

**DIN EN 62443-3-2
(VDE 0802-3-2)**
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

Einsprüche bis 2018-11-14

Entwurf
**Sicherheit für industrielle Automatisierungssysteme –
Teil 3-2: Sicherheitsrisikobeurteilung und Systemgestaltung
(IEC 65/690/CDV:2018);**
Deutsche und Englische Fassung prEN 62443-3-2:2018

Security for industrial automation and control systems –

Part 3-2: Security risk assessment and system design

(IEC 65/690/CDV:2018);

German and English version prEN 62443-3-2:2018

Sécurité des systèmes d'automatisation et de commande industriels –

Partie 3-2: Evaluation des risques de sécurité et conception des systèmes

(IEC 65/690/CDV:2018);

Version allemande et anglaise prEN 62443-3-2:2018

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2018-09-14 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 von DIN unter www.din.de/go/entwuerfe 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/go/stellungnahmen-norm-entwuerfe 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 66 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Anwendungsbeginn

Anwendungsbeginn dieser Norm ist ...

Nationales Vorwort

Die Deutsche Fassung des europäischen Dokuments prEN 62443-3-2:2018 „Sicherheit für industrielle Automatisierungssysteme – Teil 3-2: Sicherheitsrisikobeurteilung und Systemgestaltung“ (Entwurf in der Umfrage) ist unverändert in diesen Norm-Entwurf übernommen worden.

Die Internationale Elektrotechnische Kommission (IEC) und das Europäische Komitee für Elektrotechnische Normung (CENELEC) haben vereinbart, dass ein auf IEC-Ebene erarbeiteter Entwurf für eine Internationale Norm zeitgleich (parallel) bei IEC und CENELEC zur Umfrage (CDV-Stadium) und Abstimmung als FDIS (en: Final Draft International Standard) bzw. Schluss-Entwurf für eine Europäische Norm gestellt wird, um eine Beschleunigung und Straffung der Normungsarbeit zu erreichen. Dem entsprechend ist das internationale Dokument IEC 65/690/CDV:2018 „Security for industrial automation and control systems – Part 3-2: Security risk assessment and system design“ unverändert in den Entwurf Deutsche und Englische Fassung prEN 62443-3-2:2018 übernommen worden.

Da die Deutsche Fassung noch nicht endgültig mit der Englischen und Französischen Fassung abgeglichen ist, ist die englische Originalfassung des IEC-CDV entsprechend der diesbezüglich durch die IEC erteilten Erlaubnis beigefügt. Die Nutzungsbedingungen für den deutschen Text 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.

Bei der Abstimmung zu dem Europäischen Schluss-Entwurf bei CENELEC und dem Internationalen Schluss-Entwurf bei IEC [Final Draft International Standard (FDIS)] sind jeweils nur „JA/NEIN“-Entscheidungen möglich, wobei „NEIN“-Entscheidungen fundiert begründet werden müssen. Dokumente, die bei CENELEC als Europäische Norm angenommen und ratifiziert werden, sind unverändert als Deutsche Normen zu übernehmen.

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. IEC ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

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.

Inhalt

Seite

Einleitung	3
1 Anwendungsbereich	4
2 Normative Verweisungen	4
3 Begriffe und Symbole	4
3.1 Begriffe	4
3.2 Abkürzungen und Akronyme	7
3.3 Konventionen	8
4 Anforderungen an Zonen, Conduits und Risikobeurteilungen	8
4.1 Überblick	8
4.2 ZCR-1: Identifizieren des zu berücksichtigenden Systems	10
4.2.1 ZCR-1.1: Identifizieren des SUC-Bereichs und der Zugangspunkte	10
4.3 ZCR-2: Erste Cybersicherheitsrisikobeurteilung	10
4.3.1 ZCR-2.1: Durchführen der ersten Cybersicherheitsrisikobeurteilung	10
4.4 ZCR-3: Aufteilung des SUC in Zonen und Kanäle	11
4.4.1 Überblick	11
4.4.2 ZCR-3.1: Zonen und Kanäle festlegen	11
4.4.3 ZCR-3.2: Separate Geschäfts- und Steuerungssystem-Anlagen	12
4.4.4 ZCR-3.3: Separate sicherheitsbezogene Anlagen	12
4.4.5 ZCR-3.4: Separate vorübergehend angeschlossene Geräte	12
4.4.6 ZCR-3.5: Separate kabellose Geräte	13
4.4.7 ZCR-3.6: Über externe Netzwerke verbundene separate Geräte	13
4.5 ZCR-4: Risikovergleich	13
4.5.1 ZCR-4.1: Vergleich zwischen allgemeinem und tolerierbarem Risiko	13
4.6 ZCR-5: Durchführen einer ausführlichen Cybersicherheitsrisikobeurteilung	13
4.6.1 Überblick	13
4.6.2 ZCR-5.1: Bedrohungen identifizieren	16
4.6.3 ZCR-5.2: Schwachstellen identifizieren	17
4.6.4 ZCR-5.3: Bestimmen der Konsequenz und Auswirkung	17
4.6.5 ZCR-5.4: Bestimmen der unverringerten Wahrscheinlichkeit	18
4.6.6 ZCR-5.5: Bestimmen des unverringerten Cybersicherheitsrisikos	18
4.6.7 ZCR-5.6: Bestimmen des Security-Level-Ziels (SL-T)	19
4.6.8 ZCR-5.7: Vergleich zwischen unverringertem und tolerierbarem Risiko	19
4.6.9 ZCR-5.8: Identifizieren und Bewerten bestehender Gegenmaßnahmen	19
4.6.10 ZCR-5.9: Neubewerten der Wahrscheinlichkeit und der Auswirkung	20
4.6.11 ZCR-5.10: Bestimmen des Restrisikos	20
4.6.12 ZCR-5.11: Vergleich zwischen dem Restrisiko und dem tolerierbaren Risiko	20
4.6.13 ZCR-5.12: Identifizieren zusätzlicher Cybersicherheitsgegenmaßnahmen	20

4.6.14	ZCR-5.13: Dokumentieren und Kommunizieren von Ergebnissen	21
4.7	ZCR-6: Dokumentieren von Cybersicherheitsanforderungen, -annahmen und - beschränkungen	21
4.7.1	Überblick.....	21
4.7.2	ZCR-6.1: Festlegung der Cybersicherheitsanforderungen	21
4.7.3	ZCR-6.2: SUC-Beschreibung	22
4.7.4	ZCR-6.3: Zonen- und Kanalzeichnungen.....	22
4.7.5	ZCR-6.4: Zonen- und Kanaleigenschaften.....	22
4.7.6	ZCR-6.5: Annahme zur Betriebsumgebung	24
4.7.7	ZCR-6.6: Bedrohungsumgebung	24
4.7.8	ZCR-6.7: IT-Sicherheitspolitik	25
4.7.9	ZCR-6.8: Tolerierbares Risiko.....	25
4.7.10	ZCR-6.9: Gesetzliche Anforderungen	25
4.8	ZCR-7: Genehmigung des Anlagenbetreibers	25
4.8.1	ZCR-7.1: Einholen der Genehmigung des Anlagenbetreibers.....	25
	Anhang A (informativ) Security-Level	27
	Anhang B (informativ) Risikomatrizen	28
	Literaturhinweise.....	33
Bilder		
	Bild 1 – Arbeitsablauf zur Festlegung der Zonen und Kanäle und zur Beurteilung des Risikos	10
	Bild 2 – Arbeitsablauf der ausführlichen Cybersicherheitsrisikobeurteilung je Zone oder Kanal	16
	Bild 3 – Beispiel für eine 3 x 5 Risikomatrix.....	28
	Bild 4 – Beispiel für eine Konsequenz- oder Schweregradskala	30
	Bild 5 – Beispiel für eine einfache 3 x 3 Risikomatrix	31
	Bild 6 – Beispiel für eine 5 x 5 Risikomatrix.....	31
	Bild 7 – Beispiel für eine 3 x 4 Matrix.....	32
Tabellen		
	Tabelle 1 – Beispiel für eine Wahrscheinlichkeitsskala	29

