

	DIN EN IEC 62443-2-2 (VDE 0802-2-2)	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 „etx Elektrotechnik + Automation“ bekannt gegeben worden.	VDE

ICS 35.030; 35.240.50

Einsprüche bis 2021-06-09

Entwurf

**IT-Sicherheit für industrielle Automatisierungssysteme –
Teil 2-2: IACS-Sicherheitsprogramm-Einstufungen
(IEC 65/797/CD:2020);
Text Deutsch und Englisch**

Security for industrial automation and control systems –
Part 2-2: IACS Security Program Ratings
(IEC 65/797/CD:2020);
Text in German and English

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2021-04-09 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 93 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Anwendungsbeginn

Anwendungsbeginn dieser Norm ist

Nationales Vorwort

Das internationale Dokument IEC 65/797/CD:2020-03 „Security for industrial automation and control systems – Part 2-2: IACS Security Program Ratings“ (CD, en: Committee Draft) 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 CD entsprechend der diesbezüglich durch die IEC erteilten Erlaubnis beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen IEC-Text.

Das internationale Dokument wurde vom IEC/TC 65 „Industrial-process measurement, control and automation“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und unterliegt dem Copyright der IEC . Das Dokument wurde den nationalen Komitees zur Stellungnahme vorgelegt.

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. Dokumente, die bei CENELEC als Europäische Norm angenommen und ratifiziert werden, sind unverändert als Deutsche Normen zu übernehmen.

Da der Abstimmungszeitraum für einen FDIS bzw. Schluss-Entwurf FprEN nur 6 Wochen 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 CD als DIN-Norm-Entwurf veröffentlicht, um die Stellungnahmen aus der Öffentlichkeit frühzeitig berücksichtigen zu können.

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

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DKE (www.dke.de) und DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

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.

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.

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.

Inhalt

	Seite
Einleitung.....	6
1 Anwendungsbereich.....	7
2 Normative Verweisungen.....	7
3 Begriffe, Abkürzungen und Vereinbarungen.....	8
3.1 Begriffe.....	8
3.2 Abkürzungen.....	9
3.3 Vereinbarungen.....	10
4 Rollen und Verantwortlichkeiten.....	10
5 Ganzheitliches Schutzsystem.....	12
5.1 Übersicht.....	12
5.2 Ganzheitliches Schutzsystem im IACS-Lebenszyklus.....	13
5.3 Organisationsstruktur.....	14
6 Sicherheitsprogramm-Einstufung.....	16
6.1 Übersicht.....	16
6.2 2.2-SM-001 – Anwendung der Sicherheitsprogramm-Einstufungen auf Zonen.....	18
6.2.1 Anforderung.....	18
6.2.2 Begründung und zusätzliche Hinweise.....	19
6.3 2.2-SM-002 – Anwendung der Sicherheitsprogramm-Einstufungen je Sicherheitsziel.....	19
6.3.1 Anforderung.....	19
6.3.2 Begründung und zusätzliche Hinweise.....	19
6.4 2.2-SM-003 – Kombinierte Evaluation von technischen und organisatorischen Maßnahmen.....	19
6.4.1 Anforderung.....	19
6.4.2 Begründung und zusätzliche Hinweise.....	20
6.5 2.2-SM-004 – Einstufung der Security-Level der Zonen der Automatisierungslösung.....	20
6.5.1 Anforderung.....	20
6.5.2 Begründung und zusätzliche Hinweise.....	20
6.6 2.2-SM-004 – Einstufung der organisatorischen Sicherheitsmaßnahmen für den Betrieb.....	20
6.6.1 Anforderung.....	20
6.6.2 Begründung und zusätzliche Hinweise.....	20
6.7 2.2-SM-005 – Bestimmung der SPR-Werte.....	21
6.7.1 Anforderung.....	21
6.7.2 Begründung und zusätzliche Hinweise.....	21
7 Verwendung der Sicherheitsprogramm-Einstufungen.....	23
7.1 Verwendung der SPR bei der Risikominderung.....	23
7.2 SPR-Typen.....	24
7.3 Verwendung von SPR im IACS-Lebenszyklus.....	25
Anhang A (informativ) Rollenbasierte Aktivitäten bei der Entwicklung, dem Betrieb und der Instandhaltung eines ganzheitlichen Schutzsystems.....	27
A.1 Übersicht.....	27

A.2	Spezifikation.....	27
A.3	Entwurf.....	30
A.4	Implementierung.....	36
A.5	Verifizierung und Validierung.....	38
A.6	Betrieb.....	39
A.7	Instandhaltung.....	40
A.8	Außerbetriebsetzung.....	41
Anhang B (informativ) Ansichten.....		43
Anhang C (informativ) Anwendung dieser Internationalen Norm.....		46
C.1	Anwendung von ISA 62443-2-2 durch externe Parteien.....	46
C.2	Anwendung von ISA 62443-2-2 durch IACS-Betreiber.....	46
C.3	Anwendung von ISA 62443-2-2 durch IACS-Dienstleister.....	46
C.4	Anwendung von ISA 62443-2-2 durch IACS-Hersteller.....	47
C.5	Anwendung von ISA 62443-2-2 durch unabhängige Evaluationsstellen.....	47
Anhang D (informativ) Methodik zur Evaluation.....		48
D.1	Übersicht.....	48
D.2	Detaillierte Beurteilung, auf Grundlage der Anforderungen.....	48
D.3	Detaillierte Beurteilung, basierend auf Risiko.....	48
D.4	Vereinfachte Evaluation, basierend auf Fragen.....	48
Literaturhinweise		49

