DIN EN IEC 62443-2-4 (VDE 0802-2-4)

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 2-4: Anforderungen an das IT-Sicherheitsprogramm von Dienstleistern für industrielle Automatisierungssysteme (IEC 62443-2-4:2015 + Cor.:2015 + A1:2017); Deutsche Fassung EN IEC 62443-2-4:2019 + A1:2019, mit CD-ROM

Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers (IEC 62443-2-4:2015 + Cor.:2015 + A1:2017); German version EN IEC 62443-2-4:2019 + A1:2019, with CD-ROM

Sécurité des automatismes industriels et des systèmes de commande – Partie 2-4: Exigences de programme de sécurité pour les fournisseurs de service IACS (IEC 62443-2-4:2015 + Cor.:2015 + A1:2017); Version allemande EN IEC 62443-2-4:2019 + A1:2019, avec CD-ROM

Gesamtumfang 134 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

AVA Documents Document Sharing Hub

Full document details: DIN EN IEC 62443-2-4:2020-07

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2019-04-03 angenommene Europäische Norm und die am 2019-04-03 angenommene Änderung A1 als DIN-Norm ist 2020-07-01.

Nationales Vorwort

Vorausgegangene Norm-Entwürfe: E DIN IEC 62443-2-4 (VDE 0802-2-4):2017-01 und E DIN IEC 62443-2-4-100 (VDE 0802-2-4-100):2017-09.

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 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 diese Publikation

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

A1 Die Änderung A1 wurde in den Text eingearbeitet und durch eine senkrechte Linie am linken Seitenrand gekennzeichnet.

Tabelle A .1 wird als CD-Rom beigefügt.

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.

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62443-2-4:2020-07

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
EN 61508 (alle Teile)	IEC 61508 (alle Teile)	DIN EN 61508 (VDE 0803) (alle Teile)	VDE 0803
EN 61511-1 (alle Teile)	IEC 61511 (alle Teile)	DIN EN 61511-1 (VDE 0810) (alle Teile)	VDE 0810
EN 62264-1:2013	IEC 62264-1:2013	DIN EN 62264-1:2014-07	–
–	IEC/TS 62351-8:2011	–	–
–	IEC 62443-2-1:2010	–	–
EN 62443-3-2[a]	IEC 62443-3-2[a]	DIN EN 62443-3-2 (VDE 0802-3-2)[a]	VDE 0802-3-2
EN IEC 62443-3-3:2019	IEC 62443-3-3:2013	DIN EN IEC 62443-3-3 (VDE 0802-3-3):2020-01	VDE 0802-3-3
EN IEC 62443-4-1	IEC 62443-4-1[a]	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 IEC 62443-4-2 (VDE 0802-4-2)	VDE 0802-4-2
–	IEC/TS 62443-1-1	–	–
–	IEC/TR 62443-1-2[b]	–	–
–	IEC/TR 62443-1-3[a]	–	–
–	IEC/TR 62443-2-3[a]	–	–
–	IEC TR 62443-4-2-1[a]	–	–
–	ISO/IEC 27036-3	–	–
EN ISO/IEC 30111	ISO/IEC 30111	DIN EN ISO/IEC 30111	–

[a] In Vorbereitung.

[b] In Beratung.

AVA Documents Document Sharing Hub

Full document details: DIN EN IEC 62443-2-4:2020-07

Nationaler Anhang NB
(informativ)

Literaturhinweise

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

DIN EN 61511 (VDE 0810) (alle Teile), *Funktionale Sicherheit – PLT-Sicherheitseinrichtungen für die Prozessindustrie*

DIN EN 62264-1:2014-07, *Integration von Unternehmensführungs- und Leitsystemen – Teil 1: Modelle und Terminologie (IEC 62264-1:2013); Deutsche Fassung EN 62264-1:2013*

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

DIN EN IEC 62443-3-3 (VDE 0802-3-3):2020-01, *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*

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 IEC 62443-4-2 (VDE 0802-4-2), *IT-Sicherheit für industrielle Automatisierungssysteme – Teil 4-2: Technische Sicherheitsanforderungen an Komponenten industrieller Automatisierungssysteme (IACS)*

DIN EN ISO/IEC 30111, *Informationstechnik – IT-Sicherheitsverfahren – Prozesse für die Behandlung von Schwachstellen*

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62443-2-4:2020-07

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

EN IEC 62443-2-4

April 2019

+ A1

April 2019

ICS 35.110; 25.040.40

Deutsche Fassung

IT-Sicherheit für industrielle Automatisierungssysteme – Teil 2-4: Anforderungen an das IT-Sicherheitsprogramm von Dienstleistern für industrielle Automatisierungssysteme

(IEC 62443-2-4:2015 + A1:2017)

Security for industrial automation and control systems –
Part 2-4: Security program requirements for IACS service providers
(IEC 62443-2-4:2015 + A1:2017)

Sécurité des automatismes industriels et des systèmes de commande –
Partie 2-4: Exigences de programme de sécurité pour les fournisseurs de service IACS
(IEC 62443-2-4:2015 + A1:2017)

Diese Europäische Norm wurde von CENELEC am 2019-04-03 und die A1 am 2019-04-03 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

© 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 62443-2-4:2019 + A1:2019 D

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62443-2-4:2020-07

Europäisches Vorwort

Dieses Dokument (EN IEC 62443-2-4:2019) enthält den Text der IEC 62443-2-4:2015, 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 62443-2-4:2015 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 61508 (Reihe)	ANMERKUNG	Harmonisiert in der Reihe als EN 61508.
IEC 61511 (Reihe)	ANMERKUNG	Harmonisiert in der Reihe als EN 61511.
IEC 62264-1:2013	ANMERKUNG	Harmonisiert als EN 62264-1:2013 (nicht modifiziert).
IEC 62443-3-3:2013	ANMERKUNG	Harmonisiert als EN IEC 62443-3-3:2019 (nicht modifiziert).
IEC 62443-4-1	ANMERKUNG	Harmonisiert als EN IEC 62443-4-1.
IEC 62443-4-2	ANMERKUNG	Harmonisiert als EN IEC 62443-4-2.

Europäisches Vorwort zu A1

Dieses Dokument (EN IEC 62443-2-4:2019/A1:2019) enthält den Text der IEC 62443-2-4:2015/A1:2017, 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 Texte dieses Dokuments Patentrechte berühren können. CENELEC ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Anerkennungsnotiz

Der Text der Internationalen Norm IEC 62443-2-4:2015/A1:2017 wurde von CENELEC ohne irgendeine Abänderung als Europäische Norm angenommen.

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62443-2-4:2020-07

Inhalt

Seite

Europäisches Vorwort 2
Europäisches Vorwort zu A1 2
Einleitung 5
1 Anwendungsbereich 6
2 Normative Verweisungen 7
3 Begriffe und Abkürzungen 7
3.1 Begriffe 7
3.2 Abkürzungen 12
4 Orientierung 12
4.1 Anwendung der IEC 62443-2-4 12
4.1.1 Anwendung der IEC 62443-2-4 durch Dienstleister für industrielle Automatisierungssysteme 12
4.1.2 Anwendung von IEC 62443-2-4 durch Betreiber industrieller Automatisierungssysteme 13
4.1.3 Anwendung von IEC 62443-2-4 bei Verhandlungen zwischen Betreibern und Dienstleistern 14
4.1.4 Profile 14
4.1.5 Integratoren 15
4.1.6 Instandhaltungsdienstleister 15
4.2 Reifegradmodell 16
5 Überblick über die Anforderungen 17
5.1 Inhalte 17
5.2 Sortierung und Filterung 18
5.3 Hierarchiemodell nach IEC 62264-1 18
5.4 Anforderungen in Tabellenspalten 18
5.5 Spaltendefinitionen 19
5.5.1 Spalte „Anford.-ID“ 19
5.5.2 Spalte „BR/RE“ 19
5.5.3 Spalte „Bereich“ 20
5.5.4 Spalte „Oberbegriff“ 21
5.5.5 Spalte „Unterbegriff“ 21
5.5.6 Spalte „Dokumentation“ 23
5.5.7 Spalte „Beschreibung der Anforderung“ 23
5.5.8 Spalte „Begründung“ 24
Anhang A (normativ) IT-Sicherheitsanforderungen 25
Literaturhinweise 129

Bilder

Bild 1 – Struktur der Normenreihe IEC 62443 5
Bild 2 – Anwendungsbereich der Fähigkeiten des Dienstleisters 6

AVA Documents
Document Sharing Hub
Full document details: DIN EN IEC 62443-2-4:2020-07

Seite

Tabellen

Tabelle 1 – Reifegrade 17
Tabelle 2 – Spalten 18
Tabelle 3 – Werte der Spalte „Bereich“ 20
Tabelle 4 – Werte der Spalte „Oberbegriff“ 21
Tabelle 5 – Werte der Spalte „Unterbegriff“ 22
Tabelle A.1 – Anforderungen an das IT-Sicherheitsprogramm 25

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62443-2-4:2020-07

Einleitung

Die vorliegende Norm ist der Teil der Normenreihe IEC 62443, der die IT-Sicherheitsanforderungen an Integratoren und Instandhaltungsdienstleister von industriellen Automatisierungssystemen (industrielles Automatisierungssystem) enthält. Sie wurde vom TC 65 ausgearbeitet in Zusammenarbeit mit der International Instrumentation Users Association, abgekürzt WIB, was von ihrem ursprünglichen und jetzt veralteten niederländischen Namen abgeleitet ist, sowie von Mitgliedern des ISA 99-Komitees.

Bild 1 stellt die Zusammensetzung der Normenreihe IEC 62443 zum Zeitpunkt der Ausarbeitung vorliegender Norm dar. Diejenigen Teile, auf die normativ verwiesen wird, sind in Abschnitt 2 aufgeführt, und diejenigen Teile, die nur den Informationen dienen oder noch in Beratung sind, in den Literaturhinweisen.

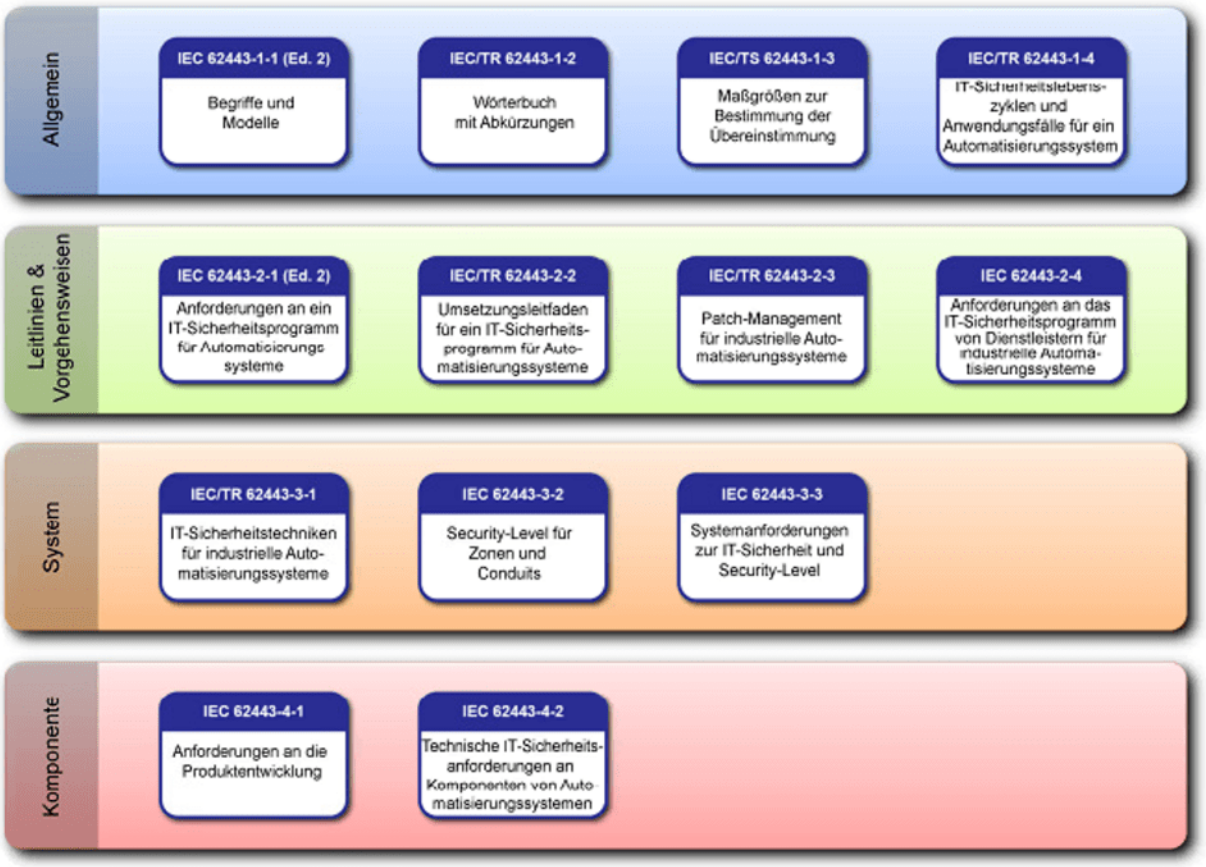


Bild 1 – Struktur der Normenreihe IEC 62443

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62443-2-4:2020-07

1 Anwendungsbereich

A1

Dieser Teil von IEC 62443 legt umfangreiche Anforderungen an die Fähigkeiten im Hinblick auf die IT-Sicherheit von Dienstleistern für industrielle Automatisierungssysteme fest, die ihre Leistungen Betreibern während der Integration und Instandhaltung einer Automatisierungslösung anbieten möchten. Da nicht alle Anforderungen für alle Branchengruppen und Organisationen gelten, behandelt 4.1.4 die Entwicklung von Profilen für eine gezielte Auswahl dieser Anforderungen. Profile **werden verwendet**, um dieses Dokument an bestimmte Umgebungen anzupassen, einschließlich solcher, die nicht auf industriellen Automatisierungssystemen beruhen.

ANMERKUNG 1 Der Begriff „Automatisierungslösung" wird in diesem Teil der IEC 62443 als Eigenname benutzt, um die Unstimmigkeiten bei der Nutzung dieses Begriffs für andere Zwecke zu vermeiden.

Zusammenfassend werden die Fähigkeiten im Hinblick auf die IT-Sicherheit, die durch einen Dienstleister für industrielle Automatisierungssysteme angeboten werden, als IT-Sicherheitsprogramm bezeichnet. Die verwandte Spezifikation IEC 62443-2-1 beschreibt die Anforderungen an das IT-Sicherheitsprogramm des Betreibers.

