TeleTrusT – Bundesverband IT-Sicherheit e.V.
Der IT-Sicherheitsverband.

TeleTrusT-Prüfschema nach IEC 62443-4-2

Industrielle Kommunikationsnetze - IT-Sicherheit für industrielle Automatisierungssysteme

2018-09

TeleTrusT-AG "Smart Grids / Industrial Security"

Federführung und Ansprechpartner für Rückfragen:

Sebastian Fritsch, secuvera GmbH

Tobias Glemser, secuvera GmbH
Steffen Heyde, secunet Security Networks AG
Dr. Holger Mühlbauer, TeleTrusT - Bundesverband IT-Sicherheit e.V.

Impressum

Herausgeber:

TeleTrusT - Bundesverband IT-Sicherheit e.V.
Chausseestraße 17
10115 Berlin
Tel.: +49 30 4005 4306
Fax: +49 30 4005 4311
E-Mail: info@teletrust.de
https://www.teletrust.de

© 2018 TeleTrusT

TeleTrusT-Prüfschema nach IEC 62443-4-2

2018-09

Industrielle Kommunikationsnetze - IT-Sicherheit für industrielle Automatisierungssysteme

Security for industrial automation and control systems

[DIN EN 62443-4-2:2017 "Industrielle Kommunikationsnetze - IT-Sicherheit für industrielle Automatisierungssysteme - Teil 4-2: Anforderungen an Komponenten industrieller Automatisierungssysteme" (IEC 65/663/CDV:2017); Deutsche Fassung prEN 62443-4-2:2017]

Inhaltsverzeichnis

Inhalt

1 Einführung

1.1 Zielsetzung und Anwendungsbereich

Die noch "junge" und zum Teil noch in Arbeit befindliche Norm IEC 62443 hat das Ziel, Cybersicherheit im industriellen Umfeld (primär der Automatisierungstechnik) ganzheitlich zu betrachten. Es werden die drei Ebenen (Betreiber, Integrator und Komponentenhersteller) betrachtet.

Der in diesem Prüfschema fokussierte Normteil IEC 62443-4-2 (Norm-Entwurf DIN EN 62443-4-2; VDE 0802-4-2:2017-10) adressiert die Ebene des Komponentenherstellers. Das Konzept der IEC 62443-4-Ebene in der Norm adressiert die Sicherheit in Komponenten zum einen mit Anforderungen an einen sicheren Entwicklungsprozess, dies erfolgt im Normteil IEC 62443-4-1, sowie mit technischen Sicherheitseigenschaften (oder Fähigkeiten), welche von industriellen Komponenten gefordert werden können (IEC 62443-4-2). Die Anforderungen an technische Sicherheitseigenschaften von ganzen industriellen Systemen (Anlagen) wird im Normteil IEC 62443-3-3 behandelt.

Die Norm IEC 62443 enthält über ihre Teile Vorgehensmodelle und Anforderungen, um sichere industrielle Anlagen zu erstellen und zu betreiben. Es werden allerdings keine Anforderungen formuliert, wie eine dritte Partei die korrekte und effektive Umsetzung der Norm prüfen kann. Dies ist allerdings insbesondere im Kontext von Zertifizierung relevant, da von Anwendern hinter Zertifikaten vergleichbare Bewertungsergebnisse erwartet werden.

Das vorliegende Dokument "Prüfschema nach IEC 62443-4-2" ist ein Vorschlag für eine Vorgehensweise zur Prüfung oder Evaluierung, ob die Anforderungen der IEC 62443-4-2 eingehalten wurden.

Das Prüfschema begrenzt sich auf die Perspektive der technischen Fähigkeiten einer Komponente und nimmt nicht den Entwicklungsprozess der Komponenten (entsprechend IEC 62443-4-1) in den Fokus. Hierzu müssen zukünftig noch eigene Prüfschemen entwickelt werden.

Das Prüfschema geht davon aus, dass die Entwicklung einer Komponente nach den Prozessen der IEC 62443-4-1 erfolgt ist, d.h. es liegen Ergebnisse (Deliverables) des Entwicklungsprozesses vor, welche im Rahmen der Prüfung der Komponente herangezogen werden können. Jegliche Bezüge in diesem Prüfschema beziehen sich auf diese Deliverables und nicht den Entwicklungsprozess an sich.

Das Prüfschema stellt auch kein Zertifizierungsschema dar. Zertifizierungsrelevante Aspekte wie die Definition beteiligter Rollen, Verfahren zur Beantragung, Abnahme und Überwachung von zertifizierten Produkten und weitere müssen hierauf aufbauend von Schemabetreibern oder Zertifizierungsstellen definiert werden.

Das Prüfschema kann flexibel für Zertifizierungen nur nach IEC 62443-4-2 genutzt werden, oder auch für kombinierte Zertifizierungen nach IEC 62443-4-1 und IEC 62443-4-2. Das vorliegende Prüfschema bezieht keine Position, ob einfache oder kombinierte Zertifizierungen zu bevorzugen sind.

Dieses Prüfschema kann aber neben der Zertifizierungen auch für andere Zwecke eingesetzt werden. Es kann als internes oder externes Vorgehensmodell zur sicherheitstechnischen Beurteilung von industriellen Komponenten genutzt werden, siehe Kapitel 4.1.3. In diesen Fällen sollten ziel- und risikoorientierte Adaptionen durchgeführt werden.

Ziel der Aussage einer Prüfung nach diesem Schema ist, die korrekte und robuste Implementierung der Anforderungen der IEC 62443-4-2, bezogen auf eine konkrete Komponente, zu bestätigen oder Mängel zu benennen. Zudem soll die Prüfung eine Aussage dazu machen, ob die Komponente resistent entsprechend dem Niveau des definierten Angreifers (entsprechend Security Level, siehe Kapitel 1.3) ist oder ob die Komponente nicht ausreichend resistent zu dem erwarteten Niveau ist.

1.2 Übersicht zum Normteil IEC 62443-4-2

Industrielle Komponenten nach IEC 62442-4-2 werden in vier Gerätetypen eingeteilt:

- Embedded Devices
  BEISPIELE PLC, Sensoren, SIS (Safety Instrumented Systems) Controller, DCS (Distributed Control System) Controller
- Host Devices

BEISPIELE Notebooks, PC, Workstations
- Network Devices
  BEISPIEL Industrial Router
- Applications
  BEISPIELE Konfigurations-Software, Historisierungssoftware

In der Regel werden durch den Normteil COTS (Commercial off-the-shelf) Produkte adressiert, die einem größeren Anwenderkreis zur Verfügung gestellt werden. Der Normteil kann aber auch aus Sicht eines Systemherstellers/Integrators genutzt werden, der für die Mitigation von Risiken einer in Planung befindlichen Anlage eine spezifische Komponente entwickeln lassen will, die ausgewählte Sicherheitsfunktionaltäten beinhalten soll.

Der Normteil sortiert die Einzelanforderungen in sogenannte Foundational Requirements (FR), die als Themenkategorisierung gelesen werden können. Darunter befinden sich die Component Requirements (CR), welche die technische Detailanforderungsebene darstellt.

Der Normteil IEC 62443-4-2 ist zum aktuellen Zeitpunkt noch nicht final veröffentlicht. Es liegt allerdings mittlerweile eine Fassung mit hohem Reifegrad innerhalb der Standardisierungsgremien vor, siehe Dokument [IEC62443-4-2]. Es wird erwartet, dass die Veröffentlichung ohne größere Veränderungen zum aktuellen Entwurfsstand bis Anfang 2019 erfolgen wird.

1.3 Nutzung des Normteils

Aus der Definition des Normteils sowie der gesamten IEC 62443 lassen sich zwei Einstiege in die Prüfung nach IEC 62443-4-2 ableiten:

1. Auswahl einer SL-Stufe mit verbundenen Anforderungen (CR) und Resistenz-Stufe
2. Gezielte Auswahl von Anforderungen (CR) sowie definierter Resistenz-Stufe.

Das erste Modell geht von der Perspektive eines Komponenten-Herstellers aus, der für verschiedene Einsatzvarianten seiner Produkte eine Bestätigung seiner Sicherheitseigenschaften erhalten möchte. Ein Hersteller definiert hierzu über die SL-Stufe das Zielniveau seiner Sicherheitseigenschaften, dies leitet sich wiederum u.a. aus der Analyse einer üblichen Einsatzumgebung seiner Komponente oder Befragung seiner Kunden ab.

