DAkkS
Deutsche
Akkreditierungsstelle

Akkreditierungsanforderungen für Konformitätsbewertungsstellen im Bereich der Informationssicherheit/Cyber-Security für industrielle Automatisierungssysteme gemäß IEC 62443

---

71 SD 2 019 | Revision: 1.0 | 05. März 2018

Geltungsbereich:

Diese Anforderungen gelten verbindlich für die Akkreditierung von Prüflaboratoren, Inspektionsstellen und Zertifizierungsstellen, die Konformitätsbewertungstätigkeiten im Bereich der Informationssicherheit/Cyber-Security für industrielle Automatisierungssysteme gemäß IEC 62443, durchführen.

Diese Regel dient der Konkretisierungen bestimmter Anforderungen der Normen DIN EN ISO/IEC 17020, der DIN EN ISO/IEC 17025, der DIN EN ISO/IEC 17065 sowie der DIN EN ISO/IEC 17021-1 in Verbindung mit der ISO/IEC 27006 zum Akkreditierungsverfahren sowie an die Konformitätsbewertungsstellen. Außerdem enthält diese Regel Anforderungen zur Darstellung und Formulierung des Akkreditierungsbereichs von Stellen, die Prüfungen oder Inspektionen durchführen oder von Stellen, die Produkte, Prozesse und Dienstleistungen oder Managementsysteme zertifizieren.

Weitere Anforderungen können in nachgeordneten, sektoralen Regeln festgelegt sein.

Datum der Bestätigung durch den Akkreditierungsbeirat: 19.02.2018

Gemäß § 2 i.V.m. § 3 Nr. 9 BGleiG ist § 4 Abs. 3 BGleiG nicht direkt auf die DAkkS anwendbar. In diesem Dokument wird im Interesse der Lesbarkeit für Funktionsbezeichnungen auch das generische Maskulinum verwendet, soweit eine konkrete Ansprache nach dem natürlichen Geschlecht nicht sinnvoll möglich ist und das natürliche Geschlecht unwichtig ist oder männliche und weibliche Personen gleichermaßen gemeint sind.

DAkkS-Regeln und sonstige technische Spezifikationen müssen problemlos lesbar sein und dürfen deshalb keine Schrägstriche enthalten, was eine Benutzung des Binnen-/s und Doppelbezeichnungen ausschließt (vgl. zur Zulässigkeit § 115 Handbuch der Rechtsförmlichkeit). Es gelten daneben die weiteren Anforderungen der DIN 820-2:2012-12 Normungsarbeit - Teil 2: Gestaltung von Dokumenten (ISO/IEC-Direktiven - Teil 2:2011) für die Formulierung technischer Spezifikationen.

Inhaltsverzeichnis

1 Zweck / Geltungsbereich

Diese Anforderungen gelten verbindlich für die Akkreditierung von Prüflaboratoren, Inspektionsstellen und Zertifizierungsstellen, die Konformitätsbewertungstätigkeiten im Bereich der Informationssicherheit/Cyber-Security für industrielle Automatisierungssysteme gemäß IEC 62443, durchführen.

Diese Regel dient der Konkretisierungen bestimmter Anforderungen der Normen DIN EN ISO/IEC 17020, der DIN EN ISO/IEC 17025, der DIN EN ISO/IEC 17065 sowie der DIN EN ISO/IEC 17021-1 in Verbindung mit der ISO/IEC 27006 zum Akkreditierungsverfahren sowie an die Konformitätsbewertungsstellen. Außerdem enthält diese Regel Anforderungen zur Darstellung und Formulierung des Akkreditierungsbereichs von Stellen, die Prüfungen oder Inspektionen durchführen oder von Stellen, die Produkte, Prozesse und Dienstleistungen oder Managementsysteme zertifizieren.

Weitere Anforderungen können in nachgeordneten, sektoralen Regeln festgelegt sein.

Die IEC 62443 kennt drei Objektklassen (siehe Kapitel 3.5): Richtlinien und Verfahrensanweisungen, Industrielle Automatisierungssysteme und Komponenten, die in industriellen Automatisierungssystemen gemäß IEC 62443 verwendet werden sollen. Die einzelnen Teile der IEC 62443 betreffen jeweils unterschiedliche Objektklassen. Die Konformitätsbewertung erfolgt damit gemäß eines bestimmten (klar benannten) Teils der Norm für eine Objektklasse, wobei Schnittstellen und Abhängigkeiten bestehen. Die Zuordnung der Konformitätsbewertungstätigkeiten zu den Teilen der Norm IEC 62443 sowie die betroffenen Kundengruppen der Konformitätsbewertungsstellen kann der Tabelle 1 entnommen werden.

