IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung
Prüf- und Zertifizierungsstelle im DGUV Test

Grundsätze für die Prüfung und Zertifizierung von Security-Aspekten in der funktionalen Sicherheit von industriellen Automatisierungssystemen

Stand 01.2020

Prüfgrundsatz

GS-IFA-M24

Institut für Arbeitsschutz der DGUV
Prüf- und Zertifizierungsstelle im DGUV Test
Alte Heerstr. 111
53757 Sankt Augustin

GS-IFA-M24

Inhaltsverzeichnis

Versionshistorie

Version	Datum	Bearbeitungsinhalt	Bearbeiter
1.0	15.01.2020	Ersterstellung	Werner
1.1	16.04.2020	Überarbeitung nach Kommentierung	Werner

Vorwort:

Der hier vorliegende Prüfgrundsatz ist eine Gemeinschaftsarbeit der folgenden Prüf- und Zertifizierungsstellen im DGUV Test:

- Prüf- und Zertifizierungsstelle Druck und Papierverarbeitung (DP)
  Fachbereich Energie Textil Elektro Medienerzeugnisse
- Prüf- und Zertifizierungsstelle Elektrotechnik (ET)
  Fachbereich Energie Textil Elektro Medienerzeugnisse
- Prüf- und Zertifizierungsstelle Hebezeuge, Sicherheitskomponenten und Maschinen (HSM)
  Fachbereich Holz und Metall
- Institut für Arbeitsschutz der DGUV (IFA), Prüf- und Zertifizierungsstelle im DGUV Test
- Prüf- und Zertifizierungsstelle Maschinen und Fertigungsautomation (MF)
  Fachbereich Holz und Metall
- Prüf- und Zertifizierungsstelle Nahrungsmittel und Verpackung (NV)
  Fachbereich Nahrungsmittel
- Prüf- und Zertifizierungsstelle Fachbereich Rohstoffe und chemische Industrie (RCI)

Jegliche Änderungen an den Inhalten des Prüfgrundsatzes muss unter den beteiligten Prüf- und Zertifizierungsstellen abgestimmt werden. Aktuelle Kontaktdaten der Prüf- und Zertifizierungsstellen sind auf der Internetseite „www.dguv.de/dguv-test“ hinterlegt.

1 Anwendungsbereich

Dieser Prüfgrundsatz findet Anwendung bei der Teil- und Gesamtprüfung sowie bei der Zertifizierung von Komponenten der funktionalen Sicherheit (Safety). Er ist dann anzuwenden, wenn die Eignung einer Safety-Komponente im Hinblick auf die Security festgestellt werden soll, kann aber nicht alleinige Prüfgrundlage sein.

HINWEIS:
In diesem Prüfgrundsatz werden Anforderungen für das Erreichen eines Security Levels 1 (SL 1) nach DIN EN 62443-3-3 beschrieben. Es besteht kein Zusammenhang zwischen einem Security Level (SL) und einem Performance Level (PL) nach DIN EN ISO 13849-1 bzw. Safety Integrity Level (SIL) nach DIN EN 61508-1.

In diesem Prüfgrundsatz wird zwischen „Hersteller von Maschinen“ (Integrator) und „Hersteller von elektronischen Komponenten“ (Komponentenhersteller) unterschieden. Im weiteren Text werden deshalb die Bezeichnungen „Integrator“ und „Komponentenhersteller“ verwendet. Maßnahmen, die von Maschinenbetreibern umzusetzen sind, werden nur insofern berücksichtigt, wie sie in Betriebsanleitungen genannt werden müssen.

HINWEIS:
Einige Anforderungen, die in diesem Prüfgrundsatz genannt werden, können vom Komponentenhersteller auf den Integrator übertragen werden. In diesem Fall müssen diese Anforderungen und ggf. Angaben, die zur Realisierung benötigt werden, dem Integrator vom Komponentenhersteller zur Verfügung gestellt werden (z. B. in der Betriebsanleitung).

1.1 Security Level

In der Normenreihe DIN EN 62443 werden insgesamt fünf Security Level genannt (SL 0 bis SL 4). Sie werden wie folgt beschrieben (siehe z. B. E DIN IEC 62443-3-3:2015):

Security Level	Beschreibung
SL 0	Keine besonderen Anforderungen oder Schutzmaßnahmen notwendig
SL 1	Schutz gegen gelegentlichen oder zufälligen Verstoß
SL 2	Schutz gegen einen absichtlichen Verstoß mit einfachen Mitteln und geringem Aufwand, allgemeinen Fertigkeiten und geringer Motivation
SL 3	Schutz gegen einen absichtlichen Verstoß mit raffinierten Mitteln und mittlerem Aufwand, automatisierungstechnischen Fertigkeiten und mittlerer Motivation
SL 4	Schutz gegen einen absichtlichen Verstoß mit raffinierten Mitteln und erheblichem Aufwand, automatisierungstechnischen Fertigkeiten und hoher Motivation