Sicherheit für industrielle Automatisierungssysteme – Teil 3-2: Sicherheitsrisikobeurteilung und Systemgestaltung

Einleitung

ANMERKUNG Das Format dieses Dokuments folgt den in den ISO/IEC-Richtlinien, Teil 2 [14] behandelten ISO/IEC-Anforderungen. Dieses Dokument legt das Format des Dokuments sowie die Verwendung der Begriffe „müssen“, „sollen“ und „dürfen“ fest. Die in normativen Abschnitten festgelegten Anforderungen verwenden die in Anhang H zu dem Richtliniendokument behandelten Konventionen.

Überblick

Es besteht keine einfache Lösung für die Sicherung eines industriellen Automatisierungssystems (eng: Industrial Automation and Control System (IACS)) und dies hat einen guten Grund. Sicherheit ist eine Frage des Risikomanagements. Jedes IACS stellt je nach den Bedrohungen, denen es ausgesetzt ist, der Wahrscheinlichkeit, dass diese Bedrohungen auftreten, den inhärenten Schwachstellen des Systems und den Konsequenzen der Kompromittierung des Systems ein anderes Risiko für die Organisation dar. Darüber hinaus besteht in jeder Organisation, die ein IACS besitzt und betreibt, eine unterschiedliche Risikotoleranz.

Ziel dieser Norm ist es, eine Reihe von technischen Maßnahmen festzulegen, die eine Organisation durch den Prozess der Beurteilung des Risikos eines bestimmten IACS und der Identifizierung und Anwendung von Sicherheitsgegenmaßnahmen zur Reduzierung des Risikos auf ein tolerierbares Maß leiten.

Die Anwendung von Sicherungszonen und Kanälen für IACS ist ein wesentliches Konzept in diesem Dokument. Zonen und Elektroinstallationsrohre werden in IEC 62443-1-1 [1] eingeführt. Lesern wird empfohlen, sich mit diesen Konzepten vertraut zu machen, bevor sie dieses Dokument lesen.

Zweck und vorgesehene Zielgruppe

Die vorgesehene Zielgruppe für diese Norm umfasst Anlagenbetreiber, Systemintegratoren, Produktlieferanten, Dienstleister und Genehmigungsbehörden.

Nutzung innerhalb anderer Teile der IEC 62443-Normenreihe

Diese Norm bietet eine Grundlage für die Festlegung von Sicherheitsgegenmaßnahmen durch die Abstimmung des in dieser Norm angegebenen Ziel-Security-Levels (SL-T) mit den in IEC 62443-3-3 festgelegten Security-Level-Kapazitäten (SL-C).

1 Anwendungsbereich

Diese Norm legt Anforderungen fest für:

- die Festlegung eines zu betrachtenden System (SUC) für ein industrielles Automatisierungssystem (IACS);
- die Aufteilung des SUC in Zonen und Conduits;
- die Beurteilung des Risikos für jede Zone und jeden Conduit;
- die Festlegung des zu erreichenden Security-Level (SL-T) für jede Zone und jeden Conduit; und
- die Dokumentation der Sicherheitsanforderungen.

2 Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

IEC 62443-1-1, *Security for industrial automation and control systems – Part 1-1: Concepts and models* [1]

IEC 62443-2-1, *Security for industrial automation and control systems – Part 2-1: Requirements for an IACS security management system* [5]

IEC 62443-3-3, *Security for industrial automation and control systems – Part 3-3: System security requirements and security levels* [10]

3 Begriffe und Symbole

3.1 Begriffe

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

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

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

3.1.1

Kanal

eine spezifische logische oder physische Kommunikationsverbindung zwischen Schutzobjekten

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

3.1.2

Genehmigungsbehörde

eine Behörde, die für die Bestimmung der Angemessenheit einer Sicherheitsbeurteilung oder der Effektivität der Implementierung in Übereinstimmung mit einem maßgebenden Dokument zuständig ist

Anmerkung 1 zum Begriff: Beispiele für Genehmigungsbehörden sind Regierungsbehörden, Regulierer, externe und interne Prüfer.

3.1.3

Conduit

eine logische Gruppierung von Kommunikationskanälen, die gemeinsamen Sicherheitsanforderungen unterliegen und zwei oder mehr Zonen miteinander verbinden

3.1.4

Vertraulichkeit

die Aufrechterhaltung autorisierter Beschränkungen des Zugangs zu und der Offenlegung von Informationen einschließlich Mitteln zum Schutz personenbezogener und geheimer Informationen

3.1.5

Konsequenz

das Ergebnis eines Zwischenfalls, üblicherweise beschrieben durch seine Gesundheits- und Sicherheitsauswirkungen, Umweltauswirkungen, Sachschäden, Informationsverlust (z. B. geistiges Eigentum) und/oder die Kosten von Betriebsunterbrechungen aufgrund eines bestimmten Zwischenfalls

3.1.6

Maßnahme

ein Gerät, ein Verfahren oder eine Technik, das/die eine Bedrohung, eine Schwachstelle oder die Konsequenzen eines Angriffs reduziert, indem es/sie diese eliminiert oder verhindert, den potenziellen Schaden minimiert oder erkennt und meldet, sodass Korrekturmaßnahmen getroffen werden können

3.1.7

IT-Sicherheit

getroffene Maßnahmen zum Schutz eines Computers oder Computersystems gegen unbefugten Zugang oder Angriffe

Anmerkung 1 zum Begriff: IACS sind Computersysteme

3.1.8

Datenfluss

die Bewegung von Daten durch ein aus Software, Hardware oder einer Kombination aus beidem bestehenden System

3.1.9

Externes Netzwerk

Jedes mit dem SUC verbundene Netzwerk, das nicht Teil des SUC ist

3.1.10

Auswirkung

die Messung des gesamten Verlusts oder Schadens in Verbindung mit einer Konsequenz

Anmerkung 1 zum Begriff: Auswirkung kann als Anzahl von Verletzungen und/oder Todesfällen, Umfang von Umweltschäden und/oder Höhe von Verlusten wie etwa Sachschäden, Materialverluste, Verlust geistigen Eigentums, Produktionsverluste, Marktanteilverluste und Wiederherstellungskosten ausgedrückt werden.

BEISPIEL Die Konsequenz eines Zwischenfalls war verschüttetes Material. Die Auswirkung des Verschüttens bestand in einer Geldstrafe von 100 000 \$ und 25 000 \$ Reinigungskosten.

