO 9001	DIN EN ISO 9001	–
–	ISO/IEC 10746-1	–	–
–	ISO/IEC 10746-2	–	–
–	ISO/IEC 15408-1	–	–
–	ISO/IEC 15408-2	–	–
–	ISO/IEC 15408-3	–	–
EN ISO/IEC 27001	ISO/IEC 27001	DIN EN ISO/IEC 27001	–
EN ISO/IEC 27002	ISO/IEC 27002	DIN EN ISO/IEC 27002	–
–	ISO/IEC 27034 (alle Teile)	–	–
–	ISO/IEC 27036-3	–	–
–	ISO/IEC 29147	–	–
–	ISO/IEC 30111	–	–

[a] In Vorbereitung.

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62443-4-1:2018-10

Nationaler Anhang NB
(informativ)

Literaturhinweise

DIN EN 61508 (VDE 0803) (alle Teile), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme*

DIN EN 62443 (VDE 0802) (alle Teile), *IT-Sicherheit für industrielle Automatisierungssysteme*

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 62740, *Grundursachenanalyse*

DIN EN ISO 9001, *Qualitätsmanagementsysteme – Anforderungen*

DIN EN ISO/IEC 27001, *Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Anforderungen*

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

DIN IEC 62443-2-4 (VDE 0802-2-4) (in Vorbereitung), *IT-Sicherheit für industrielle Automatisierungssysteme – Teil 2-4: Anforderungen an das IT-Sicherheitsprogramm von Dienstleistern für industrielle Automatisierungssysteme (IEC 62443-2-4:2015 + Cor.:2015), mit CD-ROM*

DIN IEC 62443-3-3 (VDE 0802-3-3) (in Vorbereitung), *Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme – Teil 3-3: Systemanforderungen zur IT-Sicherheit und Security-Level*

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62443-4-1:2018-10

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

EN IEC 62443-4-1

März 2018

ICS 35.030; 25.040.40

Deutsche Fassung

IT-Sicherheit für industrielle Automatisierungssysteme – Teil 4-1: Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung

(IEC 62443-4-1:2018)

Security for industrial automation and control systems –
Part 4-1: Secure product development lifecycle requirements
(IEC 62443-4-1:2018)

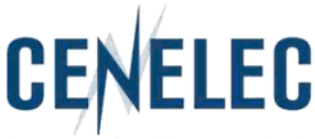
Sécurité des automatismes industriels et des systèmes de commande –
Partie 4-1: Exigences applicables au cycle de vie de développement sécurisé des produits
(IEC 62443-4-1:2018)

Diese Europäische Norm wurde von CENELEC am 2018-02-19 angenommen. 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

© 2018 CENELEC – Alle Rechte der Verwertung, gleich in welcher Form und in welchem Verfahren, sind weltweit den Mitgliedern von CENELEC vorbehalten.

Ref. Nr. EN IEC 62443-4-1:2018 D

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62443-4-1:2018-10

Europäisches Vorwort

Der Text des Dokuments 65/685/FDIS, zukünftige 1. Ausgabe der IEC 62443-4-1, erarbeitet vom IEC/TC 65 „Industrial-process measurement, control and automation“, wurde zur parallelen IEC-CENELEC-Abstimmung vorgelegt und von CENELEC als EN IEC 62443-4-1:2018 angenommen.

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): 2018-11-19

– spätestes Datum, zu dem nationale Normen, die diesem Dokument entgegenstehen, zurückgezogen werden müssen (dow): 2021-02-19

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 62443-4-1:2018 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 62740	ANMERKUNG	Harmonisiert als EN 62470.
IEC 61508 (Reihe)	ANMERKUNG	Harmonisiert in der Reihe EN 61508.
ISO/IEC 27001	ANMERKUNG	Harmonisiert als EN ISO/IEC 27001.
ISO/IEC 27002	ANMERKUNG	Harmonisiert als EN ISO/IEC 27002.
ISO 9001	ANMERKUNG	Harmonisiert als EN ISO 9001.

AVA Documents
Document Sharing Hub

Full document details: DIN EN IEC 62443-4-1:2018-10

Inhalt

Seite

Europäisches Vorwort 2
Einleitung 8
1 Anwendungsbereich 11
2 Normative Verweisungen 11
3 Begriffe, Abkürzungen, Akronyme und Vereinbarungen 11
3.1 Begriffe 11
3.2 Abkürzungen und Akronyme 18
3.3 Vereinbarungen 18
4 Allgemeine Grundsätze 19
4.1 Ziele 19
4.2 Reifegradmodell 20
5 Ansatz 1 – Verwaltung der IT-Sicherheit 22
5.1 Zweck 22
5.2 SM-1: Entwicklungsprozess 22
5.2.1 Anforderung 22
5.3 Begründung und zusätzliche Leitfäden 22
5.4 SM-2: Kennzeichnung von Verantwortlichkeiten 23
5.4.1 Anforderung 23
5.4.2 Begründung und zusätzliche Leitfäden 23
5.5 SM-3: Kennzeichnung der Anwendbarkeit 23
5.5.1 Anforderung 23
5.5.2 Begründung und zusätzliche Leitfäden 23
5.6 SM-4: Fachkenntnisse im Hinblick auf die IT-Sicherheit 24
5.6.1 Anforderung 24
5.6.2 Begründung und zusätzliche Leitfäden 24
5.7 SM-5: Prozesseingrenzung 24
5.7.1 Anforderung 24
5.7.2 Begründung und zusätzliche Leitfäden 24
5.8 SM-6: Integrität von Dateien 24
5.8.1 Anforderung 24
5.8.2 Begründung und zusätzliche Leitfäden 25
5.9 SM-7: IT-Sicherheit der Entwicklungsumgebung 25
5.9.1 Anforderung 25
5.9.2 Begründung und zusätzliche Leitfäden 25
5.10 SM-8: Überwachung privater Schlüssel 25
5.10.1 Anforderung 25
5.10.2 Begründung und zusätzliche Leitfäden 25