Das zweite Modell geht von der Perspektive der Anlagenplanung aus. Hierzu wird eine Risikoanalyse nach dem Vorgehensmodell aus dem Normteil IEC 62443-3-2 durchgeführt und auf Basis der ermittelten Risiken ein Systemdesign durchgeführt. Um die identifizierten Risiken zu mitigieren, können entsprechend notwendige Anforderungen an die Komponenten abgeleitet werden. Diese Menge an Anforderungen kann gezielt über eine Auswahl von Anforderungen (CR) definiert werden.

Unabhängig von den beiden Vorgehensmodellen muss ein Komponentenhersteller bei der Entwicklung seiner Komponente Vorgaben in seinem Entwicklungsprozess einhalten. Ein wichtiges Ergebnis dieser Prozesse ist u.a. die Definition des Verwendungszwecks oder Kontexts der Komponente. Diese und weitere Angaben geben einem Anwender sowie Prüfer wichtige Informationen, über das zu erwartende Verhalten der Komponente.

Der Begriff der "SL-Stufe", konkret SL-C für SL Capability, nach IEC 62443-4-2 definiert sich über zwei Anteile. Zum einen über die Auswahl von Anforderungen (CR) und zum anderen über einen definierten Angreifer Typ. Im Rahmen des Normteils IEC 62443-4-2 wurde versucht dies allgemeingültig, sinnvoll miteinander abzugleichen. Bei der Risikoanalyse einer gesamten Anlage bzw. Systems kann jedoch herauskommen, dass sowohl die Auswahl der Anforderungen als auch die Definition des Angreifer Typs angepasst werden muss. Komponentenhersteller haben allerdings oft das Problem, dass die genauen Einsatzszenarien der Anlagen ihrer Kunden nicht bekannt sind oder sich deutlich unterscheiden. Für Komponentenhersteller ist es daher sinnvoll und effektiv, auf die vordefinierten SL-Stufen zurückzugreifen, da das Vorgehen damit vereinfacht wird.

Aus Sicht der Angriffsresistenz definiert die SL-Stufe folgende abstrakte Angriffstypen:

Stufe	Originaltext	Angriffstyp
SL-Stufe 1	Prevent the unauthorized disclosure of information via eavesdropping	nicht gezielter Angriff
SL-Stufe 2	Prevent the unauthorized disclosure of information to an entity actively searching for it using simple means with low resources, generic skills and low motivation.	aktiver, gerichteter Angriff, einfache Mittel, allgemeines IT-Wissen, geringe Motivation
SL-Stufe 3	Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with moderate resources, IACS specific skills and moderate motivation.	aktiver, gerichteter Angriff, erweiterte Werkzeuge und Ressourcen (Zeit, Geld), industrie-spezifisches Wissen, mittlere Motivation
SL-Stufe 4	Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with extended resources, IACS specific skills and high motivation.	aktiver, gerichteter Angriff, umfangreiche Werkzeuge und Ressourcen (Zeit, Geld), industrie-spezifisches Wissen, hohe Motivation.

Tabelle 1

1.4 Abgrenzung zu SL-Stufen

Dieses Prüfschema orientiert sich ausschließlich an den Anforderungen der Stufen SL-2 und SL-3. Die Stufen SL-1 und SL-4 werden aktuell nicht betrachtet. Dies begründet sich daraus, dass hiermit zunächst Prüfungen im mittleren Vertrauenswürdigkeitsbereich (medium/substantial assurance) adressiert werden sollen, um zunächst Erfahrungen im Umgang mit der Norm zu sammeln.

Die Stufe SL-4 legt einen Angreifer mit hohem Potential, hoher Motivation und hohen Ressourcen zugrunde, aktuell wird empfohlen hierzu spezifische Sicherheitskonzepte zu entwickeln, z. B. auf Basis des Normteil IEC 62443-3-2.

Die SL-1 wird dagegen als zu gering betrachtet, um die erste zu erreichende Stufe für eine Prüfung zu sein. Für einzelne Komponenten mag dies eine sinnvoll anzunehmende Menge an Sicherheitsfunktionalität sein, ein spezielles oder vereinfachtes Prüfvorgehen wird allerdings nicht als sinnvoll erachtet. In diesen Fällen kann das Vorgehensmodell für SL-2 genutzt werden.

Eine Erweiterung dieses Prüfschemas auf SL-1 bzw SL-4 im Rahmen einer Fortschreibung ist zukünftig möglich.

1.5 Adressaten

Die primären Adressaten dieses Prüfschemas sind Zertifizierungsschemen, Akkreditierer, Prüfer, Prüfstellen und interne QS-/IT-Prüfabteilungen. Desweiteren richtet sich das Dokument an Komponentenhersteller, welche sich auf eine Prüfung Ihrer Produkte vorbereiten wollen, also Entwicklungsabteilungen.

1.6 Normative Terminologie

Im folgenden Text werden die Schlüsselworte MUSS, SOLLTE, KANN und DARF entsprechend der normativen Bedeutung genutzt und werden jeweils in Großbuchstaben dargestellt. Dabei bedeutet MUSS eine strikte Anforderung, SOLLTE eine Empfehlung, KANN eine Möglichkeit und DARF eine Erlaubnis für eine mögliche Verwendung.

1.7 Definitionen

Begriff	Definition
Akzeptanzkritierien (acceptance criteria)	Kriterien für den Prüfer zur Beurteilung, ob eine vorgefundene Implementierung im Sinne der Anforderung akzeptiert umgesetzt wurde
Angriffsresistenz	Fähigkeit eines Systems oder Komponente bei einem Angriff gegenüber dieser (vgl. SL-Stufe) resistent zu bleiben
Resistenz-Stufe	Kategorien zur Beschreibung einer erwarteten Angriffsresistenz aus Perspektive des Angriffs-potentials (Definition der SL-Stufen)
Robustheit	Aufrechthaltung der korrekten Funktionalität im Fall von ungültigen Eingaben oder ungünstigen Umgebungsbedingungen, z. B. Sonderzeichen in an sich regulären Benutzereingaben

Tabelle 2

2 Prüfkonzept

2.1 Generelles Konzept

Die Prüfung des Normteils IEC 62443-4-2 MUSS entlang folgender Prüfschritte erfolgen:

1. Prüfung des Verwendungszwecks
2. Dokumentation (Design/Prüfung)
3. Dokumentation (Anwender)
4. Konformitätsprüfung
5. Schwachstellenanalyse

Der erste Prüfschritt leitet sich aus zwei Punkten ab. Zum einen wird normativ gefordert, dass die Entwicklung von Komponenten basierend auf den Prozessen des Normteil IEC 62443-4-1 entwickelt wurde. Hierzu MUSS ein Security Kontext und die Erstellung eines Bedrohungsmodells erfolgen. Zum anderen bedingen die zum Teil abstrakten Beschreibungen der Anforderungen der IEC 62443-4-2, dass eine Berücksichtigung der Komponenten-spezifische Rahmenparameter berücksichtigt werden MUSS, um eine Evaluation durchführen zu können. Hierzu MUSS der Verwendungszweck des Produkts beschrieben werden.

Um eine Komponente auf sicherheitstechnische Eigenschaften prüfen zu können, werden je nach Konzept und Tiefe der Prüfung Details über die Komponente vom Hersteller benötigt. In etablierten IT-Produkt-Evaluierungsstandards ist es üblich, dass eine zunehmende Resistenz unter anderem durch eine tiefere Prüfung und damit zunehmende Vertrauenswürdigkeit (Assurance) unterstützt wird. Dieses Prinzip wird in diesem Prüfkonzept ebenfalls so angewandt, dass bei höherer SL-Stufe der Hersteller detailliertere Entwickler- oder Design-Dokumente vorlegen MUSS.

Im folgenden Prüfschritt MUSS die Anwender-Dokumentation untersucht werden, ob diese vollständig und korrekt ist. Die mindestens zu beschreibenden Themen ergeben sich aus den Prozessen der IEC 62443-4-1, eine Übersicht findet sich in Kapitel 2.4 in diesem Dokument.

Der nächste, deutlich umfangreichere Prüfschritt ist die Prüfung auf konforme Implementierung der definierten Anforderungen, z. B. definiert über die SL-Stufe. Für die Evaluation durch den Prüfer werden hierzu Akzeptanzkriterien definiert. Ein Nachweis über die Einhaltung einzelner Kriterien MUSS über einen oder mehrere Tests stattfinden.

Der folgende, ebenfalls umfangreiche Prüfschritt ist die Durchführung einer Schwachstellenanalyse zur Feststellung, ob die erwartete Angriffsresistenz eingehalten wurde. In diesem Prüfschritt MUSS der Bezug zum angenommenen Angriffspotential hergestellt werden, welches ebenfalls durch die gewählte SL-Stufe definiert wird. Sollten die Anforderungen nicht durch die SL-Stufe definiert worden sein, MUSS ein entsprechender Angreifertyp explizit angenommen werden.