Bilder

	Seite
Bild 1 – Teile der Normenreihe ISA/IEC-63443.....	6
Bild 2 – Hauptrollen in der Normenreihe ISA/IEC 62443.....	11
Bild 3 – Entwicklung und Betrieb eines ganzheitlichen Schutzsystems.....	14
Bild 4 – Beispiele von Matrizen für die Bestimmung der SPR-Werte.....	22
Bild 5 – Verwendung von SPR zur Risikominderung.....	23
Bild 6 – Schematische Darstellung der Korrelation der Verwendung verschiedener SL- und SPR-Typen.....	24
Bild 7 – SPR- und SL-Typen im IACS-Lebenszyklus.....	26
Bild 8 – Prozessschritte und Verantwortlichkeiten in der Spezifikationsphase.....	27
Bild 9 – Prozessschritte und Beiträge in der Entwurfsphase.....	31
Bild 10 – Verwendung von SPR Risikominderungsanalyse.....	34
Bild 11 – Verwendung der SPR-Werte bei der Gestaltung von Sicherheitsmaßnahmen.....	36
Bild 12 – Prozessschritte und Verantwortlichkeiten in der Implementierungsphase.....	37
Bild 13 – Prozessschritte und Verantwortlichkeiten in der Verifizierungs- und Validierungsphase.....	38
Bild 14 – Prozessschritte und Verantwortlichkeiten in der Betriebsphase.....	40
Bild 15 – Prozessschritte und Verantwortlichkeiten in der Instandhaltungsphase.....	41
Bild 16 – Prozessschritte und Verantwortlichkeiten in der Außerbetriebsetzungsphase.....	42
Bild 17 – Beispiel für ein Dashboard für die allgemeine Ansicht.....	44
Bild 18 – Verwendung von Ansichten in der Spezifikationsphase.....	44

Bild 19 – Verwendung von Ansichten bei der Entwicklung oder Instandhaltung eines ganzheitlichen Schutzsystems.....	45
Bild 20 – Verwendung von Ansichten während des Betriebs eines ganzheitlichen Schutzsystems.....	45

Tabellen

	Seite
Tabelle 1 – Organisationsstruktur.....	15
Tabelle 2 – Reifegradmodell.....	17
Tabelle 3 – Allgemeine Ansicht.....	43

Einleitung

ANMERKUNG Das Format dieses Dokuments folgt den in den ISO/IEC-Richtlinien, Teil 2 behandelten ISO/IEC-Anforderungen.¹ Die ISO/IEC-Direktiven legen sowohl das Format einer Norm als auch die Verwendung von Wörtern wie „muss“, „sollte“, und „darf“ fest. Die Anwendung dieser Begriffe für die in den [Abschnitten 4 bis 14](#) dieses Dokuments festgelegten Anforderungen folgt den in den ISO/IEC-Direktiven, Teil 2, [Abschnitt 7](#), behandelten Konventionen.

Diese Norm ist Teil der Normenreihe ISA/IEC 63443 und legt eine Methodik zur Evaluation des Schutzes in Betrieb befindlicher industrieller Automatisierungssysteme (IACS, en: Industrial Automation and Control Systems) fest, indem sie die Evaluation organisatorischer und technischer Maßnahmen in einzelnen Werten kombiniert, die als Sicherheitsprogramm-Einstufungen (SPR, en: security program ratings) bezeichnet werden. Sie wurde von der Arbeitsgruppe 3, Task Group 3 des ISA 99-Komitees erarbeitet.

[Bild 1](#) veranschaulicht die verschiedenen Teile von ISA/IEC 63443, die entwickelt werden. Die normativen Dokumente sind in der Liste der normativen Verweisungen in [Abschnitt 2](#) aufgeführt und die Dokumente, auf die zu Informationszwecken verwiesen wird oder die in Vorbereitung sind, sind in den Literaturhinweisen enthalten.

ANMERKUNG DER REDAKTION: [Bild 1](#) wird vor der endgültigen Annahme dieses Teils aktualisiert.

IEC 62443			
Industrielle Kommunikationnetze - IT-Sicherheit für Netze und Systeme			
Allgemeines		Leitlinien und Vorgehensweisen	System
1-1	Konzepte und Modelle	2-1 Anforderungen des Sicherheitsprogramms für IACS-Betreiber	3-1 Sicherheitstechnologien für IACS
1-2	Master-Glossar der Begriffe und Abkürzungen	2-2 IACS-Sicherheitsprogramm-Einstufungen	3-2 Sicherheitsrisikobeurteilung und Systemgestaltung
1-3	Maßgrößen der Konformität der Systemsicherheit	2-3 Patchverwaltung in der IACS-Umgebung	3-3 Systemsicherheitsanforderungen und Security-Level
1-4	IACS-Sicherheitslebenszyklus und Anwendungsfälle	2-4 Anforderungen des Sicherheitsprogramms für IACS-Dienstleister	
		2-5 Implementierungsanleitung für IACS-Betreiber	
			4-1 Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung
			4-2 Technische Sicherheitsanforderungen an IACS-Komponenten

Bild 1 – Teile der Normenreihe ISA/IEC-63443

¹ Nummern in eckigen Klammern beziehen sich auf die Literaturhinweise.

IT-Sicherheit für industrielle Automatisierungssysteme – Teil 2-2: IACS-Sicherheitsprogramm-Einstufungen

1 Anwendungsbereich

Dieser Teil der Normenreihe ISA/IEC 62443 behandelt die Evaluation der Cybersicherheit, die von einem ganzheitlichen Sicherheitssystem für ein in Betrieb befindliches IACS vernünftigerweise erwartet werden kann. Es umfasst die Methodik zur Kombination der Evaluation organisatorischer und technischer Sicherheitsmaßnahmen auf Grundlage einer Defense-in-Depth-Strategie. Das Ergebnis wird in numerischen Werten angegeben, die als Sicherheitsprogramm-Einstufung (SPR) bezeichnet werden. Der Begriff ist vom Begriff „Sicherheitsprogramm“ abgeleitet, der in ISA/IEC 63443-2-1 für die Festlegung der Sicherheitsmaßnahmen verwendet wird, die ein Betreiber als Teil der Betriebsaktivitäten des IACS festlegen muss. Die Methodik basiert auf der Erfüllung technischer und organisatorischer Anforderungen, die in den relevanten Dokumenten der Normenreihe ISA/IEC 62443 festgelegt sind. Organisatorische Sicherheitsmaßnahmen eines ganzheitlichen Schutzsystems sind im Sicherheitsprogramm der für den Betrieb des IACS verantwortlichen Organisationen enthalten. Zu den technischen Maßnahmen gehören sowohl Cybersicherheitsmaßnahmen als auch physische Sicherheitsmaßnahmen, die auf die im IACS verwendete Automatisierungslösung angewendet werden.