AVA Documents
Document Sharing Hub

Full document details: DIN EN IEC 62443-4-1:2018-10

Seite

5.11 SM-9: Anforderungen an die IT-Sicherheit von extern bereitgestellten Komponenten ... 25
5.11.1 Anforderung ... 25
5.11.2 Begründung und zusätzliche Leitfäden ... 26
5.12 SM-10: Kundenspezifische Komponenten von Fremdanbietern ... 26
5.12.1 Anforderung ... 26
5.12.2 Begründung und zusätzliche Leitfäden ... 26
5.13 SM-11: Bewertung und Behandlung sicherheitsbezogener Probleme ... 27
5.13.1 Anforderung ... 27
5.13.2 Begründung und zusätzliche Leitfäden ... 27
5.14 SM-12: Prozessverifikation ... 27
5.14.1 Anforderung ... 27
5.14.2 Begründung und zusätzliche Leitfäden ... 27
5.15 SM-13: Ständige Verbesserung ... 27
5.15.1 Anforderung ... 27
5.15.2 Begründung und zusätzliche Leitfäden ... 27
6 Ansatz 2 – Spezifikation der IT-Sicherheitsanforderungen ... 29
6.1 Zweck ... 29
6.2 SR-1: IT-Sicherheitsumfeld des Produkts ... 29
6.2.1 Anforderung ... 29
6.2.2 Begründung und zusätzliche Leitfäden ... 29
6.3 SR-2: Bedrohungsmodell ... 30
6.3.1 Anforderung ... 30
6.3.2 Begründung und zusätzliche Leitfäden ... 30
6.4 SR-3: IT-Sicherheitsanforderungen für das Produkt ... 31
6.4.1 Anforderung ... 31
6.4.2 Begründung und zusätzliche Leitfäden ... 31
6.5 SR-4: Anforderungen an das IT-Sicherheitsumfeld des Produkts ... 31
6.5.1 Anforderung ... 31
6.5.2 Begründung und zusätzliche Leitfäden ... 31
6.6 SR-5: Überblick über IT-Sicherheitsanforderungen ... 32
6.6.1 Anforderung ... 32
6.6.2 Begründung und zusätzliche Leitfäden ... 32
7 Ansatz 3 – IT-Sicherheit durch den Entwurf ... 32
7.1 Zweck ... 32
7.2 SD-1: Grundsätze für einen gesicherten Entwurf ... 32
7.2.1 Anforderung ... 32
7.2.2 Begründung und zusätzliche Leitfäden ... 33
7.3 SD-2: Entwurf eines Defense-in-Depth-Konzepts ... 34
7.3.1 Anforderung ... 34

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62443-4-1:2018-10

Seite

7.3.2 Begründung und zusätzliche Leitfäden 34
7.4 SD-3: Entwurfsprüfung der IT-Sicherheit 34
7.4.1 Anforderung 34
7.4.2 Begründung und zusätzliche Leitfäden 35
7.5 SD-4: Bewährte Verfahren des gesicherten Entwurfs 35
7.5.1 Anforderung 35
7.5.2 Begründung und zusätzliche Leitfäden 35
8 Ansatz 4 – Gesicherte Implementierung 36
8.1 Zweck 36
8.2 Anwendbarkeit 36
8.3 SI-1: Überprüfung der gesicherten Implementierung 36
8.3.1 Anforderung 36
8.3.2 Begründung und zusätzliche Leitfäden 36
8.4 SI-2: Codierungsnormen für IT-Sicherheit 37
8.4.1 Anforderung 37
8.4.2 Begründung und zusätzliche Leitfäden 37
9 Ansatz 5 – Verifikations- und Validierungsprüfungen der IT-Sicherheit 37
9.1 Zweck 37
9.2 SVV-1: Prüfung der IT-Sicherheitsanforderungen 38
9.2.1 Anforderung 38
9.2.2 Begründung und zusätzliche Leitfäden 38
9.3 SVV-2: Prüfung der Bedrohungsabschwächung 38
9.3.1 Anforderung 38
9.3.2 Begründung und zusätzliche Leitfäden 38
9.4 SVV-3: Prüfung von Sicherheitslücken 39
9.4.1 Anforderung 39
9.4.2 Begründung und zusätzliche Leitfäden 39
9.5 SVV-4: Eindringprüfung 39
9.5.1 Anforderung 39
9.5.2 Begründung und zusätzliche Leitfäden 39
9.6 SVV-5: Unabhängigkeit der Prüfer 40
9.6.1 Anforderung 40
9.6.2 Begründung und zusätzliche Leitfäden 41
10 Ansatz 6 – Behandlung sicherheitsbezogener Probleme 41
10.1 Zweck 41
10.2 DM-1: Empfang von Meldungen über sicherheitsbezogene Probleme 41
10.2.1 Anforderung 41
10.2.2 Begründung und zusätzliche Leitfäden 41
10.3 DM-2: Überprüfung sicherheitsbezogener Probleme 42