Die Security-Level (SL) beruhen nach IEC 62443-1-1 auf den folgenden sieben grundlegenden Anforderungen (FR, en: Foundational Requirement) der IT-Sicherheit:

FR 1 Identifizierung und Authentifizierung (IAC, en: identification and authentication control},
FR 2 Nutzungskontrolle (UC, en: use control},
FR 3 Systemintegrität (SI, en: system integrity),
FR 4 Vertraulichkeit der Daten (DC, en: data confidentiality),
FR 5 Eingeschränkter Datenfluss (RDF, en: restricted data flow),
FR 6 Rechtzeitige Reaktion auf Ereignisse (TRE, en: timely response to events),
FR 7 Verfügbarkeit der Ressourcen (RA, en: resource availability).

Diese grundlegenden Anforderungen werden unter Abschnitt 5 näher erläutert.

2 Normative Verweise

Grundlagen dieses Prüfgrundsatzes bilden:

IEC/TS 62443-1-1	Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models
DIN EN IEC 62443-4-1	lndustrielle Kommunikationsnetze - IT-Sicherheit für industrielle Automatisierungssysteme – Teil 4-1: Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung
DIN EN IEC 62443-4-2	lndustrielle Kommunikationsnetze - lT-Sicherheit für industrielle Automatisierungssysteme - Teil 4-2: Anforderungen an Komponenten industrieller Automatisierungssysteme

Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

3 Begriffe

3.1
eingebettetes Gerät
(en: embedded device)

Gerät, auf dem eingebettete Software läuft und das für eine direkte Überwachung, Steuerung oder Auslösung eines technischen Prozesses vorgesehen ist.
(Quelle: DIN EN IEC 62443-4-2)

3.2
Fernzugriff
(en: remote access)

Zugriff auf ein Automatisierungssystem durch beliebige Nutzer (menschliche Nutzer, Softwareprozesse oder Geräte), die von außerhalb der adressierten lT-Sicherheitszone kommunizieren.
(Quelle: DIN EN IEC 62443-4-2)

3.3
Host-Gerät
(en: host device)

Allgemein verwendbares Gerät, auf dem ein Betriebssystem läuft (z.B. Microsoft Windows oder Linux) und das eine oder mehrere Softwareanwendungen, Datenspeicher oder Funktionen eines oder mehrerer Hersteller(s) hosten kann.
(Quelle: DIN EN IEC 62443-4-2)

3.4
Industrielles Automatisierungssystem
(en: industrial automation and control system)

Zusammenstellung von Personal, Hardware, Software und Leitlinien, die in den Betrieb eines industriellen Prozesses eingebunden sind und dessen sicheren und zuverlässigen Betrieb gewährleisten oder beeinträchtigen können.
(Quelle: DIN EN IEC 62443-4-2)

3.5
Integrator

Hersteller von Maschinen, der vorgefertigte elektronische Komponenten in einer Maschine kombiniert

3.6
Integrität
(en: integrity)

Vorgesehene Funktion auf der Grundlage angegebener Anforderungen unter spezifischen Betriebsbedingungen
(Quelle: DIN EN IEC 62443-4-2)

3.7
IT-Sicherheitsfunktionen

Zusätzliche zur funktionalen Sicherheit in Soft- und/oder Hardware abgebildete Maßnahmen, die dazu dienen, den funktional sicheren Betrieb der Komponente zu gewährleisten und die angemessene Fehlerreaktion einzuleiten.

3.8
Komponentenhersteller

Hersteller von elektronischen Komponenten für die Umsetzung einer Sicherheitsfunktion in einer Maschine.

3.9
mobiler Code
(en: mobile code)

Von einem abgesetzten, möglicherweise nicht vertrauenswürdigen System über ein Netzwerk oder mittels mobiler Datenträger übertragenes Programm, welches unverändert in einem lokalen System durch den Empfänger ohne explizite lnstallation oder Nutzerbestätigung ausgeführt werden kann.
(Quelle: DIN EN IEC 62443-4-2)

3.10
Netzwerkkomponente
(en: network device)

Komponente, die den Datenfluss zwischen Geräten ermöglicht oder einschränkt, aber dabei nicht direkt mit einem Steuervorgang in Wechselwirkung tritt.
(Quelle: DIN EN IEC 62443-4-2)

3.11
nicht vertrauenswürdig
(en: untrusted)

Nichterfüllung vorher festgelegter Anforderungen an die Vertrauenswürdigkeit.
(Quelle: DIN EN IEC 62443-4-2)

3.12
Safety

Safety (funkt. Sicherheit) ist der Schutz des Menschen oder der Umwelt vor dem Produkt (z.B. Maschine).