Der Prüfgegenstand selbst, d.h. die Komponente, SOLLTE in mindestens zweifacher Ausführung zur Prüfung übergeben werden. Die Komponente MUSS dabei einem normalen Serienmodell entsprechen. Sofern noch in Entwicklung befindlich, MUSS sichergestellt sein, dass die geprüften Eigenschaften denen im späteren Serienmodell entsprechen.

Die zuvor benannten Punkte definieren den Umfang der durch den Hersteller zu übergebenden Informationen für die Prüfung nach IEC 62443-4-2. Nachfolgend werden die einzelnen Angaben noch einmal detailliert innerhalb der jeweiligen Prüfschritte beschrieben.

2.2 Prüfung des Verwendungszwecks

Der Verwendungszweck des Produkts definiert betriebliche und sicherheitstechnische Rahmenparameter einer Komponente. Diese KÖNNEN beispielsweise als Annahmen an die Einsatzumgebung beschrieben werden. Ein Format für diese Beschreibung ist nicht in der IEC 62443 definiert. Die zugehörigen Inhalte werden für eine effektive Prüfung allerdings benötigt.

Indirekt lassen sich die Inhalte aus den Prozessen der IEC 62443-4-1 herauslesen. Es MUSS die Definition eines Security Kontexts (SR-1) und die Erstellung eines Bedrohungsmodells (SR-2) für die Komponente erfolgen.

Aus Sicht dieses Prüfschema SOLLTEN die Informationen als beschriebenes Ergebnis (Dokument) Eingabe in die Prüfung finden. In Anhang A dieses Dokuments wird eine Komponentenspezifikation angegeben, welche genutzt werden SOLLTE, um alle notwendigen Informationen zusammenzustellen. Die Komponentenspezifikation KANN als Gliederung für ein Dokument genutzt werden, oder als Checkliste für referenzierte Dokumente.

Der Prüfer MUSS die bereitgestellten Informationen nach Vollständigkeit und Korrektheit analysieren.

2.3 Dokumentation (Design/Prüfung)

Etablierte Prüfstandards nutzen als Konzept eine stufenweise Steigerung der Vertrauenswürdigkeit (Assurance). Zusätzlich wird ein direkter Bezug zwischen der Vertrauenswürdigkeit und der Resistenz gegenüber Schwachstellen hergestellt. Die zugrundeliegende Überlegung ist, dass eine gegenüber den Prüfern weitgehende Transparenz bei den technischen Details zu einer effektiven Möglichkeit zur Bewertung des Komponenten-Designs führt. Damit werden zudem in diesem Analyseschritt ermöglicht grundsätzliche Design-Schwächen aufzudecken.

In diesem Prüfschema wird dieses Konzept aufgegriffen und den betrachteten Stufen SL-2 und SL-3 die folgende geforderte Design-Dokumentation zugeordnet.

SL-Stufe / Angreifertyp	**Geforderte Design-Dokumentation**	**Kommentar**
SL-1 / nicht gezielt	nicht definiert	nicht relevant für Prüfschema in dieser Version
SL-2 / gering	Schnittstellenbeschreibung, u.a.: alle kabelgebundenen und funkbasierten Kommunikationsschnittstellen sowie elektrische Schnittstellen mit Beschreibung der Funktionalität und Konfigurationsmöglichkeiten, z. B. eine Schnittstelle zur Gerätekonfiguration mit technischer Beschreibung des Protokolls und aller Konfigurationsparameter, zusätzlich detaillierte Informationen zu eingesetzter Software mit 3rd-Party-Libraries und exakter Version	

SL-3 / mittel	zusätzlich internes Design, u.a.: Nennung von Subsystemen und Modulen mit Funktionalität und Konfigurationsmöglichkeiten	
SL-4 / hoch	nicht definiert	nicht relevant für Prüfschema in dieser Version

Tabelle 3

Der Prüfer MUSS eine Prüfung auf Verständlichkeit und Vollständigkeit durchführen. Die Informationen MÜSSEN dann in der Konformitätsprüfung und Schwachstellenanalyse aufgegriffen werden.

2.4 Dokumentation (Anwender)

Die Entwicklung der Komponente MUSS die Prozesse der IEC 62443-4-1 beachten, daher sind folgende Inhalte in der Anwender-Dokumentation gefordert. In Klammern wird der korrespondierende Prozess aus dem nach Normteil IEC 62443-4-1 angegeben:

- Durchführung von Security Updates der Komponente selbst (SUM-2) und weiterer, abhängiger Komponenten oder darunterliegender Betriebssysteme (SUM-3)
- Auslieferung von Security Updates (SUM-4)
- Durchführung von Security Härtungen durch Komponenten-Konfiguration (SG-3)
- Durchführung einer sicheren Außerbetriebnahme/Entsorgung (SG-4)
- Durchführung eines sicheren Betriebs (SG-5)
- Durchführung des Account Managements (SG-6)

Durch den Prüfer MUSS bewertet werden, ob die bereitgestellte Anwender-Dokumentation die geforderten Informationen angemessen und vollständig beinhaltet.

2.5 Konformitätsprüfung

Der Normteil IEC 62443-4-2 benennt Anforderungen (Component Requirements, CR), die zum Teil bereits spezifisch definiert und zu anderen Teilen technologie-unabhängig beschrieben sind. Für eine konkrete Komponente MÜSSEN die Anforderungen daher im Rahmen einer Testfallerstellung durch den Prüfer konkretisiert werden.

Als Zwischenschritt sind sogenannte Akzeptenzkriterien zu definieren, die im Rahmen der Testfallerstellung als Testerwartung aufgegriffen werden können. Das vorliegende Prüfschema leitet aus den Anforderungen der Norm die Akzeptanzkriterien ab und benennt falls möglich auch Fälle für eine Nicht-Akzeptanz.

Die Akzeptanzkriterien können im Gegensatz zur Norm technologisch präzisiert werden, d.h. es ist möglich, aktuell empfohlene Technologien konkret zu benennen. Im Gegensatz zur Norm kann eine relativ kurzfristige Aktualisierung des Prüfschemas erfolgen, um aktuelle Entwicklungen zu berücksichtigen.

Das Vorgehensmodell zur Überführung der Anforderungen zu Testfällen läuft entsprechend folgender Hierarchie ab, der Schritt 3 ist in der Prüfdokumentation zu benennen:

1. Anforderungen des Normteils (CR der IEC 62443-4-2, sortiert nach FR)
2. Akzeptanzkriterien (dieses Prüfschemas, Anhang)
3. Testfälle (Komponenten-spezifisch)

Zu jeder Anforderung der Norm MUSS mindestens ein Testfall referenziert werden. In vielen Fällen SOLLTEN allerdings mehrere Tests zugeordnet werden, da sich Anforderungen auf mehrere Schnittstellen oder Komponenten-Funktionen beziehen können.

Ein Testfall MUSS mindestens mit folgenden Eigenschaften beschrieben werden:

- Testbeschreibung mit Testerwartung, Testvorbereitung und Testschritten
- Testergebnis
- Bewertung (pass/fail)

Im Nachfolgenden wird anhand eines Beispiels mit Bezug zu CR 3.1 Communication Integrity das zuvor beschriebene Vorgehensmodell veranschaulicht:

	Ebene		**Konkretisierung im Beispiel**
1	IEC 62443-4-2	CR 3.1: Communication Integrity	The component shall provide the capability to protect integrity of transmitted information.
2	Prüfschema	Akzeptanzkriterien	Accept: - capability to protect integrity of transmitted information - use of any standardized cryptographic protocol - use of BSI recommended protocols (TR-02102), see CR4.3 Not accept: - no encryption - use of CRC
3	Komponenten-spezifisch, Prüfdokumentation	Testfälle für angenommene Kommunikations-protokolle HTTPS und FTP mit einer fiktiven Komponente	Test description: Connections for 1) Test HTTPS against BSI recommended protocols, 2) Test FTP Test expectation: No manipulation due to man-in-the-middle attack is successful. Test -conditions: ARP spoofing for diverting local network traffic to man-in-the-middle attacker. Test steps: a. Establish connection b. Manipulate network packets c. Observe if data is still transmitted, received and processed Test results: 1. HTTPS: manipulation is not possible, but analyse of available cipher suites showed not recommended ciphers were active (not accepted) 2. FTP → Manipulation is possible (not accepted) Assessment: if all cases are accepted → pass, otherwise → fail; in this example all cases were not accepted therefore the test failed

Tabelle 4

2.6 Schwachstellenanalyse

Zielsetzung der Schwachstellenanalyse in der Gesamtprüfung ist es, festzustellen, ob die Komponente keine bekannten Schwachstellen beinhalten. Zudem soll betrachtet werden, ob Sicherheitsfunktionen über Mechanismen implementiert wurden, welche eine ausreichende Resistenz gegenüber einem angenommenen Angreifertyp (definiert über die SL-Stufe) bieten. Eine ausreichende Resistenz liegt vor, wenn kein Angriff skizziert werden kann, welcher oberhalb der behaupteten Resistenz zu finden ist. Die dazu genutzte Bewertungsmethodik wird im Folgenden dargestellt.