3.1.11

Wahrscheinlichkeit

die Möglichkeit, dass etwas passieren wird

Anmerkung 1 zum Begriff: In der Risikomanagement-Terminologie bezeichnet dieser Begriff die Wahrscheinlichkeit, dass etwas passieren wird, das objektiv oder subjektiv, qualitativ oder quantitativ festgelegt, gemessen oder bestimmt und anhand allgemeiner Begriffe oder mathematisch beschrieben wird (wie etwa als eine Wahrscheinlichkeit oder Häufigkeit über einen gegebenen Zeitraum).

Anmerkung 2 zum Begriff: Bei der Einschätzung der Wahrscheinlichkeit im Risikomanagement für Informationssysteme werden eine Reihe verschiedener Faktoren wie etwa die Motivation und Fähigkeit der

Bedrohungsquelle, frühere vergleichbare Bedrohungen, bekannte Schwachstellen, die Attraktivität des Ziels usw. berücksichtigt.

[QUELLE: ISO Guide 73:2009 und ISO/IEC 27005:2011]

3.1.12

Auswirkung

die Messung des gesamten Verlusts oder Schadens in Verbindung mit einer Konsequenz

Anmerkung 1 zum Begriff: Auswirkung kann als Anzahl von Verletzungen und/oder Todesfällen, Umfang von Umweltschäden und/oder Höhe von Verlusten wie etwa Sachschäden, Materialverluste, Verlust geistigen Eigentums, Produktionsverluste, Marktanteilverluste und Wiederherstellungskosten ausgedrückt werden.

BEISPIEL: Die Konsequenz eines Zwischenfalls war verschüttetes Material. Die Auswirkung des Verschüttens bestand in einer Geldstrafe von 100 000 \$ und 25 000 \$ Reinigungskosten.

3.1.13

Prozessgefährdungsanalyse

eine Reihe organisierter und systematischer Beurteilungen der potenziellen Gefährdungen in Verbindung mit einem industriellen Prozess

3.1.14

Restrisiko

das nach der Berücksichtigung bestehender Gegenmaßnahmen verbleibende Risiko (d. h. das Nettorisiko oder Risiko nach Anwendung der Gegenmaßnahmen)

3.1.15

Risiko

der erwartete Verlust, angegeben als Wahrscheinlichkeit, dass eine bestimmte Bedrohung eine bestimmte Anfälligkeit mit einer bestimmten Konsequenz nutzt

3.1.16

Security-Level

ein Messwert für die Wahrscheinlichkeit, dass das zu berücksichtigende System, die Sicherungszone oder das Conduit frei von Anfälligkeiten ist und in der vorgesehenen Weise funktioniert

3.1.17

IT-Sicherheitszone

eine logische oder physische Grenze, die alle von der Sicherungszone kontrollierten und geschützten Anlagen umgibt

3.1.18

Betrachtetes System

eine festgelegte Sammlung von IACS-Anlagen, die zur Bereitstellung einer kompletten Automatisierungslösung benötigt werden, einschließlich aller relevanten Netzwerkinfrastrukturanlagen

Anmerkung 1 zum Begriff: Ein SUC besteht aus einer oder mehreren Zonen und den damit verbundenen Kanälen. Alle Anlagen innerhalb eines SUC gehören entweder zu einer Zone oder einem Kanal.

3.1.19

Bedrohung

alle Umstände oder Ereignisse, die geeignet sind, den Betrieb einer Organisation (einschließlich Missionen, Funktionen, den Ruf oder das Ansehen) und/oder die Anlagen einer Organisation einschließlich IACS zu beeinträchtigen

Anmerkung 1 zum Begriff: Umstände umfassen Personen, die entgegen den Sicherheitsrichtlinien absichtlich oder versehentlich den Zugang zu Daten verhindern oder die Vernichtung, die Offenlegung oder die Änderung von Daten wie etwa Steuerungslogik/-parameter, Schutzlogik/-parameter oder Diagnostik verursachen

3.1.20

Bedrohungsumgebung

Zusammenfassung von Informationen über Bedrohungen wie etwa Bedrohungsquellen, Bedrohungsvektoren und Trends, die geeignet sind, ein festgelegtes Ziel (z. B. Unternehmen, Werk oder SUC) zu beeinträchtigen

3.1.21

Bedrohungsquelle

Zweck und angestrebtes Verfahren zur vorsätzlichen Ausnutzung einer Schwachstelle oder Situation oder ein Verfahren, das versehentlich eine Schwachstelle ausnutzen kann

3.1.22

Bedrohungsvektor

ein Pfad oder Mittel, durch den/die eine Bedrohungsquelle Zugang zu einer Anlage erhalten kann

3.1.23

tolerierbares Risiko

der als für eine Organisation als tolerierbar angesehene Risikograd

Anmerkung 1 zum Begriff: Weitere Anleitungen zur Bestimmung des tolerierbaren Risikos sind in ISO 31000 und NIST 800-39 enthalten.

3.1.24

unverringertes IT-Sicherheitsrisiko

Grad des in einem System vorhandenen IT-Sicherheitsrisikos vor der Berücksichtigung von IT-Sicherheitsgegenmaßnahmen

Anmerkung 1 zum Begriff: Dieser Grad hilft festzustellen, wie weit das IT-Sicherheitsrisiko durch eine Gegenmaßnahme reduziert werden muss.

3.1.25

Sicherheitslücke

ein Fehler oder eine Schwachstelle in der Gestaltung, der Implementierung oder dem Betrieb und Management eines Systems, der/die ausgenutzt werden könnte, um die Integrität oder Sicherheitsrichtstrategie des Systems zu verletzen

3.1.26

Zone

die Gruppierung logischer oder physischer Anlagen auf der Grundlage des Risikos oder anderer Kriterien wie etwa der Kritikalität der Anlagen der Betriebsfunktion, des physischen oder logischen Standorts, des erforderlichen Zugangs (zum Beispiel Prinzip des geringsten Rechts) oder der verantwortlichen Organisation

Anmerkung 1 zum Begriff: Die Sammlung logischer oder physischer Anlagen, die der Partitionierung eines zu berücksichtigenden Systems auf der Grundlage ihrer gemeinsamen Sicherheitsanforderungen der Kritikalität (z. B. hohe finanzielle, Gesundheits-, Sicherheits- oder Umweltauswirkung), Funktionalität oder logischen und physischen (einschließlich des Standorts) Beziehung entspricht

3.2 Abkürzungen und Akronyme

Die folgenden Abkürzungen und Akronyme werden in diesem Dokument verwendet.