3.13
Security

Security ist die Angriffssicherheit. Sicherheitsrelevante Daten und Funktionen eines Produktes (z.B. Maschine) sollen vor unberechtigtem Zugriff geschützt werden.

3.14
Security Level (SL)

Maß des Vertrauens, dass das industrielle Automatisierungssystem in einem definierten Grad (Level) frei von Sicherheitslücken ist und in der beabsichtigten Weise funktioniert.
(Quelle: DIN EN IEC 62443-4-2)

3.15
Schnittstelle

Eine Schnittstelle (Interface) ermöglicht die Kommunikation zwischen Systemen. Beispiele USB, Fire Wire, SCSI u.a.).

3.16
Softwareanwendung
(en: software application)

Ein oder mehrere Programme und ihre Abhängigkeiten, mit denen eine Verbindung mit dem Prozess oder dem Automatisierungssystem selbst hergestellt wird (z. B. Konfigurations-software und Historie).
(Quelle: DIN EN IEC 62443-4-2)

3.17
Portnummer

Ganzzahliger Wert zur Zuordnung welche Software die Verarbeitung eines Netzwerkpaketes übernehmen soll. Der Header eines Netzwerkpaketes kann dazu einen Quellport und einen Zielport enthalten. Die genaue Definition ist vom verwendeten Protokoll - wie etwa RFC 793 - abhängig.

3.18
vertrauenswürdig
(en: trusted)

Erfüllung festgelegter Anforderungen an die Vertrauenswürdigkeit.

3.19
Zone
(en: zone)

Zusammenfassung von Einheiten, die eine Aufteilung eines betrachteten Systems auf der Grundlage ihrer funktionalen, logischen oder physikalischen (einschließlich des Ortes) Beziehungen wiedergeben.
(Quelle: DIN EN IEC 62443-4-2)

4 Durchführung von Prüfung und Zertifizierung

4.1 Allgemeines

Die Prüfung der Security-Aspekte kann nur entweder in Kombination mit einer Zertifizierung der funktionalen Sicherheit durchgeführt werden oder auf einer bestehenden Zertifizierung der funktionalen Sicherheit aufbauen.

Die Prüfung besteht aus einer einmaligen Durchführung einzelner Prüfabschnitte sowie gegebenenfalls aus Wiederholungsprüfungen. Die einzelnen Abschnitte bei einer sicherheitstechnischen Gesamtprüfung/-zertifizierung werden in folgender Reihenfolge durchgeführt:

- Konzeptprüfung
- Baumusterprüfung
  - Prüfung auf Einhaltung der Security-Anforderungen
  - Prüfung der Anwenderdokumentation
  - Konformitätsbewertung (Zertifizierung)

Konzeptprüfungen können von der Prüf- und Zertifizierungsstelle auch als separater Vorgang durchgeführt werden. Diese werden mit einem Konzeptprüfbericht abgeschlossen und dienen als Basis für die Erstellung eines Angebots für die Baumusterprüfung und Zertifizierung.

4.2 Grundlagen und Ablauf von Prüfung und Zertifizierung

Der organisatorische Ablauf einer Prüfung/Zertifizierung ist in der DGUV Test Prüf- und Zertifizierungsordnung Teil 1: Zertifizierung von Produkten, Prozessen und Qualitätsmanagementsystemen (DGUV Grundsatz 300-003), gültig in der jeweils aktuellen Fassung, geregelt.

4.2.1 Einreichung von Unterlagen

Zu den einzureichenden Unterlagen gehören soweit zutreffend:

- Dokumentationsliste (Übersicht der eingereichten Unterlagen),
- Betriebsanleitung,
- Spezifikationen mit Blockschaltbildern und Beschreibung der jeweiligen Funktionsblöcke,
- V+V-Plan (Validierung + Verifikation),
- Spezifikation von Hardware und Software inkl. Schnittstellen,
- Security (related) requirements specification,
- Implementierte Security Maßnahmen,
- Software-Beschreibung,
- Kommentierter Source-Code,
- Dokumentation der verwendeten Tools, Sprachen bzw. Techniken,
- Deklaration und Beschreibung aller Variablen
- Ausfallarten- und Effektanalyse (FMEA),
- Wirksamkeitsanalyse der getroffenen Security Maßnahmen,
- Externe Prüfberichte, z.B. von akkreditierten Prüflaboren,
- Anwenderdokumentation,
- Security risk- and threat analysis,
- Dokumentation der empfohlenen Security Einstellungen,
- Dokumentationen zum Entwicklungsprozess,
- Spezifikation der IT-Sicherheitsanforderungen,
- Defense-in-Depth Konzept,
- Nachweis der gesicherten Implementierung,
- Beschreibung des internen Prozesses für Behandlung sicherheitsbezogener Probleme,
- Nachweis zur Verwaltung von IT-Sicherheitsupdates,
- IT-Sicherheitsrichtlinien

Die Prüfstelle kann weitere Unterlagen auch im Hinblick auf die in Abschnitt 2 aufgeführten Regelwerke anfordern.