Als Methodik zur Identifizierung von Schwachstellen wird die in der Regel vorab durchgeführte Konformitätsprüfung genutzt, um Indizien für potentielle Schwachstellen zu finden. In der Analyse werden zudem alle orthogonal zu den Anforderungen (CR) liegenden Bedrohungen betrachtet, unter anderem die folgenden:

- Schwachstellen in 3rd-Party-Software
- Schwachstellen in Betriebssystem
- Manipulation der Hardware-Firmware bzw. des BIOS
- fehlende Integritätssicherung von Datenexporten

Nach der durchgeführten Analyse liegt eine Liste von identifizierten Schwachstellen vor, welche dann im Rahmen einer Schwachstellenbewertung hinsichtlich Relevanz und Kritikalität für die Komponente eingestuft werden müssen. Hierzu ist insbesondere der zugrundeliegende Verwendungszweck zu berücksichtigen.

Bei der Bewertung MUSS die Definition des Angreifertyps beachtet werden. Der Angreifertyp wird in der IEC 62443 über die SL-Stufe definiert. Beispielsweise definiert SL-3 einen Angreifer mit mittlerem Angriffspotential. Eine Komponente für die behauptet wird SL-3 zu entsprechen, muss resistent gegenüber einem solchen Angreifer sein.

Hierzu wird ein Bewertungsmodell benötigt, welche alle relevanten Faktoren für einen Angriff berücksichtigt. Als Bewertungsmodell hat sich hierzu die „Vulnerability Assessment (AVA)“ Methodik aus der Common Evaluation Methodology [CEM] oder ISO/IEC 18045 [ISO18045] bewährt. Für die Nutzung im Zusammenhang mit der IEC 62443 MUSS eine adaptierte Variante genutzt werden, um die definierten SL-Stufen nutzen zu können. Diese adaptierte Variante wird im Folgenden beschrieben.

Diese Methodik wurde gewählt, da keine anderen standardisierten Bewertungsmethoden von Angriffen in Bezug zu einer definierten Angriffsresistenz existieren. Die Methode definiert nicht, wie Schwachstellen oder sogar Angriffe identifiziert werden können, die Methode deckt nur die Bewertung ab.

Bei der Bewertung MUSS nicht nur die einzelne Schwachstelle zugrunde gelegt werden, sondern es MUSS der gesamte Angriffspfad skizziert werden. Hiermit wird der Bezug zum Verwendungszweck hergestellt. Ein Angriff KANN dabei durchaus einen noch nicht praktischen aber theoretisch skizzierbaren Teilschritt beinhalten, die Fachexperten (Prüfer) müssen dabei argumentieren können, dass dieser Schritt zukünftig realistisch ausführbar werden wird.

Folgende Punkte werden dann zur Bewertung eines kompletten Angriffs zugrunde gelegt:

- Zeitbedarf (sowohl zur Entwicklung des Angriffs sowie zur Durchführung)
- Expertise
- Wissen über die Komponente
- Möglichkeit (window of opportunity)
- Ausstattung

Jeder Einstufung werden Punkte zugeordnet, welche dann aufsummiert und mit einem Zielniveau abgeglichen werden. Die Definition der Punkte und die detaillierte Beschreibung finden sich in [CEM] im Anhang B.

Um die Methodik auf die IEC 62443 anwenden zu können, muss die Definition der SL-Stufen auf die nummerischen Werte der [CEM] durchgeführt werden. Dies erfolgt in der folgenden Tabelle:

SL-Stufe / Angreifertyp	**Wertebereich für ausreichende Resistenz**	**Kommentar**
SL-1 / nicht gezielt	-	nicht relevant für Prüfschema in dieser Version
SL-2 / gering	> 4	geringes Angriffspotential bedeutet im Wesentlichen der zeitliche Faktor ist ausschlaggebend, als Schwelle wird hier weniger als 1 Monat Angriffszeit angenommen, zusammen für Entwicklung und Durchführung, ein Monat wird mit 4 Punkten bewertet, siehe [CEM] Anhang B

SL-3 / mittel	> 14	das angenommene mittlere Angriffspotential ergibt eine Mindestsumme von 14 Punkten, dies bedingt sich durch eine Angriffszeit von zwei Monaten (7 Punkte), entweder weitergehender Expertise (3 Punkte) oder Zugriff auf restriktive Daten (ebenfalls 3 Punkte) sowie spezialisiertes Equipment (4 Punkte), hiermit ergeben sich in Summe 14 Punkte, siehe [CEM] Anhang B
SL-4 / hoch	-	nicht relevant für Prüfschema in dieser Version

Tabelle 5

Die Spalte "Wertebereich für ausreichende Resistenz" ist so zu lesen, dass ein skizzierbarer Angriff in diesem Wertebereich liegen MUSS, damit das Produkt in entsprechender SL-Stufe als ausreichend resistent bezeichnet werden kann.

Als Beispiel sei folgendes Szenario angenommen. Die betrachtete Komponenten-Schnittstelle ist SSH (Secure Shell) mit einer Passwort-Authentifizierung, weiter wird mindestens ein 4-stelliges Passwort (ohne weitere Restriktionen) gewählt, eine Beschränkung der Anmeldeversuche existiert nicht. Auf Basis des Szenarios lässt sich ein Angriff skizzieren, indem mit einem SSH-Bruteforce-Tool versucht wird das Passwort einer Benutzerkennung zu raten. Ein solches Bruteforce-Tool ist beispielsweise Hydra. In einer LAN-Umgebung sind beispielsweise 180 SSH-Anmeldeversuche pro Minute möglich, entsprechende Werte könnten im Rahmen eines Labortests ermittelt werden.

Nimmt man weiter an, dass das zu ratende Passwort tatsächlich vier Stellen hat und aus großen und kleinen Buchstaben sowie Ziffern besteht, ergeben sich 62^4 mögliche Kennwörter. Mit oben genannter Brute-Force-Rate wäre der Angriff in unter 23 Stunden durchführbar. Hinzu kommt noch ein gewisser Aufwand zum Aufbau und Durchführung des Angriffs. Im Ergebnis wird damit ein Gesamtaufwand von etwas mehr als einem Tag angesetzt.

Werden die Eckdaten des Angriffs mit Hilfe der Kennzahlen aus der [CEM] abgeschätzt, ergibt sich folgende Tabelle:

Kategorie	**Begründung**	**Wert nach [CEM]**	**Punktzahl nach [CEM]**
Zeitbedarf	mehr als 1 Tag, weniger als eine Woche	<= one week	1
Expertise	Angriffswerkzeug ist mit vielen Beispielen öffentlich dokumentiert	Layman	0
Wissen über die Komponente	SSH ist ein per RFC dokumentiertes Protokoll und ein offener Port kann über einen Netzwerk-Portscan gefunden werden	Public	0
Möglichkeit (window of opportunity)	dies hängt stark vom Verwendungszweck ab, falls keine Restriktionen definiert sind, dann sind diese unbegrenzt	Unnecessary/unlimited access	0
Ausstattung	das Tool Hydra ist öffentlich und leicht zugänglich verfügbar	Standard	0

Tabelle 6

Daraus ergibt sich eine Gesamtzahl von 1 Punkt. In diesem Beispiel wäre die Resistenz der Komponente also nicht ausreichend, um sich für SL-2 zu qualifizieren, d.h. die Schwachstellenanalyse hätte an dieser Stelle ein negatives Prüfergebnis.

Optional kann zusätzlich auch noch eine Bewertung gefundener Schwachstellen nach CVSS durchgeführt werden. Diese Betrachtung beachtet allerdings nicht den Verwendungszweck des Produkts und bietet damit eine eher oberflächliche Einstufung. Diese Bewertung kann aber wiederum hilfreich für den Entwicklungsprozess der Komponente sein. Ein Prüfer KANN diese Information optional angeben.

