IEC 62443-4-1:2018 Sicherer Entwicklungsprozess für Produkte der industriellen Automatisierung

Sicherer Entwicklungslebenszyklus, acht Praktiken

47 Anforderungen. Diese Norm ist akkreditiert zertifizierbar. Stand 07/2026.

IEC 62443-4-1 ist zertifizierbar, aber der Gegenstand ist ungewöhnlich: zertifiziert wird der Entwicklungsprozess einer benannten Entwicklungsorganisation, also eine konkrete dokumentierte Fassung des sicheren Lebenszyklus. Nicht zertifiziert werden ein Produkt oder eine Person. Wege sind ISASecure SDLA und das IECEE CB Scheme. Ein solches Zertifikat begründet nach heutigem Stand keine Konformitätsvermutung zum EU Cyber Resilience Act. Nicht verwechseln mit IEC 62443-4-2, die Anforderungen an die Komponente selbst stellt. Diese Liste ist eine Arbeitshilfe für den Selbstcheck, kein Nachweis.

Betrieb	Datum	Bearbeiter

5 Praktik 1: Sicherheitsmanagement (SM) 13

SM-1 **Es existiert ein beschriebener Entwicklungsablauf, der Sicherheit über alle Phasen hinweg mitführt, von der ersten Idee bis zur Ausserbetriebnahme des Produkts, und dieser Ablauf ist derjenige, nach dem tatsächlich gearbeitet wird.** Dokument

Woran man es festmacht: Prozessbeschreibung oder Verfahrensanweisung mit Phasen, Ergebnissen je Phase und Übergabepunkten, dazu Belege aus einem laufenden Vorhaben, die zeigen, dass die Phasen wirklich durchlaufen wurden. Ein kleiner Betrieb kommt mit einer Seite pro Phase plus Checkliste im Ticketsystem aus, wichtig ist nur, dass Plan und gelebte Praxis zusammenpassen.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SM-2 **Für jede Aufgabe im sicheren Entwicklungsablauf ist festgelegt, wer sie verantwortet, und diese Zuordnung ist den Beteiligten bekannt.** Dokument

Woran man es festmacht: Rollen- und Aufgabenmatrix, in der jeder Prozessschritt einer benannten Rolle zugeordnet ist, ergänzt um die aktuelle Besetzung der Rollen. Bei wenigen Köpfen reicht eine Tabelle mit Rolle, Aufgabe und Person, wichtig ist die Vertretungsregelung für Urlaub und Krankheit.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SM-3 **Es ist nachvollziehbar bestimmt, welche Produkte, Varianten, Releases und Komponenten unter den sicheren Entwicklungsablauf fallen und welche nicht.** Dokument

Woran man es festmacht: Liste der betroffenen Produkte und Versionsstände mit Begründung für Ein- und Ausschlüsse, gepflegt bei jedem neuen Release. Praktisch ist eine Spalte in der Produktübersicht, die je Zeile Ja oder Nein und einen Satz zur Begründung trägt.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SM-4 **Die Personen, die Sicherheitsaufgaben übernehmen, verfügen über die dafür nötige Fachkenntnis, und diese Kenntnis wird gezielt aufgebaut und aufgefrischt.**

Woran man es festmacht: Kompetenzprofil je Sicherheitsrolle, Qualifikationsnachweise, Schulungsplan und Teilnahmebelege, ergänzt um eine Lücken-Übersicht. Kleine Betriebe belegen das über Zertifikate, Konferenz- oder Webinarteilnahmen und einen kurzen jährlichen Abgleich, wer welche Lücke bis wann schliesst, notfalls ergänzt durch eingekaufte Expertise.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SM-5 **Der Geltungsbereich des sicheren Entwicklungsablaufs ist abgegrenzt und benennt die beteiligten Standorte, Organisationseinheiten, Zulieferbeiträge und Entwicklungsumgebungen samt der Grenzen dieses Bereichs.** Dokument

Woran man es festmacht: Geltungsbereichsbeschreibung mit Standorten, Teams, ausgelagerten Anteilen und Systemen, dazu eine Skizze der Schnittstellen nach aussen. Wer nur an einem Standort entwickelt, hält das in wenigen Sätzen fest und benennt ausdrücklich, was ausserhalb liegt, etwa fremdentwickelte Baugruppen oder Hosting durch Dritte.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SM-6 **Für alle an Anwender ausgelieferten Bestandteile, Software, Firmware, Konfigurationen und begleitende Dateien, ist eine Prüfung der Unversehrtheit möglich, sodass Empfänger unbemerkte Veränderungen erkennen können.**

Woran man es festmacht: Signaturen oder veröffentlichte Prüfsummen je Auslieferungspaket, Beschreibung des Verfahrens und ein Beispiel aus einem realen Release samt Anleitung für den Kunden, wie er die Prüfung durchführt. Für kleine Teams genügt eine signierte Prüfsummendatei neben dem Download plus ein Absatz in der Release-Notiz.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SM-7 **Die Umgebungen, in denen entwickelt, gebaut und getestet wird, sind gegen unbefugten Zugriff und gegen Manipulation an Quellcode, Build-Werkzeugen und Artefakten geschützt.**

Woran man es festmacht: Berechtigungskonzept für Repository, Build-Server und Testsysteme, Zugriffslisten mit letztem Prüfdatum, Protokolle sicherheitsrelevanter Änderungen und Nachweis der Trennung von Produktiv- und Entwicklungszugängen. Ohne eigene IT-Abteilung reichen Zwei-Faktor-Anmeldung, geschützter Hauptzweig mit Pflichtreview und eine halbjährliche Sichtung, wer noch Zugriff hat.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SM-8 **Private Schlüssel, mit denen Auslieferungen signiert werden, sind gegen Offenlegung und Missbrauch abgesichert, ihr Einsatz ist auf berechtigte Personen und Systeme begrenzt.**

Woran man es festmacht: Beschreibung von Aufbewahrung, Zugriff, Erneuerung und Sperrung der Schlüssel, Nachweis der geschützten Ablage, etwa Hardware-Token oder Schlüsseldienst, sowie Aufzeichnungen über Signiervorgänge. Ein kleiner Betrieb legt den Signaturschlüssel auf einen Hardware-Token, dokumentiert die zwei Personen mit Zugriff und hält einen Ablauf für den Verlustfall bereit.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SM-9 **Für zugekaufte oder übernommene Bestandteile, einschliesslich quelloffener Software, sind die sicherheitsbezogenen Erwartungen an den Lieferanten festgelegt und werden bei der Auswahl herangezogen.** Dokument