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62443-4-1:2018-10

Seite

10.3.1 Anforderung ... 42
10.3.2 Begründung und zusätzliche Leitfäden ... 42
10.4 DM-3: Bewertung sicherheitsbezogener Probleme ... 42
10.4.1 Anforderung ... 42
10.4.2 Begründung und zusätzliche Leitfäden ... 43
10.5 DM-4: Behandlung sicherheitsbezogener Probleme ... 43
10.5.1 Anforderung ... 43
10.5.2 Begründung und zusätzliche Leitfäden ... 44
10.6 DM-5: Offenlegung sicherheitsbezogener Probleme ... 44
10.6.1 Anforderung ... 44
10.6.2 Begründung und zusätzliche Leitfäden ... 45
10.7 DM-6: Periodische Überprüfung der Behandlungsverfahren für Mängel der IT-Sicherheit ... 45
10.7.1 Anforderung ... 45
10.7.2 Begründung und zusätzliche Leitfäden ... 45
11 Ansatz 7 – Verwaltung von IT-Sicherheits-Updates ... 45
11.1 Zweck ... 45
11.2 SUM-1: Eignung von IT-Sicherheits-Updates ... 46
11.2.1 Anforderung ... 46
11.2.2 Begründung und zusätzliche Leitfäden ... 46
11.3 SUM-2: Dokumentation von IT-Sicherheits-Updates ... 46
11.3.1 Anforderung ... 46
11.3.2 Begründung und zusätzliche Leitfäden ... 46
11.4 SUM-3: Dokumentation der IT-Sicherheits-Updates für abhängige Komponenten oder Betriebssysteme ... 47
11.4.1 Anforderung ... 47
11.4.2 Begründung und zusätzliche Leitfäden ... 47
11.5 SUM-4: Auslieferung von IT-Sicherheits-Updates ... 47
11.5.1 Anforderung ... 47
11.5.2 Begründung und zusätzliche Leitfäden ... 47
11.6 SUM-5: Rechtzeitige Auslieferung von IT-Sicherheitspatches ... 47
11.6.1 Anforderung ... 47
11.6.2 Begründung und zusätzliche Leitfäden ... 48
12 Ansatz 8 – IT-Sicherheitsrichtlinien ... 48
12.1 Zweck ... 48
12.2 SG-1: Defense-in-Depth-Strategie für das Produkt ... 48
12.2.1 Anforderung ... 48
12.2.2 Begründung und zusätzliche Leitfäden ... 48
12.3 SG-2: Maßnahmen des Defense-in-Depth-Konzepts, die von der Umgebung zu erwarten sind ... 49

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62443-4-1:2018-10

Seite

12.3.1 Anforderung 49
12.3.2 Begründung und zusätzliche Leitfäden 49
12.4 SG-3: Richtlinien für die Härtung der IT-Sicherheit 49
12.4.1 Anforderung 49
12.4.2 Begründung und zusätzliche Leitfäden 50
12.5 SG-4: Richtlinien für eine gesicherte Entsorgung 50
12.5.1 Anforderung 50
12.5.2 Begründung und zusätzliche Leitfäden 50
12.6 SG-5: Richtlinien für einen gesicherten Betrieb 50
12.6.1 Anforderung 50
12.6.2 Begründung und zusätzliche Leitfäden 50
12.7 SG-6: Richtlinien für die Nutzerkontoverwaltung 51
12.7.1 Anforderung 51
12.7.2 Begründung und zusätzliche Leitfäden 51
12.8 SG-7: Überprüfung der Dokumentation 51
12.8.1 Anforderung 51
12.8.2 Begründung und zusätzliche Leitfäden 51
Anhang A (informativ) Mögliche Maßgrößen 52
Anhang B (informativ) Tabelle der Anforderungen 54
Literaturhinweise 56
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen 59

Bilder

Bild 1 – Teile der Normenreihe IEC 62443 9
Bild 2 – Beispiel für den Anwendungsbereich eines Produktlebenszyklus 10
Bild 3 – Eine Defense-in-Depth-Strategie ist ein Kerngedanke des gesicherten Produktlebenszyklus 20

Tabellen

Tabelle 1 – Reifegrade 21
Tabelle 2 – Beispiele für Aktivitäten der ständigen Verbesserung von SDL 28
Tabelle 3 – Geforderter Grad der Unabhängigkeit der Prüfer von den Entwicklern 40
Tabelle B.1 – Zusammenfassung aller Anforderungen 54

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62443-4-1:2018-10

Einleitung

Das vorliegende Dokument ist Teil einer Normenreihe, die sich mit der IT-Sicherheit für industrielle Automatisierungssysteme (IACS) befasst. Es beschreibt die Anforderungen an den Entwicklungslebenszyklus für Produkte in Bezug auf die IT-Sicherheit der Produkte, die für einen Einsatz in der Umgebung industrieller Automatisierungssysteme vorgesehen sind, und enthält einen Leitfaden für die Einhaltung der für jedes Element beschriebenen Anforderungen.