ANSI American National Standards Institute

CRS Spezifikation der IT-Sicherheitsanforderungen (en: Cybersecurity requirements specification)

DCS Leitsystem (en: Distributed control system)

IACS Industrielle(s) Automatisierungssystem(e) (en: Industrial automation control system(s))

IEC International Electrotechnical Commission

ISA International Society of Automation

ISAC Information Sharing and Analysis Centers

ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology [USA]
PHA	Prozessgefährdungsanalyse (en: Process hazard analysis)
SIS	PLT-Sicherheitseinrichtung (en: safety instrumented system)
SUC	Betrachtetes System (en: System under consideration)
SL	Security-Level (en: Security level)
SL-T	zu erreichender Security-Level (en: Target security level)
SP	Special Publication [USA NIST]
USB	universeller serieller Bus (en: Universal Serial Bus)
ZCR	Zonen- und Conduitanforderungen (en: Zone and conduit requirement)

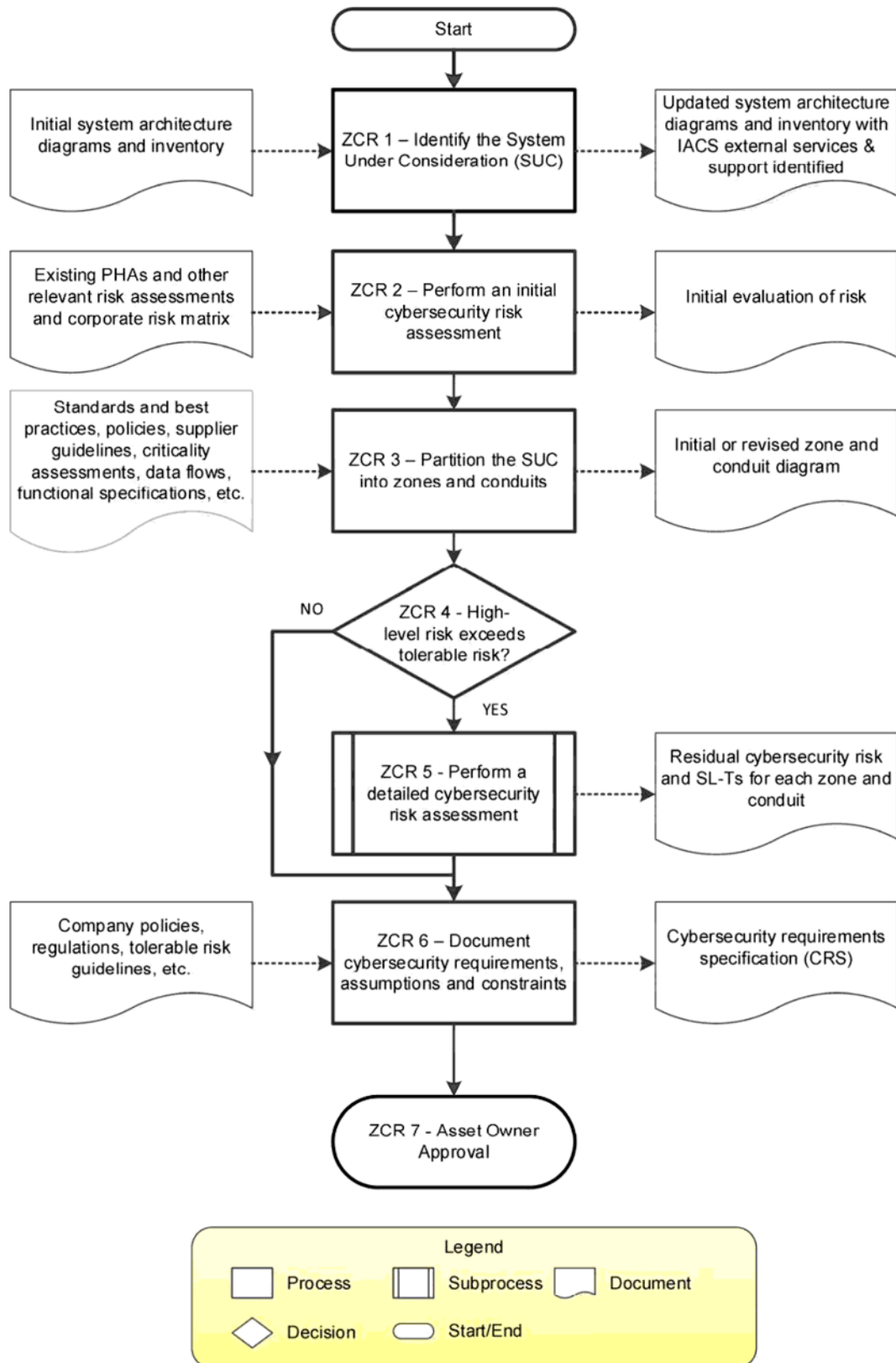
3.3 Konventionen

Dieses Dokument verwendet Ablaufdiagramme, um Arbeitsabläufe zwischen Anforderungen darzustellen. Diese Ablaufdiagramme sind informativ. Alternative Arbeitsabläufe dürfen verwendet werden.

4 Anforderungen an Zonen, Conduits und Risikobeurteilungen

4.1 Überblick

Abschnitt 4 beschreibt die Anforderungen an die Aufteilung eines SUC in Zonen und Kanäle sowie die Anforderungen an die Beurteilung des Cybersicherheitsrisikos und die Bestimmung des SL-T für alle festgelegten Zonen und Kanäle. Die in diesem Abschnitt vorgestellten Anforderungen werden als Anforderungen an Zonen und Kanäle (ZCR) bezeichnet. Der Abschnitt enthält darüber hinaus Erwägungen und zusätzliche Anleitungen zu jeder Anforderung. [Bild 1](#) ist ein Arbeitsablaufdiagramm, das die erforderlichen Hauptschritte zur Festlegung der Zonen und Kanäle und zur Beurteilung des Risikos darstellt. Die Schritte sind nummeriert, um ihre Beziehung zu den ZCR anzugeben.



Initial system architecture diagrams and inventory	Erste Systemarchitekturdiagramme und Bestandsaufnahmen
Existing PHAs and other relevant risk assessments and corporate risk matrix	Bestehende PHA und andere relevante Risikobeurteilungen und Risikomatrix des Unternehmens
Standards and best practices, policies, supplier guidelines, criticality assessments, data flows, functional	Normen und beste Praktiken, Richtlinien, Lieferantenleitfäden, kritische Beurteilungen, Datenflüsse, funktionelle Festlegungen usw.

specifications, etc.	
Company policies, regulations, tolerable risk guidelines, etc	Unternehmensprinzipien, Vorschriften, Richtlinien zu tolerierbaren Risiken usw.
ZCR 1 – Identify the system under consideration (SUC)	ZCR 1 – Identifizieren des zu berücksichtigenden Systems (SUC)
ZCR 2 – Perform an initial cybersecurity risk assessment	ZCR 2 – Durchführen einer ersten Cybersicherheitsrisikobeurteilung
ZCR 3 – Partition the SUC into zones and conduits	ZCR 3 – Aufteilen des SUC in Zonen und Kanäle
ZCR 4 – High-level risk exceeds tolerable risk?	ZCR 4 – Übersteigt ein allgemeines Risiko das tolerierbare Risiko?
ZCR 5 – Perform a detailed cybersecurity risk assessment	ZCR 5 – Durchführen einer ausführlichen Cybersicherheitsrisikobeurteilung
ZCR 6 – Document cybersecurity requirements, assumptions and constraints	ZCR 6 – Dokumentieren der Cybersicherheitsanforderungen, -annahmen und -beschränkungen
ZCR 7 – Asset owner approval	ZCR 7 – Genehmigung des Anlagenbetreibers
Updated system architecture diagrams and inventor with IACS external services & support	Aktualisierte Systemarchitekturdiagramme und -bestandsaufnahmen mit identifizierten externen IACS-Diensten und Unterstützung
Initial evaluation of risk	Erste Risikobewertung
Initial or revised zone and conduit diagram	Erstes oder revidiertes Zonen- und Kanaldiagramm
Residual cybersecurity risk and SL-Ts for each zone and conduit	Rest-Cybersicherheitsrisiko und SLT für alle Zonen und Kanäle
Cybersecurity requirements specification (CRS)	Festlegung der Cybersicherheitsanforderungen (CRS)
Legend, Process, Decision, Subprocess, Start/End, Document	Legende, Prozess, Entscheidung, Unterprozess, Start/Ende, Dokument

Bild 1 – Arbeitsablauf zur Festlegung der Zonen und Kanäle und zur Beurteilung des Risikos

4.2 ZCR-1: Identifizieren des zu berücksichtigenden Systems

4.2.1 ZCR-1.1: Identifizieren des SUC-Bereichs und der Zugangspunkte

4.2.1.1 Anforderung

Die Organisation muss das SUC eindeutig identifizieren und den Sicherheitsbereich klar abgrenzen sowie alle Zugangspunkte zu dem SUC ermitteln.