4.2.2 Wiederholungsprüfungen

Eine Wiederholungsprüfung ist erforderlich, wenn bei der erstmaligen Prüfung Mängel festgestellt wurden. Wenn der Auftraggeber die im Prüfbericht aufgeführten Mängel beseitigt hat, unterrichtet er die Prüfstelle, ggf. unter Beifügung geeigneter Unterlagen.
Die Prüf- und Zertifizierungsstelle entscheidet, ob für eine Wiederholungsprüfung ein geändertes Baumuster vorzustellen ist oder ob die Beseitigung der Mängel durch Vorlegen geeigneter Unterlagen nachgewiesen werden kann. Nach der ersten Wiederholungsprüfung mit negativem

Ergebnis kann eine weitere Wiederholungsprüfung stattfinden. Führt auch diese zu einem negativen Ergebnis, entscheidet die Prüf- und Zertifizierungsstelle, ob das Prüfverfahren abgebrochen wird.

4.2.3 Ausstellung und Gültigkeit des Zertifikats

Die Zertifizierung erfolgt auf der Grundlage von Prüfberichten/Prüfzeugnissen der Prüfstelle sowie ggf. unter Einbeziehung von Prüfberichten/Prüfzeugnissen/Prüfzertifikaten externer zugelassener Prüfstellen. Nach positiver Bewertung des Produkts wird durch die Prüf- und Zertifizierungsstelle ein DGUV Test Zertifikat ausgestellt, dass zur Anbringung eines DGUV Test Zeichens berechtigt. Die Gültigkeit des ausgestellten Zertifikats ist auf 5 Jahre begrenzt.

5 Anforderungen

Die Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung sind in der DIN EN IEC 62443-4-1 beschrieben. Der Lebenszyklus umfasst dabei:

- die Definition von IT-Sicherheitsanforderungen,
- einen gesicherten Entwurf,
- eine sichere Implementierung (einschließlich Programmierrichtlinien),
- eine Verifikation und Validierung,
- eine Mängelbehandlung,
- ein Patch-Management,
- das Ende des Produktlebenszyklus.

Die Anforderungen aus der DIN EN IEC 62443-4-1 sind in diesem Kapitel nicht separat mit aufgeführt. Alle Anforderungen gelten unabhängig vom zu erreichenden Security Level; ein Nachweis für die Umsetzung muss erfolgen.

In den folgenden Kapiteln sind die grundlegenden Anforderungen beschrieben, die für die Erreichung eines SL 1 nach DIN EN IEC 62443-4-2 für eine Komponente der funktionalen Sicherheit zu erfüllen sind.

Es wird unterschieden zwischen Anforderungen für

- Komponenten (CR, en: component requirement),
- Softwareanwendungen (SAR, en: software application requirements),
- Eingebettete Geräte (EDR, en: embedded device requirements),
- Host-Geräte (HDR, en: host device requirement) und
- Netzwerkkomponenten (NDR, en: network device requirement)

Die implementierten Security-Maßnahmen müssen nicht den Anforderungen eines gegebenen PL/SIL genügen.

5.1 Identifizierung und Authentifikation

5.1.1 Identifizierung und Authentifikation von (menschlichen) Nutzern (CR 1.1)

Alle (menschlichen) Nutzer müssen für alle Arten eines Zugriffs auf die Komponente identifiziert und authentifiziert werden. Nicht berechtigen Teilnehmern muss auf Grundlage der geltenden IT-Sicherheitsleitlinien der Zugang beschränkt werden.
(siehe auch DIN EN IEC 62443-4-2)

5.1.2 Nutzerkontenverwaltung (CR 1.3)

Alle verwendeten Nutzerkonten müssen entweder von der Komponente selbst oder durch eine übergeordnete Ebene verwaltet werden. Ein Ausfall der Verwaltung darf nicht zu einem gefahrbringenden Zustand führen.
(siehe auch DIN EN IEC 62443-4-2)

5.1.3 Verwaltung der Kennung (CR 1.4)

Alle verwendeten Kennungen (Anmeldenamen etc.) müssen entweder von der Komponente selbst oder durch eine übergeordnete Ebene verwaltet werden. Ein Ausfall der Verwaltung darf nicht zu einem gefahrbringenden Zustand führen.
(siehe auch DIN EN IEC 62443-4-2)

5.1.4 Verwaltung der Authentifizierung (CR 1.5)

Die Komponenten müssen in der Lage sein unter allen Umständen (Neuinstallation, periodische Änderung, etc.) den Authentifizierer zu unterstützen und vor einer nicht autorisierten Offenlegung zu schützen. Dieses gilt für alle Betriebszustände, wie z.B. Speicherung, Nutzung oder Übermittlung.
(siehe auch DIN EN IEC 62443-4-2)