ANMERKUNG 2 Im Allgemeinen hängen diese Fähigkeiten mit Leitlinien, Vorgehensweisen, Umsetzungen in der Praxis und dem Personal zusammen.

Bild 2 zeigt, wie die Fähigkeiten der Integration und der Instandhaltung mit dem industriellen Automatisierungssystem und dem Produkt, das in die Automatisierungslösung integriert wird, zusammenhängen. Einige dieser Fähigkeiten nehmen Bezug auf IT-Sicherheitsmaßnahmen nach IEC 62443-3-3, deren Unterstützung in der Automatisierungslösung der Dienstleister zusichern muss (entweder sie sind im Produkt für ein industrielles Automatisierungssystem enthalten oder zusätzlich zur Automatisierungslösung hinzugefügt worden).

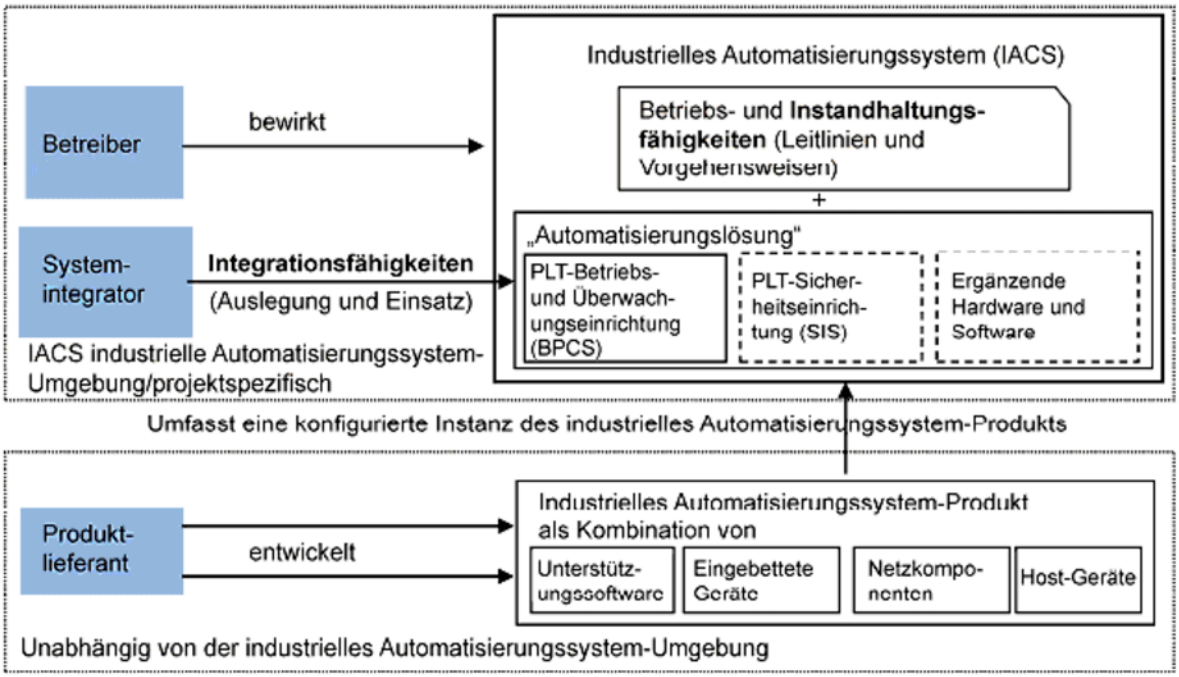


Bild 2 – Anwendungsbereich der Fähigkeiten des Dienstleisters

Die in Bild 2 dargestellte „Automatisierungslösung" umfasst eine PLT-Betriebs- und Überwachungseinrichtung (BPCS), eine PLT-Sicherheitseinrichtung (SIS) und Unterstützungssoftware wie höhere Regelungen. Die mit Strichlinien dargestellten Boxen bezeichnen Komponenten, die „vorhanden sein können oder auch nicht".

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62443-2-4:2020-07

ANMERKUNG 3 Der Begriff „Prozess" in der PLT-Betriebs- und Überwachungseinrichtung darf für eine Vielzahl von industriellen Prozessen einschließlich kontinuierlicher und Fertigungsprozesse angewendet werden.

A1

A1 ANMERKUNG 4 „Automatisierungslösungen" besitzen in der Regel ein einzelnes Automatisierungssystem (Produkt), das muss aber nicht der Fall sein. Im Allgemeinen besteht die „Automatisierungslösung" unabhängig von der Versand-Kommissionierung aus einer Kombination von Hardware und Software, mit der ein technischer Prozess (d. h. ein kontinuierlicher Prozess oder ein Fertigungsprozess) so gesteuert wird, wie vom Betreiber festgelegt.

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).

Keine

3 Begriffe und Abkürzungen

3.1 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1.1
Betreiber
(en: asset owner)
für ein oder mehrere industrielle Automatisierungssysteme verantwortliche Person oder Organisation

Anmerkung 1 zum Begriff: Der Begriff „Betreiber" wird aus Unterscheidungsgründen anstelle des allgemeinen Begriffs „Endnutzer" verwendet.

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

Anmerkung 3 zum Begriff: Im Zusammenhang mit dieser Norm gehört zu einem Betreiber auch der Bediener eines industriellen Automatisierungssystems.

3.1.2
Angriffsfläche
(en: attack surface)
körperliche (physische) und funktionale Schnittstellen eines Systems, die zugänglich sind und über die das System unter Umständen ausgenutzt werden kann

Anmerkung 1 zum Begriff: Das Ausmaß einer Angriffsfläche ist bei einer Softwareschnittstelle proportional zur Anzahl der für diese Schnittstelle festgelegten Methoden und Parameter. Einfache Schnittstellen haben daher kleinere Angriffsflächen als komplexe Schnittstellen.

Anmerkung 2 zum Begriff: Das Ausmaß der Angriffsfläche und die Anzahl der Sicherheitslücken hängen nicht notwendigerweise zusammen.

3.1.3
Automatisierungslösung
(en: Automation Solution)
Automatisierungssystem und weitere zusätzliche Hardware- und Softwarekomponenten, die zum Betrieb in einem industriellen Automatisierungssystem aufgebaut und konfiguriert wurden

AVA Documents
Document Sharing Hub
Full document details: DIN EN IEC 62443-2-4:2020-07

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

Anmerkung 2 zum Begriff: Der Unterschied zwischen dem Automatisierungssystem und der „Automatisierungslösung" besteht darin, dass das Automatisierungssystem in die Auslegung der „Automatisierungslösung" eingebunden ist (etwa eine bestimmte Anzahl von Arbeitsplatzrechnern, Steuerungen und Geräten in einer spezifischen Konfiguration), die dann umgesetzt wird. Die sich so ergebende Konfiguration wird dann als „Automatisierungslösung" bezeichnet.

Anmerkung 3 zum Begriff: Die „Automatisierungslösung" kann Komponenten verschiedener Lieferanten einschließlich des Lieferanten des Automatisierungssystems umfassen.

3.1.4
PLT-Betriebs- und Überwachungseinrichtung
(en: basic process control system)
System, das auf von einem Prozess, von dessen zugehörigen Einrichtungen und von anderen programmierbaren Systemen stammende Eingangssignale und/oder auf Bedienereingaben reagiert und Ausgangssignale erzeugt, die den Prozess und dessen zugehörige Einrichtungen veranlassen, sich in der gewünschten Art und Weise zu verhalten, das jedoch keine Sicherheitsfunktion (PLT-Sicherheitsfunktion, SIF) ausführt

Anmerkung 1 zum Begriff: Sicherheitsfunktionen sind in der Normenreihe IEC 61508 festgelegt.

Anmerkung 2 zum Begriff: Der Begriff „Prozess" in dieser Definition darf für eine Vielzahl industrieller Prozesse einschließlich von kontinuierlichen Prozessen und Fertigungsprozessen angewendet werden.

3.1.5
Berater
(en: consultant)
Unterauftragnehmer, der dem Integrator oder dem Instandhaltungsdienstleister Fachwissen oder fachliche Anleitung zur Verfügung stellt

3.1.6
Automatisierungssystem
(en: control system)
Hardware- und Softwarekomponenten eines industriellen Automatisierungssystems, die bei der Entwicklung und Umsetzung verwendet werden

Anmerkung 1 zum Begriff: Wie in Bild 2 dargestellt, setzen sich Automatisierungssysteme aus Feldgeräten, eingebetteten Steuergeräten, Netzwerkkomponenten und Host-Geräten (einschließlich von Arbeitsplatzrechnern und Servern) zusammen.

Anmerkung 2 zum Begriff: Wie in Bild 2 dargestellt, werden Automatisierungssysteme in „Automatisierungslösungen" durch eine PLT-Betriebs- und ggf. Sicherheitseinrichtung dargestellt.

3.1.7
Übergabe
(en: handover)
Vorgang der Aushändigung einer „Automatisierungslösung" an den Betreiber

Anmerkung 1 zum Begriff: Durch die Übergabe wird die Verantwortlichkeit für den Betrieb und die Instandhaltung einer „Automatisierungslösung" vom Integrator an den Betreiber übergeben; dieser Vorgang erfolgt im Allgemeinen nach einer bestandenen Systemprüfung, die oft als Abnahme der installierten Anlage (Site Acceptance Test, SAT) bezeichnet wird.

3.1.8
industrielles Automatisierungssystem
(en: industrial automation and control system)
Zusammenstellung von Personal, Hardware, Software und Vorgehensweisen, die eingebunden ist in den Betrieb eines industriellen Prozesses und dessen sicheren und zuverlässigen Betrieb beeinträchtigen oder beeinflussen kann

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62443-2-4:2020-07

Anmerkung 1 zum Begriff: Das industrielle Automatisierungssystem kann auch Komponenten enthalten, die nicht auf dem Gelände des Betreibers installiert sind.

Anmerkung 2 zum Begriff: Die Definition des industriellen Automatisierungssystems wurde IEC 62443-3-3 entnommen und ist in Bild 2 dargestellt. Beispiele für industrielles Automatisierungssystem sind Leitsysteme (DCS) und Systeme zum Bedienen und Beobachten (SCADA). In IEC 62443-2-4 wird auch der Eigenname „Lösung" definiert, der eine spezifische Instanz des industriellen Automatisierungssystem-Produkts und unter Umständen zusätzliche Komponenten bezeichnet, die in ihren Entwurf einbezogen wurden. Die „Automatisierungslösung" unterscheidet sich damit vom Automatisierungssystem, da sie eine spezifische Umsetzung (Entwicklung und Konfiguration) der Hardware- und Softwarekomponenten des Automatisierungssystems für einen bestimmten Betreiber darstellt.

3.1.9
Integrator
(en: integration service provider)
Dienstleister, der Integrationstätigkeiten für eine „Automatisierungslösung" erbringt, einschließlich Entwicklung, Installation (Aufbau), Konfiguration, Prüfung, Inbetriebnahme und Übergabe

Anmerkung 1 zum Begriff: Integratoren werden häufig als Ingenieurbüros oder als Main Automation Contractors (MAC) bezeichnet.

3.1.10
Instandhaltungsdienstleister
(en: maintenance service provider)
Dienstleister, der Unterstützungstätigkeiten für eine „Automatisierungslösung" nach der Übergabe erbringt

Anmerkung 1 zum Begriff: Zwischen Instandhaltung und Betrieb wird häufig unterschieden (z. B. wird umgangssprachlich oft davon ausgegangen, dass eine „Automatisierungslösung" entweder in Betrieb ist oder einer Instandhaltung unterzogen wird). Instandhaltungsdienstleister können Unterstützungstätigkeiten während des Betriebs ausführen, z. B. die Verwaltung von Nutzerkonten, eine IT-Sicherheitsüberwachung und IT-Sicherheitsbewertungen.

3.1.11
mobile Datenträger
(en: portable media)
tragbare Geräte mit der Fähigkeit der Datenspeicherung, die zur physischen Übertragung (Kopieren) von Daten von einem Gerät zu einem anderen benutzt werden können

Anmerkung 1 zum Begriff: Mobile Datenträger sind unter anderem, aber nicht begrenzt auf CD/DVD/BluRay-Medien, USB-Speicher, Smartphones, Flash-Speicher, Solid-State-Disks, Festplattenlaufwerke, mobile Handgeräte und tragbare Rechner.

3.1.12
Hersteller
(en: product supplier)
Erzeuger eines Hardware- und/oder Softwareprodukts

Anmerkung 1 zum Begriff: Zur besseren Unterscheidung wird dieser Begriff anstelle des allgemeinen Wortes „Verkäufer" verwendet.

3.1.13
Fernzugriff
(en: remote access)
Zugriff auf ein Automatisierungssystem über eine externe Schnittstelle des Automatisierungssystems

Anmerkung 1 zum Begriff: Beispiele für Anwendungen, die einen Fernzugriff unterstützen, sind RDP, OPC und Syslog.

Anmerkung 2 zum Begriff: Im Allgemeinen sind Fernzugriffsanwendungen und „Automatisierungslösungen" in verschiedenen IT-Sicherheitszonen nach den Festlegungen des Betreibers angesiedelt. Die Anwendung von Zonen und Conduits auf die „Automatisierungslösung" durch den Betreiber kann IEC 62443-3-2 entnommen werden.

AVA Documents
Document Sharing Hub
Full document details: DIN EN IEC 62443-2-4:2020-07

3.1.14
PLT-Sicherheitseinrichtung
(en: safety instrumented system)
System zur Implementierung der funktionalen Sicherheit

Anmerkung 1 zum Begriff: Siehe IEC 61508 und IEC 61511 für weitergehende Beschreibungen der funktionalen Sicherheit.

A1 Anmerkung 2 zum Begriff: Dieser Begriff wird nicht in allen Industriezweigen angewendet. Seine Anwendung beschränkt sich nicht auf einen bestimmten Industriezweig, sondern erfolgt allgemein für Systeme, die funktionale Sicherheit durchsetzen. Weitere gleichwertige Begriffe sind Sicherheitssysteme und sicherheitsbezogene Systeme.

