Bundesverband IT-Sicherheit e.V.

TeleTrusT
Pioneers in IT security.

TeleTrusT-Prüfschema nach IEC 62443-4-2

Industrielle Kommunikationsnetze - IT-Sicherheit für industrielle Automatisierungssysteme

2019-05

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:

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

© 2019 TeleTrusT

TeleTrusT-Prüfschema nach IEC 62443-4-2

2019-05

Industrielle Kommunikationsnetze - IT-Sicherheit für industrielle Automatisierungssysteme

Security for industrial automation and control systems

IEC 62443 Security for industrial automation and control systems -
Part 4-2: Technical security requirements for IACS components (IEC 62443-4-2:2019)

Inhaltsverzeichnis

Inhalt

1	Einführung	3
1.1	Zielsetzung und Anwendungsbereich	3
1.2	Übersicht zum Normteil IEC 62443-4-2	4
1.3	Nutzung des Normteils	4
1.4	Abgrenzung zu SL-Stufen	5
1.5	Adressaten	5
1.6	Normative Terminologie	5
1.7	Normative Referenzen	6
1.8	Definitionen	6
2	Prüfkonzept	6
2.1	Generelles Konzept	6
2.2	Prüfung des Verwendungszwecks	7
2.3	Dokumentation (Design)	7
2.4	Dokumentation (Anwender)	9
2.5	Konformitätsbewertung	9
2.6	Schwachstellenanalyse	11
3	Prüfungsablauf	13
3.1	Konformitätsbewertung	13
3.2	Zertifizierung	13
3.3	Andere Prüfverfahren	13
3.4	Durchführung der Prüfung	13
4	Anhang A (normativ) - Komponentenspezifikation	14
4.1	Vorbemerkung	14
4.2	Beschreibung der Komponente / Konformitätsbehauptung	14
4.3	Verwendungszweck	14
4.4	Dokumentation	14
5	Anhang B (normativ) - Anforderungen an Prüfdokumentation	16
5.1	Vorbemerkung	16
5.2	Übersicht zur Prüfung	16
5.3	Bewertung der Design-Dokumentation	16
5.4	Prüfung der Anwender-Dokumentation	16
5.5	Testergebnisse der Konformitätsbewertung	16
5.6	Schwachstellenanalyse	16
5.7	Gesamtbewertung	16
6	Anhang C (normativ) - Akzeptanzkriterien	17
6.1	Vorbemerkung	17
6.2	FR-1: Identification and Authentication Control	17
6.3	FR-2: Use Control	23
6.4	FR-3: System Integrity	27
6.5	FR-4: Data Confidentiality	32
6.6	FR-5: Restricted Data Flow	33
6.7	FR-6: Timely Response To Events	35
6.8	FR-7: Resource Availability	35
7	Anhang D (informativ) – Methoden zur Schwachstellenbewertung	38
7.1	Einführung	38
7.2	AVA/CEM Bewertung	38
7.3	Beispiel einer Bewertung nach AVA/CEM	39
8	Anhang E (informativ) – Übersicht zur Nutzung der Ergebnisse des IEC 62443-4-1-Entwicklungsprozesses	40
9	Anhang F (informativ) – Übersicht der Ergänzungen zur Norm	43
10	Abkürzungsverzeichnis	44
11	Literaturverzeichnis	44

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 Rollen (Betreiber, Integrator und Komponentenhersteller) betrachtet.

Der in diesem Prüfschema fokussierte Normteil IEC 62443-4-2 (IEC 62443-4-2:2019) stellt Anforderungen an die technischen Security Eigenschaften von industriellen Komponenten. Daneben existiert im Abschnitt 4, welcher konkret Komponentenhersteller adressiert, der Normteil 62443-4-1. Dieser beinhaltet die Anforderungen an einen sicheren Entwicklungsprozess für Komponentenhersteller. Die Anforderungen an technische Security Eigenschaften 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 bezieht sich primär auf die technischen Fähigkeiten einer Komponente, setzt allerdings gleichzeitig voraus, dass bei der Entwicklung der Komponente ein Entwicklungsprozess entsprechend IEC 62443-4-1 zugrunde gelegt wurde. Umgekehrt kann aber nach Anwendung des Prüfschemas keine Aussage über den Reifegrad des Entwicklungsprozesses gemacht werden.

Dies bedeutet, das Prüfschema fordert entsprechend der Norm, 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 auf die Bewertung des Reifegrads des Entwicklungsprozesses an sich.

Das Prüfschema stellt kein Zertifizierungsschema sondern eine Grundlage für eine Konformitätsbewertung dar. Zertifizierungsrelevante Aspekte wie die Definition beteiligter Rollen, Verfahren zur Beantragung, Abnahme und Überwachung von zertifizierten Komponenten und weitere müssen hierauf aufbauend von Schemabetreibern oder Zertifizierungsstellen definiert werden, dies wird im vorliegenden Dokument nicht behandelt.

Das Prüfschema versteht sich im Sinne des IECEE Programmdokuments [OD-2061] als Umsetzung einer Produkt Zertifizierung nach IEC 62443-4-2 entsprechend Szenario 1. Abweichend betrachtet das Prüfschema das Vorhandensein einer IEC 62443-4-1 Zertifizierungen nicht als ausreichend. Wie oben beschrieben werden immer die Ergebnisse (Deliverables) eines IEC 62443-4-1 konformen Entwicklungsprozesses betrachtet, d.h. aus Prüfungssicht wird die Evidenzebene und nicht die Zertifikatsebene betrachtet.

Das Prüfschema kann für kombinierte Zertifizierungen nach IEC 62443-4-2 mit Berücksichtigung eines Entwicklungsprozesses nach IEC 62443-4-1 genutzt werden. In diesem Fall handelt es sich um Drittparteienbewertungen. Eine weitere typische Anwendung des Prüfschemas ist die Konformitätsbewertung eines Herstellers der eigenen Komponenten also Erstparteienbewertung.

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 des Niveaus des definierten Angreifers (entsprechend Security Level, siehe Kapitel 1.3) ist oder ob die Komponente nicht ausreichend resistent zu dem erwarteten Niveau ist. Das Ergebnis der Prüfung bezieht sich immer auf die der Prüfung zugrunde liegenden Version der Komponente unter Beachtung der zu diesem Zeitpunkt bekannten Schwachstellen und Angriffsmethoden.