2 Begriffe und Abkürzungen

Akkreditierungsbereich (Scope of accreditation)	Bestimmte Konformitätsbewertungstätigkeiten, für die die Akkreditierung beantragt oder erteilt wurde (DIN EN ISO/IEC 17011:2005-02)
Dienstleistung	Ergebnis aus mindestens einer Tätigkeit, die notwendigerweise an der Schnittstelle zwischen Lieferant und Kunden durchgeführt wird und die im Allgemeinen immateriell ist (DIN EN ISO/IEC 17065:2013)
Geltungsbereich der Zertifizierung	Festlegung: • des/der Produkts(e), des/der Prozesses(e) bzw. der Dienstleistung(en), für die die Zertifizierung gewährt wird; • des zutreffenden Zertifizierungsprogrammes; und

- der Norm(en) und anderer normativer Dokumente (einschl. Zeitpunkt der Veröffentlichung), deren Erfüllung in Bezug auf das/die Produkt(e), den/die Prozess(e), die Dienstleitung(en) beurteilt wurde.
- (DIN EN ISO/IEC 17065:2013)

Produkt

Ergebnis eines Prozesses (DIN EN ISO/IEC 17065:2013,
z.B. Systeme und Teilsysteme, bestimmte Software und Hardware).
Produkt ist auch ein Produkt plus ein Service, der für wesentliche Funktionen zum Einsatz kommt.

Produktanforderung

Anforderung, die sich direkt auf ein Produkt bezieht und die in Normen oder anderen normativen Dokumenten festgelegt ist, die vom Zertifizierungsprogramm benannt sind
(DIN EN ISO/IEC 17065:2013)

Prozess

Satz von in Wechselbeziehung und Wechselwirkung stehenden Tätigkeiten, der Eingaben in Ergebnisse umwandelt
(DIN EN ISO/IEC 17065:2013)
(z.B. bestimmte Fertigungsprozesse)

Validierung

Bestätigung durch Bereitstellung eines objektiven Nachweises, dass die Anforderungen für einen spezifischen beabsichtigten Gebrauch oder eine spezifische beabsichtigte Anwendung erfüllt worden sind
(DIN EN ISO 9000 Abschn. 3.8.5.)

Zertifizierungsprogramm

Zertifizierungssystem, das sich auf bestimmte Produkte, Dienstleistungen, Prozesse bzw. Managementsysteme bezieht, auf welche dieselben festgelegten Anforderungen, spezifischen Regeln und Verfahren angewendet werden

Anmerkung 1:
Aus DIN EN ISO/IEC 17067:2013: Die Regeln, Verfahren sowie die Leitung und Lenkung der Zertifizierung von Produkten, Prozessen und Dienstleistungen werden durch das Zertifizierungsprogramm festgelegt

Anmerkung 2:
Zur Abgrenzung der Begriffe Zertifizierungssystem und -programm - Siehe DIN EN ISO/IEC 17067:2013; Abschn. 6.2

Anmerkung 3:
Unter festgelegten Anforderungen werden Zertifizierungsanforderungen gemäß DIN EN ISO/IEC 17065 Abschnitt 3.7 verstanden

	Anmerkung 4: Konformitätsbewertungsprogramm, das sich auf Managementsysteme bezieht, auf welche dieselben festgelegten Anforderungen, spezifische Regeln und Verfahren angewendet werden (siehe Begriffsdefinition 3.15 der ISO/IEC 17021-1:2015)
Zertifizierungssystem	Regeln, Verfahren und das Management für die Durchführung von Zertifizierungen
Komponente	Definition gemäß IEC 62443-1-2, gegliedert in: • Embedded Device • Host Device • Application Software • Network Device
System	Hard- und Softwarekomponenten eines industriellen Automatisierungssystems
IS	Inspektionsstelle gemäß DIN EN ISO/IEC 17020
PL	Prüflaboratorium gemäß DIN EN ISO/IEC 17025
ZE	Zertifizierungsstelle für Produkte, Prozesse und Dienstleistungen gemäß DIN EN ISO/IEC 17065
ZM	Zertifizierungsstelle für ISMS-Managementsysteme gemäß DIN EN ISO/IEC 17021-1 und ISO/IEC 27006

3 Beschreibung der Anforderungen

Die folgenden Anforderungen dienen zur Sicherstellung der technischen Kompetenz und fachlich fundierten Beurteilung der Konformitätsbewertungsstellen im Bereich der Informationssicherheit/Cyber-Security für industrielle Automatisierungssysteme gemäß IEC 62443. Grundsätzlich kommen die allgemeinen Anforderungen für die KBS aus den relevanten DIN EN ISO/IEC 17000er-Normen zur Anwendung.