3 Prüfungsablauf

3.1 Zertifizierung

Für den Fall einer Zertifizierung eines oder mehrerer Normteile der IEC 62443 SOLLTE das vorliegende Prüfschema herangezogen und eingebunden werden.

Eine Bewertung im Rahmen einer Zertifizierung muss von spezialisierten Prüfstellen für IT-Sicherheit durchgeführt werden. Die Prüfstelle sollte die eigenen Prüfverfahren basierend auf die DIN EN ISO/IEC 17025 ausrichten. Dies entspricht den [DAkkS-]Akkreditierungsanforderungen für die IEC 62443. Die Tätigkeit von Inspektionsstellen im Kontext der IEC 62443 kann aufgrund der vorhandenen Expertise nur auf nachrangige Prüfungen bezogen werden, wie beispielsweise der Prüfung, ob eine Komponente mit definierten technischen Fähigkeiten in einer konkreten Anlage die gesetzten Anforderungen erfüllt.

Antragsdokumente, Formulare oder weitergehende Anforderungen an Dokumente SOLLTEN in den Zertifizierungsschemen ausgearbeitet werden. Die inhaltlichen Anforderungen an die Dokumente des Herstellers, welche für dieses Prüfschema benötigt werden sind in Anhang A "Komponentenspezifikation" angegeben.

Im Unterschied zu einem Zertifizierungsschema werden in diesem Dokument explizit nur vollständige Akzeptenzkriterien für die Prüfungsdurchführung angegeben. Gegebenenfalls KÖNNEN im Rahmen einer Zertifizierung auch Bewertungen wie "nicht anwendbar" (not applicable) oder ähnliche aufgrund des Fokus der Zertifizierung zugelassen werden, dies liegt allerdings hinter dem Fokus dieses Prüfschemas. Beispielsweise KÖNNEN bei einem angenommenen Bedrohungsszenario mit nur logischen Angriffen, physische Sicherheitsfunktionen eventuell ausgeschlossen werden. In diesem Dokument wird die vollständige technische Prüfung adressiert.

3.2 Andere Prüfverfahren

Das Prüfschema KANN auch für andere Prüfverfahren genutzt werden, wie:

- technische Assessments in Lieferanten-Auftragnehmer-Beziehungen
- interne Prüfung der technischen Fähigkeiten und Resistenz der eigenen Produkte durch eine organisationseigene Prüfabteilung

3.3 Durchführung der Prüfung

Vor der Durchführung der Prüfung SOLLTE ein Zeitplan erstellt werden, diese sollte zum einen die Abgabetermine der Prüfgegenstände beinhalten sowie die Zeiträume und Fertigstellungstermine der Prüfschritte aus Kapitel 2 beinhalten.

Desweiteren SOLLTE die Fachkompetenz der an der Prüfung beteiligten Prüfexperten nachgewiesen werden. Dies gilt insbesondere, wenn das Prüfschema im Rahmen von Zertifizierung genutzt wird und eine hohe Vergleichbarkeit der Prüfergebnisse gefordert ist.

4 Querbeziehungen des Normteils (informativ)

4.1 Zusammenhänge in der IEC 62443

Die IEC 62443 definiert Zusammenhänge zwischen den verschiedenen Normteilen, die für die IEC 62443-4-2 relevanten werden nachfolgend beschrieben.

4.1.1 Entwicklungsprozess (IEC 62443-4-1)

Der Normteil IEC 62443-4-2 definiert in Kapitel 4.5.1 Software development process, dass bei der Entwicklung einer Komponente die Prozesse der IEC 62443-4-1 einzuhalten sind. Dies wird in diesem Prüfschema berücksichtigt, indem verschiedene Ergebnisse (deliverables) des beschrieben Entwicklungsprozesses als Eingabe in das Prüfverfahren genutzt werden.

Der Normteil IEC 62443-4-1 erfordert ein eigenes, weiteres Prüfschema zur Bewertung, da die Prozesse über ein Reifegradmodell bewertet werden.

4.1.2 Sicherheitsanalyse (SVV-5 aus IEC 62443-4-1)

Der Software-Entwicklungsprozess nach Normteil IEC 62443-4-1 fordert in der Practice SVV-5 Independence of testers unter anderem diese Punkte:

- Security requirements testing
- Attack surface analysis
- Known vulnerability scanning
- Penetration testing

Das vorliegende Prüfschema hilft diese Anforderungen zu erfüllen, sofern entsprechend unabhängige Prüfer mit ausreichender Qualifizierung eingesetzt werden.

4.1.3 Produktprüfung (SVV-1, SVV-3 und SVV-5 aus IEC 62443-4-1)

Ebenfalls fordert der Software-Entwicklungsprozess nach Normteil IEC 62443-4-1 die Durchführung von Sicherheitsanalysen mit unterschiedlicher Ausgestaltung als Teil der Produktprüfung, der Normteil fordert unter anderem diese:

- Security requirements testing (SVV-1)
- Vulnerability testing (SVV-3)
- Penetration testing (SVV-4)

Das vorliegende Prüfschema hilft, diese Anforderungen durch die Prüfschritte Konformitätsprüfung und Schwachstellenanalyse zu erfüllen.

4.2 Akkreditierung

Als Rahmen für Zertifizierungsverfahren im Geltungsbereich der Deutschen Akkreditierungsstelle (DAkkS) wurden Akkreditierungsanforderungen für Konformitätsbewertungsstellen im Dokument [DAkkS] definiert.

Das hier dargestellte Prüfschema ist ein Arbeitsprogramm für Prüfstellen, welche eine Konformitätsbewertung nach IEC 62443-4-2 durchführt. Die Arbeiten einer Inspektionsstelle sind nicht im Fokus dieses Dokuments.

Welche Aussage Inspektionsstellen zu den sicherheitstechnischen Anforderungen nach IEC 62443-4-2 im Rahmen einer Konformitätsbewertung machen können, und wie ein adäquates Vorgehen für eine Prüfung wäre, sollte ebenfalls in einem Prüfschema ausgearbeitet werden.

4.3 IECEE

Das IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE) ist ein multilaterales Zertifizierungssystem welches IEC Standards zugrunde legt. Zertifikate im Gültigkeitsbereich der IECEE werden international gegenseitig anerkannt.

Im Kontext IEC 62443 wurde innerhalb des IECEE bereits der Normteil IEC 62443-2-4 berücksichtigt. Weitere bereits veröffentlichte Normteile werden aktuell vorbereitet.

Es wird angestrebt das vorliegende Prüfschema mittelfristig in den Standardisierungsprozess des IECEE als Vorschlag für Prüfungen des Normteils IEC 62443-4-2 einzubringen.

4.4 Common Criteria

Die Common Criteria (CC) oder ISO/IEC 15408 definiert ein generisches Modell zur Prüfung von Sicherheitseigenschaften in Produkten. Dem Konzept der Norm liegt eine zunehmende Vertrauenswürdigkeit mit entsprechend tiefer gehenden Prüfungen zugrunde, dies drückt sich in der EAL-Stufe aus.

Der Einstieg in die eigentliche Prüfung ist ein formalisierter Ansatz, welcher zum einen die Definition des zugrundeliegenden Sicherheitsproblems fordert sowie die Definition von Sicherheitsfunktionen, welche zusammen mit Einsatzparametern (u.a. Annahmen) das Sicherheitsproblem lösen sollen. Diese Informationen werden in den Sicherheitsvorgaben (Security Target) beschrieben.

Die CC beinhaltet ebenfalls die Durchführung eines unabhängigen Testens, vergleichbar mit der Konformitätsprüfung in diesem Dokument, sowie die Durchführung einer Schwachstellenanalyse. Die Methodik der CC Schwachstellenanalyse wird in diesem Prüfschema als Basis genommen und adaptiert. Neben diesen Prüfaspekten definiert die CC zudem noch diese Punkte:

- Prüfung der Sicherheitsvorgaben
- Prüfung der Entwicklungsumgebung
- Prüfung der Handbücher bzgl. der Aspekte sichere Inbetriebnahme und Verwendung
- Prüfung von Designdokumenten (Schnittstellen, interne Architektur, Sicherheitsarchitektur, abhängig von EAL-Stufe)
- Prüfung des Quellcodes (ab EAL4)
- Prüfung der Produkt- und Modul-Tests des Herstellers

4.5 CSPN (Frankreich)

Als Alternative zu CC wurde in Frankreich das CSPN (Certification de Sécurité de Premier Niveau) entwickelt, welches primär einen Penetrationstest-basierten Ansatz verfolgt. D.h. es wird über eine Analyse versucht Schwachstellen zu identifizieren. Hierzu wird in der Regel eine Black-Box-Methodik verwendet, welche zum Teil aber durch Design- oder Detail-Informationen des Herstellers ergänzt werden.