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

Dies sind Komponenten die in industriellen Automatisierungssystemen eingesetzt werden. Unter anderem sind dies COTS (Commercial off-the-shelf) Komponenten, 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 Security Eigenschaften 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 darstellen.

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 eine Bewertung der Security Eigenschaften der verschiedene Einsatzvarianten der Komponenten durchführen möchte. Ein Hersteller definiert hierzu über die SL-Stufe das Zielniveau seiner Security Eigenschaften, 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 die Vorgaben der IEC 62443-4-1 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 Angreifertyp. Im Rahmen des Normteils IEC 62443-4-2 wurde versucht dies allgemeingültig, sinnvoll miteinander abzugleichen. Ergebnis der Risikoanalyse eines Systems kann jedoch sein, dass sowohl die Auswahl der Anforderungen als auch die Definition des Angreifertyps 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. Bei der Wahl einer SL-Stufe sollte inhaltlich der Verwendungszweck der Komponente berücksichtigt werden.

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

Stufe	Originaltext	Angriffstyp
SL-1	Protection against casual or coincidental violation.	nicht gezielter Angriff
SL-2	Protection against intentional violation using simple means with low resources, generic skills and low motivation	aktiver, gerichteter Angriff, einfache Mittel, allgemeines IT-Wissen, geringe Motivation
SL-3	Protection against intentional violation 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-4	Protection against intentional violation 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 an den Anforderungen der Stufen SL-1 bis SL-3. Die Stufe SL-4 wird 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.

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

1.5 Adressaten

Die primären Adressaten dieses Prüfschemas sind Prüfer, Prüfstellen und interne QS-/IT-Prüfabteilungen. Zertifizierungsschemen können das Prüfschema anwenden. Des Weiteren richtet sich das Dokument an Komponentenhersteller, welche sich auf eine Prüfung Ihrer Komponenten 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 Normative Referenzen

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

IEC 62443-3-3, *Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels* [IEC62443-3-3]

IEC 62443-4-1, *Security for industrial automation and control systems – Part 4-1: Product development requirements* [IEC62442-4-1]

IEC 62443-4-2, *Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components* [IEC62442-4-2]

1.8 Definitionen

Begriff	Definition
Akzeptanzkriterien (acceptance criteria)	Kriterien für den Prüfer zur Beurteilung, ob eine vorgefundene Implementierung im Sinne der Anforderung akzeptabel umgesetzt wurde
Angriffsresistenz	Fähigkeit einer Komponente bei einem Angriff gegenüber diesem (vgl. SL-Stufe) resistent zu bleiben
Resistenz-Stufe	Kategorien zur Beschreibung einer erwarteten Angriffsresistenz aus Perspektive des Angriffspotentials (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 einer Komponente auf Einhaltung des Normteils IEC 62443-4-2 MUSS entlang folgender Prüfschritte erfolgen:

1. Prüfung des Verwendungszwecks
2. Dokumentation (Design/Prüfung)
3. Dokumentation (Anwender)
4. Konformitätsbewertung
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-spezifischen Rahmenparameter erfolgen MUSS, um eine Evaluation durchführen zu können. Hierzu MUSS der Verwendungszweck der Komponente beschrieben werden.

Um eine Komponente auf Security Eigenschaften prüfen zu können, werden je nach Konzept und SL-Stufe 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 höhere (SL-)Stufe ausgedrückt wird, einhergehend mit einer tieferen Prüfung und damit zunehmender Vertrauenswürdigkeit (Assurance). Dieses Prinzip wird in diesem Prüfkonzept ebenfalls so ange-

wandt, 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 hinsichtlich der Security Eigenschaften 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 in Abhängigkeit der gewählten die SL-Stufe. Für die Evaluation durch den Prüfer wurden hierzu im vorliegenden Dokument Akzeptanzkriterien definiert. Ein Nachweis über die Einhaltung einzelner Kriterien MUSS über einen oder mehrere Tests stattfinden. Falls dies nicht möglich, z. B. falls die Funktionalität nicht über eine Schnittstelle getestet werden kann, dann KANN ein Nachweis über eine Design-Dokument-Prüfung erbracht werden.

Der folgende 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 mittels einer gewählten SL-Stufe definiert wird. Falls die Sicherheitsanforderungen nicht über eine SL-Stufe gewählt wurden, MUSS ein entsprechender Angreifertyp explizit ausgewählt werden.

Die zu prüfende Komponente SOLLTE in mindestens zweifacher Ausführung zur Prüfung übergeben werden, diese optionale Forderung soll helfen einen reibungslosen Prüfungsablauf sicherzustellen. 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 der Komponente definiert betriebliche und Security-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.

Die Inhalte lassen sich aus den Prozessen der IEC 62443-4-1 herauslesen und werden in diesem Dokument teilweise noch präzisiert. Es MUSS die Definition eines Security Kontexts (SR-1) und die Erstellung eines Bedrohungsmodells (SR-2) für die Komponente erfolgen.

Aus Sicht dieses Prüfschema MÜSSEN 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 auf Vollständigkeit und Korrektheit analysieren.

2.3 Dokumentation (Design)

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 wird in diesem Analyseschritt zudem ermöglicht, grundsätzliche Design-Schwächen aufzudecken.

In diesem Prüfschema wird dieses Konzept aufgegriffen und den betrachteten Stufen SL-1 bis SL-3 (Resistenzstufe) die folgende geforderte Design-Dokumentation zugeordnet.

Die Wahl der technischen Implementierung MUSS angemessen zur gewählten SL-Stufe (im Sinne der Resistenz) sein, dies ist über die Design-Dokumentation darzustellen. Diese Forderung ergibt sich aus den Definitionen der sieben Foundational Requirements (FR) jeweils zu Beginn der einzelnen Kapitel 5 bis 11 der [IEC62442-4-2].

Dies bedeutet beispielsweise, dass bzgl. der Anforderung CR 4.1 Information confidentiality darzustellen ist, warum die gewählte Implementierung bei SL-2 das in FR 4 Data confidentiality geforderte Niveau erreicht: „Prevent the unauthorized disclosure of information to an entity actively searching for it using simple means with low resources, generic skills and low motivation."

Die abschließende Beurteilung, ob die technische Implementierung der geforderten Stufe entspricht, findet final im Prüfschritt 5 Schwachstellenanalyse statt.