Woran man es festmacht: Sicherheitsanforderungen in Lieferantenvorgaben oder Verträgen, Auswahlkriterien für Fremdbestandteile, Bestandsliste aller Fremdbestandteile mit Version und Bezugsquelle sowie die Bewertung, ob der Lieferant die Erwartungen erfüllt. Ohne Einkaufsabteilung reicht eine gepflegte Komponentenliste mit einer Spalte, ob Sicherheitsupdates und Meldewege des Lieferanten geprüft wurden.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SM-10 **Bestandteile, die ein Dritter im Auftrag eigens entwickelt, unterliegen denselben sicherheitsbezogenen Anforderungen wie die Eigenentwicklung, und die Einhaltung wird überprüft.**

Woran man es festmacht: Auftrags- oder Vertragsunterlagen mit den geforderten Sicherheitspflichten, Nachweise des Dienstleisters über die angewandten Praktiken, Abnahmeprotokolle und Ergebnisse eigener Prüfungen an der gelieferten Arbeit. Ohne eigenes Auditbudget genügen eine vertragliche Zusicherung, die Vorlage der Testergebnisse des Dienstleisters und eine eigene Stichprobe vor der Abnahme.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SM-11 **Sicherheitsbezogene Feststellungen aus allen Quellen, Tests, Reviews, Meldungen von Anwendern und Hinweisen Dritter, werden erfasst, in ihrer Tragweite eingeschätzt, mit Verantwortlichem und Frist versehen und bis zum Abschluss verfolgt.** Dokument

Woran man es festmacht: Fehler- oder Ticketsystem mit einer eigenen Kennzeichnung für Sicherheitsthemen, je Eintrag die Einschätzung der Tragweite, der Verantwortliche, die Frist und der Abschlussvermerk, dazu eine Auswertung offener Punkte. Ein kleines Team nutzt dafür ein Label im vorhandenen Ticketsystem und einen festen Tagesordnungspunkt in der Wochenrunde.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SM-12 **Vor der Freigabe eines Produkts ist geprüft und belegt, dass die vorgesehenen Schritte des sicheren Entwicklungsablaufs tatsächlich durchgeführt und die zugehörigen Nachweise erzeugt wurden.** Dokument

Woran man es festmacht: Freigabeprüfung je Release mit Abgleich gegen die Prozessschritte, Verweis auf die jeweiligen Nachweise und eine dokumentierte Freigabeentscheidung mit Datum und Unterschrift. Praktisch ist eine Freigabecheckliste, die ohne vollständige Haken keine Auslieferung zulässt, offene Punkte werden begründet und terminiert.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SM-13 **Der sichere Entwicklungsablauf selbst wird regelmässig hinterfragt und weiterentwickelt, wobei Erkenntnisse aus Vorfällen, Prüfergebnissen, Kundenrückmeldungen und der Bedrohungslage einfliessen.**

Woran man es festmacht: Aufzeichnungen der Prozessbewertung, etwa Managementbewertung oder Retrospektive, mit den ausgelösten Prozessänderungen, deren Umsetzungsstand und einem Verweis auf die Ursache. Wer die Reifegrade der Norm nutzt, hält je Praktik den heutigen Stand und das Ziel fest, Maturity Level 4 verlangt genau diesen Nachweis fortlaufender Verbesserung. Für einen kleinen Betrieb reicht ein Termin pro Jahr mit Protokoll und drei konkreten Verbesserungen.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

6 Praktik 2: Festlegung der Sicherheitsanforderungen (SR) 5

SR-1 **Der vorgesehene Einsatzrahmen des Produkts ist beschrieben: erwartete Einsatzumgebung, unterstellte Schutzmaßnahmen der Umgebung, vorgesehene Nutzergruppen und Rollen, angenommene Vertrauensgrenzen sowie die Fälle, für die das Produkt ausdrücklich nicht gedacht ist.** Dokument

Woran man es festmacht: Beschreibung des Einsatzrahmens als eigenes Dokument oder als fester Abschnitt der Produktspezifikation, mit Netzumgebung, angenommenen externen Schutzmaßnahmen wie Firewall oder physischer Zutrittsschutz, Rollenliste und einer ausdrücklichen Negativliste. Ein kleiner Betrieb hält das auf zwei Seiten fest, ergänzt um eine einfache Skizze der Anlagenumgebung, und lässt sie vom Produktverantwortlichen datieren und freigeben.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SR-2 **Für das Produkt liegt eine Bedrohungsbetrachtung vor, die Datenflüsse, Schnittstellen, Vertrauensgrenzen und Angriffswege abbildet, die daraus abgeleiteten Bedrohungen und ihre möglichen Auswirkungen benennt und Gegenmaßnahmen zuordnet. Sie wird bei relevanten Änderungen und mindestens einmal je Produktversion überprüft und aktualisiert, offene Punkte werden bis zur Klärung verfolgt.** Dokument

Woran man es festmacht: Bedrohungsmodell mit Datenflussdiagramm, Bedrohungsliste je Schnittstelle, zugeordneten Gegenmaßnahmen und Status der offenen Punkte, dazu die Änderungshistorie mit Datum und Autor. Ein kleiner Betrieb kommt mit einer Tabelle je Schnittstelle aus, Spalten: Was kann dort passieren, wie schlimm wäre es, was tun wir dagegen, wer prüft es.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SR-3 **Die Sicherheitsanforderungen an das Produkt sind festgelegt und dokumentiert. Sie decken die Ergebnisse der Bedrohungsbetrachtung, den beschriebenen Einsatzrahmen, geltende gesetzliche und vertragliche Vorgaben sowie das angestrebte Schutzniveau ab und beziehen die Sicherheitsfunktionen ein, die das Produkt selbst bereitstellen muss.** Dokument

Woran man es festmacht: Anforderungsliste oder Anforderungsverwaltung mit eindeutiger Nummerierung je Anforderung, Quellenangabe je Eintrag, etwa Bedrohung, Kundenvertrag oder Gesetz, und Angabe des angestrebten Schutzniveaus. Ein kleiner Betrieb führt das als eine Tabelle mit fester ID-Spalte, an der Verifikation und Test später andocken.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR-4 **Jede einzelne Sicherheitsanforderung ist so formuliert, dass sie eindeutig, widerspruchsfrei, prüfbar und einer konkreten Produktfunktion oder Schnittstelle zuordenbar ist, und sie enthält die Angaben, die eine spätere Prüfung ohne Rückfrage möglich machen.**