3.1 Allgemeine Anforderungen an die Konformitätsbewertungsstellen

3.1.1 Überblick

Die Normenfamilie ist folgendermaßen gegliedert:

General	Policies and procedures	System	Component
IEC 62443-1-1 Terminology, concepts and models	**IEC 62443-2-1** Requirements for an IACS security management system	**IEC 62443-3-1** Security technologies for IACS	**IEC 62443-4-1** Product development requirements
IEC 62443-1-2 Master glossary of terms and abbreviations		**IEC 62443-3-2** Security risk assessment and system design	**IEC 62443-4-2** Technical security requirements for IACS products
IEC 62443-1-3 System security compliance metrics	**IEC 62443-2-3** Patch management in the IACS environment	**IEC 62443-3-3** System security requirements and security levels	
	IEC 62443-2-4 Requirements for IACS solution suppliers		
IEC 62443-1-5 Protection levels			
Definition Metrics	*Requirements placed on security organisation and processes of the plant owner and suppliers*	*Requirements to achieve a secure system*	*Requirements to secure system components*

Die nachfolgende Tabelle ordnet die zertifizierungsrelevanten Normenteile zur Übersicht den jeweiligen Konformitätsbewertungsaktivitäten (PL, IS, ZE, ZM) sowie den jeweiligen primären Rollen gemäß der IEC 62443 zu.

	Konformitäts-bewertungsstelle: (KBS)	PL	IS	ZE	ZM	**Primäre Rolle gemäß IEC 62443:**	Hersteller	System-Integrator[1]	Betreiber
Teil der IEC 62443:									
IEC 62443-2-1					x				x
IEC 62443-2-4				x	x			x	
IEC 62443-3-2			x	x	x			x	x
IEC 62443-3-3			x	x			x[2]	x	x
IEC 62443-4-1			x	x			x		
IEC 62443-4-2		x	x	x			x		

Tabelle 1

[1] *Die Rolle „Service Provider" wird hier unter der Rolle „Integrator" mitbetrachtet. Bedient sich ein Betreiber der dauernden Unterstützung eines „Service Providers", so wird dieser wie ein Systemintegrator betrachtet.*

[2] *Gilt nur für Systeme und nicht für Einzelkomponenten*

Zusätzliche Anmerkungen zur Anwendbarkeit der jeweiligen Teile der Norm IEC 62443:

- 62443-1-1 bis-1-4: Nur informativ
- 62443-2-1: Managementsystem des Betreibers (nach heutigem Stand ISO/IEC 27001)
- 62443-2-2: Leitfaden, nur informativ
- 62443-2-3: Technical Report, nur informativ
- 62443-2-4: System Integrator: SP11
- 62443-3-1: Nur informativ
- 62443-4-2: beinhaltet 62443-4-1, gilt nur für Zertifizierungsstellen (ZE)

Hinweis: Das Patch-Management ist in 62443-4-1 Komponenten enthalten
(Stichwort: Update Management = Patch Management)

3.1.2 Art der Tätigkeiten

Folgende Tabelle gibt eine Übersicht der unterschiedlichen Tätigkeiten für die verschiedenen Konformitätsbewertungsaktivitäten:

Art der Tätigkeit	PL	IS	ZE	ZM
Konzept-prüfung	- Prüfung auf Übereinstimmung mit den Anforderungen eines Standards aus der IEC 62443-Familie, insbesondere und z.B. IEC 62443-4-1 und -4-2.		Bewertung der PL-Ergebnisse und Plausibilisierung des technischen Sicherheits-konzepts	
Hardware-prüfung	- Prüfung der Architektur (Blockschaltbild) - Prüfung auf Informations-sicherheit in Bezug auf Verfügbarkeit, Integrität und Vertraulichkeit - Anwendung gemäß der IEC 62443-4-2	- Untersuchung der Produktentwicklung in Bezug auf die Hardware-entwicklungen und den Schnittstellen zu anderen Phasen des gesicherten Entwicklungslebens zyklus	Bewertung der PL- und IS-Ergebnisse und Plausibilisierung der angewendeten Methoden.	
Software-prüfung	- Prüfung der Architektur auf - Informationssicher-heit in Bezug auf Verfügbarkeit, Integrität und Vertraulichkeit. - Anwendung gemäß der IEC 62443-4-2	- Untersuchung des Lebenszyklus Management in Bezug auf die Software-entwicklung und den Schnittstellen zu anderen Phasen des gesicherten Entwicklungslebens zyklus	Bewertung der PL- und IS-Ergebnisse und Plausibilisierung der angewendeten Methoden.	

Art der Tätigkeit	PL	IS	ZE	ZM
System-Integration	- Prüfung der Verifikation der Integration des Systems	- Untersuchung des Lebenszyklus-management in Bezug auf die Integration und den Schnittstellen zu anderen Phasen des gesicherten Entwicklungslebens zyklus	Bewertung der PL- und IS-Ergebnisse und Plausibilisierung der angewendeten Methoden.	Bewertung der Schnittstellen im Rahmen der Wartung gemäß IEC 62443-2-4
Dokumentierte Information	- Prüfung der dokumentierten Information für den Integrator und Betreiber		Prüfung der dokumentierten Information für den Integrator und Betreiber	
Produktion der Komponenten im Herstellungs-prozess		- Untersuchung der Fertigung durch die Inspektionsstelle. - Prüfung auf Übereinstimmung mit den Anforderungen eines Standards aus der IEC 62443-Familie, insbesondere und z.B. IEC 62443-4-1 und -4-2	Bewertung der PL- und IS-Ergebnisse und Plausibilisierung der angewendeten Methoden.	