Dieses Dokument wurde in großen Teilen nach „Secure Development Life-cycle Assessment (SDLA) – Certification Requirements“ [26][1] erarbeitet, welches vom ISA Security Compliance Institute (ISCI) entwickelt wurde. Dabei ist zu beachten, dass das SDLA-Verfahren auf folgende Quellen gestützt wurde:

– ISO/IEC 15408-3 (Common Criteria) [18];
– Open Web Application Security Project (OWASP) Comprehensive, Lightweight Application Security Process (CLASP) [36];
– The Security Development Life-cycle by Michael Howard and Steve Lipner [43];
– IEC 61508 Functional safety of electrical/electronic/ programmable electronic safety-related systems [24], und
– RCTA DO-178B Software Considerations in Airborne Systems and Equipment Certification [28].

Alle angegebenen Dokumente können als Quellen für das vorliegende Dokument angesehen werden.

Das vorliegende Dokument ist Teil der Normenreihe IEC 62443, die IT-Sicherheitsanforderungen für Entwickler beliebiger Produkte für industrielle Automatisierungssysteme beinhaltet, sofern die IT-Sicherheit von Belang ist.

Bild 1 veranschaulicht die Beziehung der verschiedenen Teile von IEC 62443, die zum Zeitpunkt der Zirkulation dieses Dokuments vorlagen bzw. geplant waren. Die normativen Dokumente sind in der Liste der normativen Verweisungen in Abschnitt 2 aufgeführt und die Dokumente, die nur informativ angewendet werden oder in Vorbereitung sind, sind in den Literaturhinweisen enthalten.

[1] Ziffern in eckigen Klammern verweisen auf die Literaturhinweise.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62443-4-1:2018-10