SL-Stufe	**Geforderte Design-Dokumentation**	**Kommentar**
SL-1	Beschreibung aller externen Schnittstellen, u.a.: alle kabelgebundenen und funkbasierten Kommunikationsschnittstellen, elektrische Schnittstellen und Debugschnittstellen mit Beschreibung der Funktionalität und Konfigurationsmöglichkeiten, z. B. eine Schnittstelle zur Gerätekonfiguration mit technischer Beschreibung des Protokolls (oder Protokollstacks) und aller Konfigurationsparameter, sowie Kommunikationsmatrix (Quelle, Ziel und Zweck) Informationen zu eingesetzten kryptographischen Algorithmen, dabei auch Verweis auf empfehlende Stelle und Begründung für die Wahl des Algorithmus Informationen zu eingesetzter Software mit 3rd-Party-Libraries und exakter Version Informationen zum Schutz der Integrität der Komponente, z. B. Firmware-Datei-Integrität (Begriff aus [IEC62442-4-1]: product integrity verification mechanisms)	
SL-2	wie SL-1	
SL-3	zusätzlich internes Design, u.a.: Nennung von Subsystemen und Modulen mit Funktionalität und externen Konfigurationsmöglichkeiten und zusätzlich Beschreibung der Sicherheitsarchitektur Auflistung aller verwendeten System-Benutzer der Komponente. Diese müssen sich auch in der Dokumentation wiederfinden.	
SL-4	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 Konformitätsbewertung und Schwachstellenanalyse aufgegriffen werden. Das erfolgte Threat Modeling (SR-2) MUSS bei der Prüfung der erfolgten Design-Entscheidungen mit beachtet werden und auf Schlüssigkeit geprüft 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 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)
- Beschreibung der Defense-in-Depth-Strategie der Komponente (SG-1)
- Geforderte Maßnahmen des Defense-in-Depth-Konzepts an die operationelle Einsatzumgebung (SG-2)
- Durchführung von Security Härtungen durch Komponenten-Konfiguration (SG-3), u.a. wie kann die gehärtete Minimalkonfiguration (CR 7.7 least functionality) konfiguriert werden
- 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, und dass die Anwender-Dokumentation widerspruchsfrei ist.

2.5 Konformitätsbewertung

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 werden Akzeptanzkriterien definiert, die im Rahmen der Testfallerstellung als Testerwartung aufgegriffen werden. 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.

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 C)
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)

Die Testerwartung beschreibt das anzunehmende Testergebnis, welches bei korrektem Verhalten der Komponente auftritt. Die Testerwartung MUSS sich aus dem intendierten Verhalten der Komponente und den Akzeptanzkriterien ergeben. Das Testergebnis ist das effektiv, festgestellte Verhalten der getesteten Komponente entsprechend der durchgeführten Testschritte. Die Wahl der technischen Implementierung MUSS angemessen zur gewählten SL-Stufe (im Sinne der Resistenz) sein, dies ist über die Design-Dokumentation darzustellen, siehe Prüfpunkt Dokumentation (Design) in Kapitel 2.3. Im Rahmen der Konformitätsbewertung MUSS geprüft werden, ob die gewählte technische Implementierung korrekt umgesetzt wurde. Die Testbeschreibung MUSS Details der technischen Implementierung ausreichend reflektieren. Die abschließende Beurteilung, ob die technische Implementierung der geforderten Stufe entspricht, findet final im Prüfschritt 5 Schwachstellenanalyse statt.

Falls das Testergebnis der Testerwartung entspricht, fällt die Bewertung entsprechend positiv aus (pass). Falls das Testergebnis abweicht, fällt die Bewertung negativ aus (fail).

Falls für eine CR kein Testfall spezifiziert werden kann, falls bspw. ein Aspekt der Implementierung nicht über eine externe Schnittstelle angesprochen werden kann, MUSS in diesen Fällen ein alternativer Nachweis der korrekten Umsetzung erbracht werden. Hierzu KANN ein Review der zugehörigen Design-Dokumentation mit Fokus auf das jeweilige CR unter Beachtung der Akzeptanzkriterien durchgeführt werden. Die Detailtiefe der Design-Dokumentation MUSS entsprecht detailliert sein. Es MUSS ein begründetes Votum des Prüfers vorliegen, der die Einhaltung der Akzeptanzkriterien bestätigt.

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 CRC (protection against casual or coincidental manipulation) - use of standardized cryptographic protocol - use of recommended protocols (e.g. BSI TR-02102), see CR4.3
3	Komponenten-spezifisch, Prüfdokumentation	Testfälle für angenommene Kommunikations-protokolle HTTPS und FTP mit einer fiktiven Komponente	Test description: Connections for 1) Test HTTPS against 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 ist es, festzustellen, ob die Komponente keine bekannten und ausnutzbaren Schwachstellen beinhaltet. Zudem soll betrachtet werden, ob Security Eigenschaften über Mechanismen implementiert wurden, welche eine ausreichende Resistenz gegenüber einem angenommenen Angreifertyp (definiert über die SL-Stufe) bieten. Eine ausreichende Resistenz liegt vor, wenn nur Angriffe skizziert werden können, welche oberhalb der behaupteten Resistenz zu finden sind. Die dazu genutzte Bewertungsmethodik wird im Folgenden dargestellt.

Die Identifizierung von Schwachstellen KANN über verschiedene Phasen der Komponentenentwicklung integriert werden. Folgende Praktiken der IEC 62443-4-1 können hierzu genutzt werden:

- Threat model (SR-2)
- Threat mitigation testing (SVV-2)
- Vulnerability testing (SVV-3)
- Penetration testing (SVV-4)

Ein Prüfer MUSS entsprechend der jeweiligen Prüfungsrolle (Erst-, Zweit- oder Drittpartei) die notwendige Unabhängigkeit in der Durchführung und Bewertung der jeweiligen Ergebnisse einnehmen (SVV-5).

Zudem KANN der zuvor beschriebene Prüfschritt „Konformitätsbewertung“ genutzt werden, 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

Unabhängig von Phase und Methode MUSS das Ziel erreicht werden, dass alle bekannten und ausnutzbaren Schwachstellen identifiziert und zu bewertet werden.