Woran man es festmacht: Stichprobe aus der Anforderungsliste, an der sich zu jeder Anforderung ein messbares Abnahmekriterium und die betroffene Funktion oder Schnittstelle ablesen lässt, sowie die Zuordnung Anforderung zu Testfall. Ein kleiner Betrieb prüft das mit einer festen Formulierungsvorlage und der Kontrollfrage, ob sich aus der Anforderung ohne Nachfrage ein Testfall schreiben lässt.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR-5 **Die Sicherheitsanforderungen werden vor ihrer Verwendung in Entwurf und Umsetzung geprüft, und zwar unter Beteiligung der betroffenen Seiten wie Entwicklung, Test, Produktverantwortung und, wo sinnvoll, Vertrieb oder Kunde. Geprüft wird auf Vollständigkeit gegenüber Bedrohungsbetrachtung und Einsatzrahmen, auf Korrektheit und auf Prüfbarkeit. Befunde werden erfasst und bis zum Abschluss nachverfolgt.**

Woran man es festmacht: Prüfprotokoll mit Datum, Teilnehmern und ihren Rollen, geprüfter Fassung der Anforderungen, Liste der Befunde mit Verantwortlichem und Erledigungsstand sowie Freigabevermerk. Ein kleiner Betrieb löst das als Vier-Augen-Prüfung zwischen Entwicklung und Test mit einem kurzen Protokoll und einer Freigabezeile in der Anforderungsliste.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

7 Praktik 3: Sicherer Entwurf (SD) 4

SD-1 **Für jedes Produkt existiert eine Entwurfsbeschreibung, die die sicherheitsrelevanten Aspekte der Architektur festhält: welche Bausteine es gibt, wie sie miteinander sprechen, wo die Vertrauensgrenzen verlaufen, welche externen Schnittstellen nach aussen offen sind und mit welchen Mechanismen die zuvor festgelegten Sicherheitsanforderungen im Entwurf umgesetzt werden.** Dokument

Woran man es festmacht: Architekturdokument oder Entwurfsspezifikation mit einem Diagramm, das Komponenten, Datenflüsse und Vertrauensgrenzen zeigt, plus einer Zuordnungstabelle von Sicherheitsanforderung zu umsetzendem Entwurfselement. Ein kleiner Betrieb kommt mit einem gepflegten Diagramm plus zwei bis drei Seiten Erläuterung aus, wichtig ist nur, dass es versioniert im Repository liegt und bei Architekturänderungen mitgezogen wird.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SD-2 **Der Entwurf wird systematisch auf Bedrohungen untersucht. Die Analyse benennt Angreiferziele, betroffene Vertrauensgrenzen und Schnittstellen, die daraus folgenden Bedrohungen samt ihrer Einstufung sowie die Gegenmaßnahmen im Entwurf. Sie wird bei relevanten Änderungen an Architektur oder Umfeld erneut durchlaufen, und die identifizierten Bedrohungen werden bis zu einer Entscheidung nachverfolgt.** Dokument

Woran man es festmacht: Bedrohungsmodell je Produkt oder je grösserem Release, zum Beispiel als Tabelle mit Spalten für Bedrohung, betroffene Schnittstelle, Einstufung, Gegenmaßnahme und Status, dazu das Protokoll der Modellierungssitzung mit Teilnehmern und Datum. Ein kleines Team modelliert pragmatisch in einem Workshop von zwei bis drei Stunden entlang des Architekturdiagramms und hält die offenen Punkte als Tickets fest, damit der Nachweis der Nachverfolgung ohne Extraaufwand entsteht.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SD-3 **Der Entwurf folgt nachvollziehbar anerkannten Gestaltungsprinzipien für Sicherheit, unter anderem geringstmögliche Rechte, sparsame Angriffsfläche, gestaffelte Verteidigung, sichere Voreinstellungen, sicheres Verhalten im Fehlerfall und möglichst einfache, prüfbare Sicherheitsmechanismen. Die Anwendung dieser Prinzipien ist im Entwurf erkennbar und begründet.**

Woran man es festmacht: Abschnitt in der Entwurfsbeschreibung oder eine hausinterne Entwurfsrichtlinie, die die Prinzipien benennt, dazu je Prinzip ein konkreter Beleg im Produkt, etwa die Rechtematrix der Dienste, die Liste der offenen Ports mit Begründung, die Auslieferungsvoreinstellungen oder die dokumentierte Fehlerreaktion. Ein kleiner Betrieb nutzt eine kurze Checkliste dieser Prinzipien als festen Punkt im Entwurfsreview und legt das ausgefüllte Blatt zum Entwurf.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SD-4 **Der Entwurf wird vor der Umsetzung fachlich gegengelesen. Die Prüfung deckt die Vollständigkeit gegenüber den Sicherheitsanforderungen, die Richtigkeit und Wirksamkeit der Sicherheitsmechanismen sowie die Ergebnisse der Bedrohungsanalyse ab. Beteiligt sind Personen mit ausreichender Sicherheitskompetenz, Befunde werden festgehalten und bis zur Erledigung verfolgt.** Dokument

Woran man es festmacht: Reviewprotokoll mit Datum, Prüfgegenstand samt Version, Teilnehmern und deren Rolle, Befundliste mit Status und der Freigabeentscheidung. Ein kleines Team hängt das Review an den Pull Request der Entwurfsdokumente und lässt die Befunde als Kommentare mit Erledigungsvermerk stehen, dann ist die Nachverfolgung ohne zusätzliches Werkzeug belegt. Fehlt intern die Sicherheitskompetenz, ist ein externer Gutachter auf Stundenbasis für die kritischen Entwürfe der pragmatische Weg.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

8 Praktik 4: Sichere Umsetzung (SI) 2

SI-1 **Es besteht ein festgelegtes Vorgehen, mit dem die tatsächliche Umsetzung gegen das sichere Design geprüft wird: geprüft wird, ob die im Entwurf vorgesehenen Schutzmaßnahmen im Code wirklich vorhanden und wirksam sind, ob die Verteidigungstiefe erhalten bleibt und ob bei der Umsetzung neue Schwachstellen entstanden sind. Die Prüfung wird durch fachlich geeignete Personen durchgeführt, gefundene Abweichungen werden erfasst und bis zur Klärung verfolgt.**