Die Entwicklung, der Betrieb und die Pflege eines ganzheitlichen Schutzsystems erfordert die Mitwirkung der Betreiber, der Serviceanbieter für Integration und Wartung sowie der Produktlieferanten in den verschiedenen Phasen eines IACS-Lebenszyklus. Dieses Dokument beschreibt die Mitwirkung dieser Beteiligten in jeder Phase des IACS-Lebenszyklus und den Einsatz von SPR zur Unterstützung der Evaluation der Ergebnisse der Aktivitäten.

Zweck des Dokuments ist es, eine einheitliche und reproduzierbare Methode zur Evaluation des Schutzes des sich in Betrieb befindlichen IACS auf Grundlage einer Defense-in-Depth-Strategie bereitzustellen. Es liegt nicht im Anwendungsbereich dieses Dokuments, vorzugeben, wie die Evaluation durchgeführt werden soll. [Anhang C](#) enthält Richtlinien für die Entwicklung von Evaluationsmethoden. Da es noch keinen Konsens bezüglich mathematischer Messungen von Sicherheit gibt, basieren die meisten Methoden derzeit auf einer qualitativen Evaluation, die auf dem Fachwissen des Prüfers über die zum Zeitpunkt der Evaluation bekannte Bedrohungslage beruht.

2 Normative Verweisungen

ISA/IEC-TS62443-1-1: 2009, *Security for industrial automation and control systems: Terminology, concepts and models*

ANMERKUNG DER REDAKTION: Zum Zeitpunkt der Veröffentlichung dieses Dokuments wird ISA/IEC-TS 62443-1-1:2009 überarbeitet. Es können einige Inhalte von ISA/IEC-TS 62443-1-1: 2009, auf die in diesem Dokument verwiesen wird, vorkommen. Dieses Dokument wird entsprechend angepasst.

ISA/IEC-TR62443-2-3:2015, *Security for industrial automation and control systems –Part 2-3: Patch management in the IACS environment*

ISA/IEC-62443-2-4:2017, *Security for industrial automation and control systems –Part 2-4: Security program requirements for IACS service providers*

ISA/IEC-62443-3-3:2013, *Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels*

ANMERKUNG DER REDAKTION: Zum Zeitpunkt der Veröffentlichung dieses Dokuments wird ISA/IEC **62443-3-3:2013** überarbeitet. Einige Inhalte von ISA/IEC 62443-3-3:2013 werden mit dem Inhalt dieses Dokumentes harmonisiert werden. Dieses Dokument wird entsprechend angepasst.

ISA/IEC-62443-4-1:2018, *Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements*

ISA/IEC-62443-4-2:2019, *Security for industrial automation and control systems – Part 4-1: Technical security requirements for IACS components*

3 Begriffe, Abkürzungen und Vereinbarungen

3.1 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach den in [Abschnitt 2](#) angegebenen normative Verweisungen und die folgenden Begriffe.

ANMERKUNG DER REDAKTION: Zum Zeitpunkt der Veröffentlichung dieses Dokuments werden einige Begriffe noch überprüft. Die Begriffe in diesem Dokument werden bei der Weiterentwicklung zu einer internationalen Norm entsprechend angepasst.

3.1.1

Schutzobjekt (en: asset)

physikalisches oder logisches Objekt im Eigentum oder in der Obhut einer Organisation, das für diese Organisation entweder einen wahrgenommenen oder einen tatsächlichen Wert hat

3.1.2

auf die Automatisierungslösung angewandte Sicherheitsmaßnahmen

Maßnahmen, die in der Automatisierungslösung mit dem Ziel umgesetzt werden, einen angestrebten Security-Level zu erreichen. Dabei handelt es sich im Wesentlichen um technische Maßnahmen und gegebenenfalls technische und/oder organisatorische ausgleichende Gegenmaßnahmen zur Verbesserung der technischen Fähigkeiten der in der Automatisierungslösung verwendeten Produkte.

Anmerkung 1 zum Begriff: Wenn ausgleichende Gegenmaßnahmen von Natur aus organisatorischer Art sind, müssen sie als Teil der organisatorischen Sicherheitsmaßnahmen für den Betrieb hinzugefügt werden.

3.1.3

ganzheitliches Schutzsystem

eine Reihe von technischen und organisatorischen Sicherheitsmaßnahmen mit dem Ziel, ein in Betrieb befindliches IACS vor Cyber-Bedrohungen zu schützen

3.1.4

Industrielles Automatisierungssystem

IACS, en: Industrial Automation and Control System

Gesamtheit von Personal, Hardware und Software, die den sicheren und zuverlässigen Betrieb eines industriellen Prozesses beeinträchtigen oder beeinflussen kann

Anmerkung 1 zum Begriff: Im Rahmen eines IACS beziehen sich in ISO/IEC 27001 alle Verweisungen auf „Information“ auf das IACS.

Anmerkung 2 zum Begriff: Im Rahmen eines IACS beziehen sich in ISO/IEC 27001 alle Verweisungen auf „Informationssicherheitssystem“ auf die Cybersicherheit.

3.1.5

Reifegrad (en: maturity level)

Grad, in dem eine Prozessfähigkeit (ein Prozess) durchgeführt, formalisiert, eingeführt und optimiert wird

3.1.6

organisatorische Sicherheitsmaßnahmen für den Betrieb

organisatorische Sicherheitsmaßnahmen, die während des Betriebs der Automatisierungslösung durchgeführt werden müssen, um die gewünschte Sicherheitsprogramm-Einstufungen zu erreichen und aufrechtzuerhalten. Dies umfasst auch, die in den Sicherheitsmaßnahmen verwendeten Informationen auf dem neuesten Stand zu halten.

Anmerkung 1 zum Begriff: Beispiele für Daten, die für Sicherheitsmaßnahmen verwendet werden, sind unter anderem

Virenmuster, Firewall-Regeln, die Liste aktiver Konten, Sicherungs- und Wiederherstellungsdaten.

3.1.7

Produkt (en: product)

Hardware- und/oder Software-Einheit, die entwickelt wurde, um unabhängig von einer spezifischen IACS-Umgebung in verschiedenen Anwendungen eingesetzt zu werden.

Anmerkung 1 zum Begriff: Beispiele für Produkte sind unter anderem Komponenten und Steuerungssysteme.