Die Bewertung der Schwachstellen MUSS zu der Aussage führen, dass zum Zeitpunkt des Abschlusses der Prüfung keine Schwachstellen bekannt sind, die mit dem angenommenen Angreifertyp erfolgreich ausnutzbar sind.

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, welches alle relevanten Faktoren für einen Angriff berücksichtigt. Das vorliegende Prüfschema gibt das Bewertungsmodell nicht vor.

Das genutzte Bewertungsmodell MUSS die nachfolgend benannten Eigenschaften erfüllen. In Anhang D des vorliegenden Prüfschemas wird ein Bewertungsmodell auf Basis der [CEM] Methodik definiert und erläutert.

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.

Die gewählte Bewertungsmethodik MUSS sicherstellen, dass ein skizzierter Angriff mit Angriffspfad eindeutig oberhalb der Schwelle einer Resistenzstufe, also oberhalb SL-1 bis SL-3, liegen muss. Dies

KANN durch die Auswahl einer Quantifizierung oder durch Kategorien erfolgen. Es SOLLTE hierfür auf standardisierte Verfahren zurückgegriffen werden, um eine Vergleichbarkeit der Prüfungsaussage zu unterstützen.

Für die inhaltliche Bewertung der Angriffspfade SOLLTE auch die Design-Dokumentation herangezogen werden. Für die Bewertung möglicher Gegenmaßnahmen SOLLTE die Sicherheitsarchitektur betrachtet werden (SD-2).

Folgende Liste an Bewertungsaspekten MUSS in der gewählten Bewertungsmethodik eines kompletten Angriffs zumindest indirekt genutzt werden:

- Zeitbedarf (sowohl zur Entwicklung des Angriffs sowie zur Durchführung)
- Expertise
- Wissen über die Komponente (z. B. öffentlich zugänglich oder nur im Entwicklungsteam)
- Möglichkeit zur Ausnutzung (window of opportunity)
- Ausstattung / Equipment des Angreifers

Ein Beispiel zur Anwendung auf Basis der vorgeschlagenen [CEM] Methodik findet sich zudem in Anhang D.

Optional kann zusätzlich auch noch eine Bewertung gefundener Schwachstellen nach CVSS durchgeführt werden. Diese Betrachtung beachtet allerdings nicht den vollständigen Angriffspfad im oben genannten Sinne und nicht den Verwendungszweck der Komponente und bietet damit nur eine Einstufung einer vorgefundenen Schwachstelle. Diese Bewertung kann aber wiederum hilfreich sein, identifizierte Schwachstellen mit einer Kritikalität für den weiteren Entwicklungsprozess der Komponente zu versehen. Ein Prüfer KANN diese Information optional angeben. CVSS ist eine Metrik zur Bewertung der Kritikalität gefundener Schwachstellen.

3 Prüfungsablauf

3.1 Konformitätsbewertung

Eine Konformitätsbewertung im Rahmen einer Zertifizierung MUSS von spezialisierten Prüfstellen mit Fachkompetenz 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.

Die Qualifizierung der eingesetzten Prüfer MUSS sich bezogen auf die vorhandene Fachkompetenz am gewählten SL-Level (im Sinne Angriffsresistenz) orientieren.

Die Unabhängigkeit der eingesetzten Prüfer MUSS den Anforderungen der [IEC62442-4-1] entsprechen (SVV-5: Independence of testers).

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

In diesem Dokument werden explizit nur vollständige Akzeptanzkriterien für die Prüfungsdurchführung angegeben. Gegebenenfalls KÖNNEN im Rahmen einer Konformitätsbewertung auch Feststellungen wie "nicht anwendbar" (not applicable) zugelassen werden, dies liegt allerdings außerhalb des Fokus dieses Prüfschemas. Beispielsweise KÖNNEN bei einem angenommenen Bedrohungsszenario mit nur logischen Angriffen, physische Security Eigenschaften eventuell ausgeschlossen werden. In diesem Dokument wird die vollständige technische Prüfung adressiert.

Das Ergebnis einer positiven Konformitätsbewertung ist die Bestätigung der Fähigkeit einer Komponente, also des SL-C.

3.2 Zertifizierung

Für den Fall einer Zertifizierung (außerhalb IECEE) nach dem Normteil IEC 62443-4-2 SOLLTE das vorliegende Prüfschema herangezogen und eingebunden werden.

(geplant) Für den Fall einer IECEE-Zertifizierung MUSS das vorliegende Prüfschema verpflichtend angewandt werden.

Im Rahmen von Zertifizierungen MUSS die Fachkompetenz der Prüfer entsprechend der Anforderungen der ISO/IEC 17025 nachgewiesen werden.

3.3 Andere Prüfverfahren

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

- technische Assessments in Lieferanten-Auftragnehmer-Beziehungen (Zweitparteienbewertung)
- interne Prüfung der technischen Fähigkeiten und Resistenz der eigenen Komponente durch eine organisationseigene Prüfabteilung (Erstparteienbewertung)

3.4 Durchführung der Prüfung

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

Des Weiteren MUSS die Fachkompetenz der an der Prüfung beteiligten Prüfexperten nachgewiesen werden. Dies MUSS im Vorfeld einer Prüfung erfolgen.

4 Anhang A (normativ) - Komponentenspezifikation

4.1 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)". Die Prüfung dieser Angaben erfolgt im Schritt „Prüfung des Verwendungszwecks“, siehe Kapitel 2.2.

4.2 Beschreibung der Komponente / Konformitätsbehauptung

- Kurzbeschreibung der Komponente
- Identifizierung der Komponente
- Bezeichnung der Komponente
- Version
- Identifizierungsmöglichkeit im Betrieb während der Installation und bei einem Update
- Integritätsnachweis der Komponente, primär Software (SM-6)
- Komponentenkategorie
  - entsprechend IEC 62443-4-2: Software Application, Embedded Component, Host Component oder Network Component
- Ausgeschlossener Produktumfang der Komponente
- Funktionalitäten der Komponente, die nicht betrachtet werden
  - standardmäßig deaktiviert
  - nur für Sonderfälle aktiviert und dann nicht im Fokus der Konformitätsbewertung
- Deklaration der Sicherheitsanforderungen
  - über eine SL-Stufe: SL-1, SL-2, SL-3 oder SL-4

  oder
  - über eine Auflistung einzelner Anforderungen, mit Angabe möglicher ergänzter Anforderungen (requirement enhancements)
- Angabe zum betrachteten Angreifertyp (Resistenzstufe)
  - über eine SL-Stufe: SL-1, SL-2, SL-3 oder SL-4 (analog zur Konformitätsbehauptung oder abweichend, in der Regel nur höher)

  oder
  - über eine Beschreibung des Angreifers (basierend auf IEC 62443-Definition)