Woran man es festmacht: Verfahrensbeschreibung zur Umsetzungsprüfung sowie Prüfaufzeichnungen je Komponente oder Release: geprüftes Modul, Bezug zum Designdokument, Datum, prüfende Person, Befunde und deren Abarbeitungsstand. Als Beleg eignen sich Pull Request Reviews mit einer verbindlichen Sicherheits Checkliste, Ergebnisse statischer Codeanalyse mit dokumentierter Bewertung der Treffer sowie Protokolle von Review Runden. Ein kleines Team löst das mit dem Vier Augen Prinzip, einem Review Template im Repository, in dem jede Designmaßnahme einzeln abgehakt wird, und einem Ticket je offenem Befund. Wichtig ist, dass der Ersteller des Codes nicht sein eigener Prüfer ist.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SI-2 **Für alle sicherheitsrelevanten Entwicklungsarbeiten gelten verbindliche Programmierregeln, die mindestens die Vermeidung bekannter unsicherer Konstrukte und Funktionen, die Behandlung von Eingaben und Fehlern, den Umgang mit Speicher und Ressourcen sowie die Nutzung geprüften statt selbst entwickelten Sicherheitscodes abdecken. Die Regeln gelten je eingesetzter Programmiersprache, sind allen Entwickelnden bekannt und werden bei Bedarf, etwa bei neuen Angriffsmustern oder neuen Werkzeugen, aktualisiert.** Dokument

Woran man es festmacht: Freigegebene Programmierrichtlinie mit Versionsstand, Geltungsbereich je Sprache und Freigabedatum, ergänzt um den Nachweis, dass sie im Alltag greift: Konfiguration der Linter und Analysewerkzeuge im Repository, eine Build Regel, die Verstösse sichtbar macht, und die Teilnahmeliste der Einweisung. Kleine Betriebe schreiben keine eigene Richtlinie von Grund auf, sondern erklären einen etablierten öffentlichen Regelsatz für verbindlich, ergänzen ihn um eine kurze Liste eigener Zusatzregeln und verankern die Prüfung in der Pipeline, sodass die Einhaltung automatisch belegt wird.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

9 Praktik 5: Prüfen und Nachweisen der Sicherheit im fertigen Produkt (SVV) 5

SVV-1 Dokument

Zu jeder sicherheitsbezogenen Produktanforderung existiert mindestens ein zugeordneter Testfall, der belegt, dass die Schutzfunktion im vorgesehenen Betrieb wirkt, dass sie sich bei ungültigen Eingaben und Fehlbedienung wie festgelegt verhält und dass die ausgelieferten Standardeinstellungen dem sicheren Zustand entsprechen. Die Durchführung und das Ergebnis sind je geprüftem Softwarestand aufgezeichnet.

Woran man es festmacht: Zuordnungstabelle Anforderung zu Testfall zu Ergebnis, dazu Testprotokolle mit Datum, geprüftem Versions- oder Buildstand und Name der prüfenden Person. Ein kleiner Betrieb ergänzt in seiner Anforderungsliste einfach eine Spalte mit der Testfall-ID und archiviert den Ausgabe-Log des automatisierten Testlaufs aus der Build-Pipeline als Datei zur jeweiligen Version.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SVV-2

Die Gegenmaßnahmen, die aus der Bedrohungsanalyse hervorgegangen sind, werden gezielt daraufhin geprüft, ob sie den unterstellten Angriffsweg tatsächlich schliessen. Geprüft wird gegen die identifizierten Bedrohungen, nicht nur gegen die gute Bedienung, und offene Punkte gehen in die Fehlerbehandlung ein.

Woran man es festmacht: Testfälle, die direkt auf die Einträge des Bedrohungsmodells verweisen, zum Beispiel je Bedrohungs-ID ein Missbrauchsszenario mit erwartetem Abwehrverhalten, sowie die Protokolle dieser Läufe. Ohne grossen Apparat genügt eine Spalte im Bedrohungsmodell mit Verweis auf den Testfall und dem Datum der letzten erfolgreichen Prüfung.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SVV-3 Dokument

Das Produkt wird vor der Freigabe systematisch auf Schwachstellen untersucht. Der Umfang deckt mindestens ab: Untersuchung der von aussen erreichbaren Schnittstellen und Dienste, Prüfung mit fehlerhaften und zufällig verfremdeten Eingaben, Abgleich der eingesetzten Fremdbestandteile gegen bekannte gemeldete Schwachstellen sowie Prüfung auf bekannte Fehlerklassen im eigenen Code. Die Funde sind mit Bewertung festgehalten.

Woran man es festmacht: Berichte der eingesetzten Werkzeuge mit Angabe von Werkzeugname, Version und Datenstand der Schwachstellendatenbank, Fuzzing-Protokolle, Liste der Fremdbestandteile mit Abgleichdatum und die Fundliste mit Bewertung und Entscheidung. Ein kleiner Betrieb kombiniert kostenfreie Standardwerkzeuge, einen Abhängigkeits-Scan und einen Port- und Dienste-Scan gegen das installierte Produkt und legt die Ausgaben je Release in einem Ordner ab.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SVV-4

Am freigabereifen Produkt wird ein Angriffsversuch unter realistischen Bedingungen durchgeführt, der die Schutzmechanismen aktiv zu umgehen versucht, statt sie nur abzufragen. Umfang, Rahmenbedingungen und Grenzen der Prüfung sind vorab festgelegt, und die dabei gefundenen Schwächen werden wie Fehler behandelt und nachverfolgt.

Woran man es festmacht: Beauftragung oder Prüfauftrag mit Umfang und Testumgebung, Bericht mit Vorgehen, ausgenutzten Schwächen und Bewertung, dazu die Einträge im Fehler- oder Ticketsystem mit Nachweis der Behebung oder der begründeten Risikoannahme. Kleine Anbieter kaufen diese Prüfung typischerweise als abgegrenztes Zeitkontingent extern ein oder lassen sie von einer Person durchführen, die nicht am Produkt entwickelt hat.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SVV-5

Die Unabhängigkeit der prüfenden Personen ist geregelt und dem angestrebten Reifegrad angemessen. Wer einen Bestandteil selbst entwickelt hat, prüft ihn nicht in eigener Verantwortung frei, und mit steigendem Reifegrad wird die Prüfung von einer organisatorisch getrennten Stelle oder einer externen Partei verantwortet. Die tatsächliche Zuordnung ist je Prüfung nachvollziehbar.