5.1.5 Stärke der Authentifikation durch Passwörter (CR 1.7)

Werden Passwörter zur Authentifizierung verwendet muss die Stärke der Passwörter beruhend auf der Länge des Passwortes und der verwendeten Vielfalt an Zeichen konfigurierbar sein. Diese Anforderung kann entweder auf der Komponente selbst oder in einer höheren Integrationsebene umgesetzt werden.
Die Stärke des Passworts ist nicht alleine durch die verwendeten Kriterien (z.B. Sonderzeichen, Zahlen, Groß- und Kleinschreibung), sondern von der Länge und in Kombination mit CR 1.11 zu betrachten.
(siehe auch DIN EN IEC 62443-4-2)

5.1.6 Rückmeldung vom Authentifizierer (CR 1.10)

Wenn eine Passworteingabe erfolgt, muss die Anzeige des eingegebenen Passwortes verdeckt erfolgen, z.B. Sternchen anstelle von Zeichen.
(siehe auch DIN EN IEC 62443-4-2)

5.1.7 Erfolglose Anmeldeversuche (CR 1.11)

Die Komponente muss bei einer einstellbaren Anzahl an aufeinanderfolgender Fehlversuche innerhalb einer einstellbaren Zeit, die Anmeldung für eine definierte Zeit sperren oder die Freigabe nur durch einen Systemadministrator erlauben.
(siehe auch DIN EN IEC 62443-4-2)

5.1.8 Nutzungshinweis des Systems (CR 1.12)

Bei der Verwendung eines Human Machine Interface (HMI) müssen die notwendigen Nutzungshinweise dem Bedienenden angezeigt werden.
(siehe auch DIN EN IEC 62443-4-2)

5.2 Nutzungskontrolle

5.2.1 Durchsetzung der Autorisierung (CR 2.1)

Die Komponente muss auf der Grundlage der ihr zugeordneten Verantwortlichkeiten und minimal erforderlichen Rechte einen Mechanismus für die Durchsetzung der Autorisierung für alle identifizierten und authentifizierten menschlichen Nutzer bereitstellen. Für den Schutz der Autorisierungsinformationen gelten weitere Anforderungen. 7.3 und 7.6 der DIN EN IEC 62443-4-2 enthalten z. B. weitere Anforderungen für den Schutz der Integrität.

5.2.2 Nutzungskontrolle von Funkverbindungen (CR 2.2)

Bei Komponenten, die den drahtlosen Zugriff unterstützen gelten dieselben Anforderungen wie bei drahtgebundenen Komponenten.
(siehe auch DIN EN IEC 62443-4-2)

5.2.3 Mobiler Code (SAR 2.4; EDR 2.4; HDR 2.4 und NDR 2.4)

Der ausgeführte Code muss dem Code aus der Prüfung entsprechen. Externer Code (mobiler Code) darf zu keinem Zeitpunkt nachgeladen werden.
(siehe auch DIN EN IEC 62443-4-2)
Hinweis aus der DIN EN IEC 62443-4-2: Technologien mit mobilem Code sind unter anderem Java, Javascript, ActiveX, PDF, Postscript, ShockwaveMovies, Flash-Animationen und VBScript.

5.2.4 Sitzungssperrung (CR 2.5)

Schnittstellen, die einem menschlichen Nutzer bereitgestellt werden, müssen nach einer definierten Zeit der Inaktivität oder bei Aktivierung der Schnittstelle durch einen weiteren Teilnehmer, eine Sitzungssperrung einleiten. Diese Sperrung darf nur durch autorisierte Nutzer wieder aufgehoben werden.
(siehe auch CR 2.6 der DIN EN IEC 62443-4-2)
Anmerkung: Gleiches gilt auch für den Fernzugriff.

5.2.5 Prüfbare Ereignisse (CR 2.8)

Ereignisdatensätze müssen zur IT-Sicherheit für die Zugriffskontrolle, fehlerhafte Anfragen etc. erzeugt werden. Diese Datensätze müssen so aufgebaut sein, dass eine eindeutige Zuordnung zum Zeitstempel, Ereignisklassifizierung, Herkunft (Teilnehmer, Gerät, etc.) und dem Ergebnis des Ereignisses möglich ist.
(siehe DIN EN IEC 62443-4-2)

5.2.6 Speicherkapazität für Ereignisdatensätze (CR 2.9)

Die Komponente (oder das übergeordnete System) muss genügend Speicherkapazitäten bereitstellen. Ein Erreichen der maximalen Speicherkapazität darf nicht zu einem gefahrbringenden Zustand der Komponente führen. Die Komponente muss eine angemessene Fehlerreaktion einleiten.