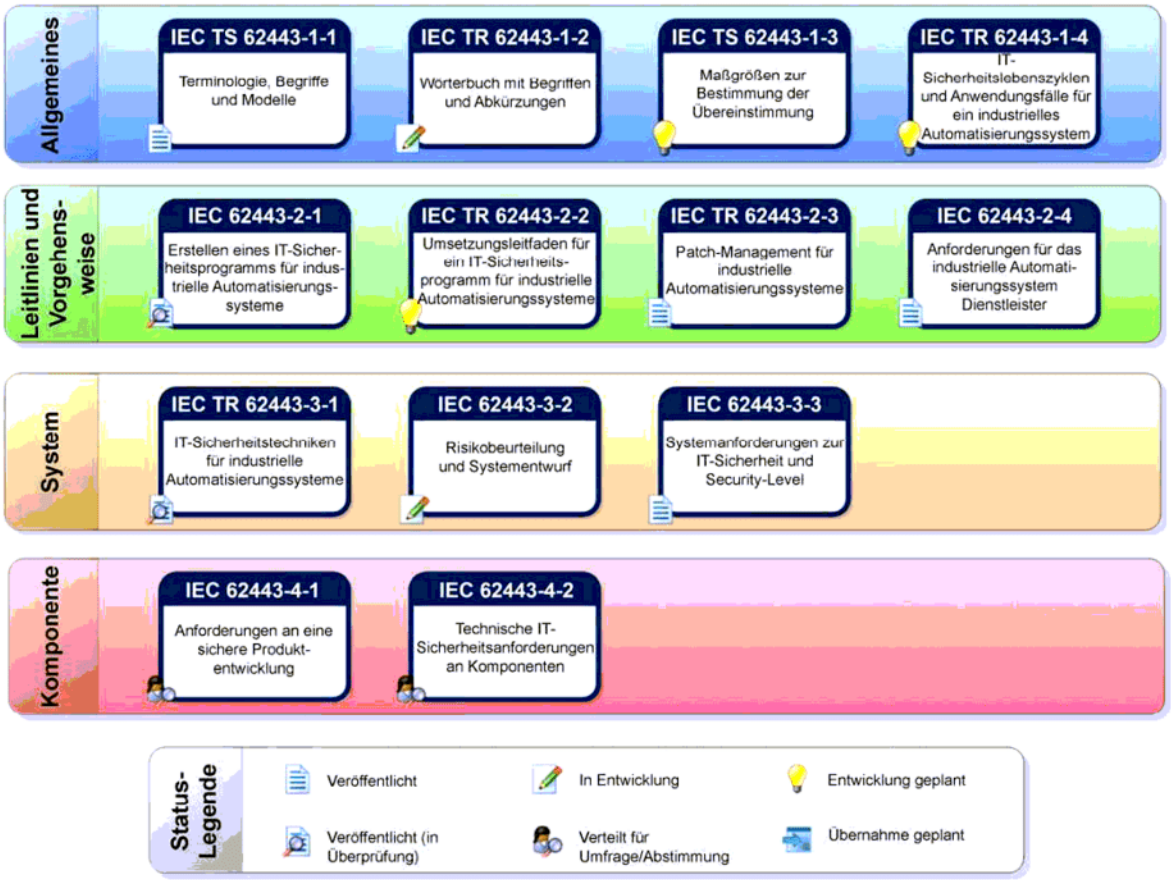


Bild 1 – Teile der Normenreihe IEC 62443

Bild 2 veranschaulicht, wie die entwickelten Produkte mit den in IEC 62443-2-4 definierten Instandhaltungs- und Integrationsfähigkeiten und mit ihrem Betrieb durch den Betreiber in Verbindung stehen. Der Hersteller entwickelt Produkte mithilfe eines mit dem vorliegenden Dokument übereinstimmenden Prozesses. Diese Produkte dürfen eine einzelne Komponente wie eine eingebettete Steuerung sein oder eine Gruppe von Komponenten, die als System oder Teilsystem zusammenwirken. Die Produkte werden dann in der Regel von einem Systemintegrator mit einem Prozess nach IEC 62443-2-4 in eine Automatisierungslösung integriert. Anschließend wird die Automatisierungslösung an einem bestimmten Standort installiert und Teil des industriellen Automatisierungssystems (IACS). Einige dieser Fähigkeiten beziehen sich auf die in IEC 62443-3-3 [10] festgelegten IT-Sicherheitsmaßnahmen, die vom Dienstleister in der Automatisierungslösung sicher unterstützt werden (entweder als Produktmerkmale oder als Kompensationsmechanismen). Das vorliegende Dokument betrifft nur den für die Entwicklung des Produkts angewendeten Prozess; es ist nicht auf den Entwurf, die Installation oder den Betrieb der Automatisierungslösung oder des IACS ausgerichtet.

In Bild 2 wird die Automatisierungslösung mit einem oder mehreren Teilsystem(en) und wahlfreien Zusatzkomponenten wie einer hochentwickelten Steuerung dargestellt. Die mit Strichlinien umrandeten Felder geben an, dass diese Komponenten wahlfrei sind.

ANMERKUNG 1 Automatisierungslösungen bestehen in der Regel aus einem einzelnen Produkt, sie sind aber nicht darauf beschränkt. In manchen Industrien liegt möglicherweise eine hierarchische Produktstruktur vor. Im Allgemeinen setzt sich die Automatisierungslösung unabhängig von der Bauform des Produkts aus einer Menge von Hardware und Softwareelementen zusammen, mit denen ein physikalischer Prozess (z. B. ein kontinuierlicher Prozess oder ein Herstellungsprozess) nach den Festlegungen des Betreibers gesteuert wird.

ANMERKUNG 2 Wenn ein Dienstleister Produkte für den Einsatz in Automatisierungslösungen bereitstellt, übernimmt er in dieser grafischen Darstellung die Rolle eines Herstellers.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62443-4-1:2018-10

ANMERKUNG 3 Wenn ein Dienstleister Produkte für den Einsatz in Automatisierungslösungen bereitstellt, übernimmt er in dieser grafischen Darstellung die Rolle eines Herstellers.