Art der Tätigkeit	PL	IS	ZE	ZM
Beurteilung der Informations-sicherheit/ Cyber-Security für industrielle Automati-sierungs-systeme	- auf Nachweise gestützte Untersuchung, um Informations-sicherheit / Cyber-Security für industrielle Automatisierungs-systeme gemäß IEC 62443 zu beurteilen, die durch ein oder mehrere sicherheits-bezogene Systeme und/oder andere risiko-mindernde Maßnahmen erreicht wird. Metriken gemäß IEC/TS 62443-1-3 - Beurteilung des Prozesses beim Integrator (62443-3-1, 62443-3-2)	- auf Nachweise gestützte Untersuchung, um Informations-sicherheit / Cyber-Security für industrielle Automatisierungs-systeme gemäß IEC 62443 zu beurteilen, die durch ein oder mehrere sicherheits-bezogene Systeme und/oder andere risikomindernde Maßnahmen erreicht wird. Metriken gemäß IEC/TS 62443-1-3 - Beurteilung des Prozesses beim Integrator (62443-3-1, 62443-3-2)	Bewertung der PL- und IS-Ergebnisse und Plausibilisierung der angewendeten Methoden. Sollen „Policies & Procedures“ Gegenstand der Zertifizierung sein, wird gemäß IEC 62443-2-x ein von einer gemäß ISO/IEC 17021-1 und ISO/IEC 27006 akkreditierten Stelle zertifiziertes Management verlangt.	Prüfung (Auditierung) des ISMS des Betreibers durch eine gemäß ISO/IEC 17021-1 und ISO/IEC 27006 akkreditierte Stelle, vorläufig gemäß DIN EN ISO/IEC 27001 (perspektivisch gemäß IEC 62443-2-1)

Art der Tätigkeit	PL	IS	ZE	ZM
Audit der Informations-sicherheit / Cyber-Security für industrielle Automati-sierungs-systeme	systematische und unabhängige Untersuchung, die bestimmt, ob die Verfahren zur Festlegung der Anforderungen an die Informations-sicherheit/Cyber-Security für industrielle Automatisierungs-systeme gemäß IEC 62443 mit den geplanten Vereinbarungen übereinstimmen, wirksam durchgeführt wurden und angemessen sind, die spezifizierten Ziele zu erreichen	systematische und unabhängige Untersuchung, die bestimmt, ob die Verfahren zur Festlegung der Anforderungen an die Informations-sicherheit/Cyber-Security für industrielle Automatisierungs-systeme gemäß IEC 62443 mit den geplanten Vereinbarungen übereinstimmen, wirksam durchgeführt wurden und angemessen sind, die spezifizierten Ziele zu erreichen	Bewertung der PL- und IS-Ergebnisse und Plausibilisierung der angewendeten Methoden. Falls „Policies & Procedures“ zertifiziert werden, ist das Management-system gemäß IEC 62443-2-x zu auditieren.	

Tabelle 2

3.1.3 Kompetenzen

Die Konformitätsbewertungsstelle muss die in Tabelle 2 aus Kapitel 3.1.2 notwendigen Kompetenzen nachweisen. Hier sind in Ergänzung zu dieser und zu den allgemeinen Anforderungen an die Kompetenzen (Wissen, Fertigkeiten und Erfahrungen) des Personals der Konformitätsbewertungsstellen (PL/IS/ZE/ZM) die für den Bereich Informationssicherheit/Cyber-Security für industrielle Automatisierungssysteme gemäß IEC 62443 zusätzlich relevanten Anforderungen mit X gelistet.

Nr.	Kompetenzbereich	PL	IS	ZE	ZM
W1	Terminologie, Grundsätze, Praktiken und Techniken der Informationssicherheit/Cyber-Security für industrielle Automatisierungssysteme gemäß IEC 62443	X	X	X	X
W2	Basis Normen/Standards/normative Dokumente der Informationssicherheit/Cyber-Security für industrielle Automatisierungssysteme gemäß IEC 62443	X	X	X	X
W3	Sektor-/Produkt spezifische Normen/Standards/normative Dokumente2)	X	X	X	X
W4	Sektor spezifische Technologie bzw. Erfahrungen	X	X	X	X
W5	Weiterbildungsmaßnahmen bzw. periodische interne Schulungen zur Vermittlung der neuesten Entwicklungen auf dem Gebiet der Funktionalen Sicherheit	X	X	X	X
W6	Bewerten eines PL-/IS-Berichtes für die Informations-sicherheit/Cyber-Security für industrielle Automatisierungs-systeme gemäß IEC 62443			X	X