4.3 Verwendungszweck

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

4.4 Dokumentation

Anwender-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)
  - Defense-in-Depth-Maßnahmen der Komponente (SG-1)

- Defense-in-Depth-Maßnahmen der operationellen Einsatzumgebung (SG-2)
- Informationen für Sicherheitshärtung (SG-3)
- Informationen zur sicheren Außerbetriebnahme (SG-4)
- Informationen zum sicheren Betrieb (SG-5)
- Informationen zum Account Management (SG-6)

Design-Dokumentation:

- für SL-1 bis SL-3
    - Beschreibung aller externen Schnittstellen,
        - alle kabelgebundenen und funkbasierten Kommunikationsschnittstellen, elektrische Schnittstellen und Debugschnittstellen mit Beschreibung der Funktionalität und Konfigurationsmöglichkeiten, z. B. eine Schnittstelle zur Gerätekonfiguration mit technischer Beschreibung des Protokolls (oder Protokollstacks) und aller Konfigrationsparameter, sowie Kommunikationsmatrix (Quelle, Ziel und Zweck)
    - Informationen zu eingesetzten krypto-graphischen Algorithmen, dabei auch Verweis auf empfehlende Stelle und Begründung für die Wahl des Algo-rithmus
    - Informationen zu eingesetzter Software mit 3rd-Party-Libraries und exakter Version
    - Informationen zum Schutz der Integrität der Komponente, z. B. Firmware-Datei-Integrität (Begriff aus [IEC62442-4-1]: product integrity verification mechanisms)

- für SL-3
    - Nennung von Subsystemen und Modulen mit Funktionalität und externer Konfigurationsmöglichkeiten
    - Beschreibung der Sicherheitsarchitektur
    - Auflistung aller verwendeten System-Benutzer der Komponente

5 Anhang B (normativ) - Anforderungen an Prüfdokumentation

5.1 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 Komponenten 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.

5.2 Übersicht zur Prüfung

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

5.3 Bewertung der Design-Dokumentation

- Ergebnisse der Design-Dokumentations-Prüfung

5.4 Prüfung der Anwender-Dokumentation

- Ergebnisse der Anwender-Dokumentations-Prüfung

5.5 Testergebnisse der Konformitätsbewertung

- Detaillierte Testergebnisse
- Übersicht/Zusammenfassung der Testergebnisse

5.6 Schwachstellenanalyse

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

5.7 Gesamtbewertung

- Übersicht der Prüfergebnisse
- Votum der Prüfstelle, d.h. Zusammenfassung über die Einhaltung aller Anforderungen
- Empfehlungen der Prüfstelle (u.a. bezogen auf Schwachstellen)

6 Anhang C (normativ) - Akzeptanzkriterien

6.1 Vorbemerkung

Die Anforderungen werden nachfolgend im ursprünglichen englischen Text angegeben, da geplant ist das vorliegende Prüfschema zukünftig zu übersetzen und international einzubringen, siehe Kapitel 3.2 "Zertifizierung".

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

6.2 FR-1: Identification and Authentication Control

ID	Requirement	SL-1	SL-2	SL-3
CR 1.1	Human user identification and authentication	Accept: - authentication of human users on all interfaces with human access	Accept: - unique authentication for every human user on all interfaces, for example with username and password	Accept: - capability to employ multifactor authentication for all human user access to the component
CR 1.2	Software process and device identification and authentication	no requirements	Accept: - the component identifies itself and authenticates 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 - no recommended encryption (e.g. BSI TR-02102)

CR 1.3	Account management	Not relevant if only one fixed administrative account is implemented on the component. Accept: - capability to integrate into a higher level account management system - account management capability (only by authorized users, including adding, activating, modifying, disabling and removing accounts) - the core functionality of the component is not affected by an availability problem of the higher-level system Not accept: - no capability to enable/disable accounts	no additional requirements	no additional requirements
CR 1.4	Identifier management	Not relevant if only one fixed administrative account is implemented on the component. 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	no additional requirements

CR 1.5	Authenticator management	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	no additional requirements	Accept: - authenticators are protected via hardware mechanisms (e.g. Password protected memory, OTP memory, hardware data integrity checks, and device security boot mechanism) Not accept: - no hardware protection mechanism
CR 1.6	Wireless access management	Network Component Requirement Accept: - capability to identify and authenticate all users (human, software processes and devices) engaged in wireless communication	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	Accept: - enforce configurable password strength based on minimum length and variety of character types - configurable password strength according to internationally recognized and proven password guidelines, e.g. NIST SP800-63-2, BSI TR-02102 - external authentication	no additional requirements	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 - external authentication 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	no requirements	Relevant if PKI or public keys are in use. 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	no requirements	Relevant if PKI or public keys are in use. 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 mechanisms (e.g. smart cards) Not accept: - no additional protection mechanisms
CR 1.10	Authenticator feedback	Accept: - sensitive data concerning the authentication process is obscured Not accept: - feedback not distinguish between wrong password or wrong username - no timing differences for error and no error response - displaying password, wireless key, SSH token in input field instead of asterisks - usage of WEP	no additional requirements	no additional requirements

CR 1.11	Unsuccessful login attempts	Accept: - capability to enforce, for each user type (human, software, device), a configurable limit of consecutive invalid access attempts performed in a configurable time period - capability to deny access for a specified period of time or until unlocked, when limit reached	no additional requirements	no additional requirements
CR 1.12	System use notification	Accept: - capability to display a system use notification message before authenticating to the local user interface - capability as an authorized user to configure the message	no additional requirements	no additional requirements
CR 1.13	Access via untrusted networks	Network Component Requirement 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	no additional requirements	Accept: - deny access requests via untrusted networks unless approved by an assigned role - for each connection a device-internal or external physical key is used to authorize the connection
CR 1.14	Strength of symmetric key-based authentication	no requirements	Relevant if symmetric key authentication (e.g. pre-shared-secrets) is used. 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	Accept: - control system provides the capability to protect the relevant shared keys via hardware mechanisms