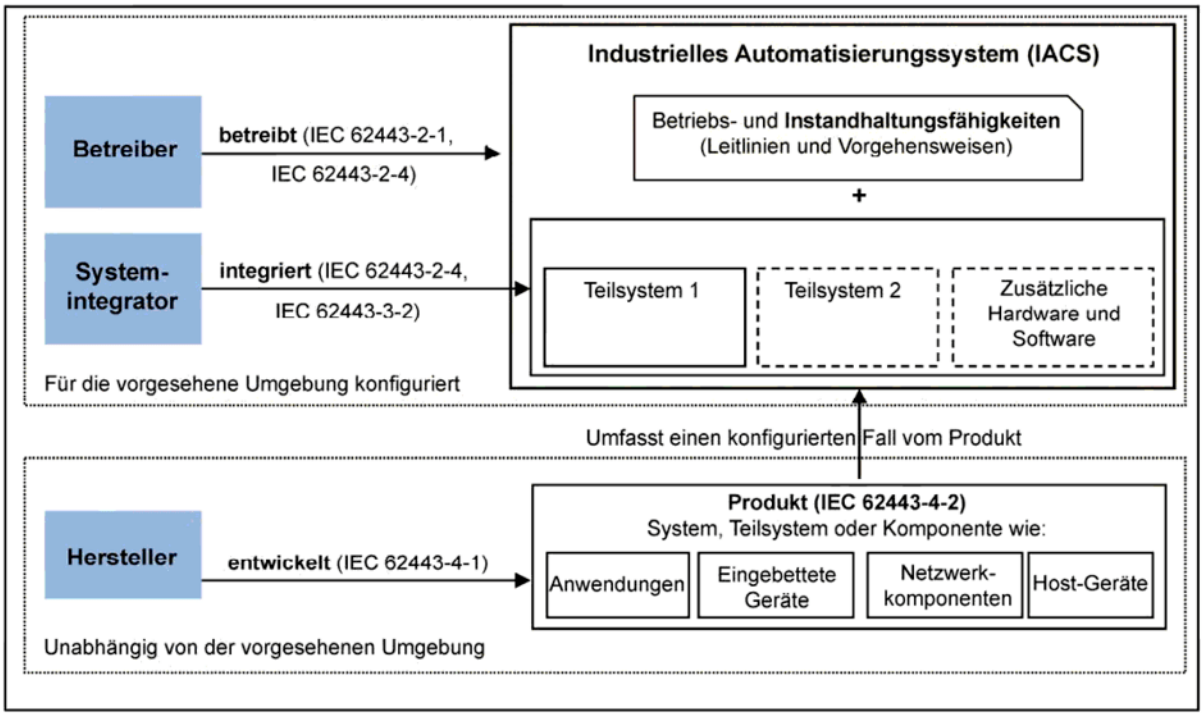


Bild 2 – Beispiel für den Anwendungsbereich eines Produktlebenszyklus

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62443-4-1:2018-10

1 Anwendungsbereich

Dieser Teil von IEC 62443 legt Anforderungen an den gesicherten Entwicklungsprozess für Produkte fest, die in industriellen Automatisierungssystemen eingesetzt werden. Er definiert einen gesicherten Entwicklungslebenszyklus (SDL) zum Zweck der Entwicklung und Instandhaltung sicherer Produkte. Dieser Lebenszyklus umfasst die Definition von IT-Sicherheitsanforderungen, einen gesicherten Entwurf, eine sichere Implementierung (einschließlich Programmierrichtlinien), Verifikation und Validierung, eine Mängelbehandlung, ein Patch-Management und das Ende des Produktlebenszyklus. Diese Anforderungen können für neue oder vorhandene Prozesse der Entwicklung, der Instandhaltung und Pflege sowie der Zurückziehung von Hardware, Software oder Firmware für neue oder vorhandene Produkte angewendet werden. Diese Anforderungen gelten für den Entwickler und Instandhalter des Produkts, jedoch nicht für den Integrator oder einen Produktanwender. Eine Zusammenfassung der Anforderungen des vorliegenden Dokuments ist in Anhang B enthalten.

2 Normative Verweisungen

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).

IEC 62443-2-4:2015, *IT-Sicherheit für industrielle Automatisierungssysteme – Part 2-4:* Security *program requirements for IACS service providers*
IEC 62443-2-4:2015/AMD1:2017

3 Begriffe, Abkürzungen, Akronyme und Vereinbarungen

3.1 Begriffe

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

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

– IEC Electropedia: unter http://www.electropedia.org/
– ISO Online Browsing Platform: unter http://www.iso.org/obp

3.1.1
Missbrauchsfall
(en: abuse case)
Prüffall zur Durchführung einer negativen Arbeitsweise eines Anwendungsfalls

Anmerkung 1 zum Begriff: Missbrauchsprüfungen sind nachgebildete Angriffe, die häufig auf dem Bedrohungsmodell beruhen. Ein Missbrauchsfall ist ein Typ einer vollständigen Wechselwirkung zwischen einem System und einem oder mehreren Akteur(en), wobei die Ergebnisse der Wechselwirkung bewusst schädlich für das System, einen der Akteure oder eine der Interessengruppen im System sind.

3.1.2
Zugriffskontrolle
(en: access control)
<Schutz> Schutz einer Systemressource gegen nicht autorisierten Zugriff

[2] In Beratung.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62443-4-1:2018-10

3.1.3
Zugriffskontrolle
(en: access control)
<Prozess> Vorgang, der die Verwendung von Systemressourcen gemäß einer Sicherheitsleitlinie regelt und der ausschließlich von dazu berechtigten Stellen gemäß dieser Leitlinie erlaubt wird

Anmerkung 1 zum Begriff: Zugriffskontrolle umfasst die Anforderungen an die Identifizierung und Authentifikation, die in anderen Teilen der Normenreihe IEC 62443 festgelegt sind.

3.1.4
Administrator
(en: administrator)
Nutzer, der zur Verwaltung von IT-Sicherheitsrichtlinien und -fähigkeiten für ein Produkt oder ein System autorisiert ist

3.1.5
Schutzobjekt
(en: asset)
physikalisches oder logisches Objekt im Eigentum oder in der Obhut einer Organisation, das für diese Organisation entweder einen wahrgenommenen oder einen tatsächlichen Wert hat

Anmerkung 1 zum Begriff: In diesem spezifischen Fall ist ein Schutzobjekt ein Objekt, das Teil eines IACS ist.

3.1.6
Betreiber
(en: asset owner)
Person oder Organisation, die für ein oder mehrere IACS verantwortlich ist

3.1.7
Angriffsfläche
(en: attack surface)
physikalische und funktionale Schnittstellen eines Systems, die zugänglich sind und dadurch von einem Angreifer möglicherweise ausgenutzt werden können

3.1.8
Ereignisprotokoll
(en: audit log)
Ereignisprotokoll, das einen höheren Integritätsschutz erfordert, als ihn typische Ereignisprotokolle bieten

Anmerkung 1 zum Begriff: Auditprotokolle dienen dem Schutz gegen Ansprüche, die aus der Nichtanerkennung der Verantwortlichkeit für eine Aktion resultieren.

