

DIN IEC 62443-2-4-100
(VDE 0802-2-4-100)
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 35.030; 35.240.50

Einsprüche bis 2017-10-04

Entwurf
**IT-Sicherheit für industrielle Automatisierungssysteme –
 Teil 2-4: Anforderungen an das IT-Sicherheitsprogramm von Dienstleistern
 für industrielle Automatisierungssysteme
 (IEC 65/637A/CDV:2016)**

Security for industrial automation and control systems –
 Part 2-4: Security program requirements for IACS service providers
 (IEC 65/637A/CDV:2016)

Sécurité des automatismes industriels et des systèmes de commande –
 Partie 2-4: Exigences de programme de sécurité pour les fournisseurs de service IACS
 (IEC 65/637A/CDV:2016)

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2017-08-04 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal des DIN unter www.entwuerfe.din.de bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an dke@vde.com möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/stellungnahme oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 35 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Anwendungsbeginn

Anwendungsbeginn dieser Norm ist

Nationales Vorwort

Das internationale Dokument IEC 65/637A/CDV:2016 „Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers“ (CDV, en: Committee Draft for Vote) ist der internationale Norm-Entwurf für die Änderung 1 der IEC 62443-2-4:2015. Es ist unverändert in diesen Norm-Entwurf übernommen worden. Dieser Norm-Entwurf enthält eine noch nicht autorisierte deutsche Übersetzung.

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung des CDV entsprechend der diesbezüglich durch die IEC erteilten Erlaubnis beigelegt. Die Nutzungsbedingungen für den deutschen Teil des Norm-Entwurfes gelten gleichermaßen auch für den englischen IEC-Text.

Das internationale Dokument wurde vom TC 65 „Industrial-process measurement and control“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und den nationalen Komitees zur Stellungnahme und Abstimmung vorgelegt. Es wird jedoch nicht zeitgleich (parallel) bei IEC und CENELEC zur Umfrage gestellt. Derzeit ist also nicht vorgesehen, dieses Dokument als Europäische Norm zu übernehmen.

Da der Abstimmungszeitraum für einen FDIS (en: Final Draft International Standard) nur 2 Monate beträgt, und dann keine sachlichen Stellungnahmen mehr abgegeben werden können, sondern nur noch eine „JA/NEIN“-Entscheidung möglich ist, wobei eine „NEIN“-Entscheidung fundiert begründet werden muss, wird bereits der CDV als DIN-Norm-Entwurf veröffentlicht, um die Stellungnahmen aus der Öffentlichkeit noch vor der Abstimmung berücksichtigen zu können.

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.

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.

Der Zusammenhang der zitierten Dokumente mit den entsprechenden Deutschen Dokumenten ergibt sich, soweit ein Zusammenhang besteht, grundsätzlich über die Nummer der entsprechenden IEC-Publikation. Beispiel: IEC 60068 ist als EN 60068 als Europäische Norm durch CENELEC übernommen und als DIN EN 60068 ins Deutsche Normenwerk aufgenommen.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO [und/oder] IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

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

Einleitung

Die vorliegende Änderung 1 beseitigt durch Aktualisierungen von IEC 62443-2-4 festgestellte Unklarheiten, die bei der Überprüfung der Norm mit dem Ziel der Konformitätsbewertung festgestellt wurden. Außerdem werden Mehrdeutigkeiten in Bezug auf die Anwendbarkeit innerhalb von TC 44 behandelt.

1 Anwendungsbereich

Der erste Absatz wird durch den folgenden neuen Text ersetzt:

IEC 62443-2-4 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. Die vorliegende Internationale Norm kann mithilfe von Profilen an bestimmte Umgebungen einschließlich solcher, die nicht auf industriellen Automatisierungssystemen beruhen, angepasst werden.

1 Anwendungsbereich

Anmerkung 4 wird gestrichen und Anmerkung 5 wird Anmerkung 4:

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 Produktbaugruppe 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.

3.1.14 sicherheitstechnisches System

Anmerkung 2 zum Begriff wird ergänzt und die bestehende Anmerkung wird „Anmerkung 1 zum Begriff“:

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

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.

4.1.4 Profile

Der Text wird wie folgt ersetzt:

Diese Norm berücksichtigt, dass nicht alle der in [Anhang A](#) angegebenen Anforderungen für alle Industriezweige/Umgebungen gelten. Die gezielte Auswahl und Anpassung dieser Anforderungen erfolgt in dieser Norm mit „Profilen“.