			- ensure that the algorithms and keys used comply with CR 4.3 (Use of cryptography)	

6.3 FR-2: Use Control

ID	Requirement	SL-1	SL-2	SL-3
CR 2.1	Authorization enforcement	Accept: - authorization mechanism is enforced on all interfaces which can accessed by human users based on their responsibilities, as dictated by the least privilege principle Not accept: - interface without authorization mechanism (e.g. HMI, web interface, console)	Accept: - authorization mechanism on all interfaces which are exposed, independent of user type (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	Accept: - capability to deny critical action via wireless connection (i.e. only use wired) - monitor devices	no additional requirements	no additional requirements
CR 2.3	Use control for portable and mobile devices	no requirements	no additional requirements	no additional requirements

CR 2.4	Mobile code	Only relevant if components allows to execute mobile code. 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 Embedded Component Requirements - only upload to device - perform integrity checks on the code prior to code execution - perform authenticity checks to verify origin prior to code execution	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	no additional requirements
CR 2.5	Session lock	Accept: - for HMI (local or via network): - Session Lock after configurable time period of inactivity - option to explicitly disable Session Lock (e.g. in control room scenarios) - 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	no additional requirements
CR 2.6	Remote session termination	no requirements	Remote session is interpreted as logical network session. Accept: - remote session terminated by user who initiated session (minimum requirement) - remote session manually terminated by a local authority/user	no additional requirements

			- remote session terminated after configurable inactive period of time	
CR 2.7	Concurrent session control	no requirements	No requirements	Accept: - ability to limit the number of session per interface for any user Not accept: - Sessions cannot be limited per interface - Sessions cannot be limited per user
CR 2.8	Auditable events	Accept: - audit records for following security relevant cases are generated: access control, request errors, control system events, backup and restore events, configuration changes, audit log events - audit records include at least the following information: timestamp, source, category, type, event ID, event result	no additional requirements	no additional requirements
CR 2.9	Audit storage capacity	Accept: - capability to allocate audit record storage Not accept: - failure of audit functionality when a threshold is reached or the storage capacity is exceeded	no additional requirements	Accept: - a warning message informs when a configurable threshold is reached Not accept: - no warning is produced if the used storage capacity reaches the threshold - the hreshold not configurable
CR 2.10	Response to audit processing failures	Accept: - no loss of essential services or functions during an audit processing failure - optional support of	no additional requirements	no additional requirements

		appropriate actions in response to an audit processing failure - e.g. alerting personnel could be an appropriate action		
CR 2.11	Timestamps	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 server	no additional requirements
CR 2.12	Non-repudiation	Relevant if HMI is used. Accept: - possibility to determine which human user took a particular action - logging user id in audit trail	no additional requirements	no additional requirements
CR 2.13	Use of physical diagnostic and test interfaces	No requirements	Exempt are software applications 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

6.4 FR-3: System Integrity

ID	Requirement	SL-1	SL-2	SL-3
CR 3.1	Communication integrity	Accept: - capability to protect integrity of transmitted information - use of CRC (protection against casual or coincidental manipulation) - use of standardized cryptographic protocol - use of recommended protocols (e.g. BSI TR-02102), see CR4.3	Accept: - capability to authenticate information during communication Not accept: - use of error detection codes, weak hashing or weak signature functions - authentication of information is not possible - fallback to not recommended protocols	no additional requirements
CR 3.2	Protection from malicious code	Software Application Component Accept: - list at least one compatible security component which implements the protection functionality (user documentation requirement)	no additional requirements	no additional requirements
		Embedded Component Accept: - capability to protect from installation and execution of unauthorized software - environment is allowed to provide malicious code protection mechanism, has to be required by component intended -use description (user documentation requirement) - allowed detection techniques: binary integrity, attributes monitoring, hashing, signature techniques - allowed prevention techniques (e.g. removable media control, sandbox techniques, specific computing platforms mechanisms (e.g. restricted firmware	no additional requirements	no additional requirements

		update), No Execute (NX) bit, data execution prevention (DEP), address space layout randomization (ASLR), stack corruption detection. mandatory access controls) Not accept: - reference to IACS capabilities which are not implemented by the component itself		
		Host Component Accept: - need to support the use of malicious code protection (design documentation requirement)	Accept: - able to automatically report version of the malicious code protection which is actually in use	no additional requirements
		Network Component Accept: - provided by the network device directly - allowed to use compensating control	no additional requirements	no additional requirements
CR 3.3	Security functionality verification	Accept: - definition of (manual) verification procedures for verifying the 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, no notification	no additional requirements	no additional requirements

CR 3.4	Software and information integrity	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: - authenticity check of data at rest (e.g. software, configuration)	Accept: - unauthorized change is reported to a configurable entity upon discovery of the attempt
CR 3.5	Input validation Note: Not-accept-criteria give guidance which insufficient input validation methods are most relevant for the SL levels to plan test cases with reasonable effort.	Accept: - every input, that directly impacts the action of the application or device is validated for syntax and content Not accept: - out-of-range values for a defined field type - invalid characters in data fields - missing or incomplete data and buffer overflow	Not accept: - SQL injection attacks - cross-site scripting - commonly known malformed packets	Not accept: - malformed packets as commonly generated by protocol fuzzers
CR 3.6	Deterministic output	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	no additional requirements
CR 3.7	Error handling	Accept: - error conditions are identified and handled - no unintended information is leaked - no security relevant information is visible	no additional requirements	no additional requirements

CR 3.8	Session integrity	no requirements	Accept: - use of mechanisms to protect the integrity of communication sessions - sessions are invalidated after termination - sessions are invalidated after reboot - use of unique session IDs Not accept: - session hijacking - man in the middle attack - insertion of false information into a session - replay attacks	no additional requirements
CR 3.9	Protection of audit information	no 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	Accept: - capability to be updated and upgraded once commissioned - 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	no additional requirements
CR 3.11	Physical tamper resistance and detection	no requirements	Not relevant in case of software applications. Relevant if intended use does not offer physical protection of component according to threat modelling. Accept: - anti-tamper resistance: specialized materials to make tampering difficult; e.g.: hardened enclosures, locks, encapsulation, security screws - detection mecha-	Accept: - capability to automatically notify upon discovery of an attempt to make an unauthorized physical access

			nisms for unauthorized physical access into the device, e.g. seal	
CR 3.12	Provisioning product supplier roots of trust	no requirements	Not relevant in case of software applications. 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	no requirements	Not relevant in case of software applications. Relevant if CR 2.4 Mobile Code is selected. 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	Not relevant in case of software applications. Accept: - integrity verification of boot process relevant firmware, software and configuration data prior to the use	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