Tabelle 3

Beispiele für Kompetenznachweise:

- Erfahrung als Assessor bzw. Auditor im Bereich Informationssicherheit/Cyber-Security für industrielle Automatisierungssysteme gemäß IEC 62443
- Berufserfahrung im Entwicklungs- oder Fertigungsbereich
- Erfahrung in Anwendung der Verfahren der ISO/IEC 17020, ISO/IEC 17025, ISO/IEC 17065 und/oder ISO/IEC 17021-1 (bzw. der ISO/IEC 27006).
- Weiterbildungsnachweise (Besuch von Fachseminaren, Konferenzen oder Fachmessen)
- Liste schon durchgeführter Prüfungen bzw. Inspektionen bzw. Zertifizierungen

3.2 Anforderungen an Zertifizierungsstellen im Bereich Informationssicherheit/Cyber-Security für industrielle Automatisierungssysteme gemäß IEC 62443

3.2.1 Allgemeine Anforderungen

Neben der Erfüllung der allgemeinen Anforderungen aus der DIN EN ISO/IEC 17021-1 bzw. der DIN EN ISO/IEC 17065 an eine Zertifizierungsstelle sind vor Allem die Bewertung der PL- und IS-Ergebnisse und Plausibilisierung der angewendeten Methoden zu nennen. Die Bestätigung der Ergebnisse erfolgt durch ein Zertifikat und den entsprechenden Zertifikatsbericht auf der Grundlage eines entsprechenden Zertifizierungsprogrammes. Diese Zertifizierungsprogramme sind gemäß DAkkS-Dokument 71 SD 0 016 zu erstellen.

3.2.2 Anforderungen an die Zertifizierungsstellen für Managementsysteme (ZM) und deren Auditoren

Abschnitt 7.1 der ISO/IEC 27006 definiert die grundlegenden Anforderungen an die Auditoren, welche auch im Rahmen dieser Akkreditierungsanforderungen gelten. Zusätzlich zu den dort genannten Anforderungen müssen alle Auditoren über folgende Kenntnisse verfügen:

- Kenntnis der IEC 62443 und ISO/IEC 27000 Normenreihen
- Rechtliche Rahmenbedingungen und Anforderungen an die Industrie
- Erfahrung in der Anwendung der Standards der IEC 62443 und ISO/IEC 27000 Normenreihen
- Technische Grundlagen von Industrieprotokollen und Industrieanlagen
- Lebens- und Entwicklungszyklus von Hard- und Software
- Grundlagen für den Netzbetrieb, z.B. die Trennung von Operational-IT und Office-Netzen
- IT-Kritische Infrastrukturen für den Netzbetrieb-Scope des ISMS
- Grundkenntnisse der Anforderungen an ein Managementsystem gemäß IEC 61508
- Branchenspezifische Grundlagen

Ferner müssen regelmäßige Weiterbildungsnachweise in Bezug auf die vorgenannten Kenntnisse vorgelegt werden.

3.2.3 Anforderungen an die Zertifizierungsstellen für Produkte, Prozesse und Dienstleistungen (ZE) und deren Auditoren

Die Anforderungen gemäß Abschnitt 6 der ISO/IEC 17065 an das Personal sowie zusätzlich des Abschnitts 7 der ISO/IEC 17021-1 an die Auditoren (wenn das Managementsystem in die Betrachtung des zu zertifizierenden Prozesses einbezogen wird) gelten auch im Rahmen dieser Akkreditierungsanforderungen. Zusätzlich zu den dort genannten Anforderungen müssen alle Auditoren über folgende Kenntnisse verfügen:

- Kenntnis der IEC 62443 Normenreihe
- Grundkenntnisse der ISO/IEC 27000 Normenreihe
- Rechtliche Rahmenbedingungen und Anforderungen an die Industrie
- Erfahrung in der Anwendung der Standards der IEC 62443 und ISO/IEC 27000 Normenreihen
- Technische Grundlagen von Industrieprotokollen und Industrieanlagen
- Lebens- und Entwicklungszyklus von Hard- und Software
- Grundlagen für den Netzbetrieb, z.B. die Trennung von Operational-IT und Office-Netzen
- IT-Kritische Infrastrukturen für den Netzbetrieb-Scope des ISMS
- Grundkenntnisse der Anforderungen an ein Managementsystem gemäß IEC 61508
- Branchenspezifische Grundlagen

Ferner müssen regelmäßige Weiterbildungsnachweise in Bezug auf die vorgenannten Kenntnisse vorgelegt werden.

Anmerkung:

Industrieanlagen sind sehr heterogen. Daher muss die Zertifizierungsstelle Zugriff auf Fachexperten haben, die den Auditor bei Bedarf beim konkreten Audit unterstützen.