3.1.15
IT-Sicherheitsverstoß
(en: security compromise)
Verletzung der IT-Sicherheit eines Systems, durch die eine (1) nicht genehmigte Offenlegung oder Änderung von Informationen oder eine (2) Denial-of-Service-Situation aufgetreten sein kann

Anmerkung 1 zum Begriff: Ein IT-Sicherheitsverstoß stellt eine Verletzung der IT-Sicherheit eines Systems oder eine Übertretung seiner IT-Sicherheitsleitlinien dar. Er ist unabhängig von der Auswirkung oder der möglichen Auswirkung auf das System.

3.1.16
IT-Sicherheitsvorfall
(en: security incident)
IT-Sicherheitsverstoß mit einer gewissen Bedeutung für den Betreiber oder fehlgeschlagener Versuch, einen solchen herbeizuführen

Anmerkung 1 zum Begriff: Die Wortgruppe „gewisse Bedeutung" bezieht sich auf die Umgebung, in der der IT-Sicherheitsverstoß festgestellt wird. Es kann z. B. der Fall eintreten, dass der gleiche IT-Sicherheitsverstoß in einer Umgebung zum IT-Sicherheitsvorfall erklärt wird, in einer anderen aber nicht. Die Bewertung von IT-Sicherheitsverstößen nimmt der Betreiber häufig durch Auswahlverfahren vor, bei denen diejenigen Verstöße festgestellt werden, die so bedeutend sind, dass sie als IT-Sicherheitsvorfälle betrachtet werden.

Anmerkung 2 zum Begriff: In einigen Umgebungen werden fehlgeschlagene Versuche der Gefährdung des Systems wie erfolglose Anmeldeversuche als so bedeutend angesehen, dass sie als IT-Sicherheitsvorfälle klassifiziert werden.

3.1.17
IT-Sicherheitspatch
(en: security patch)
ein für die Sicherheit einer Softwarekomponente relevanter Softwarepatch

Anmerkung 1 zum Begriff: Im Zusammenhang mit dieser Definition wird Firmware als Software angesehen.

Anmerkung 2 zum Begriff: Softwarepatches können bekannte oder mögliche IT-Sicherheitslücken betreffen oder einfach die Sicherheit der Softwarekomponente einschließlich ihres zuverlässigen Betriebes verbessern.

3.1.18
IT-Sicherheitsprogramm
(en: security program)
Bestand der IT-Sicherheitsmaßnahmen einschließlich von Integrations- und Instandhaltungsdiensten und deren zugehörige Leitlinien, Vorgehensweisen und Produkte, die für das industrielle Automatisierungssystem anwendbar sind

Anmerkung 1 zum Begriff: Das IT-Sicherheitsprogramm eines Dienstleisters für industrielle Automatisierungssysteme bezieht sich auf die von ihm für diese festgelegten Leitlinien und Vorgehensweisen.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62443-2-4:2020-07

3.1.19
Dienstleister
(en: service provider)
Einzelperson oder Organisation (interne oder externe Organisation, Hersteller usw.), die nach Vereinbarung mit dem Betreiber einen bestimmten Unterstützungsdienst und damit verbundene Zulieferungen erbringt

Anmerkung 1 zum Begriff: Zur besseren Unterscheidung wird dieser Begriff anstelle des allgemeinen Wortes „Verkäufer" verwendet.

3.1.20
Unterauftragnehmer
(en: subcontractor)
vertraglich vom Integrator oder Instandhaltungsdienstleister oder von einem anderen Unterauftragnehmer bestellter Dienstleister, der dem Integrator oder Instandhaltungsdienstleister direkt oder indirekt vertraglich untersteht

3.1.21
System
(en: system)
Satz von in Wechselbeziehung oder Wechselwirkung stehenden oder voneinander abhängigen Elementen, die zusammen ein komplexes Ganzes bilden

Anmerkung 1 zum Begriff: Ein System darf wie ein Produkt versandt werden.

Anmerkung 2 zum Begriff: In der Praxis wird die Bedeutung häufig durch Beiworte verdeutlicht wie z. B. bei einem Automatisierungssystem. Seine Elemente sind meist Hard- und Softwareelemente.

3.1.22
verifizieren
(en: verify)
prüfen, ob die festgelegten Anforderungen erfüllt wurden

3.1.23
Sicherheitslücke
Verletzlichkeit
(en: vulnerability)
Fehler oder Schwäche der Auslegung, der Umsetzung oder des Betriebs und Managements einer Komponente, der bzw. die ausgenutzt werden kann, um einen IT-Sicherheitsverstoß hervorzurufen

Anmerkung 1 zum Begriff: IT-Sicherheitsleitlinien schließen in der Regel Leitlinien zum Schutz von Vertraulichkeit, Integrität und Verfügbarkeit von Systembetriebsmitteln ein.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62443-2-4:2020-07

3.2 Abkürzungen

Abkürzungen

Abkürzung	Bedeutung englisch	Bedeutung deutsch
AES_GCM	Advanced Encryption Standard Galois/Counter Mode	erweiterter Verschlüsselungsstandard
BPCS	Basic Process Control System	Betriebs- und Überwachungseinrichtung
BR	Base Requirement	Basisanforderung
CA	Certification Authority	Zertifizierungsstelle für digitale Zertifikate
CEF	Common Event Format	Allgemeines Ereignisformat
DCOM	Distributed Common Object Model	Verteiltes Objektmodell
DCS	Distributed Control System	Leitsystem
EWS	Engineering Workstation	Programmiersystem
IACS	Industrial Automation and Control System	Industrielles Automatisierungssystem
RE	Requirement Enhancement	Weitergehende Anforderung
RDP	Remote Desktop Protocol	Remote-Desktop-Protokoll
RFC	Request For Comment	Reihe technischer und organisatorischer Dokumente zum Internet
RFQ	Request For Quote	Ausschreibung
SCADA	Supervisory Control And Data Acquisition	Bedienen und Beobachten
SIEM	Security Information and Event Management	Sicherheitsinformations- und Ereignismanagement
SIF	Safety Instrumented Function	Sicherheitstechnische Funktion, PLT-Sicherheitsfunktion
SIL	Safety Integrity Level	Sicherheits-Integritätslevel
SIS	Safety Instrumented System	PLT-Sicherheitseinrichtung
SNMP	Simple Network Management Protocol	einfaches Netzwerkverwaltungsprotokoll (en: simple network management protocol)
SOW	Statement Of Work	Leistungsbeschreibung
SSID	Service Set Identifier	Bezeichner des Dienstes
SP	Security Program	IT-Sicherheitsprogramm
TR	Technical Report	Fachbericht
VPN	Virtual Private Network	Virtuelles privates Netz

4 Orientierung

4.1 Anwendung der IEC 62443-2-4

4.1.1 Anwendung der IEC 62443-2-4 durch Dienstleister für industrielle Automatisierungssysteme

In diesem Teil der Normenreihe IEC 62443 werden Anforderungen an die Fähigkeiten im Hinblick auf die IT-Sicherheit festgelegt, die durch IT-Sicherheitsprogramme von Integratoren und Instandhaltungsdienstleistern (siehe 4.1.3 und 4.1.6) unterstützt werden sollen. Unterstützung für diese Fähigkeiten bedeutet, dass der Dienstleister dem Betreiber die Fähigkeiten auf Anfrage zur Verfügung stellen kann. Die Geschäftsbedingungen für die Bereitstellung dieser Fähigkeiten gehören nicht zum Anwendungsbereich der vorliegenden Norm. Außerdem kann IEC 62443-2-4 von diesen Dienstleistern zur Strukturierung und Verbesserung ihrer IT-Sicherheitsprogramme angewendet werden.

Darüber hinaus können solche Dienstleister für industrielle Automatisierungssysteme die Normen IEC 62443-3-3 und IEC 62443-4-2 in Verbindung mit IEC 62443-2-4 für die Zusammenarbeit mit den Lieferanten der zugrunde liegenden Automatisierungssysteme und Komponenten anwenden. Diese Zusammen-

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62443-2-4:2020-07

arbeit kann für den Dienstleister bei der Ausarbeitung von Leitlinien und Vorgehensweisen im Zusammenhang mit den Fähigkeiten eines Systems oder dessen Komponenten nützlich sein, beispielsweise bei der Datensicherung und Wiederherstellung gemäß den Empfehlungen der Lieferanten der eingesetzten Systeme und Komponenten.

Von den IT-Sicherheitsprogrammen, die diese Anforderungen umsetzen, wird erwartet, dass sie unabhängig von den verschiedenen Versionen (Release) des Automatisierungssystems sind, das in die Automatisierungslösung eingebettet ist. Das heißt, dass eine neue Version des industriellen Automatisierungssystem-Produkts nicht notwendigerweise eine Änderung am IT-Sicherheitsprogramm des Dienstleisters erfordert. Änderungen am IT-Sicherheitsprogramm sind jedoch dann erforderlich, wenn Änderungen am zugrunde liegenden Automatisierungssystem vorgenommen wurden, durch die das bestehende IT-Sicherheitsprogramm hinsichtlich der Anforderungen nach IEC 62443-2-4 unzulänglich wird.

BEISPIEL 1 Ein Dienstleister kann Erfahrungen mit einer bestimmten Produktlinie von Automatisierungssystemen haben. Die Entwicklung von Leitlinien und Vorgehensweisen für diese Produktlinie wird auf die Empfehlungen des Produktlieferanten und die Fähigkeiten der Produktlinie gestützt. Wenn die Fähigkeiten des Produkts für die Datensicherung und Wiederherstellung verändert werden, müssen demzufolge unter Umständen auch die entsprechenden Fähigkeiten des IT-Sicherheitsprogramms des Dienstleisters (gemäß SP.12.XX) geändert werden, damit die Übereinstimmung mit den aktualisierten Fähigkeiten des Produkts erhalten bleibt. Andererseits sind die Leitlinien und Vorgehensweisen des Dienstleisters im Zusammenhang mit Geheimhaltungsvereinbarungen oder Überprüfungen der Vergangenheit der Mitarbeiter (gemäß SP.01.03 und SP.01.04) sehr wahrscheinlich unabhängig vom industriellen Automatisierungssystem-Produkt, welches in der „Automatisierungslösung" eingesetzt wird.

Diese Zusammenarbeit kann auch der Verbesserung der IT-Sicherheit in diesen Systemen und Komponenten dienen. Zum einen kann der Dienstleister dem System- und Komponentenlieferanten neue oder aktualisierte IT-Sicherheitsmerkmale empfehlen. Zum anderen kann der Dienstleister tiefergehende Kenntnisse über die Systeme und Komponenten erwerben, wodurch es ihm möglich sein wird, der „Automatisierungslösung" während des Einsatzes und der Instandhaltung eigene hinzuzufügen.

Die Anforderungen sind in Anhang A mit Hilfe der Fähigkeiten, die diese IT-Sicherheitsprogramme leisten müssen, festgelegt. In 4.1.4 werden die Möglichkeiten von Branchengruppen behandelt, von diesen Fähigkeiten mit Hilfe von Profilen Untermengen zu bilden, um so eine Risikominderung zu erzielen. Weitere Einzelheiten zu IT-Sicherheitsrisiken können IEC 62443-3-2 entnommen werden.

In der vorliegenden Norm wird davon ausgegangen, dass sich IT-Sicherheitsprogramme weiterentwickeln und auch die Fähigkeiten einen eigenen Lebenszyklus durchlaufen, der häufig vollkommen manuell beginnt und sich dann mit der Zeit zu einer mehr formalen, konsistenteren und wirksameren Vorgehensweise entwickelt. In 4.2 wird dieses Thema der sich weiterentwickelnden Fähigkeiten behandelt, indem ein Reifegradmodell definiert wird, das zusammen mit dieser Norm anzuwenden ist.

BEISPIEL 2 Eine besondere Fähigkeit könnte zunächst als eine Menge manueller Vorgehensweisen eingeführt werden, die dann später durch automatisierte Werkzeuge ergänzt wird.

Aufgrund dessen werden die Anforderungen in Anhang A abstrakt festgelegt und erlauben somit einen breiten Bereich an Umsetzungen. Es wird davon ausgegangen, dass Dienstleister und Betreiber darüber verhandeln und sich darüber einigen werden, welche dieser geforderten Fähigkeiten im Einzelnen zu erbringen und wie sie bereitzustellen sind. Diese Aspekte des Erfüllens der Anforderungen gehören nicht zum Anwendungsbereich der IEC 62443-2-4, obwohl sie durch die Nutzung von Profilen erleichtert werden sollten.

BEISPIEL 3 Ein Dienstleister, der in der Lage ist, komplexe Passwörter zu unterstützen, muss auch gewisse Variationen komplexer Passwörter unterstützen können, wie dies in den Passwortleitlinien des Betreibers festgelegt ist.

BEISPIEL 4 Viele Fähigkeiten haben einen Zeitbezug hinsichtlich ihrer Ausführung. Was als zeitgerecht angesehen wird, sollte zwischen dem Betreiber und dem Dienstleister vereinbart werden.

4.1.2 Anwendung von IEC 62443-2-4 durch Betreiber industrieller Automatisierungssysteme

IEC 62443-2-4 kann von Betreibern auch dazu verwendet werden, beim Dienstleister bestimmte Fähigkeiten im Hinblick auf die IT-Sicherheit anzufragen. Insbesondere kann mit ihr vor einer solchen Anfrage vom

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62443-2-4:2020-07

Betreiber ermittelt werden, ob das IT-Sicherheitsprogramm eines bestimmten Dienstleisters über diejenigen Fähigkeiten verfügt, die er benötigt.

Im Allgemeinen wird in IEC 62443-2-4 berücksichtigt, dass die Anforderungen des Betreibers variieren können, so dass die Norm in einer Weise abgefasst wurde, dass Dienstleister dazu angeregt werden, die geforderten Fähigkeiten so festzulegen, dass sie an eine Vielzahl von Betreibern angepasst werden können. Das Reifegradmodell fördert außerdem das Verständnis des Betreibers dafür, wie ausgereift die Fähigkeiten eines bestimmten Dienstleisters sind.