6.5 FR-4: Data Confidentiality

ID	Requirement	SL-1	SL-2	SL-3
CR 4.1	Information confidentiality	Accept: - capability to protect against unauthorized disclosure of information via **eavesdropping or casual exposure** - capability to protect the confidentiality of information at rest for which explicit read authorization is supported - protection of the confidentiality of information in transit - (wireless) use of encryption Not accept: - outdated or deprecated encryption protocols - use of cleartext protocols (e.g. FTP)	Accept: - capability to protect against unauthorized disclosure of information caused by an attacker actively searching for vulnerabilities with **low resources, generic skills and low motivation**	Accept: - capability to protect against unauthorized disclosure of information caused by an attacker actively searching for vulnerabilities with **moderate resources, IACS specific skills and moderate motivation**
CR 4.2	Information persistence	no requirements	Accept: - capability to purge component - capability to erase all information with explicit read authorization Not accept: - existence of data after component was decommissioned	Accept: - capability to protect against unauthorized and unintended information transfer via volatile shared memory resources - capability to verify that the erasure of information occurred effectively
CR 4.3	Use of cryptography	If cryptography is required by CR 1.14, CR 3.1 and CR 4.1. Accept: - use of standardized cryptographic protocol - use of recommended protocols (e.g. BSI TR-02102), see CR4.3 - used according to proven practic-	no additional requirements	no additional requirements

		es or documentation		

Tabelle 9

6.6 FR-5: Restricted Data Flow

ID	Requirement	SL-1	SL-2	SL-3
CR 5.1	Network segmentation	Network Component Requirement Accept: - support of network segmentation, e.g. multiple network cards, VLANs - network configuration with routing and router capability	no additional requirements	no additional requirements
		Non-Network Component Requirement Not Accept: - component opens or requires network connections that make a network segmentation non-feasible or hard to maintain		

CR 5.2	Zone boundary protection	Network Component Requirement 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	Accept: - capability to deny network traffic by default - allow network traffic by exception	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	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 application-level gateways Not accepted: - no/insufficient traffic inspection	no additional requirements	no additional requirements

Tabelle 10

6.7 FR-6: Timely Response To Events

ID	Requirement	SL-1	SL-2	SL-3
CR 6.1	Audit log accessibility	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 to unauthorized users	no additional requirements	Accept: - programmatic access to audit records by either using an application programming interface (API), or - capability to send the audit logs to a centralized system
CR 6.2	Continuous monitoring	no requirements	Accept: - capability to provide an active interface for continuous monitoring, or - capability to send continuous monitoring information to a centralized system	no additional requirements

Tabelle 11

6.8 FR-7: Resource Availability

ID	Requirement	SL-1	SL-2	SL-3
CR 7.1	Denial of service protection	Accept: - capability to operate in a degraded mode (essential functions) during a DoS event	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	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	no additional requirements
CR 7.3	Control system backup	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	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	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 set-	no additional requirements	no additional requirements

		tings - recovery uses a backup selected explicitly by an authorized person or the recovery uses an internal authentic backup source		
CR 7.5	Emergency power	no requirements	no additional requirements	no additional requirements
CR 7.6	Network and security configuration settings	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	no additional requirements	Accept: - capability to generate a report listing the currently deployed security settings in a machine-readable format
CR 7.7	Least functionality	Accept: - capability to restrict the use of unnecessary functions, ports, protocols and/or services (security-by-configuration) - functions beyond a baseline configuration should be able to be deactivated	no additional requirements	no additional requirements
CR 7.8	Control system component inventory	no 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

7 Anhang D (informativ) – Methoden zur Schwachstellenbewertung

7.1 Einführung

Der Prüfschritt der Schwachstellenanalyse bedingt die Bewertung von möglichen Angriffen hinsichtlich der gewählten SL-Stufe (im Sinne Angriffsresistenz). Das zu nutzende Bewertungsmodell wird nicht im vorliegenden Prüfschema fest vorgegeben. Die Anforderungen an das Bewertungsmodell sind in Kapitel 2.6 zu finden.

Nachfolgend wird das Bewertungsmodell nach [CEM] Methodik eingeführt, dieses erfüllt alle definierten Anforderungen an ein Bewertungsmodell für die Schwachstellenanalyse.

7.2 AVA/CEM Bewertung

Als Bewertungsmodell hat sich 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.

Die Methode hat nicht das Ziel Schwachstellen oder Angriffe zu identifizieren. Die Methode dient nur dazu skizzierbare Angriffspfade zu bewerten.

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

SL-Stufe	**Schwelle für ausreichende Resistenz**	**Kommentar**
SL-1	> 0	angenommenes Angriffspotential betrifft nur nicht gezielte Angriffe; umgekehrt bedeutet dies, dass damit gefundene Schwachstellen gegen eine explizite Anforderung (CR) verstoßen müssen, um im Rahmen einer Prüfung nach SL-1 bewertet zu werden
SL-2	> 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	> 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	-	nicht relevant für Prüfschema in dieser Version

Tabelle 5

Folgende Eigenschaften werden 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

Die Spalte "Schwelle für ausreichende Resistenz" ist so zu lesen, dass ein skizzierbarer Angriff oberhalb dieser Schwelle liegen MUSS, damit die Komponente in entsprechender SL-Stufe als ausreichend resistent bezeichnet werden kann.

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

7.3 Beispiel einer Bewertung nach AVA/CEM

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.