4.2.1.2 Erwägungen und zusätzliche Anleitung

Für die Zwecke der Durchführung der Cybersicherheitsanalyse ist vorgesehen, dass ein SUC alle IACS-Anlagen enthält, die für eine komplette Automatisierungslösung benötigt werden.

Die Systembestandsaufnahme und die Architekturdiagramme können genutzt werden, um die IACS-Anlagen, die in der SUC-Beschreibung enthalten sind, zu bestimmen und darzustellen.

Das SUC kann mehrere Subsysteme wie etwa DCS, SIS, SCADA und Lieferantenpakete enthalten.

4.3 ZCR-2: Erste Cybersicherheitsrisikobeurteilung

4.3.1 ZCR-2.1: Durchführen der ersten Cybersicherheitsrisikobeurteilung

4.3.1.1 Anforderung

Die Organisation muss eine Cybersicherheitsrisikobeurteilung des SUC durchführen oder bestätigen, dass eine vorherige erste Cybersicherheitsrisikobeurteilung weiterhin anwendbar ist, um das unverringerte Cybersicherheitsrisiko, das im ungünstigsten Fall aus einer Interferenz mit, Unterbrechung von oder Verhinderung von missionskritischen IACS-Aktivitäten resultieren könnte, zu identifizieren.

4.3.1.2 Erwägungen und zusätzliche Anleitung

Die erste Cybersicherheitsrisikobeurteilung dient dazu, ein allgemeines Verständnis des Risikos im ungünstigsten Fall, dass das SUC für die Organisation im Fall einer Kompromittierung darstellt, zu gewinnen. Die Beurteilung unterstützt die Priorisierung der ausführlichen Risikobeurteilungen und ermöglicht die Gruppierung der Anlagen in Zonen und Kanäle innerhalb des SUC.

Bei potenziell gefahrbringenden Prozessen sollte auf die Ergebnisse der Prozessgefahrenanalyse (PHA) und die Beurteilung der funktionalen Sicherheit nach IEC 61511-1 [18] als Teil der allgemeinen Cybersicherheitsrisikobeurteilung Bezug genommen werden, um Auswirkungen im ungünstigsten Fall zu identifizieren. Organisationen sollten Bedrohungsinformationen von Regierungen, sektorspezifischen Information Sharing and Analysis Centers (ISAC) und anderen relevanten Quellen berücksichtigen.

Die Beurteilung des allgemeinen Risikos erfolgt oftmals mithilfe einer Risikomatrix, die die Beziehung zwischen der Wahrscheinlichkeit, der Auswirkung und dem Risiko herstellt (wie etwa eine Unternehmensrisikomatrix). Der informative [Anhang B](#) enthält Risikomatrixbeispiele.

4.4 ZCR-3: Aufteilung des SUC in Zonen und Kanäle

4.4.1 Überblick

Die folgenden Abschnitte beschreiben die ZCR für die Aufteilung des SUC in Zonen und Kanäle und enthalten Erwägungen und zusätzliche Anleitungen für jede Anforderung. ZCR-3.1 ist die grundlegende Anforderung für die Festlegung von Zonen und Kanälen innerhalb des SUC. Die ZCR 3.2 bis 3.6 dienen als Anleitung für die Zuweisung von Anlagen zu Zonen auf der Grundlage der anerkannten Industriepraktiken. Diese Liste erhebt keinen Anspruch auf Vollständigkeit.

4.4.2 ZCR-3.1: Zonen und Kanäle festlegen

4.4.2.1 Anforderung

Die Organisation muss Zonen und Kanäle durch die Gruppierung von IACS und damit verbundenen Anlagen anhand des festgestellten Risikos festlegen. Die Gruppierung muss auf den Ergebnissen der ersten Cybersicherheitsrisikobeurteilung wie etwa der Kritikalität der Anlagen, der Betriebsfunktion, des physischen oder logischen Standorts, des erforderlichen Zugangs (zum Beispiel Prinzip des geringsten Rechts) oder der verantwortlichen Organisation basieren.

4.4.2.2 Erwägungen und zusätzliche Anleitung

Die Gruppierung von Anlagen in Zonen und Kanälen dient dazu, die Anlagen zu identifizieren, die gemeinsamen Sicherheitsanforderungen unterliegen, und die Identifizierung der gemeinsamen Sicherheitsmaßnahmen zur Verringerung des Risikos zu ermöglichen. Die Zuweisung von IACS-Anlagen in Zonen und Kanälen darf auf der Grundlage der Ergebnisse der ausführlichen Risikobeurteilung angepasst werden. Dies ist eine allgemeine Anforderung, jedoch sollte den sicherheitsbezogenen Systemen einschließlich der sicherheitstechnischen Systeme, kabellosen Systeme, direkt mit Internet-Endpunkten verbundenen Systemen und Systemen mit Schnittstellen zum IACS, die jedoch von anderen Einheiten (einschließlich externer Systeme) gesteuert werden, und mobiler Systeme besondere Aufmerksamkeit gewidmet werden.

So kann ein Werk beispielsweise zunächst in betriebliche Bereiche wie etwa Materiallager, Verarbeitung, Oberflächenbehandlung usw. unterteilt werden. Betriebliche Bereiche können oftmals weiter in funktionale Ebenen unterteilt werden wie etwa Fertigungsleitsysteme (MES), übergeordnete Systeme (z. B. Mensch-Maschine-Schnittstellen [HMI]), primäre Steuerungssysteme (z. B. verteilte Steuerungssysteme [DCS], Fernbedienungsmodulare [RTU]) und programmierbare logische Steuerungen [PLC]) und Sicherheitssysteme. Modelle wie das in ISA-95.00.01 [19] festgelegte Purdue-Referenzmodell werden oftmals als Grundlage für diese Unterteilung verwendet. Referenzarchitekturen der Lieferanten können ebenfalls hilfreich sein.

4.4.3 ZCR-3.2: Separate Geschäfts- und Steuerungssystem-Anlagen

4.4.3.1 Anforderung

IACS-Anlagen müssen in Zonen gruppiert werden, die logisch oder physisch von den Anlagen des Geschäfts- oder Unternehmenssystems getrennt sind.