4.1.3 Anwendung von IEC 62443-2-4 bei Verhandlungen zwischen Betreibern und Dienstleistern

Bevor der Dienstleister für ein industrielles Automatisierungssystem mit den Arbeiten an der „Automatisierungslösung“ beginnt, wird der Betreiber in der Regel eine Ausschreibung mit einem Dokument (z. B. mit einer Leistungsbeschreibung) veröffentlicht haben, in dem seine IT-Sicherheitsleitlinien und -anforderungen benannt wurden einschließlich der Angabe, welche der in Anhang A festgelegten Anforderungen zutreffen. Weitere Informationen zur Festlegung von IT-Sicherheitsanforderungen können IEC 62443-3-2 entnommen werden. Dienstleister antworten auf diese Ausschreibung und es folgen Verhandlungen, bei denen sich der Dienstleister und der Betreiber über die Einzelheiten der Leistungsbeschreibung (oder eines ähnlichen Dokuments) einigen. In diese Vereinbarung bzw. diesen Vertrag zwischen dem Dienstleister und dem Betreiber werden in der Regel die spezifischen Verantwortlichkeiten und Fähigkeiten des Dienstleisters bei der Unterstützung der IT-Sicherheitsleitlinien und -anforderungen des Betreibers aufgenommen oder es wird auf diese hingewiesen.

ANMERKUNG 1 Wenn der Dienstleister ein Mitglied der Organisation des Betreibers ist, gibt es unter Umständen einen solchen Vertrag nicht.

Darüber hinaus legt der Betreiber gewöhnlich nicht fest, wie seine IT-Sicherheitsanforderungen (z. B. Datensicherung und Wiederherstellung) umgesetzt werden – dies hat der Dienstleister bereits in seinen Leitlinien und Vorgehensweisen festgelegt. Jedoch darf der Betreiber Einschränkungen und Parameter dafür festlegen (z. B. Verfallsdaten von Passwörtern), wie die Leitlinien und Vorgehensweisen in seinem spezifischen Projekt umgesetzt werden.

In Fällen, in denen der Betreiber keine IT-Sicherheitsanforderungen festlegt, darf der Dienstleister dem Betreiber anhand seiner eigenen IT-Sicherheitsanalyse solche empfehlen und dann mit ihm vereinbaren, welche in die Leistungsbeschreibung aufgenommen werden.

Des Weiteren wird erwartet, dass der industrielle Automatisierungssystem-Dienstleister über gewisse Fähigkeiten verfügt, sich an Kundenwünsche anzupassen und den Bedürfnissen des Betreibers zu entsprechen. Die Festlegung dieser Anpassung an Kundenwünsche gehört jedoch nicht zum Anwendungsbereich der vorliegenden Norm.

4.1.4 Profile

A1

Dieses Dokument berücksichtigt, dass nicht alle der in Anhang A angegebenen Anforderungen für alle Industriezweige/Umgebungen gelten. Die gezielte Auswahl und Anpassung dieser Anforderungen erfolgt in diesem Dokument mit „Profilen“.

Profile werden in Form von IEC-Fachberichten (Technical Reports, TRs) für verschiedene Branchengruppen/Industriezweige oder andere Organisationen einschließlich von Betreibern und Dienstleistern geschrieben, um die in Anhang A angegebenen Anforderungen auszuwählen/anzupassen, die am besten für ihre Bedürfnisse geeignet sind.

Jeder TR darf ein Profil oder mehrere Profile festlegen und jedes Profil kennzeichnet eine Teilmenge der in Anhang A definierten Anforderungen und legt gegebenenfalls fest, wie bestimmte Anforderungen in der vorgesehenen Umgebung anzuwenden sind.

A1

Es wird davon ausgegangen, dass sich Betreiber für bestehende Profile entscheiden, in denen die von ihnen benötigten Anforderungen für ihre Automatisierungslösungen spezifiziert sind.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62443-2-4:2020-07

4.1.5 Integratoren

Ein Integrator für industrielle Automatisierungssysteme ist eine üblicherweise vom Betreiber getrennte und ihm per Vertrag zugeordnete Organisation, die dem Betreiber Fähigkeiten zur Verfügung stellt, mit denen dieser „Automatisierungslösungen" entsprechend seinen Anforderungen umsetzen/einsetzen kann. Die Tätigkeiten eines Integrators reichen im Allgemeinen von der Entwicklungsphase bis zur Übergabe der „Automatisierungslösung" an den Betreiber.

ANMERKUNG 1 Der Integrator kann eine Organisation innerhalb der Betreiberorganisation sein.

Übliche Tätigkeiten eines industriellen Automatisierungssystem-Integrators umfassen:

a) Analyse der physikalischen, elektrischen oder mechanischen Umgebung, die die „Automatisierungslösung" beherrschen soll (z. B. den zu steuernden physikalischen Prozess, wie er in Fertigungs- und Verarbeitungsprozessen sowie pharmazeutischen Prozessen vorkommt);

b) Entwicklung eines Systemaufbaus der „Automatisierungslösung" bezüglich der Geräte und Regelkreise und ihren Verbindungen mit den Arbeitsplatz- und Bedienrechnern sowie möglicherweise die Einbeziehung von PLT-Sicherheitseinrichtungen;

c) Festlegung, wie die „Automatisierungslösung" mit externen Netzen (z. B. Anlagennetzen) verbunden wird;

d) Einrichtung, Konfiguration, Installation von Sicherheitspatches, Datensicherung und Prüfungen, die zur Übergabe der „Automatisierungslösung" an den Betreiber und zum anschließenden Betrieb führen;

e) Erlangung der Zustimmung des Betreibers zu vielen während der Ausführung dieser Tätigkeiten getroffenen Entscheidungen und erbrachten Leistungen.

Dies ist eine abstrakte Beschreibung der Tätigkeiten des Integrators und einige dieser Tätigkeiten können ausgeschlossen werden oder es können auch andere Tätigkeiten einbezogen werden, die der Übergabe der „Automatisierungslösung" vorausgehen. Diese Tätigkeiten erfordern auch die Teilnahme des Betreibers, um sicherzustellen, dass dessen Anforderungen erfüllt werden.

Aus Sicht von IEC 62443 wird vom Integrator erwartet, dass er an der Beurteilung der IT-Sicherheitsrisiken für die „Automatisierungslösung" teilnimmt oder die vom Betreiber zur Verfügung gestellten Ergebnisse solch einer Beurteilung verwendet. Vom ihm wird außerdem erwartet, dass er die in der vorliegenden Norm geforderten Fähigkeiten in sein IT-Sicherheitsprogramm zur Behandlung solcher Risiken einbringt.

ANMERKUNG 2 Leitlinien für die Nutzung von Risikobeurteilungen und die Festlegung von IT-Sicherheitsanforderungen können IEC 62443-3-2 entnommen werden.

4.1.6 Instandhaltungsdienstleister

Ein Instandhaltungsdienstleister für industrielle Automatisierungssysteme ist üblicherweise eine vom Betreiber getrennte und ihm vertraglich verpflichtete Organisation, die Tätigkeiten durchführt, um „Automatisierungslösungen" entsprechend den Anforderungen des Betreibers in Stand zu halten.

Instandhaltungstätigkeiten werden von den Tätigkeiten des Betriebs der „Automatisierungslösung" getrennt und im Allgemeinen in zwei Kategorien eingeteilt, und zwar in solche Tätigkeiten, die speziell für die Aufrechterhaltung der IT-Sicherheit der „Automatisierungslösung" durchgeführt werden, und in Tätigkeiten, die für die Erhaltung anderer Aspekte der „Automatisierungslösung" zutreffen, wie die Instandhaltung von Geräten und Einrichtungen, die denen aber sicherzustellen ist, dass die IT-Sicherheit infolge dieser Tätigkeiten nicht vermindert wird.

ANMERKUNG 1 Der Instandhaltungsdienstleister kann eine Organisation innerhalb der Betreiberorganisation sein.

ANMERKUNG 2 Es kann einen oder mehrere Instandhaltungsdienstleister geben, die die „Automatisierungslösung" gleichzeitig oder nacheinander in Stand halten.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62443-2-4:2020-07

Die Instandhaltungstätigkeiten beginnen im Allgemeinen nach der Übergabe der „Automatisierungslösung" an den Betreiber und dürfen fortgesetzt werden, bis der Betreiber diese Tätigkeiten nicht länger benötigt. Sie sind gewöhnlich kurz, wiederholen sich häufig und umfassen eine oder mehrere der folgenden Tätigkeiten:

a) Installieren von Patches und Aktualisieren der Antivirus-Software;

b) Nachrüstung und Instandhaltung von Einrichtungen einschließlich geringfügiger technischer Anpassungen, die nicht unmittelbar den Steuerungsalgorithmus betreffen;

c) Migration von Komponenten und Systemen;

d) Änderungsmanagement;

e) Management des Notfallplans.

Alle Instandhaltungstätigkeiten umfassen ein bestimmtes IT-Sicherheitsbewusstsein unabhängig davon, ob sie die IT-Sicherheit unmittelbar betreffen oder nicht. Keine Tätigkeit sollte nach ihrem Abschluss die IT-Sicherheitslage herabsetzen.

Dies ist eine abstrakte Beschreibung der Instandhaltungstätigkeiten und darf auch andere Tätigkeiten umfassen, die der Übergabe der „Automatisierungslösung" im Allgemeinen folgen. Diese Tätigkeiten bedingen auch die Teilnahme des Betreibers, um sicherzustellen, dass dessen Anforderungen erfüllt werden.

Aus Sicht der Normenreihe IEC 62443 wird von Instandhaltungsdienstleistern genauso wie von Integratoren erwartet, dass sie sich an der Bewertung der Sicherheitsrisiken für die „Automatisierungslösung" beteiligen (z. B. für vorgeschlagene Änderungen) oder dass sie die Ergebnisse einer solchen Bewertung, die vom Betreiber zur Verfügung gestellt werden, verwenden. Vom Dienstleister wird außerdem erwartet, dass er die in der vorliegenden Norm geforderten Fähigkeiten in sein IT-Sicherheitsprogramm zur Behandlung solcher Risiken einbringt.

ANMERKUNG 3 Leitlinien für die Nutzung von Risikobeurteilungen und die Definition der IT-Sicherheitsanforderungen können IEC 62443-3-2 entnommen werden.

4.2 Reifegradmodell

Inwiefern die in Anhang A festgelegten Anforderungen von einem Dienstleister bereitgestellt werden können, steht einer breiten Auslegung offen. In diesem Abschnitt wird ein Reifegradmodell vorgestellt, aus dem Orientierungswerte für die Erfüllung dieser Anforderungen abgeleitet werden können.

Diese Orientierungswerte werden mittels Reifegrade vorgegeben, wie in Tabelle 1 gezeigt. Die Reifegrade beruhen auf dem CMMI-SVC-Modell, das in CMMI® for Services, Version 1.3, definiert ist. Tabelle 1 gibt in der Spalte *Beschreibung/Vergleich mit CMMI-SVC* den Bezug zum CMMI-SVC-Modell an.

Jeder Grad zeigt fortschreitend einen höheren Reifegrad als der vorherige und gilt unabhängig für alle Anforderungen in Tabelle A.1. Dienstleister müssen den Reifegrad, der mit der Implementierung der jeweiligen Anforderung verbunden ist, angeben. Dadurch wird es den Betreibern möglich, in messbaren Angaben den Reifegrad einer bestimmten Fähigkeit eines Dienstleisters zu bestimmen.

Dieses Modell bezieht sich sowohl auf Basisanforderungen (BR) als auch weitergehende Anforderungen (RE), wie sie in Tabelle A.1 festgelegt sind. Die REs in dieser Tabelle sind Erweiterungen von BRs und spiegeln keinen Reifegrad wieder. Dagegen sind REs so festgelegt, dass sie Raum für Spezialisierungen, Einschränkungen oder Verallgemeinerungen von BRs öffnen. Sie werden auf dieselbe Weise wie in der IEC 62443-3-3 eingesetzt.

ANMERKUNG 1 Branchengruppen/Industriezweige können je nach Gegebenheit und individuellen Bedürfnissen eigene Reifegrade bestimmen.

ANMERKUNG 2 Es wird davon ausgegangen, dass sich die Fähigkeiten eines Dienstleisters bezüglich einer bestimmten Anforderung im Laufe der Zeit zunehmend weiterentwickeln, da er immer mehr Kenntnisse für die Erfüllung der Anforderung erlangt.

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62443-2-4:2020-07

Tabelle 1 – Reifegrade

Reifegrad	CMMI-SVC	IEC 62443-2-4	Beschreibung nach IEC 62443-2-4/Vergleich mit CMMI-SVC
1	Initial	am Anfang	Bei diesem Reifegrad sind die Modelle grundsätzlich gleich. Dienstleister führen den Dienst üblicherweise kurzfristig und oft ohne Dokumentation (oder nur unvollständig dokumentiert) aus. Anforderungen an den Dienst werden üblicherweise in einer Leistungsbeschreibung, die Bestandteil des Vertrages ist, definiert. Folglich wird es kaum eine projektübergreifende Konsistenz geben. ANMERKUNG Unter „dokumentiert" ist in diesem Zusammenhang ein Verfahren zu verstehen, das sich an die Ausführung des Dienstes anschließt (beispielsweise detaillierte Anweisungen an das Dienstleisterpersonal) und nicht das Ergebnis dieser Dienstausführung selbst. Meist werden in den Festlegungen des Betreibers alle sich aus der Durchführung einer Dienstaufgabe ergebenden Änderungen dokumentiert.
2	Managed	verwaltet	Bei diesem Reifegrad sind die Modelle grundsätzlich gleich, mit der Ausnahme, dass in IEC 62443-2-4 anerkannt wird, dass es eine signifikante Verzögerung zwischen der Festlegung eines Dienstes und dessen praktischer Durchführung geben kann. Daher werden die durchführungsbezogenen Aspekte von CMMI-SVC-Level 2 in den Reifegrad 3 verschoben. Bei diesem Reifegrad verfügt der Dienstleister über die Fähigkeit, die Erbringung und die Qualität des Dienstes entsprechend den schriftlichen Leitlinien (einschließlich der Zielvorgaben) zu lenken. Der Dienstleister kann auch nachweisen, dass das zur Dienstdurchführung eingesetzte Personal über bestimmte Kenntnisse und Fähigkeiten verfügt, unterwiesen ist und/oder in der Lage ist, schriftliche Anweisungen zu befolgen. Der vom Reifegrad 2 dargestellte Dienstgrad versichert, dass Dienstabläufe selbst in Stresssituationen wiederholbar sind. Wenn diese Abläufe eingeführt sind, wird ihre Ausführung entsprechend den dokumentierten Plänen gesteuert und erfolgen.
3	Defined	definiert (wurde bereits praktiziert)	Bei diesem Reifegrad sind die Modelle grundsätzlich gleich mit der Ausnahme, dass die durchführungsbezogenen Aspekte von CMMI-SVC-Reifegrad 2 hier aufgenommen sind. Daher ist ein Dienst beim Reifegrad 3 ein Reifegrad-2-Dienst, den der Dienstleister wenigstens schon einmal für einen Betreiber erbracht hat. Die Leistung eines Reifegrad-3-Dienstes kann in der Organisation des Dienstleisters wiederholbar nachgewiesen werden. Reifegrad-3-Dienste können auf einzelne Projekte maßgeschneidert werden, je nach Vertrag und Leistungsbeschreibung vom Auftraggeber.
4	quantitatively managed (quantitativ kontrolliert)	unter ständiger Verbesserung	Bei diesem Reifegrad werden in der vorliegenden Norm die CMMI-SVC-Reifegrade 4 und 5 kombiniert. Mittels passender Prozessmaßgrößen kann der Dienstleister die Wirksamkeit und Leistung des Dienstes überwachen und lenken und eine nachhaltige Verbesserung in diesen Bereichen demonstrieren, wie z. B. wirksamere Verfahren oder die Verwirklichung von Systemfähigkeiten mit höheren Security-Leveln (siehe IEC 62443-3-3). Dieses führt zu einem IT-Sicherheitsprogramm, das die Dienstleistung durch Änderungen in der Technik, der Verfahren und Prozeduren und des Managements verbessert. Siehe IEC 62443-1-3 zur Beschreibung von Maßgrößen.
5	optimizing (sich optimierend)		