Woran man es festmacht: Rollenfestlegung im Entwicklungsprozess, aus der die Trennung von Erstellung und Prüfung hervorgeht, sowie je Testlauf oder Prüfbericht der namentliche Eintrag der prüfenden Person und ihrer Rolle. Ein Zweipersonenbetrieb löst dies über gegenseitiges Prüfen mit dokumentiertem Vier-Augen-Vermerk und zieht für die tiefe Sicherheitsprüfung eine externe Person hinzu.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

10 Praktik 6: Umgang mit Sicherheitsmängeln (DM) 6

DM-1 **Es besteht ein festgelegter Weg, auf dem Hinweise auf Sicherheitsschwächen im Produkt aus allen Richtungen eingehen und erfasst werden: aus dem eigenen Team, aus Tests und Reviews, von Kunden und Integratoren, von externen Meldern sowie aus Hinweisen zu eingesetzten Fremd- und Open-Source-Bestandteilen. Der Meldeweg ist für Externe auffindbar und jede Meldung wird mit Eingangsdatum und Quelle festgehalten.** Dokument

Woran man es festmacht: Beschreibung des Meldewegs, die öffentlich erreichbare Kontaktstelle (Security-Seite, security.txt oder eine Mailadresse wie security@) und das Eingangsregister mit Datum, Quelle und Kurzbeschreibung je Meldung. Ein kleiner Betrieb kommt mit einem geteilten Postfach und einer einzigen Tabelle oder einem Ticket-Label aus, solange jede Meldung dort landet, auch die aus dem eigenen Entwicklerchat.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

DM-2 **Jede eingegangene Meldung wird gesichtet und darauf geprüft, ob sie sicherheitsrelevant ist und welche Produkte, Versionen und Bestandteile sie betrifft. Auch Meldungen, die sich als nicht sicherheitsrelevant oder als nicht zutreffend erweisen, werden mit Begründung abgeschlossen und nicht stillschweigend verworfen.**

Woran man es festmacht: Sichtungsvermerk je Meldung mit Ergebnis (sicherheitsrelevant ja oder nein), betroffenen Versionen und Begründung bei Ablehnung, sichtbar im Ticket oder in der Meldeliste. Wer wenige Meldungen hat, führt die Sichtung in einer wiederkehrenden kurzen Runde durch und hält das Ergebnis in zwei Sätzen je Eintrag fest.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

DM-3 **Bestätigte Sicherheitsmängel werden nach einem einheitlichen Verfahren bewertet: Ursache, betroffene Versionen und Konfigurationen, mögliche Auswirkung auf Betrieb und Sicherheit, Ausnutzbarkeit sowie der Schweregrad nach einem festgelegten Massstab. Das Bewertungsergebnis ist aufgezeichnet und nachvollziehbar.** Dokument

Woran man es festmacht: Bewertungsbogen oder Ticketfelder je Mangel mit Ursache, Schweregrad und dem verwendeten Massstab (zum Beispiel eine gängige Bewertungssystematik mit dokumentiertem Vektor), dazu die Liste der betroffenen Versionen. Für kleine Teams reicht eine feste Feldvorlage im Ticketsystem plus eine halbe Seite, die den Massstab und die Schwellen für sofortiges Handeln beschreibt.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

DM-4 **Für bewertete Sicherheitsmängel ist entschieden, wie damit umgegangen wird: Behebung, Ausgleichsmaßnahme oder begründete Annahme des Risikos. Die Entscheidung richtet sich nach dem Schweregrad, sie ist einer verantwortlichen Person und einem Termin zugeordnet und der Mangel wird bis zum Abschluss verfolgt.** Dokument

Woran man es festmacht: Maßnahmenliste oder Ticketstatus mit Verantwortlichem, Zieltermin, Art der Maßnahme und Abschlussvermerk, verknüpft mit dem Codestand oder der Version, in der die Behebung wirksam wird. Angenommene Restrisiken brauchen eine kurze schriftliche Begründung mit Freigabe durch die Produktverantwortung. Ein kleiner Betrieb bildet das in einem Ticketboard mit Fälligkeitsdatum ab, ohne zusätzliches Werkzeug.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

DM-5 **Betroffene Nutzer, Integratoren und weitere Beteiligte werden über Sicherheitsmängel informiert, sobald die Bewertung dies erfordert, mit Angabe der betroffenen Versionen, der Auswirkung, der verfügbaren Behebung oder Ausgleichsmaßnahme. Fristen und Empfängerkreis der Bekanntgabe sind vorab festgelegt, ebenso das Vorgehen bei Meldungen Dritter, die eine eigene Veröffentlichungsfrist mitbringen.**

Woran man es festmacht: Veröffentlichte Sicherheitshinweise oder Advisories mit Datum und Versionsbezug, der Verteiler oder Abonnentenkanal sowie die schriftliche Regel zu Fristen und koordinierter Veröffentlichung. Wer wenige Kunden hat, nutzt eine Sammelmail an eine gepflegte Kundenliste und eine datierte Hinweisseite, deren Änderungen versioniert sind.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

DM-6 **Der Umgang mit Sicherheitsmängeln wird in festen Abständen überprüft. Betrachtet werden dabei offene und überfällige Fälle, die Zeiten von der Meldung bis zur Behebung, wiederkehrende Ursachen sowie die Wirksamkeit der eingeleiteten Maßnahmen. Aus der Überprüfung abgeleitete Verbesserungen am Vorgehen werden umgesetzt und ihre Umsetzung verfolgt.** Dokument

Woran man es festmacht: Protokoll der wiederkehrenden Überprüfung mit Datum, Teilnehmern, Kennzahlen zu offenen und überfälligen Fällen sowie einer Liste beschlossener Verbesserungen mit Verantwortlichem und Termin. Ein kleiner Betrieb hängt diesen Punkt an eine bestehende Quartalsrunde und hält Kennzahlen und Beschlüsse auf einer Seite fest.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

11 Praktik 7: Verwaltung von Sicherheitsaktualisierungen (SUM) 5

SUM-1 **Jede Sicherheitsaktualisierung für das Produkt wird vor der Freigabe an Kunden gegen die unterstützten Produktversionen und Betriebsumgebungen geprüft, und es liegt eine Aufzeichnung darüber vor, dass die Aktualisierung die Schwachstelle schliesst, ohne die bestimmungsgemässe Funktion zu stören.** Dokument

Woran man es festmacht: Testprotokoll je Patch mit getesteter Produktversion, Plattform, Testfällen (Wirksamkeit gegen die Schwachstelle plus Regression der Kernfunktionen) und Freigabevermerk. Ein kleiner Betrieb kommt mit einer Patch-Freigabeliste im Ticket aus: Ticket-ID, geprüft von, geprüft am, Ergebnis, plus dem Log des automatisierten Testlaufs als Anhang.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SUM-2 **Für alle Bestandteile des Produkts, die nicht selbst entwickelt wurden (Fremdbibliotheken, Betriebssystem, Laufzeitumgebungen), ist geregelt und belegt, wie deren Sicherheitsaktualisierungen bewertet, in das eigene Produkt übernommen oder mit einer Begründung verworfen werden.** Dokument