4.4.3.2 Erwägungen und zusätzliche Anleitung

Geschäfts- und IACS-Systeme sind zwei unterschiedliche Arten von Systemen, die in separate Zonen unterteilt werden müssen, da ihre Funktionalität, die verantwortliche Organisation, das Ergebnis der Hochrisikobeurteilung und der Standort sich grundlegend unterscheiden. Es ist wichtig, den grundlegenden Unterschied zwischen Geschäfts- und IACS-Systemen und die Auswirkung der IACS auf Gesundheit, Sicherheit und Umweltschutz (HSE) zu verstehen.

4.4.4 ZCR-3.3: Separate sicherheitsbezogene Anlagen

4.4.4.1 Anforderung

Sicherheitsbezogene Anlagen müssen in Zonen gruppiert werden, die logisch oder physisch von den Zonen mit nicht sicherheitsbezogenen Anlagen getrennt sind. Wenn diese jedoch nicht getrennt werden können, muss die gesamte Zone als sicherheitsbezogene Zone gekennzeichnet werden.

4.4.4.2 Erwägungen und zusätzliche Anleitung

Sicherheitsbezogene Anlagen haben üblicherweise andere Sicherheitsanforderungen als grundlegende Steuerungssystemkomponenten oder Systeme und Komponenten, die mit den Steuerungssystemkomponenten durch Schnittstellen verbunden sind. Sicherheitsbezogene Zonen erfordern aufgrund der potenziellen Konsequenzen einer Kompromittierung der Zone für Gesundheit, Sicherheit und Umwelt ein höheres Maß an Sicherheitsschutz.

4.4.5 ZCR-3.4: Separate vorübergehend angeschlossene Geräte

4.4.5.1 Empfehlung

Geräte, die vorübergehend an das SUC angeschlossen werden dürfen, sollten in einer separaten Zone oder mehreren separaten Zonen zu den Anlagen, die für den dauerhaften Anschluss an das IACS vorgesehen sind, gruppiert werden.

4.4.5.2 Erwägungen und zusätzliche Anleitung

Bei Geräten, die vorübergehend an das SUC angeschlossen werden (z. B. tragbare Instandhaltungscomputer, tragbare Prozessgeräte, tragbare Sicherheitsgeräte und Geräte mit universellem seriellen Bus [USB]) besteht eine höhere Wahrscheinlichkeit, dass sie einer Vielzahl unterschiedlicher Bedrohungen ausgesetzt sind, als bei Geräten, die dauerhafter Teil der Zone sind. Aus diesem Grund sollten diese Geräte in einer oder mehreren separaten Zonen abgebildet werden. Das Hauptproblem bei diesen Geräten besteht darin, dass sie aufgrund der vorübergehenden Verbindung auch an andere Netzwerke außerhalb der Zone angeschlossen werden können. Es gibt jedoch Ausnahmen. Ein in der Hand gehaltenes Gerät, das nur in einer einzigen Zone verwendet wird und die physischen Grenzen dieser Zone niemals verlässt, darf in die Zone eingebunden werden.

4.4.6 ZCR-3.5: Separate kabellose Geräte

4.4.6.1 Empfehlung

Kabellose Geräte sollten einer oder mehreren von verkabelten Geräten getrennten Zonen zugewiesen werden.

4.4.6.2 Erwägungen und zusätzliche Anleitung

Kabellose Signale werden nicht durch Zäune oder Schaltschränke kontrolliert und sind daher leichter zugänglich als Kabelnetzwerke. Aus diesem Grund sind sie anfälliger für andere und vielfältigere Bedrohungen als verkabelte Systeme.

Ein kabelloser Zugangspunkt wird üblicherweise als Kanal zwischen einer kabellosen und einer verkabelten Zone dargestellt. Je nach Kapazitäten des kabellosen Zugangspunkts können zusätzliche Sicherheitskontrollen (z. B. Firewall) erforderlich sein, um ein angemessenes Maß an Trennung zu bieten.

4.4.7 ZCR-3.6: Über externe Netzwerke verbundene separate Geräte

4.4.7.1 Empfehlung

Geräte, die über externe Netzwerke an das SUC angeschlossen werden dürfen, sollten in einer oder mehreren separaten Zone(n) gruppiert werden.

4.4.7.2 Erwägungen und zusätzliche Anleitung

Unternehmen gewähren häufig Personal wie etwa Mitarbeitern, Lieferanten und anderen Geschäftspartnern einen Fernzugang zu Instandhaltungs-, Optimierungs- und Berichtszwecken. Da der Fernzugang außerhalb der physischen Grenze des SUC liegt, sollte er in einer oder mehreren separaten Zone(n) mit eigenen Sicherheitsanforderungen abgebildet werden.

4.5 ZCR-4: Risikovergleich

4.5.1 ZCR-4.1: Vergleich zwischen allgemeinem und tolerierbarem Risiko

4.5.1.1 Anforderung

Das in ZCR-2 bestimmte allgemeine Risiko muss mit dem tolerierbaren Risiko der Organisation verglichen werden. Wenn das allgemeine Risiko das tolerierbare Risiko übersteigt, muss die Organisation eine ausführliche Cybersicherheitsrisikobeurteilung vornehmen, wie in ZCR-5 festgelegt.

4.5.1.2 Erwägungen und zusätzliche Anleitung

Dieser Schritt dient dazu, zu bestimmen, ob das allgemeine Risiko tolerierbar ist oder weitere Verringerung erfordert.

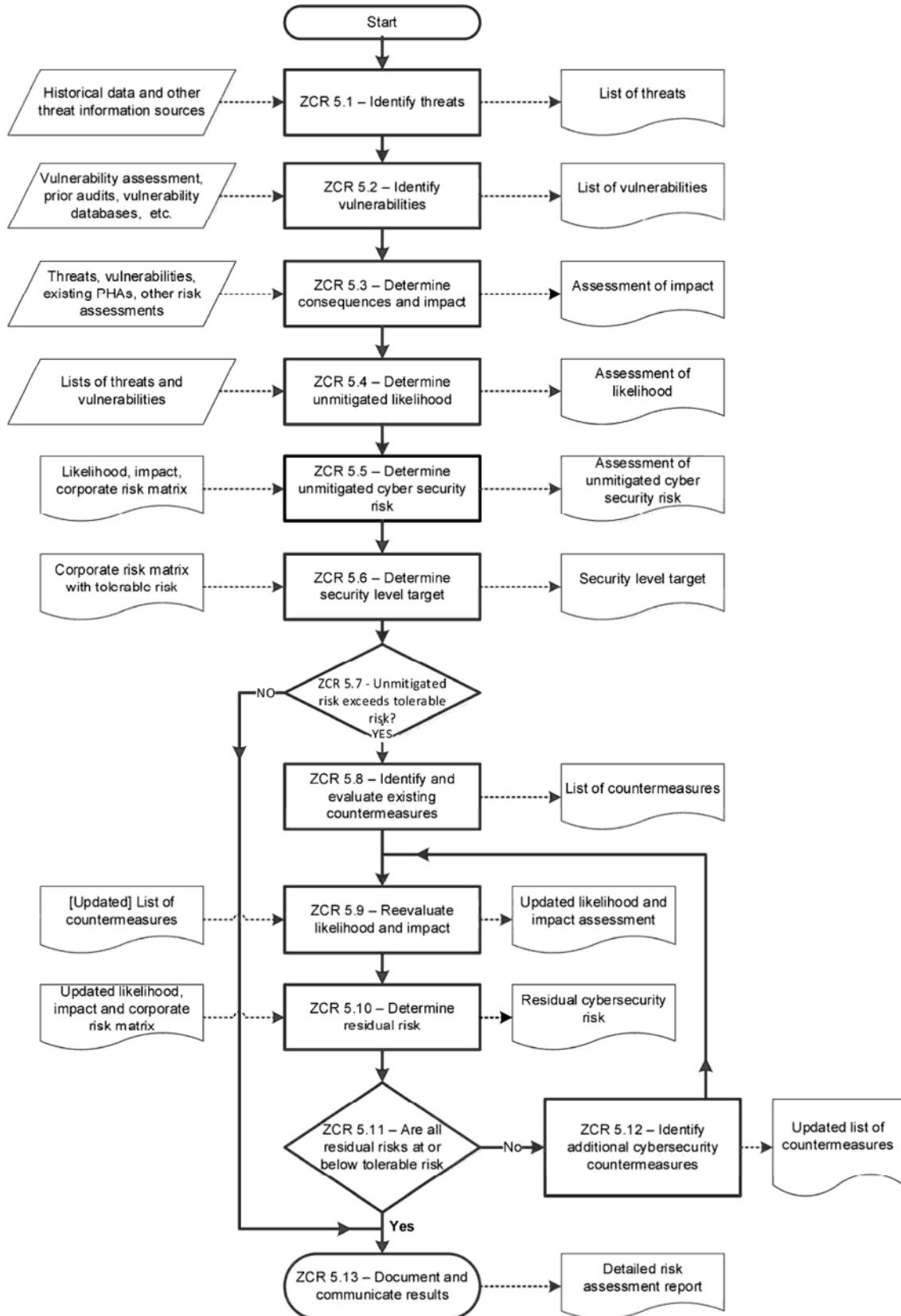
4.6 ZCR-5: Durchführen einer ausführlichen Cybersicherheitsrisikobeurteilung