3.1.9
Authentifikation
(en: authentication)
Bereitstellung einer Zusicherung, dass die Behauptung eines Merkmals einer Identität ordnungsgemäß ist

Anmerkung 1 zum Begriff: Nicht alle Identitätsnachweise zur Authentifikation einer Identität werden auf die gleiche Weise erzeugt. Die Vertrauenswürdigkeit des Identitätsnachweises wird durch den konfigurierten Authentifikationsmechanismus bestimmt. Auf Hardware oder Software basierende Mechanismen können Nutzer dazu zwingen, ihre Identität nachzuweisen, bevor auf Daten auf einem Gerät zugegriffen werden kann. Ein typisches Beispiel ist der gewöhnliche Nachweis der Identität eines Nutzers durch einen Identitätsanbieter.

Anmerkung 2 zum Begriff: Authentifikation schließt sowohl die Bestätigung menschlicher Nutzer als auch nichtmenschlicher Nutzer, z. B. Geräte oder Prozesse, ein.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62443-4-1:2018-10

3.1.10
Automatisierungslösung
(en: automation solution)
Automatisierungssystem und weitere zusätzliche Hardware- und Softwarekomponenten, die zum Betrieb in einem IACS aufgebaut und konfiguriert wurden

Anmerkung 1 zum Begriff: Der Begriff „Automatisierungslösung" wird in diesem Teil der Normenreihe IEC 62443 als ein Eigenname verwendet.

Anmerkung 1 zum Begriff: Der Unterschied zwischen dem Automatisierungssystem und der Automatisierungslösung besteht darin, dass das Automatisierungssystem in den Entwurf der Automatisierungslösung eingebunden wird (z. B. eine bestimmte Anzahl von Arbeitsplatzrechnern, Steuerungen und Geräten in einer spezifischen Konfiguration), der dann umgesetzt wird. Die sich so ergebende Konfiguration wird dann als die Automatisierungslösung bezeichnet.

Anmerkung 3 zum Begriff: Die Automatisierungslösung kann Komponenten verschiedener Hersteller einschließlich des Herstellers des Automatisierungssystems umfassen.

3.1.11
verbotene Funktion
(en: banned function)
Softwaremethode, die nicht mehr für die Anwendung in der Software empfohlen wird, weil besser gesicherte Versionen mit weniger Anfälligkeit für einen Missbrauch vorhanden sind

Anmerkung 1 zum Begriff: Verbotene Funktionen werden mitunter als verbotene Methoden oder verbotene Anwendungsprogrammierschnittstellen (API) bezeichnet.

3.1.12
bewährte Verfahren
(en: best practices)
Richtlinien für ein gesichertes Auslegen, Entwickeln, Prüfen, Instandhalten oder Zurückziehen von Produkten, für welche der Hersteller bestimmt hat, dass sie von der Sicherheitsgemeinschaft sowie der Gemeinschaft für industrielle Automatisierung gemeinsam empfohlen werden

BEISPIEL Minimal erforderliche Rechte, einfache Schutzmechanismen und Minimum an gemeinsamen Mechanismen.

3.1.13
Komponente
eines der Teile, die ein Produkt oder System bilden

Anmerkung 1 zum Begriff: Eine Komponente darf eine Hardware oder eine Software sein und darf in weitere Komponenten unterteilt sein.

3.1.14
Konfigurationsverwaltung
(en: configuration management)
Einordnung der Komponenten eines entstehenden Systems zur Kontrolle von Änderungen dieser Komponenten und Erhaltung der Kontinuität und Rückverfolgbarkeit während des gesamten Lebenszyklus

3.1.15
Defense-in-Depth-Konzept
(en: defense in depth)
Ansatz zur Verteidigung des Systems gegen einen beliebigen bestimmten Angriff mit Anwendung mehrerer unabhängiger Methoden

Anmerkung 1 zum Begriff: Ein Defense-in-Depth-Konzept bedingt selbst bei Einzelsystemen IT-Sicherheits- und Erkennungsschichten und hat folgende Merkmale:

– beruht auf dem Grundgedanken, dass jede Schutzmaßnahme überwunden werden kann und wahrscheinlich auch überwunden wird;

AVA Documents
Document Sharing Hub
Full document details: DIN EN IEC 62443-4-1:2018-10

- Angreifer müssen jede Schicht überwinden oder umgehen, ohne dabei erkannt zu werden;
- eine Schwachstelle in einer Schicht kann durch die Fähigkeiten der anderen Schichten abgeschwächt werden;
- die IT-Sicherheit des Systems wird zu einem Satz von Schichten innerhalb der gesamten IT-Netzsicherheit; und
- jede Schicht sollte eigenständig sein und nicht auf der gleichen Funktionalität wie die anderen Schichten beruhen, und sollte nicht die gleichen Ausfallarten wie diese aufweisen.