Hierzu darf der Leitfaden des National Institute of Standards and Technology (NIST) Special Publication (SP) 800-92 herangezogen werden.
(siehe DIN EN IEC 62443-4-2)

5.2.7 Verhalten bei Verarbeitungsfehlern von Ereignisdaten (CR 2.10)

Ein Verarbeitungsfehler von Ereignisdaten darf nicht zu einem gefahrbringenden Zustand der Komponente führen. Die Komponente muss eine angemessene Fehlerreaktion einleiten.

Verarbeitungsfehler von Ereignisdaten beinhalten z. B. Software- oder Hardwarefehler, Ausfälle im Erfassungsmechanismus und das Erreichen oder Überschreiten der Speicherkapazität für Ereignisdatensätze. Bei der Entwicklung geeigneter Gegenmaßnahmen kann z. B. der Leitfaden NIST SP 800-92, Guide to Computer Security Log Management herangezogen werden.
(siehe DIN EN IEC 62443-4-2)

5.2.8 Zeitstempel (CR 2.11)

Es muss ein Zeitstempel (z.B. mit Datum und Zeit) erzeugt werden, der die Rückverfolgung für jedwede Nutzung in Ereignisdatensätzen ermöglicht.
(siehe DIN EN IEC 62443-4-2)

5.2.9 Nichtabstreitbarkeit (CR 2.12)

Eingaben über eine Benutzerschnittstelle müssen von der Komponente aufgezeichnet werden um eine spätere Nachverfolgbarkeit der Eingaben zu gewährleisten.
(siehe DIN EN IEC 62443-4-2)

5.3 Systemintegrität

5.3.1 Kommunikationsintegrität (CR 3.1)

Die Komponente muss die Fähigkeit haben, die Integrität der übertragenen Information zu schützen.
(Siehe GS-ET-26)

5.3.2 Schutz vor Schadcodes (SAR 3.2)

Schutzmechanismen vor Schadcodes, die mit der Anwendung vereinbar sind, müssen vom Hersteller dokumentiert werden. Alle hierfür notwendigen Konfigurationsanforderungen müssen dem Anwender zur Verfügung gestellt werden.
(siehe DIN EN IEC 62443-4-2)

5.3.3 Schutz vor Schadcodes (EDR 3.2)

Das eingebettete Gerät darf keine nicht autorisierte Software ausführen. Sie muss einen Schutz vor der Installation oder der Ausführung von Schadcodes besitzen.
(siehe DIN EN IEC 62443-4-2)

5.3.4 Schutz vor Schadcodes (HDR 3.2)

Bei der Verwendung eines Host-Gerätes ist darauf zu achten, dass nur Mechanismen zum Schutz vor Schadcodes verwendet werden, die vom IACS-Hersteller freigegeben sind. Die hierfür notwendigen Konfigurationsanforderungen sind (vom IACS-Hersteller) zu dokumentieren.
(siehe DIN EN IEC 62443-4-2)

5.3.5 Verifikation der IT-Sicherheitsfunktionalität (CR 3.3)

Die Implementierten IT-Sicherheitsfunktionen müssen vom Hersteller verifiziert werden. Wenn IT-Sicherheitsfunktionen durch den Betreiber verifiziert werden sollen, muss der Hersteller Anleitungen zur Durchführung der Verifikation bereitstellen.
(siehe DIN EN IEC 62443-4-2)

5.3.6 Software- und Informationsintegrität (CR 3.4)

Die Komponente muss in der Lage sein sowohl die Integrität der verwendeten Software als auch alle weiteren wichtigen Informationen, z.B. Konfigurationen, zu überprüfen und die Ergebnisse bereit zu stellen. Diese Anforderung kann auch von einer höheren Ebene, in die die Komponente integriert wird, übernommen werden.
(siehe DIN EN IEC 62443-4-2)

5.3.7 Eingabevalidierung (CR 3.5)

Eingaben von (menschlichen) Nutzern müssen auf Ihre Syntax, Länge und Inhalt hin überprüft werden. Diese Anforderung gilt für alle verwendeten Schnittstellen.
(siehe DIN EN IEC 62443-4-2)
Anmerkung:
Ausführbarer Code darf nicht über eine Eingabe (z.B. Bemerkungsfeld) zur Ausführung kommen (Code Injection).

5.3.8 Vorbestimmte Zustände der Ausgänge (CR 3.6)

Falls kein sicherer Betrieb mehr aufrechterhalten werden kann (z.B. in Folge eines Angriffs), muss die Komponente in der Lage sein, Ausgänge, welche für die Prozesssteuerung vorgesehen sind, in einen definierten Zustand zu überführen.
(siehe DIN EN IEC 62443-4-2)

5.3.9 Fehlerbehandlung (CR 3.7)

Die Komponente muss Fehler erkennen und die Fehlzustände so behandeln, dass eine wirksame Abhilfe stattfinden kann. Dies muss in einer Art und Weise geschehen, die keine Informationen, die von Gegnern für Angriffe auf das Industrielle Automatisierungssysteme (IACS) verwendet werden können, liefert, außer die Offenlegung dieser Informationen ist für die rechtzeitige Behebung der Probleme unumgänglich.
(siehe DIN EN IEC 62443-4-2)