3.3 Anforderungen an Inspektionsstellen und deren Inspektoren im Bereich Informationssicherheit/Cyber-Security für industrielle Automatisierungssysteme gemäß IEC 62443

Es sind die allgemeinen Anforderungen aus der DIN EN ISO/IEC 17020 an eine Inspektionsstelle zu erfüllen. Im Fokus von „IT-Sicherheit für industrielle Automatisierungssysteme gemäß IEC 62443“-Inspektionen zu Systemen, Teil-Systemen oder Komponenten steht die Informationssicherheit, d.h. an die Kompetenz der Inspektoren werden die für diesen Bereich notwendigen Anforderungen gemäß Tabelle 3 gestellt.

Anmerkung:

Eine Inspektion im Bereich „IT-Sicherheit für industrielle Automatisierungssysteme gemäß IEC 62443“ unterscheidet sich von anderen Inspektionen im Bereich der Automatisierungstechnik. Inspektionsparameter sind unter anderem Fragen zur Quantität, Qualität, Sicherheit, Zweckmäßigkeit sowie fortdauernden Einhaltung der Sicherheit von in Betrieb befindlichen Anlagen oder Systemen.

Für „Informationssicherheit/Cyber-Security für industrielle Automatisierungssysteme gemäß IEC 62443 “-Inspektionen sind die relevanten Dokumente vom Hersteller oder dessen Beauftragten einzureichen.

3.4 Anforderungen an Prüflaboratorien im Bereich Informationssicherheit/Cyber-Security für industrielle Automatisierungssysteme gemäß IEC 62443

3.4.1 Allgemeine Anforderungen

Es sind die allgemeinen Anforderungen aus der DIN EN ISO/IEC 17025 an ein Prüflaboratorium zu erfüllen.

3.4.2 Anforderungen an Prüfungen

Die Prüfungen im Bereich der Informationssicherheit/Cyber-Security für industrielle Automatisierungssysteme gemäß IEC 62443 werden durch die Analyse folgender Aspekte (sofern anwendbar) durchgeführt:

a) Gefahren- bzw. Risikobeurteilung
b) Sicherheitsanforderungen
c) Systematische Integrität
d) Konstruktion, Design, Architektur (Hard-, Software)
e) Überprüfung vorhandener Kenngrößen (z.B. Security-Level) mit den entsprechenden Grenzwerten, die Standards zur Informationssicherheit/Cyber-Security für industrielle Automatisierungssysteme gemäß IEC 62443 empfehlen.
f) Überprüfung der Produkteigenschaften in Bezug auf Informationssicherheit.
g) Im Falle von Anlagen und Systemen (Hardware und Software) wird die korrekte Installation in einer Vor-Ort Begutachtung überprüft.

Anmerkung:

Eine Prüfung im Bereich Informationssicherheit/Cyber-Security für industrielle Automatisierungssysteme gemäß IEC 62443 gibt es in zwei Kategorien:

1. Eine Produktprüfung im klassischen Sinne, wenn es sich um die Prüfung einer Komponente gemäß IEC 62443 handelt. Produktprüfungen erfordern ein Testsystem bzw. Geräte, zum Messen oder Auswerten von Ergebniswerten. Dabei werden Ergebniswerte mit in einem Standard vorgegebenen oder vorher festgelegten Zielwerten verglichen. Als Prüfverfahren werden in den meisten Fällen in Standards vorgeschriebene Verfahren verwendet.
   Für derartige Prüfungen werden Dokumente bzw. Muster üblicherweise vom Hersteller oder dessen Beauftragten eingereicht.
2. Eine Produktprüfung von der Anlage vor Inbetriebnahme oder bei Änderungen, um die Widerstandsfähigkeit gegen Cyberangriffe (Resilienz) zu prüfen (z.B. Penetrations-Tests, Schwachstellen-Tests).

3.4.3 Anforderungen an Mitarbeiter und Penetrations-Tester von Prüflaboratorien

Die Mitarbeiter und Penetration-Tester von Prüflaboratorien müssen über folgende Kenntnisse verfügen:

- Systemadministration
- Netzwerkprotokolle
- Programmiersprachen
- IT-Sicherheitsprodukte (IT-Sicherheitsgateways, Intrusion-Detection-Systeme, etc.)
- Anwendungssysteme
- Netzkomponenten
- Kenntnis der IEC 62443-Normenserie und eingebettete Geräte (embedded devices) sowie dazugehörige Anwendungen
- Erfahrung in der Durchführung von Penetrations-Tests im industriellen Umfeld
- Beurteilung des zum Produkt vorgelegten Risiko-Assessments in Bezug auf den Security-Level
- Erweitertes technisches Wissen im Umgang und Konfiguration/Management von Industrieprotokollen/Komponenten im Zusammenhang mit Industrieanlagen
- Lebens- und Entwicklungszyklus von Hard- und Software
- Besonderheiten bei Echtzeitanforderung

Ferner müssen regelmäßige Weiterbildungsnachweise in Bezug auf die vorgenannten Kenntnisse vorgelegt werden.