Profile werden in Form von IEC-Fachberichten (Technical Reports, TR) für verschiedene Branchengruppen/Industriezweige oder andere Organisationen 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.

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

4.2 Reifegradmodell, Tabelle 1

Der zweite Absatz in der rechten Spalte von Grad 2 (der Absatz, der mit „Bei diesem Reifegrad verfügt der Dienstleister ...“ beginnt) wird wie folgt ersetzt:

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, schriftlichen Anweisungen zu befolgen.

5.1 Inhalte

Nach dem ersten Absatz und vor der Anmerkung wird der folgende neue Absatz eingefügt:

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

5.5.3 Spalte „Bereich“

Der erste Absatz in diesem Abschnitt wird wie folgt ersetzt:

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

5.5.7 Beschreibung der Anforderung

Im Titel des Abschnitts wird „Spalte“ ergänzt:

Spalte „Beschreibung der Anforderung“

5.5.7 Beschreibung der Anforderung

Der Text wird wie folgt ersetzt:

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 dieser Norm.

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.

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.

5.5.8 Begründung

Im Titel des Abschnitts wird „Spalte“ ergänzt:

Spalte „Begründung“

Anhang A

SP.01.04 BR

Der Text in den Spalten „Beschreibung der Anforderung“ und „Begründung“ wird wie folgt geändert:

Anford.-ID	BR/RE	Bereich	Oberbegriff	Unterbegriff	Doku?	Beschreibung der Anforderung	Begründung nach IEC 62443-2-4
SP.01.04	BR	Mit- arbeiter	Überprüfung der Vergangenheit der Mitarbeiter	Dienstleister	Nein	Der Dienstleister muss die Fähigkeit besitzen sicherzustellen, dass er automatisierungslösungsbezogenen Tätigkeiten ausschließlich sein eigenes Personal zuweist, das sicherheitsbezogene Überprüfungen der Vergangenheit der Mitarbeiter, soweit durchführbar und rechtlich zulässig, erfolgreich bestanden hat.	<p>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.</p> <p>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.</p> <p>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.</p>

SP.01.04 RE(1)

Der Text in den Spalten „Beschreibung der Anforderung“ und „Begründung“ wird wie folgt geändert:

Anford.-ID	BR/RE	Bereich	Oberbegriff	Unterbegriff	Doku?	Beschreibung der Anforderung	Begründung nach IEC 62443-2-4
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 automatisierungslösungsbezogene Tätigkeiten zuweist, die sicherheitsbezogene Überprüfungen ihrer Vergangenheit, soweit durchführbar und rechtlich zulässig, erfolgreich bestanden haben.	<p>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.</p> <p>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.</p>

SP.01.06 BR

Der Text in den Spalten „Beschreibung der Anforderung“ und „Begründung“ wird wie folgt geändert:

Anford.-ID	BR/RE	Bereich	Oberbegriff	Unterbegriff	Doku?	Beschreibung der Anforderung	Begründung nach IEC 62443-2-4
SP.01.06	BR	Mitarbeiter	Personaleinsatzplanung	Führungskräfte für IT-Sicherheit	Nein	Der Dienstleister muss für die Führungspositionen der IT-Sicherheit Nachweise über die Mindestqualifikationen für die IT-Sicherheit des IACS besitzen und er muss die Fähigkeit besitzen, für Automatisierungslösungen Führungskräfte für IT-Sicherheit einzusetzen, die diese Qualifikationen erfüllen.	<p>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-Sicherheitsbedrohungen und/oder –verstößen aussetzen.</p> <p>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 Automatisierungslösung mit Personal auszustatten, das dieses Fachwissen 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-Sicherheit, die der Automatisierungslösung zugewiesen werden, die entsprechenden Erfahrungen besitzen, die in Übereinstimmung mit diesen Qualifikationen stehen.</p>

SP.03.02 RE(2)

Der Text in der Spalte „Begründung“ wird wie folgt geändert:

Anford.-ID	BR/RE	Bereich	Oberbegriff	Unterbegriff	Doku?	Beschreibung der Anforderung	Begründung nach IEC 62443-2-4
SP.03.02	RE(2)	System-aufbau	Netzauslegung	Verbindungsmöglichkeiten	Nein	<p>Der Dienstleister muss die Fähigkeit besitzen sicherzustellen, dass in der Automatisierungslösung als nicht vertrauenswürdig identifizierte Schnittstellen durch Netzwerksicherheitseinrichtungen oder äquivalente Mechanismen mit dokumentierten und gepflegten IT-Sicherheitsregeln geschützt werden. Es müssen mindestens folgende Schnittstellen geschützt werden:</p> <ol style="list-style-type: none"> 1. externe Schnittstellen; 2. Schnittstellen zwischen Ebene 2 und Ebene 3 (siehe nachfolgende ANMERKUNG 2); 3. Schnittstellen zwischen BPCS und SIS; 4. Schnittstellen zur Verbindung drahtgebundener und drahtloser BPCS-Netze; 5. Schnittstellen zur Verbindung des BPCS mit einem Data-Warehouse (z. B. Unternehmenshistorie). <p>ANMERKUNG 1 Es kann vorkommen, dass die Verantwortlichkeit für die Pflege der Firewall-Regeln und der Dokumentation schon vor oder bei der Übergabe der Automatisierungslösung auf den Betreiber übergeht. In diesem Fall darf die Rolle des Dienstleisters darauf beschränkt sein, wie vom Betreiber verlangt, nur die Verifikation zu unterstützen, dass die Firewall-Regeln genau und aktuell sind.</p> <p>ANMERKUNG 2 In Abhängigkeit von der Automatisierungslösung dürfen Schnittstellen zwischen Ebene 2 und Ebene 3 „externe“ Schnittstellen sein.</p>	<p>Ein über diese Fähigkeit verfügender Dienstleister zu sein bedeutet, dass dieser über einen nachweisbaren Prozess zum Schutz der Automatisierungslösung gegen äußeren Zugriff und für die Kontrolle des Zugriffs zwischen Ebene 2 und Ebene 3 (z. B. über die Anwendung von Firewalls/Firewall-Regeln) verfügt.</p> <p>Innerhalb der Automatisierungslösung bedeutet diese Fähigkeit außerdem, dass der Dienstleister über einen nachweisbaren Prozess zum Schutz von BPCS-Schnittstellen mittels Netzwerksicherheitseinrichtungen oder äquivalenten Mechanismen verfügt und zur Übermittlung der zur Schaffung der IT-Sicherheitsregeln erforderlichen Informationen, die dazu verwendet werden, einen Zugang zu den BPCS-Ports und Anwendungen zu gewähren oder zu verweigern.</p> <p>Sollte der Dienstleister die Netzwerksicherheitseinrichtung oder den äquivalenten Mechanismus liefern oder für diesen verantwortlich sein, dann umfasst die zu erbringende Unterstützungsleistung auch die jeweils erforderliche Konfiguration der Netzwerksicherheitseinrichtung/des Mechanismus. Mittels einer Risikobewertung (siehe IEC 62443-3-2) kann bestimmt werden, welche Schnittstellen geschützt werden müssen.</p>

SP.03.10 RE(2)

Der Text in der Spalte „Begründung“ wird wie folgt geändert:

Anford.-ID	BR/RE	Bereich	Oberbegriff	Unterbegriff	Doku?	Beschreibung der Anforderung	Begründung nach IEC 62443-2-4
SP.03.10	RE(2)	Systemaufbau	Schutz der Daten	Daten- und Ereignisspeicherung	Ja	Der Dienstleister muss die Fähigkeit besitzen, dem Betreiber eine Dokumentation zu liefern, in der die von der Automatisierungslösung bereitgestellten Aufbewahrungsmöglichkeiten zur Speicherung und Archivierung schützenswerter Daten beschrieben sind. Diese Dokumentation beschreibt die Kapazitäten, Aufräum- und Löschfunktionen, Aufbewahrungsfristen usw.	Ein über diese Fähigkeit verfügender Dienstleister zu sein bedeutet, dass dieser über einen nachweisbaren Prozess zur Dokumentation verfügt, wie in der Automatisierungslösung schützenswerte Daten gespeichert und archiviert werden, wie z. B. Verlaufsdaten und frühere Ereignisse. Dazu dürfen interne Fähigkeiten der Automatisierungslösung (z. B. Datenvolumen/ Datenkapazität) gehören oder es dürfen für die Auslagerung von Verlaufsdaten/früheren Ereignissen in ein Verlaufsarchiv erforderliche Fähigkeiten bezeichnet werden. Verlaufsdaten und frühere Ereignisse können für forensische Nachforschungen und Ereignisanalysen und -zuordnungen nützlich sein.