Woran man es festmacht: Komponenteninventar der Fremdanteile mit Version und Bezugsquelle, dazu je gemeldeter Fremd-Schwachstelle ein Bewertungseintrag mit Entscheidung (übernehmen, nicht betroffen, mit Ausgleichsmaßnahme belegen) und Begründung. Kleine Teams nutzen dafür einen automatisierten Abhängigkeits-Scan im Build und pflegen die Entscheidungen direkt als Kommentar im Scan-Ergebnis oder in einer schlanken Ausnahmeliste.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SUM-3 **Zu jeder ausgelieferten Sicherheitsaktualisierung erhalten die Anwender eine verständliche Begleitinformation: welche Produktversionen betroffen sind, welche Schwachstelle behoben wird, wie schwerwiegend sie ist, ob Nebenwirkungen oder Ausgleichsmaßnahmen zu beachten sind und wie die Aktualisierung eingespielt wird.** Dokument

Woran man es festmacht: Veröffentlichte Sicherheitshinweise oder Release Notes mit Kennung der Schwachstelle, betroffenen Versionen, Einstufung der Schwere, Installationsschritten und Hinweisen zum Rückfall auf den vorherigen Stand. Kleine Anbieter führen eine einzige öffentliche Seite mit chronologischer Liste der Sicherheitshinweise und verlinken sie aus dem Produkt heraus.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SUM-4 **Es gibt einen definierten und gegen Manipulation geschützten Weg, auf dem Anwender Sicherheitsaktualisierungen beziehen, und die Echtheit und Unversehrtheit einer Aktualisierung lässt sich auf Anwenderseite prüfen, bevor sie eingespielt wird.**

Woran man es festmacht: Beschreibung des Auslieferungskanals (Downloadbereich, Update-Server, Datenträger) samt Schutzmaßnahmen, dazu die digitale Signatur oder Prüfsumme je Paket und die Anleitung, wie der Anwender sie verifiziert. Kleine Betriebe erreichen das mit Signatur über den Build-Server, veröffentlichter Prüfsumme neben dem Download und einem klar benannten Ort, an dem der öffentliche Schlüssel liegt.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SUM-5 **Für die Bereitstellung von Sicherheitsaktualisierungen bestehen festgelegte Zeitziele, die sich an der Schwere der Schwachstelle orientieren, die tatsächlich erreichten Zeiten werden nachgehalten, und Überschreitungen sind begründet und mit einer Zwischenmaßnahme für die Anwender hinterlegt.** Dokument

Woran man es festmacht: Interne Vorgabe mit Zeitfenstern je Schwerekategorie (zum Beispiel kritisch <= 30 Tage, hoch <= 90 Tage) und eine Auswertung je Schwachstelle: Meldedatum, Freigabedatum des Patches, verstrichene Tage, Abweichungsgrund. Kleine Betriebe pflegen das als zwei Datumsfelder im Schwachstellen-Ticket und schauen die Liste einmal im Quartal durch, statt ein eigenes Kennzahlensystem aufzusetzen.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

12 Praktik 8: Sicherheitsleitfäden für Einsatz und Betrieb des Produkts (SG) 7

SG-1 **Für jedes Produkt liegt eine Beschreibung der gestaffelten Schutzwirkung vor: sie benennt die im Produkt selbst verbauten Schutzebenen, ordnet ihnen die Bedrohungen zu, gegen die sie wirken, und macht sichtbar, welche Schutzwirkung erst durch das Zusammenspiel mehrerer Ebenen entsteht.** Dokument

Woran man es festmacht: Ein Abschnitt in der ausgelieferten Produktdokumentation oder ein eigenes Schutzkonzept, das je Schutzebene den Mechanismus, die abgedeckte Bedrohung und die Grenzen der Wirkung nennt. Ein kleiner Betrieb hält das als zweiseitige Tabelle: Spalte Schutzebene, Spalte Bedrohung aus der eigenen Bedrohungsanalyse, Spalte Restrisiko. Der Verweis auf die Bedrohungsanalyse aus SR-2 genügt, die Inhalte müssen nicht doppelt gepflegt werden.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SG-2 **Die Dokumentation benennt die Schutzmaßnahmen, die das Produkt nicht selbst mitbringt, sondern von der Einsatzumgebung erwartet, zum Beispiel Netzsegmentierung, vorgelagerte Firewalls, physischer Zugangsschutz oder ein externer Zeitdienst, und macht deutlich, dass die zugesicherte Sicherheit ohne diese Maßnahmen nicht erreicht wird.** Dokument

Woran man es festmacht: Kapitel Einsatzvoraussetzungen im Handbuch oder ein Referenzarchitektur-Bild mit Zonen und Übergängen, in dem die vom Betreiber zu stellenden Maßnahmen ausdrücklich markiert sind. Praktisch bewährt hat sich eine Liste der Annahmen über die Umgebung, die direkt aus dem Sicherheitskontext des Produkts abgeleitet und bei jeder Produktversion gegengelesen wird.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SG-3 **Es existiert eine Anleitung zur sicheren Grundkonfiguration, die alle sicherheitsrelevanten Einstellungen, Dienste, Ports und Schnittstellen aufführt, den empfohlenen Auslieferungszustand angibt und die Auswirkungen einer Abweichung von dieser Empfehlung beschreibt.** Dokument

Woran man es festmacht: Härtungsleitfaden mit Einstellungstabelle: Parameter, empfohlener Wert, Wirkung, Nebenwirkung beim Abweichen. Dazu die Liste der ab Werk aktiven Dienste und Ports mit Begründung, warum sie aktiv bleiben. Ein kleines Team pflegt diese Tabelle direkt neben der Konfigurationsdatei im Repository und exportiert sie in die Auslieferungsdokumentation, so bleibt sie mit dem Produkt in Deckung.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SG-4 **Für den laufenden Betrieb liegt eine Anleitung vor, die beschreibt, wie das Produkt sicher betrieben, überwacht und im Sicherheitszustand gehalten wird, einschliesslich Sicherung und Wiederherstellung, Protokollierung und Umgang mit sicherheitsrelevanten Ereignismeldungen.** Dokument

Woran man es festmacht: Betriebsanleitung mit Abschnitten zu Protokollierung, Sicherungen, Wiederanlauf und Ereignismeldungen. Als Nachweis eignet sich zusätzlich die Liste der sicherheitsrelevanten Meldungen, die das Produkt ausgibt, mit einer kurzen Handlungsempfehlung je Meldung, damit der Betreiber sie nicht selbst deuten muss.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SG-5 **Die Dokumentation erklärt, wie Benutzerkonten, Rollen und Berechtigungen des Produkts eingerichtet und gepflegt werden, insbesondere die Trennung von Rollen, das Ändern voreingestellter Zugangsdaten und das Entfernen nicht mehr benötigter Konten.** Dokument