Das Verfahren erlaubt in einem Prüfdurchlauf keine Korrekturen und ist ansonsten ebenfalls auf praktische Prüfeffektivität ausgelegt und verzichtet weitgehend auf formale Aspekte. Der Hersteller übergibt zu Beginn des Verfahrens wie bei CC ebenfalls Sicherheitsvorgaben, welche in der Prüfung zugrunde gelegt werden, diese entsprechen allerdings weniger strikten Vorgaben. Das BSI plant ein ähnliches Verfahren in Deutschland zu etablieren, welches als Basissicherheitszertifizierung (BSZ) bezeichnet werden soll.

5 Anhang A (normativ) - Komponentenspezifikation

5.1 Vorbemerkung

Nachfolgend werden die inhaltlichen Anforderungen an die Dokumente des Herstellers, welche für dieses Prüfschema benötigt werden angegeben. Aus dem Secure Development Process (nach Normteil IEC 62443-4-1) abgeleitete Anforderungen werden nachfolgend markiert mit der Abkürzung des jeweiligen Prozesses z. B. "(SM-6)".

5.2 Beschreibung der Komponente / Konformitätsbehauptung

- Kurzbeschreibung des Produkts
- Identifizierung des Produkts
- Produktname
- Version
- Identifizierungsmöglichkeit im Betrieb sowie Installation und Update
- Integritätsnachweis der Komponente, primär Software (SM-6)
- Komponenten Kategorie
- entsprechend IEC 62443-4-2: Software Application, Embedded Component, Host Component oder Network Component
- Ausgeschlossener Produktumfang
- Funktionalitäten der Komponente, die nicht betrachtet werden
- Angabe einer Konformitätsbehauptung (Stufe zur Sicherheitsfunktionalität)
- Angabe einer SL-Stufe: SL-1, SL-2, SL-3 oder SL-4
  oder
  Angabe über Auflistung einzelner Anforderungen, mit Angabe möglicher ergänzter Anforderungen (requirement enhancements)
- Angabe zum betrachteten Angreifertyp (Resistenzstufe)
- Angabe über SL-Stufe: SL-1, SL-2, SL-3 oder SL-4 (analog zur Konformitätsbehauptung oder abweichend, in der Regel nur höher)
  oder
  Angabe über Beschreibung des Angreifers (basierend auf IEC 62443-Definition)

5.3 Verwendungszweck

- Verwendungszweck (intended use) (SR-1)
- Anwendungsfälle
- Bedrohungsmodell (SR-2)
- Einsatzumgebung (zwingende und optionale)
- Sicherheitsfunktionalität (SR-3, SR-4)
- Sicherheitsmechanismen zur Umsetzung der Funktionalität
- Information ob PKI-Techniken unterstützt werden

5.4 Dokumentation

- Dokumentation
- je nach Verwendungszweck Informationen für sicheren Betrieb u.a. in einer
- Endkunden-Dokumentation
- Integrator-Dokumentation
- zwingende inhaltliche Forderungen
- Quelle und Durchführung von Updates der Komponente und darunterliegender Komponenten/Betriebssysteme (SUM-4)
- Informationen zum Update-Umfang (SUM-2)
- Informationen zu Abhängigkeiten bei Updates (SUM-3)
- Kontaktstelle für Sicherheitsprobleme (DM-1)
- Informationen für Sicherheitshärtung (SG-3)
- Informationen zum sicheren Betrieb (SG-5)
- Informationen zum Account Management (SG-6)
- Informationen für Außerbetriebnahme (SG-4)

6 Anhang B.1 (normativ) - Anforderungen an Prüfdokumentation

6.1 Vorbemerkung

Nachfolgend werden die inhaltlichen Anforderungen an die Prüfdokumentation für Prüfungen nach dem hier beschriebenen Schema aufgeführt. Durch ähnliche Dokumentation wird ein Vergleich von Prüf-Ergebnissen zwischen Prüfern sowie zwischen geprüften Produkten erst möglich.

Dabei wird nur der grobe Rahmen an den Inhalt vorgegeben, die Inhalte SOLLTEN dann in der Prüfdokumentation der Prüfer wieder erscheinen. Die exakte inhaltliche Struktur einzelner Dokumente wird an dieser Stelle nicht vorgegeben.

6.2 Übersicht zur Prüfung

- Prüfung der Komponentenspezifikation auf Vollständigkeit und Korrektheit
- Konfiguration(en) des Prüfgegenstandes
- Aufbau der Prüfumgebung (test setup)
- Nicht geprüfte Funktionalitäten (Abgrenzung)

6.3 Bewertung der Design-Dokumentation

- Ergebnisse der Design-Dokumentations-Prüfung

6.4 Prüfung der Anwender-Dokumentation

- Ergebnisse der Anwender-Dokumentations-Prüfung

6.5 Testergebnisse der Konformitätsprüfung

- Detaillierte Testergebnisse
- Übersicht/Zusammenfassung der Testergebnisse

6.6 Schwachstellenanalyse

- Identifizierte Schwachstellen
- Bewertung der Schwachstellen
- Beschreibung der verbleibenden Schwachstellen

6.7 Gesamtbewertung

- Übersicht der Prüfergebnisse
- Votum der Prüfstelle
- Empfehlungen der Prüfstelle (u.a. bezogen auf Schwachstellen)

7 Anhang B.2 (normativ) - Akzeptanzkriterien

7.1 Vorbemerkung

Die folgende Tabelle unterscheidet nicht mittels separater Spalten zwischen SL-1 und SL-2 Anforderungen. Diese Anforderungen sind zusammen in der Spalte SL-2 dargestellt, entsprechende Hinweise finden sich in den Zellen der Tabelle.

Die Anforderungen werden nachfolgend im originalen englischen Text angegeben, da geplant ist das vorliegende Prüfschema zukünftig ebenfalls zu übersehen und international einzubringen, siehe Kapitel 4.3.

Die Akzeptanzkriterien sind primär als "accept" positiv formuliert. In manchen Fällen ist ein expliziter Negativfall zur Besserungen Hervorhebung allerdings sinnvoll, diese Kriterien sind unterhalb von "not accept" aufgeführt.

7.2 FR-1: Identification and Authentication Control

ID	Requirement	SL-2	SL-3
CR 1.1	Human user identification and authentication	SL-1 requirements Accept: - authentication of human users on all interfaces with human access SL-2 requirements Accept: - unique authentication for every human user on all interfaces, for example with username and password Not accept: - group based authentication, like all service technicians use same username and password	no additional requirements
CR 1.2	Software process and device identification and authentication	SL-2 requirements Accept: - identify itself and authenticate to any other component using passwords, tokens or location (physical or logical) - authentication mechanism is capable to prevent attacks like man-in-the-middle or message spoofing	Accept: - uniquely identify and authenticate itself to any other component Not accept: - unencrypted authentication and identification

CR 1.3	Account management	SL-1 requirements Accept: - capability to integrate into a higher level account management system - capability for account management (only by authorized users, including adding, activating, modifying, disabling and removing accounts) - Is the impact of an unavailable higher-level account management system considered? Not accept: - no capability to enable/disable accounts	no additional requirements
CR 1.4	Identifier management	SL-1 requirements Accept: - capability to integrate into a system that supports management of identifiers - provide the capability to support the management of identifiers by user, group, role or control system interface	no additional requirements
CR 1.5	Authenticator management	SL-1 requirements Accept: - support of (initial) authenticator content (tokens, symmetric keys, private keys, biometrics, passwords, key cards) - enforced change of default authenticators after installation or recognition of unchanged default authenticator (combined with warning message) - periodic change of authenticators - protection of unauthorized disclosure or modification of authenticators (when stored, used, transmitted) Not accept: - transmission of cleartext passwords	Accept: - authenticators are protected via hardware (e.g. TPM) Not accept: - no additional protection mechanisms

CR 1.6	Wireless access management	Network Component Requirement SL-1 requirements Accept: - capability to identify and authenticate all users (human, software processes and devices) engaged in wireless communication SL-2 requirements Accept: - Capability to uniquely identify and authenticate all users (human, software processes and devices) engaged in wireless communication	no additional requirements
CR 1.7	Strength of password-based authentication	SL-1 requirements Accept: - enforce configurable password strength based on minimum length and variety of character types - external authentication integration	Accept: - prevent any human user account from reusing a password for a configurable number of generations - enforce password minimum and maximum lifetime restrictions for human users Not accept: - no configurable options for reusing passwords, i.e. password reuse cannot be prevented - no minimum and maximum lifetime restrictions for human user passwords
CR 1.8	Public key infrastructure certificates	Relevant if PKI or public keys are in use. SL-2 requirements Accept: - interaction and operation within the scope of the PKI according to 62443-3-3 SR 1.8 ("operate a PKI according to commonly accepted best practices (see IETF RFC 3647) or obtain a public key certificate from an existing PKI")	no additional requirements