SP.05.02 BR

Der Text in den Spalten „Beschreibung der Anforderung“ und „Begründung“ wird wie folgt geändert:

Anford.-ID	BR/RE	Bereich	Oberbegriff	Unterbegriff	Doku?	Beschreibung der Anforderung	Begründung nach IEC 62443-2-4
SP.05.02	BR	SIS	Netzauslegung	Kommunikation	Nein	<p>Der Dienstleister muss die Fähigkeit besitzen sicherzustellen, dass die sicherheitskritische SIS-Kommunikation nicht durch die sonstige Kommunikation der Automatisierungslösung gestört wird und dass das SIS nicht daran gehindert wird, seine Sicherheitsfunktionen auszuführen (z. B. durch physische oder logische Trennung).</p> <p>ANMERKUNG Diese Anforderung erfordert nicht, dass die nicht-sicherheitskritische Kommunikation zwischen SIS und BPCS (z. B. Konfigurations-Downloads, Statusüberwachung, Protokollierung) von der sonstigen Kommunikation der Automatisierungslösung abgetrennt wird.</p>	<p>Mit der von dieser BR festgelegten Fähigkeit wird sichergestellt, dass die sicherheitskritische Kommunikation des SIS nicht durch eine nicht-sicherheitskritische Kommunikation beeinflusst werden kann.</p> <p>Ein über diese Fähigkeit verfügender Dienstleister zu sein bedeutet, dass dieser in der Lage ist, die sicherheitskritische Kommunikation gegen den sonstigen Datenverkehr der Automatisierungslösung zu schützen oder von diesem zu trennen (siehe IEC 61508).</p> <p>Diese Fähigkeit bedeutet außerdem, dass der Dienstleister nachweisen kann, dass Gegenmaßnahmen zur Abtrennung der funktionalen Sicherheitskommunikation nicht die Leistungsfähigkeit oder den Betrieb der sicherheitskritischen Kommunikation beeinträchtigen.</p> <p>Risikobewertungen, Zonen (Teilbereiche des Netzes) und Conduits (Verbindungen zwischen Teilbereichen des Netzes), wie in IEC 62443-3-2 beschrieben, können für die Festlegung der Anforderungen verwendet werden.</p>

SP.05.03 BR

Der Text in den Spalten „Beschreibung der Anforderung“ und „Begründung“ wird wie folgt geändert:

Anford.-ID	BR/RE	Bereich	Oberbegriff	Unterbegriff	Doku?	Beschreibung der Anforderung	Begründung nach IEC 62443-2-4
SP.05.03	BR	SIS	Netzauslegung	Kommunikation	Nein	Der Dienstleister muss die Fähigkeit besitzen sicherzustellen, dass die Kommunikation von Anwendungen einschließlich eines Fernzugriffs (z. B. RDP) außerhalb des SIS den Betrieb des SIS nicht stören kann.	<p>Mit der von dieser BR festgelegten Fähigkeit wird sichergestellt, dass das SIS nicht durch nicht zum SIS gehörende Geräte/Anwendungen gestört wird.</p> <p>Ein über diese Fähigkeit verfügender Dienstleister zu sein bedeutet, dass dieser über einen nachweisbaren Prozess verfügt, der sicherstellt, dass der Betrieb des SIS durch äußere Anwendungen nicht beeinflusst werden kann.</p>

SP.05.04 BR

Der Text in der Spalte „Beschreibung der Anforderung“ wird wie folgt geändert:

Anford.-ID	BR/RE	Bereich	Oberbegriff	Unterbegriff	Doku?	Beschreibung der Anforderung	Begründung nach IEC 62443-2-4
SP.05.04	BR	SIS	Netzauslegung	Kommunikation	Nein	Der Dienstleister muss die Fähigkeit besitzen sicherzustellen, dass Anwendungen (z. B. Anwendungen des Automatisierungssystems), die nicht zum SIS gehören, nicht an der sicherheitskritischen Kommunikation des SIS teilnehmen oder diese stören können.	<p>Mit der von dieser BR festgelegten Fähigkeit wird sichergestellt, dass eine Vertrauensgrenze zwischen SIS und BCPS aufgestellt wird, die nicht zulässt, dass die sicherheitskritische SIS-Kommunikation diese überschreitet.</p> <p>Ein über diese Fähigkeit verfügender Dienstleister zu sein bedeutet, dass dieser über einen nachweisbaren Prozess verfügt, der sicherstellt, dass keine sicherheitskritische Kommunikation (z. B. Daten und/oder Befehle) zwischen dem SIS und außerhalb des SIS laufenden Anwendungen stattfindet. Ziel dieser Anforderung ist es, sicherheitskritische Funktionen im SIS davor zu schützen, dass sie durch Quellverkehr von außerhalb des SIS gefährdet werden.</p>