Anmerkung 2 zum Begriff: Definition des Begriffs Komponente in [ISA/IEC 62443-4-2]: zu einem IACS gehörende Einheit, die die Merkmale eines oder mehrerer Host-Geräte, Netzwerkgeräte, Softwareanwendungen oder eingebetteter Geräte aufweist

Anmerkung 3 zum Begriff: Definition des Begriffs Steuerungssystem in [ISA/IEC 62443-3-3]: Hardware- und Softwarekomponenten eines industriellen Automatisierungssystems.

3.1.8

Sicherheitsprogramm-Einstufung

SPR, en: security program rating

Einstufung des Schutzes des ganzheitlichen Schutzsystems auf Grundlage der Evaluation von:

- a) den Fähigkeiten der auf die Automatisierungslösung angewandten Sicherheitsmaßnahmen; und
- b) der Reife, die organisatorischen Sicherheitsmaßnahmen für den Betrieb anzuwenden.

3.1.9

Sicherheitsziel

Sicherheits-Subdomäne, die bei der Evaluation des durch eine Reihe technischer und organisatorischer Maßnahmen gebotenen Schutzes berücksichtigt wird. Die Sicherheitsprogramm-Einstufungen können in jedem Sicherheitsziel beurteilt werden, so dass der Schutz des in Betrieb befindlichen IACS in den SPR-Werten des Sicherheitsziels dargestellt werden kann.

3.1.10

Security-Level

(en: security level)

Level, das der erforderlichen Wirksamkeit der Gegenmaßnahmen und den inhärenten Sicherheitseigenschaften von Komponenten und Systemen für eine Automatisierungslösung entspricht.

Anmerkung 1 zum Begriff: Definition des Begriffs Security-Level in [ISA/IEC 62443-3-3]: Maß an Vertrauen, dass das IACS frei von Sicherheitslücken ist und in der vorgesehenen Weise funktioniert

ANMERKUNG DER REDAKTION: Zum Zeitpunkt der Veröffentlichung dieses Dokuments wird ISA/IEC 62443-3-3:2013 überprüft. Die Definition in ISA/IEC 62443-3-3 und die Definition in diesem Dokument werden harmonisiert. Dieses Dokument wird entsprechend angepasst.

3.1.11

Ansicht

vereinfachte Darstellung des Schutzes des in Betrieb befindlichen IACS in SPR-Werten, die in Elemente der Ansicht anstelle des Sicherheitsziels strukturiert sind. Verglichen mit der Anzahl der Sicherheitsziele weisen die Ansichten weniger Elemente auf und somit eine höhere Abstraktionsebene in jedem SPR-Wert auf.

3.2 Abkürzungen

ISAN ¹	amerikanische Standardisierungsorganisation (en: American National Standards Institute)
AO	Betreiber (en: Asset Owner)
IACS	industrielles Automatisierungssystem

^{N1} Nationale Fußnote: Im CD 65/797:2020 wurde irrtümlich „ISA“ als Abkürzung für amerikanische Standardisierungsorganisation (en: American National Standards Institute) notiert. Korrekt ist die Abkürzung „ANSI“.

IEC	Internationale elektrotechnische Kommission (en: International Electrotechnical Commission)
ISA	gemeinnützige Fachgesellschaft für Automatisierung (en: International Society of Automation)
ML	Reifegrad (en: maturity level)
PIN	Persönliche Identifizierungsnummer (en: Personal Identification Number)
PS	Hersteller (en: Product Supplier)
SM	Instandhaltungsdienstleister (en: Maintenance Service Provider)
SI	Integrationsdienstleister (en: Integration Service Provider)
SL	Security-Level
SO	Sicherheitsziel (en: Security Objective)
SPR	Sicherheitsprogramm-Einstufung (en: Security Program Rating)

3.3 Vereinbarungen

[Alle in diesem Dokument verwendeten Konventionen, falls vorhanden, beschreiben.]

4 Rollen und Verantwortlichkeiten

Ein IACS ist definiert als eine Gesamtheit von Personal, Hardware und Software, die für den Betrieb eines industriellen Prozesses erforderlich ist. Angewandt auf die Cybersicherheit umfasst das IACS-Modell sowohl eine technische Lösung – die Automatisierungslösung – als auch die organisatorischen Sicherheitsmaßnahmen für den Betrieb nach Sicherheitsrichtlinien und -verfahren. Dieser Abschnitt beschreibt die Rollen, die mit dem Schutz eines in Betrieb befindlichen IACS vor Cyber-Bedrohungen verbunden sind.

Eine Rolle wird durch Verantwortlichkeiten und/oder Zuständigkeiten sowie die damit verbundenen Aktivitäten definiert, die von einer Organisation erfüllt werden müssen. Eine Organisation kann eine Einzelperson, eine juristische Instanz, wie z. B. ein Unternehmen oder eine Regierungsstelle, oder eine Unterabteilung der juristischen Instanz, wie z. B. eine Abteilung, sein.

Eine Organisation kann eine oder mehrere Rollen erfüllen. So ist es beispielsweise nicht ungewöhnlich, dass ein und dasselbe Unternehmen für den Betrieb eines IACS sowie für die Gestaltung, Umsetzung und Validierung der Automatisierungslösung verantwortlich ist. Andererseits kann eine Rolle von einer oder mehreren Organisationen ausgefüllt werden. Beispielsweise können die Instandhaltungsaktivitäten von verschiedenen Organisationen durchgeführt werden.

Die Gestaltung, der Betrieb und die Instandhaltung eines ganzheitlichen Schutzsystems für ein in Betrieb befindliches IACS erfordert die Mitwirkung und die Zusammenarbeit aller Beteiligten entsprechend der ihnen zugewiesenen Rolle. [Bild 2](#) gibt einen Überblick über die Rollen und ihre unterschiedlichen Aktivitäten, Pflichten und Verantwortlichkeiten.

ANMERKUNG Die Begriffe „Betreiber“, „Instandhaltungsdienstleister“, „Integrationsdienstleister“ und „Hersteller“ sind in den Dokumenten der Normenreihe ISA / IEC 62443 als Organisationen definiert. Für die Beschreibung der Mitwirkung der verschiedenen Beteiligten in diesem Dokument werden diese Begriffe für Aktivitäten, Pflichten und Verantwortlichkeiten der mit ihnen verbundenen Rollen verwendet.