CR 1.9	Strength of public key authentication	Relevant if PKI or public keys are in use. SL-2 requirements Accept: - provide directly or integrate into a system that provides, the capability to: - validating signature of a given certificate - validate certificate chain - in case of self-signed certificates, leaf certificates should be deployed to all hosts that communicate with the subject to which the certificate is issued - validate certification revocations status - establish user (software, human or device) control of the corresponding private key - map authenticated identity to a user by checking either the subject name, common name or distinguished name against the destination - algorithms and keys comply with CR 4.3	Accept: - protect the relevant private keys via hardware (e.g. smart cards) Not accept: - no additional protection mechanisms
CR 1.10	Authenticator feedback	SL-1 requirements Accept: - sensitive data concerning the authentication process is obscured Not accept: - feedback like wrong password, username, etc. - displaying password, wireless key, SSH token in input field instead of asterisks - usage of WEP	no additional requirements
CR 1.11	Unsuccessful login attempts	SL-1 requirements Accept: - capability to enforce a limit of configurable number of consecutive invalid access attempts by any user (human, software, device) during a configurable time period - capability to deny access for a specified period of time or until unlocked when limit reached	no additional requirements

CR 1.12	System use notification	SL-1 requirements Accept: - capability to display a system use notification message before authenticating to the local user interface - capability to configurable the message by authorized user	no additional requirements
CR 1.13	Access via untrusted networks	Network Component Requirement SL-2 requirements Accept: - monitor and control all methods of access to the network device via untrusted networks (dial-up, office network, remote access) Not accept: - access to the network device cannot be monitored / controlled - untrusted network is missing in monitoring or cannot be controlled	Accept: - deny access requests via untrusted networks unless approved by an assigned role - for each connection a physical key is used to authorize the connection
CR 1.14	Strength of symmetric key-based authentication	Relevant if symmetric key authentication (e.g. pre-shared-secrets) is used. SL-2 requirements Accept: - validate shared secret to establish the mutual trust - authentication is valid as long as shared secret remains a secret, i.e. secrets are stored securely - restrict access to the shared secret - ensure that the algorithms and keys used comply with CR 4.3 (Use of cryptography)	Accept: - control system provides the capability to protect the relevant private keys via hardware mechanisms

7.3 FR-2: Use Control

ID	Requirement	SL-2	SL-3
CR 2.1	Authorization enforcement	SL-1 requirements Accept: - authorization enforcement mechanism on all interfaces which are accessible by a human users available based on their responsibilities and least privilege Not accept: - interface without authorization mechanism (e.g. HMI, web interface, console) - user with access to HMI can log in via console or SSH SL-2 requirements Accept: - authorization enforcement mechanism on all interfaces which are accessible by all users (additionally technical users) - management of roles and permissions (definition and modification, only by privileged role) - management of users mapped to roles Not accept: - interface without authorization mechanism (e.g. HMI, web interface, console) - user with access to HMI can log in via console or SSH	Accept: - capability to configure a time or sequence of events during supervisor override without closing the current session Not accept: - no possibility to configure supervisor override
CR 2.2	Wireless use control	SL-1 requirements Accept: - capability to deny critical action via wireless connection (i.e. only use wired) - monitor devices	no additional requirements
CR 2.3	Use control for portable and mobile devices	SL-1 requirements Accept: - capability to operate in environment where use restrictions are enforced by the IACS, i.e. capability of portable/mobile device - examples for use control: restricting code and data transfer to/from portable and	no additional requirements

		mobile devices, context specific authorization	
CR 2.4	Mobile code	SL-1 requirements Accept: - capability to enforce a security policy for the usage of mobile code - control execution of mobile code - define which users are allowed to transfer mobile code to/from device (EDR: only upload to device) - perform integrity checks prior to code is executed - perform authenticity checks to verify origin prior to code execution	Software Application and Embedded Accept: - provides the capability to verify the integrity of the mobile code before execution is allowed Not accept: - execution is allowed without verifying the integrity of the mobile code
CR 2.5	Session lock	SL-1 requirements Accept: - for HMI (local or via network): - Session Lock after configurable time period of inactivity - manual session lock - access to session only possible using authentication procedures - comply with session locks requested by the underlying infrastructure (operating system, control system)	no additional requirements
CR 2.6	Remote session termination	Remote session is interpreted as logical network session. SL-2 requirements Accept: - remote session terminated by user who initiated session (minimum requirement) - remote session manually terminated by a local authority/user - remote session terminated after configurable inactive period of time	no additional requirements

CR 2.7	Concurrent session control	No requirements	Accept: - Application is able to limit session per interface for any user Not accept: - Sessions cannot be limited - Sessions cannot be limited per interface or per user
CR 2.8	Auditable events	SL-1 requirements Accept: - audit records for following cases are generated: access control, request errors, control system events, backup and restore events, configuration changes, audit log events - audit records include all information: timestamp, source, category, type, event ID, event result	no additional requirements
CR 2.9	Audit storage capacity	SL-1 requirements Accept: - capability to allocate audit record storage - log rotation to prevent log storage failures - in case of log rotation, need for persistent (undeletable) log event (e.g. special security events) Not accept: - failure of audit storage due to reached or exceeded capacity	Accept: - in case of reached audit record storage, configurable threshold a warning is caused Not accept: - no warning, if capacity reached threshold - threshold not configurable
CR 2.10	Response to audit processing failures	SL-1 requirements Accept: - no loss of essential services and functions during an audit processing failure - support of appropriate actions in response to an audit processing failure - e.g. alerting personnel could be an appropriate action	no additional requirements
CR 2.11	Timestamps	SL-1 requirements Accept: - ability to generate timestamps for audit records (see CR 2.8) - timestamps include date and time	Accept: - synchronized timestamps - e.g. external source like NTP

CR 2.12	Non-repudiation	No requirements	Relevant if HMI is used. Accept: - possibility to determine which human user took a particular action
CR 2.13	Use of physical diagnostic and test interfaces	No software applications SL-2 requirements In case factory diagnostic and test interfaces use network communication, the interfaces are to be subjected to all of the requirements of this standard Accept: - prevent unauthorized use of the physical factory diagnostic and test interfaces, e.g. JTAG - disabled diagnostic and test interface based on removed external connectors Not accept: - any diagnostic and test interface without authorization	Accept: - provides active monitoring of the device's diagnostic and test interfaces - generate log entry when attempts to access these interfaces are detected Not accept: - disabled diagnostic and test interface based on removed external connectors

Tabelle 7

7.4 FR-3: System Integrity

ID	Requirement	SL-2	SL-3
CR 3.1	Communication integrity	SL-1 requirements Accept: - capability to protect integrity of transmitted information - use of any standardized cryptographic protocol - use of BSI recommended protocols (TR-02102), see CR4.3 Not accept: - no encryption - use of CRC	Accept: - capability to authenticate information during communication Not accept: - authentication of information is not possible

CR 3.2	Protection from malicious code	SL-1 requirements Application Component Accept: - mechanism to protect from malicious code (design documentation requirement) Embedded Component Accept: - environment is allowed to provide malicious code protection mechanism, has to be required by component intended -use description (design documentation requirement) - allowed detection techniques: binary integrity, attributes monitoring, hashing, signature techniques - allowed prevention techniques: removable media control, sandbox techniques Host Component Accept: - need to support the use of malicious code protection (design documentation requirement) Network Component Accept: - provided by the network device directly - allowed to use compensating control SL-2 requirements Host Component Accept: - able to automatically report version of the malicious code protection which is actually in use	no additional requirements

CR 3.3	Security functionality verification	SL-1 requirements Accept: - definition of (manual) test verification procedure for security functionality - guidance on how to test security functionality (documentation requirement) - documented side effects if these verification procedures are running during normal operation Not accept: - no possibility to test security functionality, e.g. no log message, notification or other information as result	no additional requirements
CR 3.4	Software and information integrity	SL-2 requirements Accept: - integrity check of data at rest (e.g. software, configuration) - capability to be integrated into a system that can perform or support integrity checks Not accept: - no recording of results of checks	Accept:- unauthorized change is reported to a configurable entity upon discovery of the attempt
CR 3.5	Input validation	SL-1 requirements Accept: - every input, that directly impacts the action of the application or device is validated for syntax and content Not accept: - test/analysis results indicating insufficient input validation	no additional requirements
CR 3.6	Deterministic output	SL-1 requirements Applicable if device directly controls a process. Accept: - the deterministic output needs to be documented (documentation requirement) - in case of failsafe, allowed to demonstrate by described process	no additional requirements