A1

5 Überblick über die Anforderungen

5.1 Inhalte

Anhang A enthält die Liste der Anforderungen an die IT-Sicherheitsprogramme von Integratoren und Instandhaltungsdienstleistern industrieller Automatisierungssysteme. Die Anforderungen sind in Tabelle A.1 als eine Liste von Basisanforderungen (BRs) und erweiterten Anforderungen (REs) dargestellt. BRs und REs sind in 5.5.2 beschrieben. Jede Anforderung legt eine Fähigkeit fest, die der Dienstleister dem Betreiber während der Integrations- und Instandhaltungstätigkeiten anbieten kann.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62443-2-4:2020-07

A1 Nicht alle Anforderungen gelten für alle Dienstleister und Betreiber dürfen von Dienstleistern verlangen, nur eine Teilmenge ihrer geforderten Fähigkeiten, die in Anhang A festgelegt sind, auszuführen. Darüber hinaus dürfen Industriezweige, Dienstleister und Betreiber ihre eigenen Profile festlegen, die eine Teilmenge dieser Anforderungen umfassen (siehe 4.1.4).

ANMERKUNG Branchengruppen/Industriezweige können hiervon Teilmengen bilden, um ihren Bedürfnissen gerecht zu werden.

5.2 Sortierung und Filterung

Die Spalten in Tabelle A.1 sind mit dem Zweck einer leichten elektronischen Sortierung und Filterung durch ein Tabellenkalkulationsprogramm geschrieben worden. Daher wird diese Internationale Norm mit einer elektronischen Version der Tabelle A.1 vertrieben. Dies erlaubt unterschiedlichen Nutzern, die Anforderungen entsprechend ihren eigenen Bedürfnissen zu organisieren. Die zur Sortierung und Filterung verwendeten Spaltenwerte sind in 5.5 definiert.

5.3 Hierarchiemodell nach IEC 62264-1

A1 Viele der in Anhang A genannten Anforderungen beziehen sich auf Netz- oder Anwendungsebenen in Sätzen wie „ein drahtloses Handgerät wird in Ebene 2 verwendet“. Die Schreibweise von „Ebene“ verweist in diesem Zusammenhang auf die Position im Hierarchiemodell nach IEC 62264-1. Die „Ebene“ eines referenzierten Objekts (z. B. ein drahtloses Handgerät) wird durch die Funktion der niedrigsten Ebene, die es ausführt, dargestellt. Die Anforderungen in Anhang A nehmen Bezug auf das in IEC 62443-3-2 beschriebene Zonen- und Conduit-Modell und legen unabhängig von der Ebene des Hierarchiemodells nach IEC 62264-1 Grenzen fest, die die Automatisierungslösung in Teilbereiche unterteilen, die nach IEC 62443-3-2 als „Zonen“ bezeichnet werden.

ANMERKUNG Das Hierarchiemodell nach IEC 62264-1 ist auch unter dem Namen Purdue-Referenzmodell bekannt und ebenfalls in ISA 95 festgelegt.

5.4 Anforderungen in Tabellenspalten

Die in Tabelle A.1 verwendeten Spalteninhalte sind in Tabelle 2 definiert. Die Werte für diese Spalteninhalte sind in 5.5 festgelegt.

Tabelle 2 – Spalten

Spalte	Spaltenbeschreibung
Anford.-ID	Kennung (ID) der Anforderung
BR/RE	zeigt an, ob es eine Basisanforderung oder weitergehende Anforderung ist
Bereich	Schlüsselwort zur Bezeichnung des Bereichs einer Anforderung
Oberbegriff	Schlüsselwort zur Bezeichnung des Oberbegriffs einer Anforderung; derselbe Oberbegriff darf auf mehr als einen Bereich zutreffen
Unterbegriff	Schlüsselwort zur Bezeichnung des in der Anforderung genannten Unterbegriffs; derselbe technische Oberbegriff darf auf mehr als einen Bereich oder mehr als eine Tätigkeit zutreffen
Doku?	Dem Betreiber muss eine lieferfähige Dokumentation übergeben werden (Ja/Nein). ANMERKUNG Manche Anforderungen verlangen vom Dienstleister, eine Dokumentation zu pflegen, die jedoch nicht als eine zu liefernde Leistung angesehen wird. Jedoch kann der Betreiber mit dem Dienstleister Vereinbarungen getroffen haben, Einsicht in dessen Dokumentation zu erhalten oder diese dennoch zu bekommen.
Beschreibung der Anforderung	Text der Anforderung
Begründung	ein Text, der den Hintergrund, die Rechtfertigung und andere Aspekte der Anforderung beschreibt und dem Leser das Verständnis erleichtern soll

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62443-2-4:2020-07

5.5 Spaltendefinitionen

5.5.1 Spalte „Anford.-ID“

Diese Spalte enthält die Kennung des IT-Sicherheitsprogramms. Mit ein und derselben „Anford.-ID“ werden sowohl die Basisanforderung als auch ihre weitergehenden Anforderungen benannt. Diese Kennung ist in drei durch Punkte („.“) voneinander getrennte Teile gegliedert:

– Der erste Teil lautet „SP“ und steht für „IT-Sicherheitsprogramm“.
– Der zweite Teil ist eine zweistellige Kennung für den Bereich (Werte siehe Tabelle 3).
– Der dritte Teil ist eine zweistellige numerische Kennung für die jeweilige Anforderung innerhalb des Bereichs. Basisanforderungen und ihre weitergehenden Anforderungen haben alle dieselbe SP-Anforderungskennung. Siehe 5.5.2 für die Beschreibung der Basisanforderungen und ihrer weitergehenden Anforderungen.

5.5.2 Spalte „BR/RE“

Diese Spalte kennzeichnet die Anforderung entweder als Basisanforderung (BR) oder als eine weitergehende Anforderung (RE).

Basisanforderungen

Alle IT-Sicherheitsprogramme enthalten Basisanforderungen. Diese sind im Allgemeinen abstrakt formuliert, um den Dienstleistern Handlungsspielraum bei ihren Umsetzungen (Implementierungen) zu ermöglichen.

Weitergehende Anforderungen

Weitergehende Anforderungen schränken die Fähigkeiten der Basisanforderungen oder der erweiterten Anforderungen im Allgemeinen ein oder spezialisieren sie anderweitig. Weitergehende Anforderungen an Basisanforderungen führen eine Ebene der Einschränkung/Spezialisierung der Basisanforderung ein, während weitergehende Anforderungen an andere weitergehende Anforderungen noch höhere Ebenen der Einschränkungen/Spezialisierungen der Basisanforderung bieten. Das Ziel dieser Einschränkungen/Spezialisierungen ist die Erweiterung der Sicherheit durch die Anwendung anspruchsvollerer Fähigkeiten im Hinblick auf die IT-Sicherheit oder durch die strengere Anwendung dieser Fähigkeiten.

Implementierung der Anforderungen

Ein Dienstleister, der eine durch eine Basisanforderung definierte Fähigkeit umsetzt, darf somit auf eine breite Palette von Implementierungen zurückgreifen, um die Anforderung zu erfüllen. Ein Dienstleister, der eine durch eine erweiterte Anforderung definierte Fähigkeit umsetzt, kann dagegen nur auf einen eingeschränkten Bereich von Implementierungen zurückgreifen, die angewendet werden können.

Nummerierung der Anforderungen

Sowohl die Basisanforderung als auch ihre Erweiterungen haben dieselbe „SP-Anford.-ID“ (siehe 5.5.1). Weitergehende Anforderungen werden aufeinanderfolgend durchnummeriert, beginnend mit 1 für jede Basisanforderung.

Weitergehende Anforderungen werden aufeinanderfolgend durchnummeriert, beginnend mit 1 für jede BR und diese Folgenummer wird nach dem „RE“ in Klammern gesetzt. Daher ist der Spaltenwert RE(#), wobei # für die Folgenummer der Erweiterung steht. Weitergehende Anforderungen, die andere weitergehende Anforderungen erweitern, erhalten eine höhere Nummer als die weitergehende Anforderung, die sie erweitern.

BEISPIEL 1 „SP.01.02 BR“ ist eine Basisanforderung, die die Zuweisung von Personal, das zuvor über die IT-Sicherheitsanforderungen in IEC 62443-2-4 informiert worden ist, an die „Automatisierungslösung“ fordert und RE(1) erweitert diese Anforderung durch die Einführung der Anforderung von Überprüfungen der Vergangenheit der Mitarbeiter des der „Automatisierungslösung“ zugeordneten Dienstleisterpersonals. Diese Basisanforderung besagt, dass der Dienstleister in der Lage ist, jedermann, der zu den Anforderungen in IEC 62443-2-4 unterwiesen worden ist, der „Auto-

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62443-2-4:2020-07

matisierungslösung" zuzuordnen, wogegen RE(1) besagt, dass nur solche Personen eingesetzt werden dürfen, die die Überprüfungen der Vergangenheit als Mitarbeiter bestanden haben.

BEISPIEL 2 „SP.01.02 RE(2)" definiert eine Erweiterung der Anforderung RE(1) durch Spezialisierung der Anforderung RE(1), die so für das der „Automatisierungslösung" zugeordnete Personal des Unterauftragsnehmers gilt.[N1)]

5.5.3 Spalte „Bereich"

A1

Diese Spalte beschreibt die Organisation der Anforderungen in der obersten Ebene. Tabelle 3 enthält eine Liste der Bereiche. Die Bereiche in dieser Spalte stellen eine detaillierte Zusammenfassung der Bereiche dar, in der Dienstleister Konformität beanspruchen. Da jedoch der Bereich „Systemaufbau" sehr umfassend ist, ist seine Anwendung als Zusammenfassungsebene begrenzt. Deshalb wird er in drei Zusammenfassungsebenen mit den nachfolgend angegebenen Werten in der Spalte „Oberbegriff" unterteilt (siehe 5.5.4):

Zusammenfassungsebene	Spalte „Oberbegriff"
Netzwerksicherheit	Geräte – Netzwerk
	Netzauslegung
Vertiefung der Lösung	Geräte – Alle
	Geräte – Arbeitsplatzrechner
	Risikobewertung
	Komponenten
Schutz der Daten	Schutz der Daten

Tabelle 3 – Werte der Spalte „Bereich"

Wert	SP-Anford.-ID	Beschreibung
Mitarbeiter	SP.01.XX	Anforderungen an die Zuweisung von Personal durch den Dienstleister für Tätigkeiten in Zusammenhang mit der „Automatisierungslösung"
Zusicherung	SP.02.XX	Anforderungen an das Vertrauen, dass die IT-Sicherheitsleitlinien für die „Automatisierungslösung" durchgesetzt werden
Systemaufbau	SP.03.XX	Anforderungen an die Auslegung der „Automatisierungslösung"
Drahtlose Verbindung (drahtlos)	SP.04.XX	Anforderungen an die Verwendung von Drahtlose Verbindungen in der „Automatisierungslösung"
SIS	SP.05.XX	Anforderungen an die Integration von PLT-Sicherheitseinrichtungen in die „Automatisierungslösung"
Konfigurationsverwaltung	SP.06.XX	Anforderungen an die Konfigurationssteuerung der „Automatisierungslösung"
Fernzugriff	SP.07.XX	Anforderungen an den Fernzugriff auf die „Automatisierungslösung"
Behandlung von Ereignissen	SP.08.XX	Anforderungen an die Behandlung von Ereignissen in der „Automatisierungslösung"
Verwaltung von Nutzerkonten	SP.09.XX	Anforderungen an die Verwaltung von Nutzerkonten in der „Automatisierungslösung"
Schutz gegen Schadsoftware	SP.10.XX	Anforderungen an den Einsatz von Anti-Malware in der „Automatisierungslösung"
Patch-Management	SP.11.XX	Anforderungen an die IT-Sicherheitsaspekte der Genehmigung und Installation von Softwarepatches
Datensicherung/ -wiederherstellung	SP.12.XX	Anforderungen an die IT-Sicherheitsaspekte der Datensicherung und Wiederherstellung

[N1)] Nationale Fußnote: Diese Anforderung existiert in der Tabelle A.1 nicht.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62443-2-4:2020-07

5.5.4 Spalte „Oberbegriff“

Diese Spalte enthält das Schlüsselwort, welches den durch die Anforderung benannten Oberbegriff am besten beschreibt. Oberbegriffe sind unabhängig von Bereichen, damit Filtermechanismen eingesetzt werden können, um alle Anforderungen mit demselben Oberbegriff unabhängig vom Bereich zu ermitteln. Tabelle 4 enthält eine Liste der Werte dieser Spalte.