Die Rolle des Betreibers (AO) umfasst zwei Teile. Die erste Rolle ist die Zuständigkeit für das IACS einschließlich des Schutzes des in Betrieb befindlichen IACS und der damit verbundenen Risiken während des gesamten Lebenszyklus. Die Rolle des AO definiert das vertretbare Cybersicherheitsrisiko als eine Eingabevoraussetzung für alle Cybersicherheitsaktivitäten entlang des IACS-Lebenszyklus. Die Organisation, die diese Rolle erfüllt, bleibt zwar weiterhin zuständig, delegiert aber die Verantwortlichkeiten und die damit verbundenen Aktivitäten an Organisationen, die andere in diesem Abschnitt beschriebene Rollen erfüllen. Der zweite Teil, der der Rolle des AO zugewiesen wird, ist die Verantwortung für den Betrieb der Automatisierungslösung entsprechend den definierten Sicherheitsrichtlinien und -verfahren. Sie umfasst die Aktualisierung von Informationen, die bei Sicherheitsmaßnahmen wie Virenmustern, Firewall-Regeln, der Liste aktiver Konten oder der Sicherung und Wiederherstellung von Daten verwendet werden. Bei der Einbeziehung dieser beiden Teile in die Rolle des AO

wird davon ausgegangen, dass in vielen Fällen die Organisation, die das IACS betreibt, auch der rechtliche Eigentümer und damit für das IACS zuständig ist.

Die Rolle des Instandhaltungsdienstleisters (SM) ist für die Instandhaltung und Außerbetriebsetzung der Automatisierungslösung verantwortlich. Im Vergleich zur Aktualisierung der in den Sicherheitsmaßnahmen verwendeten Informationen, die in der Rolle des AO enthalten ist, haben die Instandhaltungsaktivitäten den Zweck, die Maßnahmen des ganzheitlichen Schutzsystems zu aktualisieren und schließlich zu ergänzen, um eine Änderung der Bedrohungslage oder eine Anpassung der Automatisierungslösung zu berücksichtigen. Eine Instandhaltungsphase wird durch das Ergebnis einer Bewertung des Cybersicherheitsrisikos ausgelöst, die aufzeigt, dass die Maßnahmen des ganzheitlichen Schutzsystems nicht mehr den gewünschten Schutzgrad bieten. Im Allgemeinen umfasst die Aktualisierung sowohl die technischen Sicherheitsmaßnahmen, die auf die Automatisierungslösung angewendet werden, als auch die organisatorischen Sicherheitsmaßnahmen für den Betrieb des ganzheitlichen Schutzsystems, um den angestrebten Schutz des IACS aufrechtzuerhalten. Die Rolle des SM umfasst die Verantwortung für die Außerbetriebsetzung von Teilen oder der gesamten Automatisierungslösung und die Sicherstellung, dass das vertretbare verbleibende Cybersicherheitsrisiko während oder nach der Außerbetriebsetzung weiterhin sichergestellt wird.

Die Rolle des Integrationsdienstleisters (SI) ist für die Gestaltung und Implementierung sowie für die Inbetriebnahme und Validierung der auf die Automatisierungslösung angewandten Sicherheitsmaßnahmen verantwortlich. Die Aktivitäten umfassen die Entwicklung und Validierung eines ganzheitlichen Schutzsystems für das in Betrieb befindliche IACS mit dem Ziel, dem vertretbaren Cybersicherheitsrisiko gerecht zu werden. Dazu gehören die Entwicklung von technischen Sicherheitsmaßnahmen, die auf die Automatisierungslösung angewendet werden, sowie Richtlinien für organisatorische Maßnahmen, die während des Betriebs implementiert werden müssen. Die Grundlage für die Richtlinien bilden häufig Richtlinien, die von der Rolle des Herstellers bereitgestellt werden. Es ist nicht ungewöhnlich, dass eine oder mehrere Organisationen Teile oder die gesamte Automatisierungslösung gestalten und bereitstellen, während eine andere Organisation für die Inbetriebnahme und Validierung der Automatisierungslösung verantwortlich ist.

Die Rolle des Herstellers (PS) ist für die Entwicklung und die Unterstützung der innerhalb der Automatisierungslösung verwendeten Produkte verantwortlich. Zu den Aktivitäten gehört die Entwicklung von Sicherheitsfähigkeiten des Produktes, die in der Automatisierungslösung nach einem etablierten Produktentwicklungs-Lebenszyklusprozess eingesetzt werden sollen, einschließlich der Handhabung von Vorfällen und Schwachstellenmanagementprozessen. Die Rolle des PS hat die Verantwortung für die Bereitstellung produktspezifischer Integrations-, Härtings- und Betriebsrichtlinien für das/die Produkt(e), das/die sie dem Betreiber liefern.

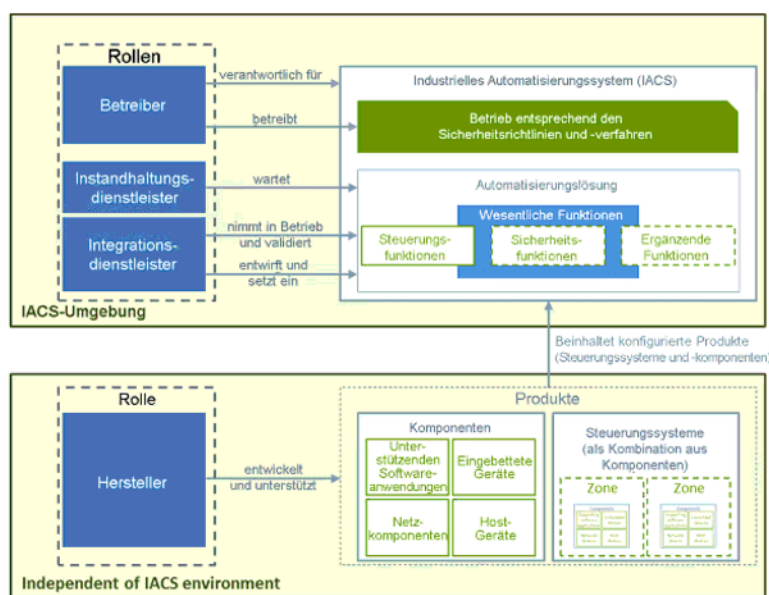


Bild 2 – Hauptrollen in der Normenreihe ISA/IEC 62443

ANMERKUNG Die Organisationen, die die in diesem Abschnitt beschriebenen Rollen ausüben, können sich von einem Projekt zum anderen unterscheiden, und die für die Benennung dieser Organisationen verwendeten Bezeichnungen können

in verschiedenen Marktsektoren, Branchen oder Ländern, einschließlich, aber nicht beschränkt auf die folgenden, stark variieren:

Role Anlagenbetreiber, Regulierungsstelle, Betriebsabteilung, Betriebsdienstleister;

AO:

Role Instandhaltungsabteilung, technischer Dienst;

SM:

Role Anlageneinrichtungs- und Inbetriebnahmeabteilung, Integrator, EPC-Unternehmen, Maschinenbauer; und

SI:

Role Hersteller, Produzent, OEM.