5.3.10 Unterstützung von Updates (EDR 3.10; HDR 3.10; NDR 3.10)

Das eingebettete Gerät bzw. die Host-Geräte / Netzwerkkomponenten müssen die Fähigkeit für Updates und Upgrades nach der Installation unterstützen.
(siehe DIN EN IEC 62443-4-2)

5.3.11 Integrität von Boot-Prozessen (EDR 3.14; HDR 3.14; NDR 3.14)

Eingebettete Geräte / Host-Geräte / Netzwerkkomponenten müssen die Integrität der für den Boot-Prozess benötigten Firmware, Software und Konfigurationsdaten vor deren Anwendung beim Booten verifizieren. (siehe DIN EN IEC 62443-4-2)

5.4 Vertraulichkeit von Informationen

5.4.1 Vertraulichkeit von Informationen (CR 4.1)

Vertrauliche Informationen dürfen nicht an Unbefugte weitergegeben werden. Dieses gilt z.B. für Informationen mit einer Leseberechtigung im gespeicherten Zustand oder wenn vertrauliche Informationen übertragen werden.
(siehe auch DIN EN IEC 62443-4-2)

5.4.2 Verwendung von Verschlüsselung (CR 4.3)

Wenn für eine Komponente eine Verschlüsselung gefordert ist (z.B. Fernzugriff), dann muss die verwendete Verschlüsselung anerkannten IT-Sicherheitsgepflogenheiten und -empfehlungen entsprechen.
(siehe DIN EN IEC 62443-4-2)

Allgemein anerkannte Verfahren und Empfehlungen können Dokumenten wie NIST SP 800-57, Recommendation for Key Management, Part 1: General entnommen werden. Die Implementierungsanforderungen können z. B. FIPS 140-2, Security Requirements for Cryptographic Modules oder ISO/IEC 19790:2012, Information technology- Security techniques - Security requirements for cryptographic modules entnommen werden.

5.5 Eingeschränkter Datenfluss

5.5.1 Netzaufteilung (CR 5.1)

Wenn erforderlich muss die Komponente ein unterteiltes Netzwerk (siehe IEC 61443-3-2) unterstützen.
(siehe DIN EN IEC 62443-4-2)

5.6 Rechtzeitige Reaktion auf Ereignisse

5.6.1 Zugriffsmöglichkeit auf Ereignisprotokolle (CR 6.1)

Ein Zugriff auf Ereignisprotokolle muss von autorisierten (menschlichen) Nutzern lesend möglich sein.
(siehe DIN EN IEC 62443-4-2)

5.7 Verfügbarkeit von Ressourcen

5.7.1 Schutz vor DoS-Ereignisse (CR 7.1)

Komponenten müssen die Fähigkeit haben, Safety relevante Funktionen während eines Denial-of-Service (DoS)-Ereignisses aufrechtzuerhalten oder in den sicheren Zustand zu wechseln.
(siehe DIN EN IEC 62443-4-2)

5.7.2 Ressourcenmanagement (CR 7.2)

Die Komponente muss über sogenannte IT-Sicherheitsfunktionen verfügen, die eine Überlastung der Ressourcen verhindert. Es darf in keinem Fall zu einem gefahrbringen Zustand führen.
(siehe DIN EN IEC 62443-4-2)

5.7.3 Datensicherung im Automatisierungssystem (Backup) (CR 7.3)

Bei Datensicherungsoperationen auf Systemebene muss die Komponente dahingehend beteiligt sein, dass eine Datensicherung über die relevanten Informationen angelegt werden kann. Der Datensicherungsprozess darf nicht zu einem gefahrbringenden Zustand führen.
(siehe DIN EN IEC 62443-4-2)

5.7.4 Wiederherstellung des Automatisierungssystems (CR 7.4)

Die Komponente muss nach einer Unterbrechung oder einem Ausfall in einen bekannten, sicheren Zustand wiederhergestellt werden können.
(siehe DIN EN IEC 62443-4-2)

5.7.5 Netzwerk- und IT-Sicherheitseinstellungen (CR 7.6)

Eine Konfiguration der Komponente muss nach vom Hersteller des Automatisierungssystems bereitgestellten Netzwerk- und IT-Sicherheitseinstellungen möglich sein.
(siehe DIN EN IEC 62443-4-2)

5.7.6 Geringste Funktionalität (CR 7.7)

Die Komponente muss gezielt die Verwendung unnötiger Funktionen, Ports, Protokolle, physikalische Schnittstellen und/oder Dienste beschränken können.
(siehe DIN EN IEC 62443-4-2)