4.6.1 Überblick

ZCR-5 behandelt die Anforderungen an die ausführliche Risikobeurteilung für ein IACS und bietet Erwägungen und eine ergänzende Anleitung zu jeder Anforderung. Die Anforderungen in ZCR-5 gelten für alle Zonen und Kanäle. Wenn Zonen oder Kanäle gleichen Bedrohungen, Konsequenzen und/oder Anlagen unterliegen, können Zonen- oder Kanalgruppen analysiert werden, wenn eine solche Gruppierung eine optimierte Analyse ermöglicht. Bestehende Ergebnisse dürfen verwendet werden, wenn die Zone genormt ist

(z. B. Replizierung mehrerer Instanzen einer Referenzgestaltung). Das Ablaufdiagramm in [Bild 2](#) stellt den Arbeitsablauf dar.

Jede ausführliche Risikobeurteilungsmethodik (wie etwa ISO 31000 [\[17\]](#), NIST SP800-39 [\[20\]](#) und ISO/IEC 27005 [\[16\]](#)) darf angewendet werden, sofern die gewählte Methodik die Anforderungen erfüllt. Die allgemeinen und ausführlichen Risikobeurteilungsmethodiken sollten aus demselben Rahmenwerk, derselben Norm oder derselben Quelle ausgewählt werden und müssen eine konsistente Risikobewertungsskala haben, um konsistente und kohärente Ergebnisse zu liefern.



Historical data and other threat information sources	Historische Daten und andere Bedrohungsinformationsquellen
Vulnerability assessment, prior audits, vulnerability databases, etc.	Schwachstellenbeurteilung, vorherige Prüfungen, Schwachstellendatenbanken usw.
Threats, vulnerabilities, existing PHAs, other risk	Bedrohungen, Schwachstellen, bestehende PHA, andere

assessments	Risikobeurteilungen
Lists of threats and vulnerabilities	Liste der Bedrohungen und Schwachstellen
Likelihood, impact, corporate risk matrix	Wahrscheinlichkeits-, Auswirkungs- und Unternehmensrisikomatrix
Corporate risk matrix with tolerable risk	Unternehmensrisikomatrix mit tolerierbarem Risiko
(updated) List of countermeasures	(aktualisierte) Liste der Gegenmaßnahmen
updated likelihood, impact and corporate risk matrix	aktualisierte Wahrscheinlichkeits-, Auswirkungs- und Unternehmensrisikomatrix
ZCR 5.1 - Identify threats	ZCR 5.1 – Bedrohungen identifizieren
ZCR 5.2 - Identify vulnerabilities	ZCR 5.2 – Schwachstellen identifizieren
ZCR 5.3 - Determine consequences and impact	ZCR 5.3 – Konsequenzen und Auswirkung bestimmen
ZCR 5.4 - Determine unmitigated likelihood	ZCR 5.4 – Unverringerte Wahrscheinlichkeit bestimmen
ZCR 5.5 - Determine unmitigated cyber security risk	ZCR 5.5 – Unverringertes Cybersicherheitsrisiko bestimmen
ZCR 5.6 - Determine security level target	ZCR 5.6 – Security-Level-Ziel bestimmen
ZCR 5.7 - Unmitigated risk exceeds tolerable risk?	ZCR 5.7 – Übersteigt das unverringerte Risiko das tolerierbare Risiko?
ZCR 5.8 - Identify and evaluate existing countermeasures	ZCR 5.8 – Identifizieren und Bewerten bestehender Gegenmaßnahmen
ZCR 5.9 - Reevaluate likelihood and impact	ZCR 5.9 – Wahrscheinlichkeit und Auswirkung neu bewerten
ZCR 5.10 - Determine residual risk	ZCR 5.10 – Restrisiko bestimmen
AZCR 5.11 - Are all residual risks at or below tolerable risk	AZCR 5.11 – Ist das Restrisiko nicht höher als das tolerierbare Risiko
ZCR 5.13 - Document and communicate results	ZCR 5.13 – Dokumentieren und Mitteilen der Ergebnisse
List of threats	Liste der Bedrohungen
List of vulnerabilities	Liste der Schwachstellen
Assessment of impact	Beurteilung der Auswirkung
Assessment of likelihood	Beurteilung der Wahrscheinlichkeit
Assessment of unmitigated cyber security risk	Beurteilung des unverringerten Cybersicherheitsrisikos
Security level target	Security-Level-Ziel
List of countermeasures	Liste der Gegenmaßnahmen
Updated likelihood and impact assessment	Aktualisierte Wahrscheinlichkeits- und Auswirkungsbeurteilung
Residual cybersecurity risk	Rest-Cybersicherheitsrisiko
ZCR 5.12 - Identify additional cybersecurity countermeasures	ZCR 5.12 – Zusätzliche Cybersicherheitsgegenmaßnahmen identifizieren
Detailed risk assessment report	Bericht der ausführlichen Risikobeurteilung
Updated list of countermeasures	Aktualisierte Liste der Gegenmaßnahmen

Bild 2 – Arbeitsablauf der ausführlichen Cybersicherheitsrisikobeurteilung je Zone oder Kanal

4.6.2 ZCR-5.1: Bedrohungen identifizieren

4.6.2.1 Anforderung

Eine Liste der Bedrohungen, die die in der Zone oder dem Kanal enthaltenen Anlagen betreffen könnten, muss erstellt werden.