PS:

5 Ganzheitliches Schutzsystem

5.1 Übersicht

Das Konzept des ganzheitlichen Schutzsystems berücksichtigt, dass der Schutz eines in Betrieb befindlichen IACS eine Kombination aus Technologie, Prozessen und Menschen umfasst. Schwächen im Schutzkonzept können in jedem dieser Bereiche ihren Ursprung haben. Folglich müssen all diese Teile bei der Evaluation des Schutzes durch ein ganzheitliches Schutzsystem in einer projektspezifischen IACS-Umgebung berücksichtigt werden. Darüber hinaus müssen alle Rollen (AO, SI, SM, PS) zur Entwicklung, zum Betrieb und zur Instandhaltung eines ganzheitlichen Schutzsystems beitragen.

Der technologische Teil besteht aus Cyber- bzw. elektronischen Sicherheitsmaßnahmen (z. B. eine Industrie-Firewall, die die Kommunikation zwischen Netzwerksegmenten kontrolliert) und physischen Sicherheitsmaßnahmen (z. B. ein Schloss, das den physischen Zugang zu einem Schrank mit einer Industrie-Firewall und deren Verkabelung schützt). Dies sind technische Sicherheitsmaßnahmen, die auf die Automatisierungslösung angewandt werden. Sie basieren auf den technischen Sicherheitsfähigkeiten der Produkte und umfassen Maßnahmen, die sich aus der Gestaltung der Automatisierungslösung selbst ergeben, z. B. die Schutzmaßnahmen, die durch die Netzwerkarchitektur bereitgestellt werden. Die meisten Sicherheitsmaßnahmen, die auf die Automatisierungslösung angewandt werden, sind von Natur aus technischer Art und basieren auf den Fähigkeiten der in der Automatisierungslösung verwendeten Produkte. Es können ausgleichende Gegenmaßnahmen erforderlich sein, um einen gewünschten Security-Level zu erzielen, um die technischen Fähigkeiten der Produkte zu verbessern. Dabei kann es sich um zusätzliche technische und/oder organisatorische Maßnahmen handeln.

Die Prozess- und Personenkomponente umfasst betriebliche Aktivitäten, die für den Schutz des IACS vor Cyber-Bedrohungen relevant sind. Diese sind von Natur aus organisatorischer Art und müssen vom verantwortlichen Personal während des Betriebs des IACS angewendet werden. Die Wirksamkeit organisatorischer Maßnahmen hängt von der Fähigkeit des verantwortlichen Fachpersonals ab, im Laufe der Zeit zuverlässig entsprechend den in den Verfahren dokumentierten Sicherheitsrichtlinien zu handeln. Dies spiegelt sich im Reifegrad der verantwortlichen Organisation wider. Der Aspekt der Reife ist besonders wichtig, da die Betriebsphase häufig viele Jahre dauert.

In vielen Fällen sind organisatorische und technische Maßnahmen zusammenhängend, und der Schutz vor Cyber-Bedrohungen erfordert die Abstimmung zwischen den auf die Automatisierungslösung angewandten Sicherheitsmaßnahmen und den damit verbundenen organisatorischen Maßnahmen. So sind beispielsweise Identifikation und Authentifizierung Voraussetzungen, um den Zugriff auf die Automatisierungslösung auf autorisierte menschliche Benutzer entsprechend ihrer jeweiligen Rolle zu beschränken. Dies kann zum Beispiel über die Vergabe von Benutzernamen und zugehörigen Passwörtern umgesetzt werden. Der technologische Teil des Schutzsystems besteht darin, dass die Automatisierungslösung die technischen Möglichkeiten für auf Benutzernamen/Passwörtern basierende Identifizierungs- und Authentifizierungsmechanismen ermöglicht. Die damit verbundenen organisatorischen Maßnahmen erfordern eine Passwortrichtlinie, welche Länge und Komplexität, Ablaufbedingungen, Änderung, Wiederverwendung, Handhabung, Weitergabe und Offenlegung von Passwörtern regelt. Die gleiche Sicherheitsfrage hinsichtlich der Identifizierung und Authentifizierung kann durch einen stärkeren Mechanismus mit Hilfe einer Multifaktor-Authentifizierung gelöst werden, z. B. mit einer Chipkarte und einer PIN (persönliche Identifizierungsnummer). Dies würde zu einer höheren Einstufung des Security-Levels der Fähigkeiten führen, die durch die auf die Automatisierungslösung angewandten

technischen Sicherheitsmaßnahmen bereitgestellt werden. In diesem Fall sind die damit verbundenen organisatorischen Maßnahmen unterschiedlich und müssen den Umgang mit der Chipkarte, die Verwaltung des Schlüsselmaterials sowie das Festlegen/Ändern der PIN abdecken.

5.2 Ganzheitliches Schutzsystem im IACS-Lebenszyklus

Die Gestaltung, der Betrieb und die Wartung eines ganzheitlichen Schutzsystems sollten in alle Aktivitäten entlang des IACS - Lebenszyklus eingebunden werden, siehe [Bild 3](#). Ausgehend von einem vertretbaren Cybersicherheitsrisiko sollte der angestrebte Schutz für das in Betrieb befindliche IACS bestimmt werden. Um diese Schutzziele zu erreichen, müssen ein Entwurf der Sicherheitsmaßnahmen, die auf die Automatisierungslösung angewendet werden, sowie Richtlinien für die damit verbundenen organisatorischen Maßnahmen entwickelt werden. Dabei handelt es sich üblicherweise um einen iterativen Prozess, bei dem nach jeder Iteration geprüft werden muss, ob die vorgeschlagenen technischen und organisatorischen Maßnahmen in der Lage sind, den gewünschten Schutzgrad zu erreichen. Als Teil des Gestaltungsprozesses werden die Produkte mit den erforderlichen Sicherheitsfähigkeiten ausgewählt. Falls solche Produkte nicht verfügbar sind, sollten entsprechende ausgleichende technische oder organisatorische Sicherheitsgegenmaßnahmen erarbeitet werden.