Woran man es festmacht: Kapitel Kontenverwaltung mit Rollenübersicht und der Zuordnung von Rechten je Rolle, dazu ein ausdrücklicher Hinweis auf voreingestellte Zugangsdaten und deren Änderung bei Inbetriebnahme. Praktisch tauglich ist eine kurze Inbetriebnahme-Checkliste im Handbuch, die der Betreiber abhaken und ablegen kann.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SG-6 **Es liegt eine Anleitung für die sichere Ausserbetriebnahme vor, die das vollständige Entfernen sensibler Daten aus dem Produkt beschreibt, etwa Zugangsdaten, Schlüssel, Konfigurationsdaten und Protokolle, bevor das Gerät weitergegeben, wiederverwendet oder entsorgt wird.** Dokument

Woran man es festmacht: Abschnitt Ausserbetriebnahme mit Aufzählung aller Speicherorte sensibler Daten im Produkt und dem jeweiligen Löschverfahren, inklusive der Fälle, in denen ein Löschen technisch nicht möglich ist und die Hardware physisch zu vernichten ist. Hilfreich ist eine Liste der persistenten Speicher aus der Architekturbeschreibung, sie verhindert, dass ein Speicherort vergessen wird.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SG-7 **Die an Anwender ausgelieferte Sicherheitsdokumentation wird vor Freigabe geprüft: sie ist fachlich richtig, mit der ausgelieferten Produktversion konsistent, vollständig gegenüber den vorgesehenen Inhalten und für die vorgesehene Zielgruppe verständlich, und sie wird nachgezogen, wenn sich das Produkt ändert.**

Woran man es festmacht: Prüfaufzeichnung je Dokument und Produktversion mit Prüfer, Datum, Befunden und deren Erledigung, verknüpft mit der Release-Freigabe. Ein kleiner Betrieb löst das über ein Vier-Augen-Prinzip im Pull-Request der Dokumentation: ein Entwickler prüft die Technik, eine zweite Person die Verständlichkeit, die Freigabe wird im Ticket festgehalten. Auslieferbar ist eine Version erst, wenn die Prüfung dokumentiert vorliegt.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

IEC 62443-3-3:2013 Systemanforderungen an die IT-Sicherheit industrieller Automatisierung

Sieben Grundfunktionen, 51 Systemanforderungen

100 Anforderungen. Diese Norm ist akkreditiert zertifizierbar. Stand 07/2026.

IEC 62443-3-3 ist zertifizierbar, zertifiziert wird ein System, nicht eine Organisation und nicht eine Person. Wege sind ISASecure SSA und das IECEE CB Scheme. Wer die Organisation zertifizieren will, braucht 62443-2-1 oder 2-4, wer die Komponente meint, 62443-4-2. Die Liste enthält die 51 Systemanforderungen und die 49 Erweiterungen. Welche davon gefordert sind, hängt vom angestrebten Security Level ab: ab SL 1 sind es 38, ab SL 2 sind es 60, ab SL 3 sind es 90, ab SL 4 alle 100. Keine Erweiterung gilt bereits ab SL 1. Diese Liste ist eine Arbeitshilfe für den Selbstcheck, kein Nachweis.

Betrieb	Datum	Bearbeiter

5 FR 1: Wer oder was greift zu, und ist es wirklich der oder das Angegebene 24

SR 1.1 **Menschliche Benutzer werden an jeder Stelle, an der sie das Automatisierungssystem bedienen oder konfigurieren können, vor dem Zugriff identifiziert und ihre Identität wird geprüft. Das gilt auch für Bedienpanels an der Maschine, Engineering-Zugänge und Netzdienste.**

Woran man es festmacht: Verzeichnis aller Anmeldepunkte im System, also HMI, Leitstand, SPS-Programmierzugang, Switch, VPN und Fernwartungsclient, jeweils mit dem dort eingesetzten Anmeldeverfahren. Dazu Konfigurationsauszug oder Bildschirmfoto der Anmeldemaske je Geräteklasse. Ein kleiner Betrieb fängt mit einer Tabelle je Gerät an, Spalten: Gerät, Schnittstelle, Anmeldung vorhanden ja oder nein, Begründung bei nein. Ab SL 1 gefordert.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 1.1 RE 1 **Jeder menschliche Benutzer arbeitet unter einer eigenen, ihm allein zugeordneten Kennung. Sammel- und Schichtkonten sind abgeschaltet, verbleibende Ausnahmen sind einzeln begründet und durch zusätzliche Maßnahmen abgesichert.**

Woran man es festmacht: Kontenexport je System mit Zuordnung Kennung zu Person, Ausnahmeliste mit Begründung und Ausgleichsmaßnahme, etwa Kamera oder Anwesenheitsbuch am Bedienplatz. Diese Zeile ist eine Erweiterung und damit nie schon ab SL 1 Pflicht, sie ist ab SL 2 gefordert.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 1.1 RE 2 **Wer sich aus einem nicht vertrauenswürdigen Netz anmeldet, etwa aus dem Internet oder über einen Fernwartungszugang, weist seine Identität über mindestens zwei unabhängige Faktoren nach.**

Woran man es festmacht: Konfiguration des Fernzugangs mit aktiviertem zweitem Faktor, Beispiel eines Anmeldeprotokolls, das beide Faktoren zeigt, sowie die Ausgabeliste der Token oder der App-Registrierungen. Ein kleiner Betrieb nutzt den zweiten Faktor des vorhandenen VPN-Gateways oder eine Authenticator-App, das kostet nichts ausser Einrichtungszeit. Erweiterung, ab SL 3 gefordert, nicht ab SL 1.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 1.1 RE 3 **Der Nachweis über zwei unabhängige Faktoren gilt nicht nur für Zugriffe von aussen, sondern für jede Anmeldung eines menschlichen Benutzers, auch innerhalb des als vertrauenswürdig eingestuften Netzes.**

Woran man es festmacht: Richtlinienauszug der zentralen Anmeldung, der den zweiten Faktor ohne Netzausnahme erzwingt, plus Stichprobenprotokolle von Anmeldungen direkt an Leitstand und Bedienpanel. Erweiterung, erst ab SL 4 gefordert.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 1.2 **Nicht nur Menschen, sondern auch Softwareprozesse und Geräte melden sich am System an, bevor sie Daten austauschen oder Dienste nutzen dürfen. Dazu gehören Kopplungen zwischen Steuerungen, Datenanbindungen an übergeordnete Systeme und Diagnosewerkzeuge.**

