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

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

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)