Vor Beginn der Betriebsphase sollte der erreichte Schutz, der durch die technischen und organisatorischen Maßnahmen erreicht wird, validiert werden. Es ist sehr erstrebenswert, dokumentierte Sicherheitsrichtlinien und -verfahren für die organisatorischen Maßnahmen zu entwickeln, da diese vom verantwortlichen Personal während des Betriebs des IACS durchgeführt werden müssen. Die Überprüfung und Aktualisierung der in den Sicherheitsmaßnahmen verwendeten Informationen wie Virenmuster, Firewall-Regeln, Liste der aktiven Konten sowie die Sicherung und Wiederherstellung von Daten sind Teil der organisatorischen Maßnahmen für den Betrieb. Die Validierung wird oft mit einem Probelauf abgeschlossen, an dem die für den Betrieb verantwortliche Organisation beteiligt ist. Die Wirksamkeit des ganzheitlichen Schutzsystems während des Betriebs wird validiert, wenn die auf die Automatisierungslösung angewandten technischen Sicherheitsmaßnahmen von Fachpersonal zuverlässig entsprechend den Sicherheitsrichtlinien und -verfahren umgesetzt werden. Dies spiegelt sich in der Reife der Organisation wider, die für den Betrieb des IACS zuständig ist.

Da sich die Bedrohungslage im Laufe der Zeit möglicherweise verändert, muss in regelmäßigen Abständen neu bewertet werden, ob der Cybersicherheitsschutz den in der Spezifikationsphase definierten angestrebten Schutzgrad noch immer erreicht. Der Auslöser für eine Revalidierung wird durch ein definiertes Intervall (z. B. behördlicher Prozess, Sicherheitsmanagement-Anforderung, planmäßige Instandhaltung) oder durch eine Änderung der Bedrohungsumgebung oder der Betriebsbedingungen vorgegeben, je nachdem, was davon zuerst eintritt. Eine Instandhaltungsphase wird eingeleitet, wenn die Notwendigkeit besteht, die technischen und/oder organisatorischen Maßnahmen zu optimieren, um sich an Änderungen der IACS-Betriebsbedingungen oder der Bedrohungsumgebung anzupassen.

Mit den Aktivitäten der Außerbetriebsetzungsphase soll verhindert werden, dass die in den außer Betrieb gesetzten Schutzobjekten gespeicherten Informationen missbraucht werden und das im Betrieb befindliche IACS gefährden können. Die Außerbetriebsetzung von Teilen eines Netzwerks kann erhebliche Auswirkungen auf die übrigen Teile des IACS haben, so dass die verbleibenden Teile neu validiert werden müssen.

ANMERKUNG In [Bild 3](#) sind die Phasen des IACS-Lebenszyklus auf die Stufen des allgemeinen repräsentativen Systemlebenszyklusmodells von IEC 24748 „Systems and software engineering – Life cycle management“ abgebildet.

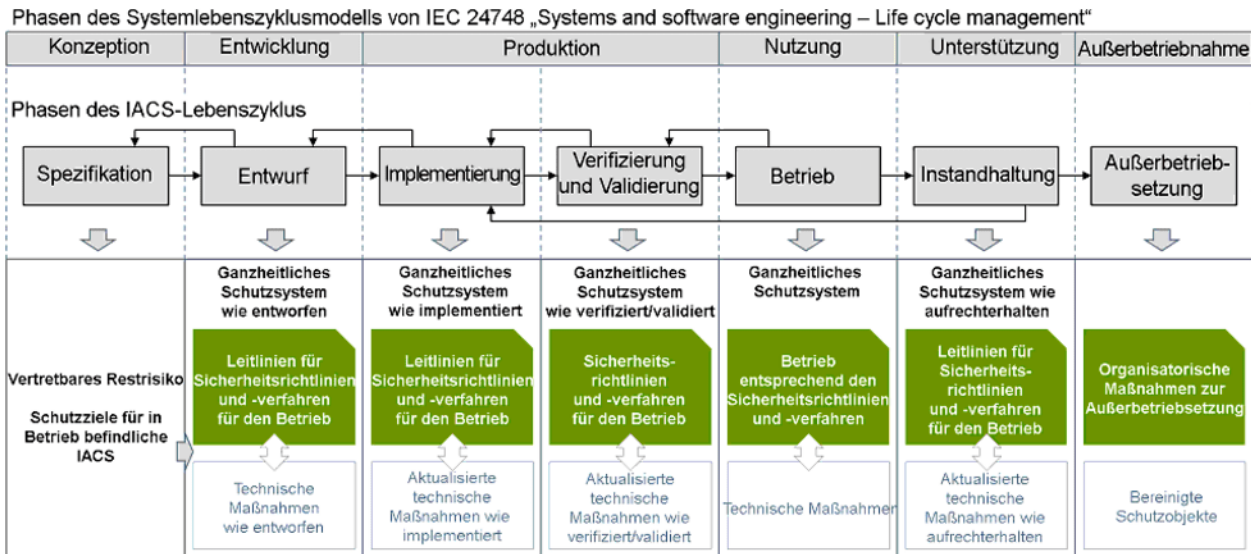


Bild 3 – Entwicklung und Betrieb eines ganzheitlichen Schutzsystems

5.3 Organisationsstruktur

ANMERKUNG DER REDAKTION: Dieser Abschnitt bezieht sich auf eine gemeinsame Organisationsstruktur für die relevanten Dokumente der Normenreihe ISA/IEC 62443, die von einer von der ISA-99-Leitung beauftragten Task Force festgelegt wurde. Die endgültige Genehmigung durch ISA-99 und IEC TC 65 steht noch aus. Die Struktur der Anforderungen in den Sicherheitszielen kann sich bei der Entwicklung dieses Dokuments zu einer internationalen Norm verändern. Sie wird gegebenenfalls angepasst; die in diesem Abschnitt beschriebenen Grundsätze bleiben unverändert.