Tabelle 4 – Werte der Spalte „Oberbegriff“

Wert	Beschreibung
Nutzerkonten – …	Anforderungen an die verschiedenen Arten von Nutzerkonten
Werkzeuge und Software für die IT-Sicherheit	Anforderungen an die in der „Automatisierungslösung“ für IT-Sicherheitszwecke eingesetzte Anwendungssoftware und Werkzeuge
Überprüfung der Vergangenheit der Mitarbeiter	Anforderungen an Überprüfungen der Vergangenheit der Mitarbeiter
Datensicherung	Anforderungen an die Datensicherung und die Wiederherstellung einer „Automatisierungslösung“ aus einer Datensicherung
Schutz der Daten	Anforderungen an den Schutz von Daten
Geräte – …	Anforderungen an die verschiedenen in der „Automatisierungslösung“ benutzten Gerätearten
Ereignisse – …	Anforderungen an die unterschiedlichen in der „Automatisierungslösung“ verwendeten Ereignisarten (z. B. sicherheitsbezogen, IT-Sicherheitsverstöße, Alarme und Ereignisse)
Härtungsrichtlinien	Anforderungen an Richtlinien, die beschreiben, wie die „Automatisierungslösung“ gehärtet werden kann
Manuelles Vorgehen	Anforderungen an manuelle Vorgehensweisen zur Bereitstellung IT-Sicherheitsbezogener Fähigkeiten (z. B. Patch-Management, Datensicherung/Wiederherstellung)
Auslegung des Netzwerks	Anforderungen an die Auslegung der Netzarchitektur der „Automatisierungslösung“
Passwörter	Anforderungen an Passwörter von Nutzerkonten
Liste der Patches	Anforderungen an eine Liste von Kennungen (ID) und Eigenschaften von IT-Sicherheitspatches, die für die „Automatisierungslösung“ gelten
Personaleinsatzplanung	Anforderungen an die Zuweisung von Personal zur „Automatisierungslösung“
Mobile Datenträger	Anforderungen an die Nutzung mobiler Datenträger in der „Automatisierungslösung“
Wiederherstellung	Anforderungen an die Wiederherstellung der „Automatisierungslösung“ aus einer Datensicherung
Risikobeurteilung	Anforderungen an die Durchführung von Risikobeurteilungen für die „Automatisierungslösung“ und ihre Komponenten
Werkzeuge und Software für die IT-Sicherheit	Anforderungen an die Werkzeuge/Software, die bei der Implementierung und Verwaltung der IT-Sicherheit innerhalb der „Automatisierungslösung“ benutzt werden
Komponenten	Anforderungen an die in der „Automatisierungslösung“ verwendeten Komponenten
Unterweisung	Anforderungen an die Unterweisung von Personal, welches der „Automatisierungslösung“ zugewiesen wurde
Bedieneroberfläche	Anforderungen an die in der „Automatisierungslösung“ verwendeten Bedieneroberflächen
Sicherheitslücken	Anforderungen in Bezug auf Sicherheitslücken in der „Automatisierungslösung“

5.5.5 Spalte „Unterbegriff“

Diese Spalte enthält das Schlüsselwort, welches den durch die Anforderung benannten technischen Oberbegriff am besten beschreibt. Schlüsselworte technischer Oberbegriffe sind unabhängig von Bereichen und Tätigkeiten, damit Filtermechanismen eingesetzt werden können, um alle Anforderungen mit demselben technischen Oberbegriff unabhängig vom Bereich oder von der Tätigkeit zu ermitteln. Tabelle 5 enthält eine Liste der Werte dieser Spalte.

AVA Documents
Document Sharing Hub
Full document details: DIN EN IEC 62443-2-4:2020-07

Tabelle 5 – Werte der Spalte „Unterbegriff“ (1 von 2)

Wert	Beschreibung
Zugriffskontrolle	Anforderungen an die Authentifikation und/oder die Autorisierung
Netzverwaltung	Anforderungen an die Verwaltungs- und Managementtätigkeiten wie Geräte- und Kontenverwaltung
Genehmigung	Anforderungen an die Erlangung von Genehmigungen vom Betreiber
Änderung	Anforderungen an die Änderung von Passwörtern
Kommunikation	Anforderungen an die interne und externe Kommunikation der „Automatisierungslösung“
Zusammensetzung	Anforderungen an den Aufbau von Passwörtern
Konfigurationsmodus	Anforderungen an den Zustand eines Geräts, in dem eine Konfiguration möglich ist
Verbindungsmöglichkeiten	Anforderungen an die Netzverbindungsmöglichkeiten von Geräten und/oder Netzteilbereichen
Kryptographie	Anforderungen an die Nutzung von kryptographischen Mechanismen (z. B. Verschlüsselung, digitale Signaturen)
Daten- und Ereignisspeicherung	Anforderungen an die Archivierung von Daten und Ereignissen
Auslieferung	Anforderungen an die Auslieferung von Sicherheitspatchen
Erkennung	Anforderungen an die Erkennung von Ereignissen
Wiederherstellung nach einer Katastrophensituation	Anforderungen an die Wiederherstellung nach einer Katastrophensituation
Ablaufregelung	Anforderungen an die Gültigkeitsdauer von Konten und Passwörtern
Installation	Anforderungen an die Installation sicherheitsbezogener Werkzeuge und Software
Bestandsverzeichnis	Anforderungen an die Dokumentation von in der „Automatisierungslösung“ eingesetzten Geräten und deren Softwarekomponenten
Geringste Funktionalität	Anforderungen an die Unterstützung der Idee der geringsten Funktionalität (z. B. Deaktivierung unnötiger Dienste oder Löschen eines temporären Kontos, welches nicht mehr benötigt wird). Weitere Einzelheiten in Bezug auf die geringste Funktionalität siehe IEC 62443-3-3.
Protokollierung	Anforderungen an Audit- und Ereignisprotokolle
Schadsoftwaredefinitionen	Anforderungen an die Freigabe und die Nutzung von Dateien mit Definitionen von Schadsoftware
Schutzmechanismen gegen Schadsoftware	Anforderungen an die Nutzung von Schutzmechanismen gegen Schadsoftware (z. B. Antivirus-Software, Whitelisting-Software)
Netzzeit	Anforderungen an die Verteilung und Synchronisierung einer Zeit im Netz
Eignung von Patches	Anforderungen an die Bewertung von Patches und deren Freigabe zur Verwendung in der „Automatisierungslösung“
Ausführen	Anforderungen an die Ausführung einer Fähigkeit für die „Automatisierungslösung“
Berichtswesen	Anforderungen an Berichte über Ereignisse (z. B. Meldungen)
Reaktion	Anforderungen an die Behandlung von Ereignissen und an die Reaktion auf Ereignisse
Wiederverwendung	Anforderungen an die Wiederverwendung von Passwörtern
Robustheit	Anforderungen an die Fähigkeit der „Automatisierungslösung“ und ihrer Komponenten, außergewöhnlichen Daten, außergewöhnlichen Abläufen oder außergewöhnlich großem Verkehr im Netz, wie Alarmhäufungen und Netzwerk-Scans, standzuhalten
Bereinigung	Anforderungen an die Säuberung von Geräten und mobilen Datenträgern von schützenswerten Daten und/oder Schadsoftware
IT-Sicherheitskontaktstelle	Anforderungen, die die Rolle der „IT-Sicherheitskontaktstelle“ definieren und vorgeben

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62443-2-4:2020-07

Tabelle 5 (2 von 2)

Wert	Beschreibung
Führungskräfte für IT-Sicherheit	Anforderungen, die die Rolle der „Führungskräfte für IT-Sicherheit" definieren und vorgeben
IT-Sicherheitsanforderungen – …	Anforderungen an die in dieser Spezifikation enthaltenen oder vom Betreiber definierten IT-Sicherheitsanforderungen
Schützenswerte Daten	Anforderungen an Daten, die besonders zu schützen sind
Dienstleister	Anforderungen an das Personal des Dienstleisters oder dessen Fähigkeiten
Sitzungssperre	Anforderungen an die Sperre der Tastatur und des Bildschirms von Arbeitsplatzrechnern oder Programmiersystem
Gemeinsame Nutzung	Anforderungen bezüglich der gemeinsamen Nutzung von Passwörtern
Unterauftragnehmer	Anforderungen an das Personal eines Unterauftragnehmers, an dessen Berater oder Vertreter sowie deren Fähigkeiten
Technische Beschreibung	Anforderungen an Beschreibungen bestimmter technischer Aspekte der „Automatisierungslösung"
Nutzung	Anforderungen an die Nutzung oder Anwendung einer geforderten Fähigkeit
Verifikation	Anforderungen an die Verifikation einer Fähigkeit (z. B. über einen Nachweis oder eine Sichtprüfung
Kennungen von drahtlosen Netzen	Anforderungen an die Kennungen für drahtlose Netze

5.5.6 Spalte „Dokumentation"

Diese Spalte enthält ein „Ja", um anzuzeigen, dass die Anforderung eine Fähigkeit beschreibt, die eine lieferbare Dokumentation für den Betreiber erfordert. Sofern in dieser Spalte ein „Nein" angegeben ist, kann es dennoch erforderlich sein, dass der Dienstleister zur Unterstützung der geforderten Fähigkeit eine Dokumentation erstellt und/oder pflegt, diese aber nicht dem Betreiber ausgehändigt werden muss. Jedoch kann der Betreiber in separaten Vereinbarungen beanspruchen, dass ihm jede Art von Dokumentation auszuhändigen ist.

A1

5.5.7 Spalte „Beschreibung der Anforderung"

Diese Spalte enthält die Beschreibung der Anforderung in Textform. Darin dürfen auch Anmerkungen mit Beispielen enthalten sein, die das Verständnis der Anforderung fördern.

Jede Anforderung definiert eine vom Dienstleister geforderte Fähigkeit. Ob ein Betreiber den Dienstleister auffordert, die Fähigkeit zu erbringen, gehört nicht zum Anwendungsbereich dieses Dokuments.

Der Begriff „sicherstellen" wird in vielen Anforderungen verwendet und bedeutet „ein hohes Vertrauensniveau bereitstellen". Er wird benutzt, wenn der Dienstleister bestimmte Mittel wie einen Nachweis, eine Verifikation oder einen Prozess besitzen muss, mit denen dieses Vertrauensniveau bereitgestellt werden kann.

A1

Die Formulierung „in den Bereichen IT-Sicherheit und industrielle Automatisierung allgemein akzeptiert" wird in diesen Beschreibungen der Anforderung anstelle einzelner Sicherheitsverfahren wie etwa speziellen Verschlüsselungsmechanismen verwendet. Mit dieser Formulierung wird die Entwicklung von Verfahren mit höherer Sicherheit als Ersatz für Verfahren, deren Schwachstellen offengelegt wurden, ermöglicht.

Um diese Anforderungen zu erfüllen, müssen Dienstleister Verfahren (z. B. Verschlüsselung) anwenden, die allgemein anerkannt sind und zu dem Zeitpunkt, zu dem die Übereinstimmung beansprucht wird, im Sicherheitsbereich und im Bereich der industriellen Automatisierung angewendet werden. Verfahren wie die Sicherheitsalgorithmen Digital Encryption Standard (DES) und Wireless Equivalent Privacy (WEP), die nicht mehr als sicher angesehen werden, entsprechen nicht den Anforderungen.

AVA Documents
Document Sharing Hub
Full document details: DIN EN IEC 62443-2-4:2020-07

A1

5.5.8 Spalte „Begründung“

Zum besseren Verständnis jeder Anforderung enthält diese Spalte die Begründung, die die Überlegungen hinter jeder Anforderung (d. h. Zweck/Nutzen der geforderten Fähigkeit) beschreibt, und gibt zusätzliche Leitlinien vor. In vielen Beschreibungen wird der Hinweis „verfügt über einen nachweisbaren Prozess“ verwendet. „Nachweisbar“ bedeutet, dass der Dienstleister über einen Prozess verfügt, den er verwenden, benennen und für den Betreiber ausführen kann. Unter Anwendung des in 4.2 beschrieben Reifegradmodells bedeutet dies, dass der Prozess noch nicht formal dokumentiert zu sein braucht (Reifegrad 1).

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62443-2-4:2020-07

Anhang A
(normativ)

IT-Sicherheitsanforderungen

Tabelle A.1 – Anforderungen an das IT-Sicherheitsprogramm[N1] (1 von 104)

Anford.-ID	BR/RE	Bereich	Oberbegriff	Unterbegriff	Doku?	Beschreibung der Anforderung	Begründung
SP.01.01	BR	Mitarbeiter	Unterweisung	IT-Sicherheitsanforderungen – IEC 62443-2-4	Nein	Der Dienstleister muss die Fähigkeit besitzen, sicherzustellen, dass er ausschließlich eigenem Personal „Automatisierungslösungs"-bezogene Tätigkeiten zuweist, das in den in dieser Spezifikation geforderten Verantwortlichkeiten, Leitlinien und Vorgehensweisen unterwiesen wurde und diese erfüllt.	Mit den von dieser BR und ihren REs festgelegten Fähigkeiten wird die „Automatisierungslösung" gegen Bedrohungen geschützt, die durch das Personal von Dienstleistern, Unterauftragnehmern und Beratern ausgelöst werden, die sich ihrer normalen IT-Sicherheitsverantwortlichkeiten (d. h. bewährten IT-Sicherheitsverfahren) nicht bewusst sind. Allzu oft sind IT-Sicherheitsverstöße das Ergebnis von Personal, das Tätigkeiten durchführt, ohne wahrzunehmen, dass es damit ein bewährtes IT-Sicherheitsverfahren verletzt (z. B. Einstecken eines nicht autorisierten USB-Speichersticks), oder das versäumt, eine entsprechende Tätigkeit durchzuführen (z. B. Unterlassen der Aktualisierung einer Firewall-Regel der IT-Sicherheitszone nach dem Entfernen eines externen Arbeitsplatzrechners). Ein über diese Fähigkeit verfügender Dienstleister zu sein, bedeutet, dass dieser sicherheitsbewusstes Personal zur Arbeit an der „Automatisierungslösung" bereitstellen kann. Zur Anleitung des Personals gehören im Allgemeinen Unterweisung und/oder Überprüfung der Vorgehensweisen. ANMERKUNG 1 Betreiber dürfen auf einer schriftlichen Bestätigung der erfolgten Unterweisung bestehen. ANMERKUNG 2 Reifegrade 3 und 4 (siehe 4.2) gelten für die Durchsetzung der (die Übereinstimmung mit den) Verantwortlichkeiten, Leitlinien und Vorgehensweisen.