8 Anhang E (informativ) – Übersicht zur Nutzung der Ergebnisse des IEC 62443-4-1 Entwicklungsprozesses

Practice 1	**Security Management**	**Nutzung im Prüfschema**
SM-1	Development Process	keine[1]
SM-2	Identification of repsonsibilities	keine
SM-3	Identification of applicability	keine
SM-4	Security expertise	keine
SM-5	Process scoping	keine
SM-6	File integrity	Prüfung Design-Dokumentation, siehe 2.3
SM-7	Development environment security	keine
SM-8	Controls for private keys	keine
SM-9	Security requirements for externally provided components	Prüfung Design-Dokumentation, siehe 2.3
SM-10	Custom development components from third-party suppliers	Prüfung Design-Dokumentation, siehe 2.3
SM-11	Assessing and addressing security-related issues	keine
SM-12	Process Verification	keine
SM-13	Continuous improvement	keine
Practice 2	**Specification of security requirements**	
SR-1	Product security context	Prüfung des Verwendungszwecks, siehe 2.2
SR-2	Threat model	Prüfung des Verwendungszwecks, siehe 2.2 Schwachstellenanalyse, siehe 2.6
SR-3	Product security requirements	Konformitätsbewertung, siehe 2.5
SR-4	Product security requirements content	Prüfung des Verwendungszwecks, siehe 2.2
SR-5	Security requirements review	Konformitätsbewertung, siehe 2.5, Rolle Tester
Practice 3	**Secure by design**	
SD-1	Secure design principles	Umgesetzte Security Eigenschaften an Schnittstellen, betrifft Prüfung De-

[1] *keine Nutzung im Prüfschema* ist so zu lesen, dass keine direkten Ergebnisse (deliverables) im Produkt oder den Design-Dokumenten ablesbar sind.

		sign-Dokumentation, siehe 2.3
SD-2	Defense in depth design	Schwachstellenanalyse, siehe 2.6
SD-3	Security design review	Umgesetzte Security Eigenschaften (Details ab SL-3 gefordert), betrifft Prüfung Design-Dokumentation, siehe 2.3
SD-4	Secure design best practices	Umgesetzte Security Eigenschaften (Details ab SL-3 gefordert), betrifft Prüfung Design-Dokumentation, siehe 2.3
Practice 4	**Secure implementation**	
SI-1	Security implementation review	keine
SI-2	Secure coding standards	keine
Practice 5	**Security verification and validation testing**	
SVV-1	Security requirements testing	Konformitätsbewertung, siehe 2.5
SVV-2	Threat mitigation testing	Schwachstellenanalyse, siehe 2.6
SVV-3	Vulnerability testing	Schwachstellenanalyse, siehe 2.6
SVV-4	Penetration testing	Schwachstellenanalyse, siehe 2.6
SVV-5	Independence of testers	Schwachstellenanalyse, siehe 2.6 Konformitätsbewertung, siehe 3.1
Practice 6	**Management of security-related-issues**	
DM-1	Receiving notifications of security-related issues	keine
DM-2	Reviewing security related issues	keine
DM-3	Assessing security-related issues	keine
DM-4	Adressing security-related issues	keine
DM-5	Disclosing in security-related issues	keine
DM-6	Periodic review of security defect management practice	keine
Practice 7	**Security update management**	
SUM-1	Security update qualification	keine
SUM-2	Security update documentation	Prüfung Dokumentation (Anwender), siehe 2.4
SUM-3	Dependent component or operating system security update documentation	Prüfung Dokumentation (Anwender), siehe 2.4
SUM-4	Security update delivery	keine
SUM-5	Timely delivery of security patches	keine

Practice 8	**Security guidelines**	
SG-1	Product defense in depth	Prüfung Dokumentation (Anwender), siehe 2.4
SG-2	Defense in depth measures expected in the environment	Prüfung Dokumentation (Anwender), siehe 2.4
SG-3	Security hardening guidelines	Prüfung Dokumentation (Anwender), siehe 2.4
SG-4	Secure disposal guidelines	Prüfung Dokumentation (Anwender), siehe 2.4
SG-5	Secure operation guidelines	Prüfung Dokumentation (Anwender), siehe 2.4
SG-6	Account management guidelines	Prüfung Dokumentation (Anwender), siehe 2.4
SG-7	Documentation review	Prüfung Dokumentation (Anwender), siehe 2.4

9 Anhang F (informativ) – Übersicht der Ergänzungen zur Norm

Zielsetzung des Prüfschemas ist es, dass langfristig keine zusätzlichen Anforderungen als in der selbst Norm definiert gefordert werden.

Da aus Sicht der Prüfung bezogen auf den aktuellen Stand der Normteile IEC 62443-4-2 und IEC 62443-4-1 noch weitere Details benötigt werden, um vergleichbare Prüfungen durchführen zu können, werden in diesem Dokument teilweise präzisierte Anforderungen definiert. Diese Ergänzungen werden an dieser Stelle aufgelistet:

- Komponentenspezifikation entsprechend Anhang A
- Akzeptanzkriterien entsprechend Anhang C
    - geänderte Akzeptenzkriterien im Vergleich zu CR des Normteils IEC 62443-4-2:
        - CR 3.5: Komplexität der referenzierten Verfahren SL-Stufen zugeordnet
        - CR 4.1: Ansteignde Mechanismenstärke der eingesetzten Verfahren aufgrund SL-Stufe (im Sinne Angriffsresistenz)
        - CR 5.1: Unterscheidung zwischen Network Component und anderen Komponententypen
- Forderung einer je SL-Stufe (im Sinne Angriffsresistenz) angemessenen Umsetzung von Anforderungen (CR), welche denen keine gestuften Anforderung (RE, Requirement Enhancements) definiert sind (beispielsweise CR 4.1), siehe Kapitel 2.3

10 Abkürzungsverzeichnis

Abkürzung	Bedeutung
CVSS	Common Vulnerability Scoring System
EDR	Embedded Device Requirement
DM	Defect management (Abkürzung aus IEC 62443-4-1)
PKI	Public Key Infrastructure
SD	Security by design (Abkürzung aus IEC 62443-4-1)
SG	Security guidelines Abkürzung aus IEC 62443-4-1)
SI	Security Implementation (Abkürzung aus IEC 62443-4-1)
SM	Security management (Abkürzung aus IEC 62443-4-1)
SR	Security requirements (Abkürzung aus IEC 62443-4-1)
SUM	Security update management (Abkürzung aus IEC 62443-4-1)
SVV	Security verification and validation testing (Abkürzung aus IEC 62443-4-1)

11 Literaturverzeichnis

[IEC62442-3-3] IEC 62443-3-3:2013

[IEC62442-4-1] IEC 62443-4-1:2018

[IEC62442-4-2] IEC 62443-4-2:2019

[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

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

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:

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
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.