Die Organisationsstruktur:

- ist eine Möglichkeit, die Anforderungen in ISA/IEC 62443 zu strukturieren;
- ist ein Ersatz für die grundlegenden Anforderungen;
- ist obligatorisch für alle Technischen Spezifikationen (TS) und Internationalen Normen (IS) der ISA/IEC 62443;
- ist nicht obligatorisch für Technischen Berichte (TR) der ISA/IEC 62443;
- wird verwendet, um die Vollständigkeit der für die ISA/IEC 62443 relevanten Dokumente zu prüfen;
- wird verwendet, um die Redundanz von Anforderungen in allen für die ISA/IEC 62443 relevanten Dokumenten zu prüfen;
- wird verwendet, um die Rückverfolgbarkeit der Anforderungen über alle für die ISA/IEC 62443 relevanten Dokumente hinweg zu erleichtern, und
- ist für Endanwender der Normenreihe ISA/IEC 62443 einfach zu verstehen.

Alle relevanten Anforderungen werden auf eines oder mehrere von neun Sicherheitszielen rückverfolgt, die eine gemeinsame Sicherheitsunterdomäne betreffen. Anstatt die SPR-Werte auf einen einzigen Wert zu reduzieren, ist es möglich, einen Vektor für die SPR-Werte entsprechend der Organisationsstruktur zu verwenden. Dies ermöglicht definierbare Trennungen zwischen SPR für die verschiedenen Sicherheitsziele und einen strukturierten Ansatz für die Einstufung eines standortspezifischen IACS-Sicherheitsprogramms, siehe [Tabelle 1](#).

SL-Werte der Automatisierungslösung werden bestimmt, indem die Sicherheitsmaßnahmen anhand der Anforderungen von [ISA/IEC 62443-3-3](#) für eine Zone in der Automatisierungslösung eingestuft werden. Die Strukturierung der SPR entlang der Sicherheitsziele bedeutet, dass jede Anforderung auf ein oder mehrere Sicherheitsziele rückverfolgt wird. Bei der Einstufung des SL-Wertes in jedem Sicherheitsziel wird die Teilmenge berücksichtigt, die auf das jeweilige Sicherheitsziel rückverfolgt wird.

Gleichermaßen wird die Teilmenge der Anforderungen von ISA/IEC 62443-2-1, die im entsprechenden Sicherheitsziel enthalten ist, bei der Evaluation der organisatorischen Sicherheitsmaßnahmen für den Betrieb bei jedem Sicherheitsziel berücksichtigt.

Die Entwicklung und der Betrieb eines ganzheitlichen Schutzsystems erfordert die Mitwirkung jeder einzelnen Rolle. Die Rückverfolgbarkeit der Anforderungen aller relevanten Teile der Normenreihe ISA/IEC 62443 bis hin zu den Sicherheitszielen bietet einen Leitfaden für die erwartete Mitwirkung jeder Rolle zur Entwicklung, zum Betrieb und zur Aufrechterhaltung des ganzheitlichen Schutzsystems im Hinblick auf das jeweilige Sicherheitsziel:

- Die rückverfolgten Anforderungen von ISA/IEC 62443-2-4 gelten für die erwartete Mitwirkung von Dienstleistern zur Integration oder zur Instandhaltung;
- Zusätzlich zu den Fähigkeiten der auf die Automatisierungslösung angewandten Sicherheitsmaßnahmen gelten die rückverfolgten Anforderungen von ISA/IEC 62443-3-3 und ISA/IEC 62443-4-2 für die erwarteten inhärenten Fähigkeiten der in der Automatisierungslösung verwendeten Produkte, und
- Die rückverfolgten Anforderungen von ISA/IEC 62443-4-1 gelten für die erwartete Mitwirkung der Hersteller hinsichtlich der Unterstützung bei Leitlinien und Schwachstellenmanagement.

ANMERKUNG DER REDAKTION: Es besteht die Absicht, eine separate Tabelle mit der Rückverfolgbarkeit der Anforderungen zu den Sicherheitszielen zu veröffentlichen.

Tabelle 1 – Organisationsstruktur

Mar- ke	Sicherheitsziel	Beschreibung	Umfasst
SM	Sicherheitsmanage- ment (en: Security Management)	Einrichtung und Aufrechterhaltung der zusätzlichen Elemente eines IACS-Sicherheitsprogramms	Anforderungen an das Management des Sicherheitsprogramms. Anmer- kung: Prozesse zur Unterstützung technischer Anforderungen sind in den anderen Elementen enthalten
LF	Sicherheitslebens- zyklus (en: Security Life cycle)	Sicherheit von Produkten und des IACS während ihres gesamten Le- benszyklus	Produktlebenszyklus, Lebenszyklus von Automatisierungslösungen, Si- cherheitslebenszyklen einschließlich Qualitätsmanagement.
RM	Risikomanagement (en: Risk Manage- ment)	Management von Risiken für Pro- dukte und IACS während ihrer Le- benszyklen	Risikobeurteilung, Sicherheitszonen und -Conduits, Spezifikation der Si- cherheitsanforderungen
AC	Zugangssteuerung (en: Access Control)	Beschränkung des physischen und logischen Zugangs zu Produkten und IACS	Physische Zugangskontrolle, Sys- tem-Zugangskontrolle, Netzwerk-Zu- gangskontrolle
SI	Systemintegrität (en: System Integrity)	Sicherstellung der System-, Netz- werk- und Datenintegrität für Produk- te und IACS	Sicherheitsintegrität, Kontrollintegri- tät, Datenintegrität, Netzwerkintegri- tät
AS	Systemverfügbarkeit (en: System Availa- bility)	Sicherstellung der Netzwerk- und Datenverfügbarkeit für Produkte und IACS	Sicherheitsverfügbarkeit, Kontrollver- fügbarkeit, Datenverfügbarkeit, Netz- werkverfügbarkeit
DC	Datenvertraulichkeit (en: Data Confiden- tiality)	Verhindern der unbefugten Offen- legung von vertraulichen Daten für Produkte und IACS	Authentifizierungs-Token, personen- bezogene Daten (PII), Daten bei der Übertragung, Daten bei der Speiche- rung