[N1] Nationale Fußnote: Tabelle A .1 ist auf CD-ROM veröffentlicht.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62443-2-4:2020-07

Tabelle A.1 (2 von 104)

Anford.-ID	BR/RE	Bereich	Oberbegriff	Unterbegriff	Doku?	Beschreibung der Anforderung	Begründung
SP.01.01	RE(1)	Mitarbeiter	Unterweisung	IT-Sicherheitsanforderungen – IEC 62443-2-4	Nein	Der Dienstleister muss die Fähigkeit besitzen, sicherzustellen, dass er ausschließlich Personal des Unterauftragnehmers oder des Beraters „Automatisierungslösungs"-bezogene Tätigkeiten zuweist, das in den in dieser Spezifikation geforderten Verantwortlichkeiten, Leitlinien und Vorgehensweisen unterwiesen wurde und diese erfüllt.	Ein über diese Fähigkeit verfügender Dienstleister zu sein, bedeutet, dass dieser sicherheitsbewusstes Personal des Unterauftragnehmers, sicherheitsbewusste Berater und Vertreter zur Arbeit an der „Automatisierungslösung" bereitstellen kann. Siehe ISO/IEC 27036-3 für weitergehende organisatorische Anforderungen an die Lieferkette.
SP.01.02	BR	Mitarbeiter	Unterweisung	IT-Sicherheitsanforderungen – Betreiber	Nein	Der Dienstleister muss die Fähigkeit besitzen, sicherzustellen, dass er ausschließlich seinem eigenen Personal, Personal des Unterauftragnehmers oder des Beraters „Automatisierungslösungs"-bezogene Tätigkeiten zuweist, das in den vom Betreiber geforderten Verantwortlichkeiten, Leitlinien und Vorgehensweisen unterwiesen wurde und diese erfüllt.	Mit der von dieser BR festgelegten Fähigkeit werden Bedrohungen für die „Automatisierungslösung" gemindert, die durch das Personal von Dienstleistern, Unterauftragnehmern und Beratern ausgelöst werden können, die sich ihrer „Automatisierungslösungs"-spezifischen IT-Sicherheitsverantwortlichkeiten (wie vom Betreiber definiert) nicht bewusst sind. Allzu oft sind IT-Sicherheitsverstöße das Ergebnis von Personal, das sich der vom Betreiber festgelegten IT-Sicherheitsanforderungen nicht bewusst ist (z. B. Missbrauch oder falsche gemeinsame Nutzung eines Instandhaltungskontos). Ein über diese Fähigkeit verfügender Dienstleister zu sein, bedeutet, dass dieser über einen nachweisbaren Prozess verfügt, mit dem sichergestellt wird, dass das zur Arbeit an der „Automatisierungslösung" bereitgestellte Personal die vom Betreiber vorgegebenen IT-Sicherheitsanforderungen kennt und diese auch befolgt. Dies gilt sowohl für das Personal des Dienstleisters als auch für Unterauftragnehmer, Berater und Vertreter. Zur Anleitung des Personals gehören im Allgemeinen Schulung und/oder Überprüfung der Vorgehensweisen.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62443-2-4:2020-07

Tabelle A.1 (3 von 104)

Anford.-ID	BR/RE	Bereich	Oberbegriff	Unterbegriff	Doku?	Beschreibung der Anforderung	Begründung
							Siehe ISO/IEC 27036-3 für weitergehende organisatorische Anforderungen an die Lieferkette. ANMERKUNG 1 Betreiber dürfen auf einer schriftlichen Bestätigung der erfolgten Unterweisung bestehen. ANMERKUNG 2 Reifegrade 3 und 4 (siehe 4.2) gelten für die Durchsetzung der (die Übereinstimmung mit den) Verantwortlichkeiten, Leitlinien und Vorgehensweisen.
SP.01.02	RE(1)	Mitarbeiter	Unterweisung	IT-Sicherheitsanforderungen – Betreiber	Nein	Der Dienstleister muss die Fähigkeit besitzen, sicherzustellen, dass er ausschließlich seinem eigenen Personal, Personal des Unterauftragnehmers oder des Beraters „Automatisierungslösungs"-bezogene Tätigkeiten zuweist, das über die vom Betreiber vorgegebenen Prozesse zur Vornahme von Änderungen (MoC) und zur Arbeitserlaubnis (PtW) für Änderungen an Geräten, Arbeitsplatzrechnern und Servern und deren Verbindungen untereinander unterwiesen wurde und diese erfüllt.	Mit der von dieser RE festgelegten Fähigkeit werden Bedrohungen für die „Automatisierungslösung" gemindert, die durch das Personal von Dienstleistern ausgelöst werden, das ohne Autorisierung auf die „Automatisierungslösung" zugreift und nicht autorisierte Änderungen an der „Automatisierungslösung" vornimmt. Ein über diese Fähigkeit verfügender Dienstleister zu sein, bedeutet, dass dieser über einen nachweisbaren Prozess verfügt, mit dem sichergestellt wird, dass das zur Arbeit an der „Automatisierungslösung" bereitgestellte Personal die vom Betreiber vorgegebenen Prozesse zur Vornahme von Änderungen (MoC) und zur Arbeitserlaubnis (PtW) kennt und diese auch befolgt und damit sichergestellt wird, dass Änderungen an Geräten, Arbeitsplatzrechnern und Servern korrekt geleitet werden. ANMERKUNG Reifegrade 3 und 4 (siehe 4.2) gelten für die Durchsetzung der (die Übereinstimmung mit den) Verantwortlichkeiten, Leitlinien und Vorgehensweisen.

AVA Documents
Document Sharing Hub

Full document details: DIN EN IEC 62443-2-4:2020-07

Tabelle A.1 (4 von 104)

Anford.-ID	BR/RE	Bereich	Oberbegriff	Unterbegriff	Doku?	Beschreibung der Anforderung	Begründung
SP.01.03	BR	Mitarbeiter	Unterweisung	Schützenswerte Daten	Nein	Der Dienstleister muss die Fähigkeit besitzen, sicherzustellen, dass er ausschließlich seinem eigenen Personal „Automatisierungslösungs"-bezogene Tätigkeiten zuweist, das über Leitlinien, Vorgehensweisen und vertragliche Verpflichtungen unterwiesen wurde, die benötigt werden, um die Vertraulichkeit der Daten des Betreibers zu schützen, und diese erfüllt.	Mit den von dieser BR und ihren REs festgelegten Fähigkeiten wird die „Automatisierungslösung" gegen die falsche Handhabung der Daten des Betreibers und damit gegen deren mögliche Offenlegung geschützt (z. B. Ausdrucken einer Rezeptur und diese unbeaufsichtigt oder für Umstehende sichtbar liegen lassen). Ein über diese Fähigkeit verfügender Dienstleister zu sein, bedeutet, dass dieser Personal zur Arbeit an der „Automatisierungslösung" bereitstellen kann, das sich seiner Verantwortlichkeit zum Schutz der dem Betreiber gehörenden Daten gegen Offenlegung bewusst ist. Es ist üblich, hierfür Geheimhaltungsvereinbarungen (Non-Disclosure Agreements, NDA) einzusetzen, in denen die Bedingungen für den Schutz vertraulicher Daten definiert sind, einschließlich einer Angabe, welche Daten zu schützen sind und welche besonderen Handhabungsanforderungen bestehen. Über diese Fähigkeit zu verfügen, bedeutet außerdem, dass der Dienstleister über einen nachweisbaren Prozess verfügen muss, um sein Personal über die Existenz und die Bedingungen einer solchen Geheimhaltungsvereinbarung zu informieren. Zusätzlich darf der Betreiber einen gewissen (z. B. schriftlichen) Nachweis verlangen, dass das Personal über diese Verantwortlichkeiten informiert wurde. Siehe ISO/IEC 27036-3 für weitergehende organisatorische Anforderungen an die Lieferkette zwischen Betreiber und Dienstleister. ANMERKUNG Reifegrade 3 und 4 (siehe 4.2) gelten für die Durchsetzung der (die Übereinstimmung mit den) Verantwortlichkeiten, Leitlinien und Vorgehensweisen.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62443-2-4:2020-07

Tabelle A.1 (5 von 104)

Anford.-ID	BR/RE	Bereich	Oberbegriff	Unterbegriff	Doku?	Beschreibung der Anforderung	Begründung
SP.01.03	RE(1)	Mitarbeiter	Unterweisung	Schützenswerte Daten	Nein	Der Dienstleister muss die Fähigkeit besitzen, sicherzustellen, dass er ausschließlich Personal von Unterauftragnehmern, Beratern oder Vertretern „Automatisierungslösungs"-bezogene Tätigkeiten zuweist, das über Leitlinien und Vorgehensweisen unterwiesen wurde, die benötigt werden, um die Vertraulichkeit der Daten des Betreibers zu schützen.	Ein über diese Fähigkeit verfügender Dienstleister zu sein, bedeutet, dass dieser sicherstellen kann, dass Unterauftragnehmer, Berater und Vertreter, die zur Arbeit an der „Automatisierungslösung" angewiesen wurden, sich ihrer Verantwortlichkeit zum Schutz der dem Betreiber gehörenden Daten gegen Offenlegung bewusst sind. Es ist üblich, hierfür Geheimhaltungsvereinbarungen (NDA) einzusetzen, in denen die Bedingungen für den Schutz vertraulicher Daten definiert sind, einschließlich einer Angabe, welche Daten zu schützen sind und welche besonderen Handhabungsanforderungen bestehen. Über diese Fähigkeit zu verfügen, bedeutet außerdem, dass der Dienstleister über einen nachweisbaren Prozess verfügen muss, um dieses Personal über die Existenz und die Bedingungen einer solchen Geheimhaltungsvereinbarung zu informieren. Zusätzlich darf der Betreiber einen gewissen (z. B. schriftlichen) Nachweis verlangen, dass das Personal über diese Verantwortlichkeiten informiert wurde. Siehe ISO/IEC 27036-3 für weitergehende organisatorische Anforderungen an die Lieferkette zwischen Betreiber und Dienstleister. ANMERKUNG Reifegrade 3 und 4 (siehe 4.2) gelten für die Durchsetzung der (die Übereinstimmung mit den) Verantwortlichkeiten, Leitlinien und Vorgehensweisen.

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62443-2-4:2020-07

Tabelle A.1 (6 von 104)

Anford.-ID	BR/RE	Bereich	Oberbegriff	Unterbegriff	Doku?	Beschreibung der Anforderung	Begründung
SP.01.04	BR	Mitarbeiter	Überprüfung der Vergangenheit der Mitarbeiter	Dienstleister	Nein	Der Dienstleister muss die Fähigkeit besitzen sicherzustellen, dass er automatisierungslösungsbezogene Tätigkeiten ausschließlich seinem eigenen Personal zuweist, das sicherheitsbezogene Überprüfungen der Vergangenheit der Mitarbeiter, soweit durchführbar und rechtlich zulässig, erfolgreich bestanden hat.	Mit den von dieser BR und ihren REs festgelegten Fähigkeiten wird die Automatisierungslösung gegen eine Personalausstattung geschützt, deren Vertrauenswürdigkeit unter Umständen fraglich ist. Obwohl durch die Überprüfung der Vergangenheit der Mitarbeiter keine Vertrauenswürdigkeit gewährleistet werden kann, können Mitarbeiter ermittelt werden, deren Vertrauenswürdigkeit bereits zu Beschwerden geführt hat. Ein über diese Fähigkeit verfügender Dienstleister zu sein bedeutet, dass dieser über einen nachweisbaren Prozess verfügt, mit dem er die Integrität seines Personals, das er der Arbeit an der Automatisierungslösung zuweist, verifizieren kann. Bei dieser Forderung wird auch berücksichtigt, dass die Durchführbarkeit von Überprüfungen der Vergangenheit der Mitarbeiter aufgrund rechtlicher Vorgaben oder aufgrund fehlender Unterstützung durch örtliche Behörden und/oder Dienstleistungsorganisationen nicht immer möglich sein wird. Es gibt beispielsweise Länder, die die Überprüfung der Vergangenheit der Mitarbeiter zwar nicht verbieten, die Durchführung solcher Überprüfungen aber nicht unterstützen, wodurch die Überprüfung für den Dienstleister unmöglich wird. Wie und wie häufig Überprüfungen der Vergangenheit der Mitarbeiter durchgeführt werden, bleibt dem Dienstleister überlassen. Zu Überprüfungen der Vergangenheit der Mitarbeiter können beispielsweise eine Identitätsprüfung und ein polizeiliches Führungszeugnis gehören.

A1

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62443-2-4:2020-07

Tabelle A.1 (7 von 104)

Anford.-ID	BR/RE	Bereich	Oberbegriff	Unterbegriff	Doku?	Beschreibung der Anforderung	Begründung
SP.01.04	RE(1)	Mitarbeiter	Überprüfung der Vergangenheit der Mitarbeiter	Unterauftragnehmer	Nein	Der Dienstleister muss die Fähigkeit besitzen sicherzustellen, dass er ausschließlich Mitarbeitern von Unterauftragnehmern, Beratern und Vertretern „Automatisierungslösungs-bezogene" Tätigkeiten zuweist, die sicherheitsbezogene Überprüfungen ihrer Vergangenheit, soweit durchführbar und rechtlich zulässig, erfolgreich bestanden haben.	Ein über diese Fähigkeit verfügender Dienstleister zu sein bedeutet, dass dieser über einen nachweisbaren Prozess verfügt, mit dem er die Integrität seiner Unterauftragnehmer, Berater und Vertreter, denen er Arbeit an der Automatisierungslösung zuweist, verifizieren kann. Bei dieser Forderung wird auch berücksichtigt, dass die Durchführbarkeit von Überprüfungen der Vergangenheit der Mitarbeiter aufgrund rechtlicher Vorgaben oder aufgrund fehlender Unterstützung durch örtliche Behörden und/oder Dienstleistungsorganisationen nicht immer möglich sein wird. Es gibt beispielsweise Länder, die die Überprüfung der Vergangenheit der Mitarbeiter zwar nicht verbieten, die Durchführung solcher Überprüfungen aber nicht unterstützen, wodurch die Überprüfung für den Dienstleister unmöglich wird. Wie und wie häufig Überprüfungen der Vergangenheit der Mitarbeiter durchgeführt werden, bleibt dem Dienstleister überlassen. Zu Überprüfungen der Vergangenheit der Mitarbeiter können beispielsweise eine Identitätsprüfung und ein polizeiliches Führungszeugnis gehören. Siehe ISO/IEC 27036-3 für weitergehende organisatorische Anforderungen an die Lieferkette.