5.8 Anforderung an Netzwerkkomponenten

5.8.1 Verwaltung drahtloser Zugriffsverfahren (NDR 1.6)

Alle (menschlichen) Nutzer müssen für einen drahtlosen Zugriff auf die Komponente identifiziert und authentifiziert werden können.
(siehe DIN EN IEC 62443-4-2)

5.8.2 Zugriff über nicht vertrauenswürdige Netzwerke/Schnittstellen (z.B. Programmierschnittstelle) (NDR 1.13)

Zugriffe aus nicht vertrauenswürdigen Netzwerken müssen von Netzwerkkomponenten überwacht und kontrolliert werden. Betrachtet werden hierbei nicht nur kabelgebundene Schnittstellen, sondern auch nicht kabelgebundene Schnittstellen
(siehe DIN EN IEC 62443-4-2 CR 2.2 und CR 2.3)

5.8.3 Schutz vor Schadcodes (NDR 3.2)

Die Netzwerkkomponente muss einen Schutz vor Schadcodes bereitstellen.
(siehe DIN EN IEC 62443-4-2)

5.8.4 Schutz der Zonengrenze (NDR 5.2)

Bei dem Einsatz einer Netzwerkkomponente an einer Zonengrenze (Zum Beispiel Übergang von einem Sicherheitsbereich in einen Nicht-Sicherheitsbereich) muss die Kommunikation überwacht werden. Bei nicht bestimmungsgemäßer Kommunikation muss diese unterbunden werden können.
Eine Kommunikation über die IT-Sicherheitszone hinaus sollte nur über Komponenten erfolgen, die den Schutz der Zonengrenze sicherstellen können (z.B. Proxies, Gateways, Router, Firewalls, unidirektionale Gateways, Guards und verschlüsselte Tunnel).
(siehe DIN EN IEC 62443-4-2)

5.8.5 Allgemeine Beschränkung der persönlichen Kommunikation (NDR 5.3)

Bei dem Einsatz einer Netzwerkkomponente muss diese die Weitergabe einer persönlichen Kommunikation zwischen Teilnehmern eines Netzwerkes an den Zonengrenzen verhindern.
(siehe DIN EN IEC 62443-4-2)

6 Typprüfung

Checkliste für Prüfung (interner Gebrauch)

Die Checkliste kann entweder von Prüfern verwendet oder dem Hersteller bereitgestellt werden, damit dort die Nachweise für die Umsetzung der Maßnahme eingetragen werden können.

7 Prüfverfahren

Prüfverfahren für Prüfung (interner Gebrauch)

8 Checkliste nach DIN EN IEC 62443-4-1

Checkliste nach DIN EN IEC 62443-4-1 (interner Gebrauch)

9 Modifikationen

In diesem Abschnitt ist das Verfahren beschreiben, wie bei einer Modifikation vorzugehen ist.

Modifikationen von bereits geprüften Security relevanten Softwareteilen und Hardwaremaßnahmen müssen der Prüfstelle in Form einer Änderungsmitteilung gemeldet werden.

Eine „Vorgängerversion“ stellt eine grundlegende Softwareversion dar, die in ihrer Gesamtheit erforderlich ist, um ein Produkt in seinem bestimmungsgemäßen Gebrauch einzusetzen.

Die Softwaremodifikation wird nach Abschluss der Prüfung als „geänderte Version“ mit in das Zertifikat bzw. in die Anlage des Zertifikats aufgenommen.

Dies setzt voraus, dass der Hersteller der Software ein Modifikationsmanagement implementiert hat, um sicherheitsrelevante Änderungen in der bereits zertifizierten Software zu verwalten.

Zur Prüfung der Modifikation sind folgende Unterlagen und Dokumente einzureichen:

- Einflussanalyse
- Dokumentation über Neuverifizierung geänderter Software-Module
- Dokumente über die Datenaufzeichnung und Analyse
- Testpläne und Testberichte

Es erfolgt eine Prüfung der eingereichten Unterlagen und der Typprüfungen aus Abschnitt 5. Ziel ist der Nachweis, dass auch nach einer Modifikation die Anforderungen an die Security-Aspekte des Systems weiterhin erfüllt sind.

IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung
Prüf- und Zertifizierungsstelle im DGUV Test

Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA)

Leiter Prüf- und Zertifizierungsstelle
Dr. Peter Paszkiewicz

Fachzertifizierer
M.Sc. Christian Werner

Bezugsquellen:

Prüfgrundsätze: DGUV Test, Prüf- und Zertifizierungssystem der Deutschen Gesetzlichen Unfallversicherung, Geschäftsstelle Sankt Augustin, Alte Heerstraße 111, 53757 Sankt Augustin
http://www.dguv.de/dguv-test/prod-pruef-zert/pruefgrundsaetze-erfahrung/pruefgrundsaetze/index.jsp

DIN-Normen: Beuth-Verlag GmbH, 10787 Berlin