3.5 Einsatz von Prüfungen (PL), Inspektionen (IS) und Zertifizierungen (ZE, ZM) in drei Objektklassen

Die Prüfungen und Inspektionen betreffen die IT-Sicherheit der folgenden drei Objektklassen.
Bei Zertifizierungen ist zwischen Zertifizierung gemäß ISO/IEC 17065 (ZE) und ISO/IEC 17021-1 mit ISO/IEC 27006 (ZM) zu unterscheiden.

3.5.1 Objektklasse 1: Richtlinien und Verfahrensanweisungen

Die Norm IEC 62443-2-1 spezifiziert die Anforderungen an die organisatorischen Maßnahmen zum sicheren Betrieb einer Automatisierungslösung: ZM

Anstatt der Norm IEC 62443-2-1 kann alternativ DIN EN ISO/IEC 27001 zum Einsatz kommen.
Mögliche Konformitätsbewertung: ZM

Installation, Maintenance und Patch Management: IEC 62443-2-3 und -2-4

Die Norm IEC 62443-2-4 richtet sich an Anbieter für Integrations- und Wartungsleistungen: Prozesse, Praktiken und Personal.
Mögliche Konformitätsbewertung: ZE

Die Norm IEC 62443-2-3 ist ein Technical Report* mit Empfehlungen zum Lebenszyklus-Management von Security-Patches im IACS-Umfeld. Sie betrifft damit den Hersteller und den Betreiber.
Mögliche Konformitätsbewertung beim Hersteller: ZE

Konformitätsbewertung beim Betreiber: Ist Bestandteil von ZM. Wird z.B. auf Basis der DIN EN ISO/IEC 27001 zertifiziert, dann muss die Zertifizierungs-Auditierung um die Anforderungen der IEC 62443-2-4 erweitert werden.

* *Ein entsprechendes Konformitätsbewertungsprogramm (siehe auch DAkkS-Dokument 71 SD 0 16) ist dafür zu schreiben.*

3.5.2 Objektklasse 2: Industrielle Automatisierungssysteme gemäß IEC 62443

Es geht um die Konformitätsbewertung derjenigen funktionalen Fähigkeiten der Automatisierungs-systeme, welche die Informationssicherheit/Cyber-Security für industrielle Automatisierungssysteme gemäß IEC 62443 bestimmen:

IEC 62443-3-1, -3-2, -3-3
Mögliche Konformitätsbewertungen: IS, PL (z.B. Penetrations-Tests), ZE
Bewertung der PL- und IS-Ergebnisse und Plausibilisierung der angewendeten Methoden sind Grundlage für ZE.

Konformitätsbewertungen sind in Bezug auf Erreichte Security Levels gemäß IEC 62443 (SL-A) (SL 1 bis SL 4) und/oder auf Protection Levels (PL 1 - PL 4) auszustellen.

3.5.3 Objektklasse 3: Komponenten, die in industriellen Automatisierungssystemen gemäß IEC 62443 verbaut werden sollen

Unterklassen von Komponenten:

- Steuerungen (Embedded Devices)
- Host Geräte (auf PC Basis)
- Netzwerkkomponenten (Firewalls, Switches, etc.)
- Software (Anwendungen)

Produktentwicklungsprozess gemäß IEC 62443-4-1
Mögliche Konformitätsbewertung: IS, ZE

Technische Anforderungen IEC 62443-4-2
Mögliche Konformitätsbewertung: PL, IS, ZE

Bewertung der PL- und IS-Ergebnisse und Plausibilisierung der angewendeten Methoden sind Grundlage für ZE.

Anmerkung 1:

Notwendige Dokumente zum Prüfen können, z.B. für Hardware, sein:

Schaltpläne, Chipdesign, HW-Architekturen, Analyseergebnisse von Hardware-Angriffen und anderes.

Anmerkung 2:

Notwendige Dokumente zum Prüfen können, z.B. für Software, sein:

Softwareanforderungen, Dokumentation der verwendeten Testmethoden, Validierungs- und Verifikationsunterlagen, Toolqualifikationen, Systemanalysen, Security-Analyse (z.B. Threat-Modell), Tests zu Softwareangriffen, Leistungstests und anderes.

Konformitätsbewertungen sind auf erreichbare Security Levels (SL) auszustellen.