A1

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62443-2-4:2020-07

Tabelle A.1 (8 von 104)

Anford.-ID	BR/RE	Bereich	Oberbegriff	Unterbegriff	Doku?	Beschreibung der Anforderung	Begründung
SP.01.05	BR	Mitarbeiter	Personal-einsatzpla-nung	IT-Sicherheits-kontaktstelle	Nein	Der Dienstleister muss die Fähigkeit besitzen, in seiner Organisation eine IT-Sicherheitskontakt-stelle für die „Automatisierungslösung" zu benen-nen, die für folgende Tätigkeiten zuständig und verantwortlich ist. 1) Verbindungsstelle zum Betreiber bezüglich der vom Dienstleister und der „Automatisie-rungslösung" erwarteten Befolgung der Anfor-derungen im Teil 2-4, soweit vom Betreiber gefordert. 2) Übermittlung der Ansichten des Dienstleisters zur IT-Sicherheit des industriellen Automati-sierungssystems an die Mitarbeiter des Betreibers. 3) Sicherstellen, dass Angebote an den Betrei-ber an die Anforderungen im Teil 2-4 ange-passt sind und diese einhalten, soweit vom Betreiber gefordert und durch die internen IT-Sicherheitsanforderungen des Dienstleisters für industrielle Automatisierungssysteme vor-gegeben. 4) Übermittlung von Abweichungen oder sonsti-gen vom Betreiber geforderten, nicht mit den Anforderungen im Teil 2-4 in Einklang ste-henden Punkten an den Betreiber. Dazu gehören Abweichungen zwischen diesen Anforderungen und den internen Anforderun-gen des Dienstleisters.	Mit der von dieser BR festgelegten Fähigkeit wird die sicher-heitsbezogene Kommunikation zwischen Betreiber und Dienstleister verbessert, damit der Dienstleister besser auf die Belange der IT-Sicherheit der „Automatisierungslösung" eingehen kann. Ein über diese Fähigkeit verfügender Dienstleister zu sein, bedeutet, dass dieser über einen nachweisbaren Prozess verfügt, der „Automatisierungslösung" eine Person zuzuwei-sen, die für die Koordinierung der auf die IT-Sicherheit bezo-genen Punkte mit dem Betreiber verantwortlich ist; dies betrifft z. B. Abweichungen von den in den Teilen 2-4 und 3-3 enthaltenen Anforderungen. Eine IT-Sicherheitskontaktstelle liefert die Organisations-struktur zwischen Betreiber und Dienstleister für eine Behandlung der Abweichungen von den Fähigkeiten nach Teil 2-4 und der Abweichungen des in der „Automatisie-rungslösung" verwendeten Automatisierungssystems von den Anforderungen nach Teil 3-3 (z. B. wie Ausgleichsmaß-nahmen zu treffen sind).

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62443-2-4:2020-07

Tabelle A.1 (9 von 104)

	Anford.-ID	BR/RE	Bereich	Oberbegriff	Unterbegriff	Doku?	Beschreibung der Anforderung	Begründung
A1	SP.01.06	BR	Mitarbeiter	Personal-einsatzpla-nung	Führungskräfte für IT-Sicherheit	Nein	Der Dienstleister muss für die Führungs-positionen der IT-Sicherheit Nachweise über die Mindestqualifikationen für die IT-Sicherheit des IACS besitzen und er muss die Fähigkeit be-sitzen, für Automatisierungslösungen Führungs-kräfte für IT-Sicherheit einzusetzen, die diese Qualifikationen erfüllen.	Mit der von dieser BR festgelegten Fähigkeit werden Fehler bei Entscheidungen, die die IT-Sicherheit betreffen, und deren Umsetzung verringert. Schlechte Entscheidungen oder Mängel bei der richtigen Umsetzung der IT-Sicherheit können die Automatisierungslösung unnötigen IT-Sicher-heitsbedrohungen und/oder -verstößen aussetzen. Ein über diese Fähigkeit verfügender Dienstleister zu sein bedeutet, dass dieser die Qualifikationen (Fachwissen/ Befähigung) nachgewiesen hat, die er von Personal verlangt, das IT-sicherheitsbezogene Tätigkeiten anleitet, und dass er über einen nachweisbaren Prozess verfügt, jede Automati-sierungslösung mit Personal auszustatten, das dieses Fach-wissen besitzt. Zum Fachwissen dürfen Erfahrungen mit der IT-Sicherheit von IACS, Unterweisung und Zertifizierung gehören und im Allgemeinen treffen Dienstleister und Betreiber vor dem Personaleinsatz eine Vereinbarung über die Qualifikation des Personals hinsichtlich der IT-Sicherheit. Die Formulierung „diese Qualifikationen erfüllen" wird für die Angabe verwendet, dass die Führungskräfte für IT-Sicher-heit, die der Automatisierungslösung zugewiesen werden, die entsprechenden Erfahrungen besitzen, die in Überein-stimmung mit diesen Qualifikationen stehen.

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62443-2-4:2020-07

Tabelle A.1 (10 von 104)

Anford.-ID	BR/RE	Bereich	Oberbegriff	Unterbegriff	Doku?	Beschreibung der Anforderung	Begründung
SP.01.07	BR	Mitarbeiter	Personal-einsatzpla-nung	Änderung	Nein	Der Dienstleister muss die Fähigkeit besitzen, den Betreiber über Veränderungen beim Perso-nal des Dienstleisters, Unterauftragnehmers oder Beraters, das Zugriff auf die „Automatisierungslö-sung" hat, zu informieren.	Mit der von dieser BR festgelegten Fähigkeit wird die „Auto-matisierungslösung" gegen Bedrohungen geschützt, die durch das Personal des Dienstleisters, Unterauftragnehmers und/oder Beraters entstehen, die keinen Zugriff auf die „Automatisierungslösung" mehr benötigen. Nach der Mitteilung über Veränderungen des Personals kann der Betreiber die Autorisierung für den Zugriff entsprechend aktualisieren (z. B. Entziehen von Dienstausweisen, Löschen von Nutzerkonten und Zugriffskontrollllisten auf den neuesten Stand bringen). Ein über diese Fähigkeit verfügender Dienstleister zu sein, bedeutet, dass dieser über einen nachweisbaren Prozess verfügt, um den Betreiber über Veränderungen bei der Per-sonalzusammensetzung des Dienstleisters zu informieren. Die Rechtzeitigkeit einer Mitteilung und welche Personaländerungen mitgeteilt werden müssen, sind typische vom Dienstleister und Betreiber zu vereinbarende Elemente. So bräuchte z. B. das Personal des Dienstleisters, das auf eine „Automatisierungslösung" über temporäre Nutzerkonten zugreift, nicht aufgenommen zu werden, da dessen tempo-räre Nutzerkonten gelöscht werden, wenn sie nicht mehr benötigt werden.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62443-2-4:2020-07

Tabelle A.1 (11 von 104)

Anford.-ID	BR/RE	Bereich	Oberbegriff	Unterbegriff	Doku?	Beschreibung der Anforderung	Begründung
SP.02.01	BR	Zusicherung	Komponenten	Verifikation	Ja	Der Dienstleister muss die Fähigkeit besitzen, eine Dokumentation vorzulegen, die verifiziert, dass Komponenten der „Automatisierungslösung", die vom Betreiber bezeichnet werden (z. B. als Ergebnis einer IT-Sicherheitsbeurteilung, einer Bedrohungsanalyse und/oder einer IT-Sicherheitsprüfung) eine ihrer Risikostufe angemessene IT-Sicherheit aufweisen.	Mit der von dieser BR festgelegten Fähigkeit wird Vertrauen geschaffen, dass Komponenten in der „Automatisierungslösung" Fähigkeiten im Hinblick auf die IT-Sicherheit besitzen, die ihrer Risikostufe der IT-Sicherheit angemessen sind. Ein über diese Fähigkeit verfügender Dienstleister zu sein, bedeutet, dass dieser über einen nachweisbaren Prozess für die Bestätigung verfügt, dass Komponenten der „Automatisierungslösung" die vom Betreiber geforderte angemessene IT-Sicherheitsstufe bereitstellen. Diese Bestätigung darf durch IT-Sicherheitsbewertungen und -zertifizierungen, Prüfungen und/oder andere Methoden erfolgen. IT-Sicherheitsprüfungen betreffen System- oder Komponentenprüfungen mit dem Hauptziel der Aufdeckung von Sicherheitslücken und andererseits zum Nachweis dafür, dass spezifische Angriffe wie vorgesehen behandelt werden (z. B. abgeschwächt, vereitelt und/oder abgelenkt/isoliert werden). Eine bestandene IT-Sicherheitsprüfung bedeutet nicht notwendigerweise, dass das geprüfte Element keine Sicherheitslücken besitzt. Beispiele für Sicherheitsprüfungen sind Penetrationstest, Fuzz-Test, Prüfung der Robustheit und Absuchen nach Sicherheitslücken. Für entsprechende Anforderungen an die Lieferkette wird auf IEC 62443-4-1, IEC 62443-4-2 und ISO 27036-3 verwiesen.

Documents
Document Sharing Hub

Full document details: DIN EN IEC 62443-2-4:2020-07

Tabelle A.1 (12 von 104)

Anford.-ID	BR/RE	Bereich	Oberbegriff	Unterbegriff	Doku?	Beschreibung der Anforderung	Begründung
SP.02.02	BR	Zusicherung	Werkzeuge und Software für die IT-Sicherheit	Technische Beschreibung	Ja	Der Dienstleister muss die Fähigkeit besitzen, Werkzeuge zur IT-Sicherheitsanalyse für den Einsatz in der „Automatisierungslösung" zu empfehlen (z. B. Werkzeuge zum Netzwerk-Scan) und: 1) Anleitungen zu deren Verwendung zu liefern; 2) auf gegebenenfalls bekannte nachteilige Auswirkungen auf die Leistung der „Automatisierungslösung" hinzuweisen; 3) empfehlen, wie nachteilige Auswirkungen vermieden werden können.	Mit den von dieser BR und ihren REs festgelegten Fähigkeiten wird sichergestellt, dass die „Automatisierungslösung" mit vom Betreiber zugelassenen Werkzeugen auf sicherheitsbezogene Probleme untersucht werden kann. Hierzu gehören die Ermittlung nicht autorisierter Geräte am Netzwerk und/oder nicht autorisierter offener Ports an einem Gerät. Ein über diese Fähigkeit verfügender Dienstleister zu sein, bedeutet, dass dieser über einen nachweisbaren Prozess verfügt, um ein oder mehrere Werkzeuge zur IT-Sicherheitsanalyse für die „Automatisierungslösung" zu empfehlen, zusammen mit Angaben zu möglichen Problemen, die deren Einsatz verursachen kann, und mit Hinweisen, wie diese vermieden werden können. Diese Anforderung schließt ein, dass sich der Dienstleister möglicher Probleme bewusst ist, die ein von ihm empfohlenes Werkzeug verursachen kann, und diese dem Betreiber meldet zusammen mit Empfehlungen dafür, wie sie vermieden werden können und wie die Werkzeuge effektiv eingesetzt werden können. Das Vermeiden möglicher Probleme im Zusammenhang mit dem Einsatz der Werkzeuge kann durch Beschränkung der Konfigurationsmöglichkeiten, Einplanen von Prüfungen zu geeigneten Zeiten oder durch andere Maßnahmen erreicht werden. Falls beispielsweise bekannt ist, dass ein Werkzeug zum Netzwerk-Scan das Netz überlasten kann, kann es so konfiguriert werden, dass es den Netzverkehr nur gering beeinträchtigt, oder das Netz kann aufgeteilt werden, um das Ausmaß der Überlastungen zu verringern.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62443-2-4:2020-07

Tabelle A.1 (13 von 104)

Anford.-ID	BR/RE	Bereich	Oberbegriff	Unterbegriff	Doku?	Beschreibung der Anforderung	Begründung
SP.02.02	RE(1)	Zusicherung	Werkzeuge und Software für die IT-Sicherheit	Genehmigung	Nein	Der Dienstleister muss die Fähigkeit besitzen sicherzustellen, dass er vom Betreiber eine Genehmigung erhält, bevor er Werkzeuge zur Untersuchung des Netzwerks (z. B. Netzwerk-Scans) am Ort des Betreibers einsetzt.	Ein über diese Fähigkeit verfügender Dienstleister zu sein, bedeutet, dass dieser über einen nachweisbaren Prozess zur Koordinierung des Einsatzes von Werkzeugen zur Untersuchung des Netzwerks in der „Automatisierungslösung" mit dem Betreiber verfügt und von diesem die Genehmigung zum Einsatz erhält. Die BR für diese RE verlangt vom Dienstleister, dass er in der Lage ist, den Betreiber über mögliche nachteilige Auswirkungen dieser Werkzeuge auf die „Automatisierungslösung" zu informieren.
SP.02.02	RE(2)	Zusicherung	Werkzeuge und Software für die IT-Sicherheit	Erkennung	Nein	Der Dienstleister muss die Fähigkeit besitzen, den Einsatz von Werkzeugen zur IT-Sicherheitsanalyse zu planen, um nicht dokumentierte und/oder nicht autorisierte Systeme oder Sicherheitslücken in der „Automatisierungslösung" zu erkennen. Zu dieser Fähigkeit gehört auch, diese Werkzeuge in Übereinstimmung mit den normalen Betriebsabläufen des Betreibers einzusetzen.	Ein über diese Fähigkeit verfügender Dienstleister zu sein, bedeutet, dass dieser über einen nachweisbaren Prozess zum Einsatz von Werkzeugen verfügt, um mit dem Netz verbundene, nicht autorisierte Geräte innerhalb der „Automatisierungslösung" sowie Sicherheitslücken wie offene Ports, die nicht offen sein sollten, zu erkennen. Zu dieser Fähigkeit gehört auch, dass der Dienstleister über einen nachweisbaren Prozess für die Koordinierung und Planung des Einsatzes von Werkzeugen zur IT-Sicherheitsanalyse verfügt, damit diese nicht den Betrieb der „Automatisierungslösung" beeinträchtigen. Die BR für diese RE verlangt vom Dienstleister, den Betreiber über mögliche nachteilige Auswirkungen dieser Werkzeuge auf die „Automatisierungslösung" zu informieren. Integratoren werden bestärkt, den Einsatz dieser Werkzeuge für kurz vor der Übergabe zu planen, um z. B. nicht autorisierte Geräte und offene Ports zu finden, während Instandhaltungsdienstleister diese Werkzeuge regelmäßig entsprechend den vom Betreiber festgelegten Zyklen einsetzen sollten.

Documents
Document Sharing Hub
Full document details: DIN EN IEC 62443-2-4:2020-07