4.6.2.2 Erwägungen und zusätzliche Anleitung

Es ist wichtig, eine umfassende und realistische Liste der Bedrohungen zu erstellen, um eine Sicherheitsrisikobeurteilung durchzuführen. Eine Beschreibung der Bedrohung sollte unter anderem Folgendes enthalten:

- a) eine Beschreibung der Bedrohungsquelle;
- b) eine Beschreibung der Kapazität oder des Fähigkeitsgrads der Bedrohungsquelle;
- c) eine Beschreibung möglicher Bedrohungsvektoren;
- d) eine Identifizierung potenziell betroffener Anlagen.

Einige Beispiele für Beschreibungen von Bedrohungen sind:

- Ein Mitarbeiter betritt ohne böse Absicht die Prozesssteuerungszone und schließt einen USB-Speicherstick an einen der Computer an;
- Ein autorisierter Support-Mitarbeiter greift mit einem infizierten Laptop auf die Prozesssteuerungszone zu; und
- Ein Mitarbeiter öffnet ohne böse Absicht eine Phishing-E-Mail, die seine Zugangsdaten kompromittiert.

Da Potenzial für eine große Anzahl möglicher Bedrohungen besteht, ist es akzeptabel, Quellen, Anlagen, Zugangspunkte usw. in Klassen zu gruppieren.

4.6.3 ZCR-5.2: Schwachstellen identifizieren

4.6.3.1 Anforderung

Die Zone oder der Kanal muss analysiert werden, um bekannte Schwachstellen in den Anlagen innerhalb der Zone oder des Kanals einschließlich der Zugangspunkte zu identifizieren und zu dokumentieren.

4.6.3.2 Erwägungen und zusätzliche Anleitung

Eine Bedrohung kann nur dann erfolgreich sein, wenn sie eine oder mehrere Schwachstellen einer Anlage ausnutzt. Bekannte Schwachstellen in Anlagen müssen daher identifiziert werden, um die Bedrohungsvektoren besser zu verstehen.

Eine Schwachstellenbeurteilung ist ein allgemein anerkannter Ansatz, um Schwachstellen in einem IACS zu identifizieren. ISA TR84.00.09 enthält zusätzliche Informationen zu Cybersicherheitsschwachstellenbeurteilungen von IACS.

Darüber hinaus stehen zahlreiche Informationsquellen zu bekannten und häufigen Schwachstellen in IACS wie etwa ICS-CERT, Lieferanten IACS usw. zur Verfügung.

4.6.4 ZCR-5.3: Bestimmen der Konsequenz und Auswirkung

4.6.4.1 Anforderung

Jedes Bedrohungsszenario muss bewertet werden, um die Konsequenz und Auswirkung bei einem tatsächlichen Auftreten der Bedrohung zu bestimmen. Die Konsequenzen sollten im Hinblick auf die Auswirkung auf Risikobereiche wie etwa die Personalsicherheit, finanzielle Verluste, Betriebsunterbrechungen und die Umwelt im ungünstigsten Fall dokumentiert werden.

4.6.4.2 Erwägungen und zusätzliche Anleitung

Die Einschätzung einer Cyberbedrohung im ungünstigsten Fall ist eine wichtige Information für die Durchführung der Kosten-Nutzen-Analyse der Sicherheitskontrollen. Wenn die Auswirkung im ungünstigsten Fall gering ist, kann das Risikobeurteilungsteam entscheiden, mit der nächsten Bedrohung fortzufahren.

Bestehende PHA und andere damit verbundene Risikobeurteilungen (wie etwa Informationstechnik, Geschäfts- und physische Sicherung) sollten geprüft werden, um die Bestimmung der Konsequenzen und der Auswirkung zu unterstützen.

Die Messung der Auswirkung kann qualitativ oder quantitativ sein. Ein Verfahren besteht darin, eine Konsequenzskala zu nutzen, die von der Organisation als Teil ihres Risikomanagementsystems festgelegt wird (siehe Beispiele im informativen [Anhang B](#)).

4.6.5 ZCR-5.4: Bestimmen der unverringerten Wahrscheinlichkeit

4.6.5.1 Empfehlung

Jede Bedrohung sollte bewertet werden, um die unverringerte Wahrscheinlichkeit zu bestimmen. Hierbei handelt es sich um die Wahrscheinlichkeit, dass eine Bedrohung tatsächlich auftritt.

4.6.5.2 Erwägungen und zusätzliche Anleitung

In der Risikomanagement-Terminologie bezeichnet dieser Begriff die Wahrscheinlichkeit, dass etwas passieren wird, das objektiv oder subjektiv, qualitativ oder quantitativ festgelegt, gemessen oder bestimmt und anhand allgemeiner Begriffe oder mathematisch beschrieben wird (wie etwa als eine Wahrscheinlichkeit oder Häufigkeit über einen gegebenen Zeitraum). Ein übliches Verfahren zur Einschätzung der Wahrscheinlichkeit besteht darin, eine semiquantitative Wahrscheinlichkeitsskala zu nutzen, die von der Organisation als Teil ihres Risikomanagementsystems festgelegt wird (siehe Beispiele im informativen [Anhang B](#)).

Bei der Einschätzung der unverringerten Wahrscheinlichkeit werden eine Reihe verschiedener Faktoren wie etwa die Motivation und Fähigkeit der Bedrohungsquelle, frühere vergleichbare Bedrohungen, bekannte Schwachstellen, die Attraktivität des Ziels usw. berücksichtigt.

Bestehende Cybersicherheitsgegenmaßnahmen für die bewertete Zone oder den bewerteten Kanal sollten bei der Bestimmung der unverringerten Wahrscheinlichkeit nicht berücksichtigt werden. Bei der Bestimmung der Wahrscheinlichkeit werden jedoch inhärente Gegenmaßnahmen für IACS-Komponenten und alle vorhandenen nicht-cyberunabhängigen Schutzebenen (IPL) sowie physische Sicherungen und mechanische Sicherungsmaßnahmen (wie etwa Drucksicherheitsventile) zur Reduzierung der Wahrscheinlichkeit anerkannt.

Die Wahrscheinlichkeit wird während der ausführlichen Risikobeurteilung zweimal bewertet. Sie wird zunächst ohne Berücksichtigung bestehender Gegenmaßnahmen bestimmt, um das unverringerte Risiko zu ermitteln. In ZCR-5.9 wird das Risiko unter Berücksichtigung der bestehenden Gegenmaßnahmen und ihrer Effektivität neu bewertet, um das Restrisiko zu bestimmen.

4.6.6 ZCR-5.5: Bestimmen des unverringerten Cybersicherheitsrisikos

4.6.6.1 Anforderung

Das unverringerte Cybersicherheitsrisiko für jede Bedrohung muss durch Kombination des in ZCR-5.3 bestimmten Auswirkungsmesswerts und des in ZCR-5.4 bestimmten unverringerten Wahrscheinlichkeitsmesswerts ermittelt werden.

4.6.6.2 Erwägungen und zusätzliche Anleitung

Die Bestimmung des unverringerten Cybersicherheitsrisikos erfolgt oftmals mithilfe einer Risikomatrix, die die Beziehung zwischen der Wahrscheinlichkeit, der Auswirkung und dem Risiko herstellt, wie etwa eine Unternehmensrisikomatrix (siehe Beispiele im informativen [Anhang B](#)).