3.1.16
abhängige Komponente
(en: dependent component)
externe Produktkomponente, von der das Produkt abhängt

BEISPIEL Java-Laufzeitumgebung oder ein Treiber.

Anmerkung 1 zum Begriff: Dazu gehören sowohl Hardware als auch Software.

3.1.17
abgelehnte Funktion
(en: deprecated function)
Softwaremethode, die zwar unterstützt wird, deren Nutzung aber nicht mehr empfohlen wird

Anmerkung 1 zum Begriff: Methoden werden grundsätzlich abgelehnt, bevor sie obsolet (aus dem vom Hersteller zur Verfügung gestellten Funktionssatz gelöscht) werden. Abgelehnte Funktionen werden mitunter als abgelehnte Methoden oder abgelehnte API bezeichnet.

3.1.18
extern bereitgestellte Komponente
(en: externally provides component)
in das Produkt integrierte Komponente, die von einer externen Organisation entwickelt wurde und nicht speziell für einen Hersteller entwickelt wurde

Anmerkung 1 zum Begriff: Beispiele schließen gekaufte Software und Open-Source-Software ein.

3.1.19
Fuzzing
Fuzz-Prüfung
(en: fuzz testing)
Prozess der Erzeugung verfälschter oder unerwarteter Daten oder Aufruffolgen zur Eingabe in die zu prüfende Einheit für den Nachweis, ordnungsgemäß

3.1.20
industrielles Automatisierungssystem
(en: industrial automation und control system, IACS)
Zusammenstellung von Personal, Hardware, Software, Vorgehensweisen und Leitlinien, die in den Betrieb eines industriellen Prozesses eingebunden sind und dessen sicheren und zuverlässigen Betrieb beeinträchtigen oder beeinflussen können

Anmerkung 1 zum Begriff: Das IACS darf Komponenten umfassen, die nicht am Standort des Betreibers errichtet sind.

Anmerkung 2 zum Begriff: Die Definition des IACS wurde IEC 62443-3-3 [10] entnommen und ist in Bild 2 dargestellt.

3.1.21
Patch-Management
(en: patch management)
Bereich der Systemverwaltung, zu dem der Erwerb, die Prüfung und die Installation von Softwarepatches (Codeänderungen) für ein Produkt gehören

Anmerkung 1 zum Begriff: Weitere Informationen können IEC TR 62443-2-3 [7] entnommen werden.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62443-4-1:2018-10

Anmerkung 2 zum Begriff: Das Patch-Management wird auch für den Prozess angewendet, mit dem eingebettete Fremdbibliotheken auf dem aktuellen Stand gehalten werden, bevor ein Produkt freigegeben wird.

3.1.22
Produkt
(en: product)
System, Teilsystem oder Komponente, das bzw. die zur Verwendung durch andere Produkte hergestellt, entwickelt oder weiterverarbeitet wird

Anmerkung 1 zum Begriff: Die Prozesse, die von den im vorliegenden Dokument definierten Ansätzen gefordert werden, sind iterativ auf allen Ebenen des Produktentwurfs (z. B. von der Systemebene bis zur Komponentenebene) anwendbar.

3.1.23
IT-Sicherheitsumfeld des Produkts
(en: product security context)
IT-Sicherheit, die dem Produkt durch die Umgebung (Einsatz beim Betreiber), in der der Einsatz des Produkts vorgesehen ist, geboten wird

Anmerkung 1 zum Begriff: Die IT-Sicherheit, die dem Produkt durch die vorgesehene Umgebung geboten wird, kann die für das Produkt zutreffenden Bedrohungen wirksam einschränken.

3.1.24
Hersteller
(en: product supplier)
Hersteller eines Hardware- und/oder Softwareprodukts

Anmerkung 1 zum Begriff: Zum Hersteller gehört auch die Stelle, die für den Entwurf und die Instandhaltung eines Produkts verantwortlich ist und die über den reinen Produzenten hinausgehen kann (z. B. Integrator).

3.1.25
Produktanwender
(en: product users)
Anwender des Hardware- und/oder Softwareprodukts einschließlich Betreiber, Integratoren und Instandhaltungspersonal, Anbieter anderer Komponenten oder Produkte, welche dieses Produkt wiederverwenden oder enthalten

3.1.26
Aufzeichnung
(en: record)
Dokument, in dem erreichte Ergebnisse oder Nachweise von ausgeführten Aktivitäten angegeben sind

Anmerkung 1 zum Begriff: Der Begriff „Artefakt“ wird häufig gleichbedeutend verwendet.

3.1.27
Regression
(en: regression)
Abänderung an einer Systemkomponente, die Funktionalität, Zuverlässigkeit oder Leistungsfähigkeit nachteilig beeinflusst hat oder zusätzliche Mängel eingebracht hat

3.1.28
Grundursache
(en: root cause)
Auslöser eines Zustands oder einer Ursachenkette, der/die zu einem Ergebnis oder einer Wirkung führt, das/die von Interesse ist

Anmerkung 1 zum Begriff: Diese Schwachstellen resultieren häufig aus der Fehlanwendung bewährter Verfahren.

AVA Documents
Document Sharing Hub
Full document details: DIN EN IEC 62443-4-1:2018-10