3.6 Anforderungen an die Beschreibung des Geltungsbereiches der Akkreditierung im Bereich der Informationssicherheit/Cyber-Security für industrielle Automatisierungssysteme gemäß IEC 62443

Grundsätzlich sind folgende Angaben bei der Beschreibung des Geltungsbereiches der Akkreditierung einer Konformitätsbewertungsstelle im Bereich der IT-Sicherheit für industrielle Informations-sicherheit / Cyber-Security für industrielle Automatisierungssysteme gemäß der in Tabelle 1 dargestellten Zuordnung der jeweiligen Normenteile der IEC 62443 zu den möglichen Konformitäts-bewertungstätigkeiten (PL, IS, ZE und ZM) zu machen:

3.6.1 Geltungsbereiche von Zertifizierungsstellen für Managementsysteme

Zertifizierungen nach (teilweise) nicht normativ festgelegten Zertifizierungsprogrammen (eigenentwickelte Zertifizierungsprogramme nach messbaren Kriterien entsprechend dem Stand der Technik; gesetzlich geregelter und gesetzlich nicht geregelter Bereich)

1) Angewendete Zertifizierungssysteme mit Ausgabestand;
2) Angewendete Zertifizierungsprogramme, ggf. Teilprogramme mit Ausgabestand;
3) Rolle(n) und Objektklasse(n), für die Zertifizierungen angeboten werden;
4) Produkte oder Produktgruppen.

3.6.2 Geltungsbereiche von Zertifizierungsstellen von Produkten, Prozessen und Dienstleistungen

- Zertifizierungen nach in europäischen und/oder nationalen Richtlinien/Verordnungen/Gesetzen festgelegten Programmen (gesetzlich geregelter Bereich)
  Festlegungen für die Anwendung der DIN EN ISO/IEC 17065 bei der Akkreditierung von Stellen, die Produkte, Prozesse und Dienstleistungen zertifizieren 71 SD 0 013 | Revision: 1.1 | 04. Dezember 2014
- Zertifizierungen nach vollständig normativ festgelegten Zertifizierungsprogrammen (vorwiegend im gesetzlich nicht geregelten Bereich)
- Zertifizierungen nach (teilweise) nicht normativ festgelegten Zertifizierungsprogrammen (Eigenentwickelte Zertifizierungsprogramme nach messbaren Kriterien entsprechend dem Stand der Technik; gesetzlich geregelter und gesetzlich nicht geregelter Bereich)
  1) Angewendete Zertifizierungssysteme mit Ausgabestand;
  2) Angewendete Zertifizierungsprogramme, ggf. Teilprogramme mit Ausgabestand;
  3) Rolle(n) und Objektklasse(n), für die Zertifizierungen durchgeführt werden;
  4) Produkte oder Produktgruppen.

In Abhängigkeit von der Ausgestaltung des jeweiligen Programmes kann es erforderlich sein, die Angabe von Produkten und/oder Produktgruppen und/oder Produktanforderungen zur eindeutigen Festlegung des Geltungsbereiches mit aufzunehmen. Dies ist insbesondere dann erforderlich, wenn diese Angaben aus der Bezeichnung der Zertifizierungsprogramme nicht eindeutig hervorgehen.

Die detaillierte Auflistung von Produktnormen, die im Rahmen der akkreditierten Zertifizierungsprogramme relevant sind, ist in der Urkunde/Urkundenanlage in der Regel nicht vorgesehen.

Die Auflistung von Prüfnormen, die zum Nachweis der Erfüllung einzelner Produktanforderungen angewandt werden, ist in der Urkunde/Urkundenanlage nicht vorgesehen.

3.6.3 Geltungsbereiche von Inspektionsstellen

Inspektionen nach (teilweise) nicht normativ festgelegten Inspektionsprogrammen (Eigenentwickelte Inspektionsprogramme nach messbaren Kriterien entsprechend dem Stand der Technik; gesetzlich geregelter und gesetzlich nicht geregelter Bereich)

1) Angewendete Inspektionsprogramme, ggf. Teilprogramme mit Ausgabestand;
2) Rolle(n) und Objektklasse(n), für die Zertifizierungen durchgeführt werden;
3) Produkte oder Produktgruppen.

3.6.4 Geltungsbereiche von Prüflaboratorien

Für die Darstellung des Geltungsbereiches gibt es keine Informationssicherheit/Cyber-Security für industrielle Automatisierungssysteme gemäß IEC 62443 spezifischen Besonderheiten. Die Darstellung erfolgt gemäß der für die Prüflaboratorien im Fachbereich "Informationstechnik-Informations-sicherheit-Datenschutz" der DAkkS üblichen Weise.

4 Mitgeltende Unterlagen

DAkkS-Dokument 71 SD 0 012	Festlegungen für die Anwendung der DIN EN ISO/IEC 17020:2012 bei der Akkreditierung von Inspektionsstellen;
DAkkS-Dokument 71 SD 0 013	Festlegungen für die Anwendung der DIN EN ISO/IEC 17065 bei der Akkreditierung von Stellen, die Produkte, Prozesse und Dienstleistungen zertifizieren;
DAkkS-Dokument 71 SD 0 016	Aufnahme neuer Akkreditierungsaktivitäten und Konformitätsbewertungsprogramme.