CR 3.7	Error handling	SL-1 requirements Accept: - error conditions are identified and handled - no unintended information is leaked - no security relevant information is visible	no additional requirements
CR 3.8	Session integrity	SL-2 requirements Accept: - use of mechanisms to protect the integrity of communication sessions	Accept: - sessions are invalidated after termination - sessions are invalidated after reboot - use of unique session IDs Fail: - session hijacking - man in the middle attack - insertion of false information into a session - replay attacks
CR 3.9	Protection of audit information	SL-2 requirements Accept: - protect audit information and audit tools (if present) Not accept: - unauthorized access, modification or deletion of audit information	no additional requirements
CR 3.10	Support for updates	SL-1 requirements Accept: - capability to be updated and upgraded once installed - if component supports or executes essential functions, needs for mechanism to support patching and updating without impacting the essential function	Accept: - the authenticity and integrity of any update is validated prior installation
CR 3.11	Physical tamper resistance and detection	Relevant if intended use does not offer physical protection of component. SL-2 requirements Accept: - anti-tamper resistance: specialized materials to make tampering difficult; e.g.: hardened enclosures, locks, encapsulation, security screws - detection mechanisms for unauthorized physical access into the device, e.g. seal	Accept: - capability to automatically notify upon discovery of an attempt to make an unauthorized physical access

CR 3.12	Provisioning product supplier roots of trust	SL-2 requirements Accept: - provision of product supplier keys and roots of trust during device manufacturing - e.g. cryptographic hashes or public key used for verification Fail: - keys or root of trust can be manipulated or leaked	no additional requirements
CR 3.13	Provisioning asset owner roots of trust	If CR 2.4 Mobile Code then requirement is mandatory. SL-2 requirements Accept: - capability to provision asset owner roots of trust - protection of asset owner roots of trust Not accepted: - export of root of trust (private key) - leakage of root of trust security information	no additional requirements
CR 3.14	Integrity of the boot process	SL-1 requirements Accept: - integrity verification of boot process relevant firmware, software and configuration data prior to the use SL-2 requirements Accept: - authentication verification of boot process relevant firmware, software and configuration data prior to the use - use of product suppliers roots of trust for verification	no additional requirements

Tabelle 8

7.5 FR-4: Data Confidentiality

ID	Requirement	SL-2	SL-3
CR 4.1	Information confidentiality	SL-1 requirements Accept: - capability to protect the confidentiality of information at rest for which explicit read authorization is supported	no additional requirements

		- protection of the confidentiality of information in transit - (wireless) use of encryption Not accept: - (wireless) outdated encryption (e.g. WEP)	
CR 4.2	Information persistence	SL-2 requirements Accept: - capability to purge component - capability to erase all information with explicit read authorization Not accept: - existence of data after component deactivation	no additional requirements
CR 4.3	Use of cryptography	SL-1 requirements If cryptography is required by CR 1.14, CR 3.1 and CR 4.1. Accept: - use of any standardized cryptographic protocol - use of BSI recommended protocols (TR-02102), see CR4.3 - used according to proven practices or documentation	no additional requirements

Tabelle 9

7.6 FR-5: Restricted Data Flow

ID	Requirement	SL-2	SL-3
CR 5.1	Network segmentation	SL-1 requirement Accept: - support segmented network, e.g. multiple network cards - network configuration with routing and router capability - no possibility to bypass segmentation	no additional requirements
CR 5.2	Zone boundary protection	Network Component Requirement SL-1 requirements Accept: - capability to monitor and control communication at zone boundaries to enforce compartmentalization defined in risk-based zones and conduits model Not accept: - demonstrate insufficient boundary protection SL-2 requirements Accept: - capability to deny network traffic by default - allow network traffic by exception	Network Component Requirement Accept: - capability to prevent any communication through the control system boundary (island mode) - provide the capability to prevent any communication through the control system boundary when there is an operational failure of the boundary protection mechanisms (fail close)
CR 5.3	General purpose person-to-person communication restrictions	Network Component Requirement Accept: - capability to prevent general purpose, person-to-person messages from being received from users/systems to the control system (email, all forms of social media, message systems) - e.g. filtering traffic with packet filters or ALGs Not accepted: - no/insufficient traffic inspection	no additional requirements

Tabelle 10

7.7 FR-6: Timely Response To Events

ID	Requirement	SL-2	SL-3
CR 6.1	Audit log accessibility	SL-1 requirements Accept: - capability for authorized humans or tools to access audit logs on a read only basis - web interface (audit perspective) - console tools (separate information system for audit access) Not accepted: - audit logs are accessible for unauthorized users	no additional requirements
CR 6.2	Continuous monitoring	In this requirement "security mechanism" is the security support of a process of the system. SL-2 requirements Accept: - capability to continuously monitor security mechanism (if application or device provides that appl. or device shall provide)	no additional requirements

Tabelle 11

7.8 FR-7: Resource Availability

ID	Requirement	SL-2	SL-3
CR 7.1	Denial of service protection	SL-1 requirements Accept: - capability to operate in a degraded mode (essential functions) during a DoS event SL-2 requirements Accept: - Manage communication load from application or device to mitigate effects of DoS events - e.g. limit network capacity of interfaces	no additional requirements

CR 7.2	Resource management	SL-1 requirements Accept: - capability to limit the use of resources by (active running) security functions to prevent resource exhaustion - e.g. software process prioritization, network traffic rate limiting	no additional requirements
CR 7.3	Control system backup	SL-1 requirements Accept: - shall provide backup abilities to safeguard application/device state (user- and system-level information) - Backup Process does not affect normal operation Not accept: - no / insufficient backup abilities - normal operation is affected by control system backup SL-2 requirements Accept: - capability to verify the reliability of backup mechanism - e.g. verify backup data mechanism, integrity of backed up information is validated prior to restoring it	no additional requirements
CR 7.4	Control system recovery and reconstitution	SL-1 requirements Accept: - capability to recovery and reconstitute to a known secure state after disruption or failure - system parameters (either default or configurable) are set to secure values - security-critical patches are reinstalled - security-related configuration settings are re-established - system documentation and operating procedures are available - components are reinstalled and configured with established settings - information from the most recent known secure backup is loaded and the system is fully tested and functional	no additional requirements

CR 7.6	Network and security configuration settings	SL-2 requirements Accept: - network and security configurations can be configured (as described in guidelines provided by the control system supplier) - component provides an interface to the deployed network and security configuration settings Not accept: - missing related guideline - insufficient description of configurations	Accept: - capability to generate a report listing the currently deployed security settings in a machine-readable format
CR 7.7	Least functionality	SL-2 requirements Accept: - capability to restrict the use of unnecessary functions, ports, protocols and/or services - functions beyond a baseline configuration should be able to be disabled	no additional requirements
CR 7.8	Control system component inventory	SL-2 requirements Accept: - capability to support a control system component inventory - e.g. vendor-specific management-system or standard-based inventory systems (e.g. with SNMP support) - capable to monitor device ID and status	no additional requirements

Tabelle 12

8 Abkürzungsverzeichnis

Abkürzung	Bedeutung
CVSS	Common Vulnerability Scoring System
PKI	Public Key Infrastructure

9 Literaturverzeichnis

[IEC62442-4-2] IEC 62443-4-2, Edition 1.0, 26.05.2017
[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, April 2017, Version 3.1, Revision 5, CCMB-2017-04-004

[Dakks] Akkreditierungsanforderungen für Konformitätsbewertungsstellen im Bereich der Informationssicherheit/Cyber-Security für industrielle Automatisierungssysteme gemäß IEC 62443, 71 SD 2 019, Revision: 1.0, 05.03.2018

[ISO18045] ISO/IEC 18045:2008, Information technology - Security techniques - Methodology for IT security evaluation, 2014-01, Edition 2

TeleTrusT – Bundesverband IT-Sicherheit e.V.

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Experten, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Expertenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie des Vertrauenszeichens "IT Security made in Germany". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Kontakt:

TeleTrusT – Bundesverband IT-Sicherheit e.V.
Dr. Holger Mühlbauer
Geschäftsführer
Chausseestraße 17
10115 Berlin
Telefon: +49 30 4005 4306
E-Mail: holger.muehlbauer@teletrust.de
https://www.teletrust.de

TeleTrusT
Pioneers in IT security.