Woran man es festmacht: Liste der maschinellen Verbindungen mit Quelle, Ziel, Protokoll und dem jeweils genutzten Nachweis, etwa Zertifikat, Dienstkonto oder Preshared Key. Dazu Konfigurationsauszug einer Kopplung, der die Authentisierung sichtbar macht. Ab SL 2 gefordert, auf SL 1 nicht verlangt.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 1.2 RE 1 **Jeder Softwareprozess und jedes Gerät tritt mit einer eigenen, eindeutigen Kennung auf. Gemeinsam genutzte Dienstkonten oder ein systemweit identischer Schlüssel für viele Geräte werden nicht verwendet.** Dokument

Woran man es festmacht: Gegenüberstellung Gerät zu Kennung oder Zertifikatsseriennummer, die zeigt, dass keine Kennung mehrfach vorkommt. Erweiterung, ab SL 3 gefordert und damit nicht Bestandteil von SL 1.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 1.3 **Konten werden über ihren gesamten Lebenslauf gesteuert: Anlegen, Ändern der Rechte, Deaktivieren beim Ausscheiden und Entfernen sind geregelt und werden von den beteiligten Systemen unterstützt. Das schliesst Benutzerkonten, Dienstkonten und Notfallkonten ein.** Dokument

Woran man es festmacht: Kontenverzeichnis mit Typ, Inhaber, Zweck und Status, dazu Nachweise für Ein- und Austritte, etwa eine unterschriebene Übergabe oder ein Ticket, aus dem die Sperrung mit Datum hervorgeht. Sinnvoll ist eine wiederkehrende Kontenprüfung, die im kleinen Betrieb als jährlicher Abgleich der Kontenliste mit der Personalliste ausreicht. Ab SL 1 gefordert.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 1.3 RE 1 **Die Kontenverwaltung läuft über alle Komponenten des Systems hinweg einheitlich zusammen, sodass eine Sperrung an einer Stelle nicht in einzelnen Geräten wirkungslos bleibt.**

Woran man es festmacht: Nachweis der zentralen Verzeichnisanbindung, etwa Verzeichnisdienst oder RADIUS, mit Liste der angebundenen Komponenten und einer ausdrücklichen Liste der nicht anbindbaren Geräte samt Ersatzverfahren. Testprotokoll einer Sperrung, die auf allen angebundenen Systemen greift. Erweiterung, ab SL 3 gefordert.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 1.4 **Kennungen werden nach festen Regeln vergeben, eindeutig einer Person, einem Gerät oder einer Rolle zugeordnet, bei Nichtgebrauch stillgelegt und nicht später an andere Träger neu vergeben.**

Woran man es festmacht: Namensregel für Kennungen, etwa Nachname und Initiale oder Anlagenkürzel und Nummer, plus die Historie stillgelegter Kennungen, aus der die Nichtwiederverwendung hervorgeht. Ein kleiner Betrieb führt dafür eine einzige fortlaufende Liste mit Vergabedatum und Stilllegungsdatum. Ab SL 1 gefordert.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 1.5 **Authentisierungsmittel wie Passwörter, Schlüssel, Zertifikate und Token werden geordnet ausgegeben, bei Verdacht auf Offenlegung gewechselt und bei Bedarf gesperrt. Ausgelieferte Standardzugänge und Werkspasswörter sind vor der Inbetriebnahme geändert.**

Woran man es festmacht: Ausgabeliste der Token und Zertifikate mit Empfänger und Datum, Wechsel- und Sperrnachweise, sowie eine Inbetriebnahme-Checkliste je Gerät mit dem Punkt Werkspasswort geändert und abgezeichnet. Ab SL 1 gefordert.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 1.5 RE 1 **Die Identitätsnachweise von Softwareprozessen liegen nicht als lesbare Datei auf dem Datenträger, sondern in einem Hardwarespeicher, der das Auslesen des geheimen Teils verhindert.**

Woran man es festmacht: Typnachweis des eingesetzten Sicherheitsbausteins, etwa TPM, Secure Element oder HSM, mit Konfigurationsauszug, der die Schlüsselablage im Baustein belegt. Beschaffungsbeleg oder Datenblatt genügt als Typnachweis. Erweiterung, ab SL 3 gefordert, auf SL 1 und SL 2 nicht verlangt.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SR 1.6 **Drahtlose Zugänge zum System, etwa WLAN, Funkfernsteuerungen oder Bluetooth-Diagnose, sind nur nach Identifizierung und Authentisierung von Benutzer und Gerät nutzbar und werden gezielt verwaltet.**

Woran man es festmacht: Verzeichnis aller Funkstrecken mit Zweck, Reichweite und Verschlüsselungsverfahren, Konfigurationsauszug des Zugangspunkts sowie die Liste der zugelassenen Endgeräte. Ein kleiner Betrieb dokumentiert zusätzlich, welche Funkschnittstellen an Geräten bewusst abgeschaltet wurden. Ab SL 1 gefordert.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SR 1.6 RE 1 **Jeder drahtlose Zugriff ist eindeutig einem bestimmten Benutzer oder einem bestimmten Gerät zuzuordnen, ein gemeinsamer Netzschlüssel für alle Teilnehmer genügt nicht.**

Woran man es festmacht: Nachweis eines Verfahrens mit individuellen Zugangsdaten, etwa unternehmensweite WLAN-Anmeldung über ein Verzeichnis oder geräteindividuelle Zertifikate, dazu ein Verbindungsprotokoll, das die einzelne Kennung zeigt. Erweiterung, ab SL 2 gefordert, damit nicht auf SL 1.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SR 1.7 **Wo mit Passwörtern gearbeitet wird, lässt sich deren Mindeststärke einstellen, etwa Mindestlänge und geforderte Zeichenarten, und die eingestellten Werte sind für alle betroffenen Konten wirksam.**

Woran man es festmacht: Konfigurationsauszug der Passwortrichtlinie je System mit den tatsächlich gesetzten Werten, zum Beispiel Länge >= 10 Zeichen und mindestens drei Zeichenarten, sowie eine Liste der Systeme, die diese Einstellung technisch nicht erlauben, samt Ersatzmaßnahme. Ab SL 1 gefordert.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SR 1.7 RE 1 **Für menschliche Benutzer gelten zusätzlich Regeln zur Erzeugung und Lebensdauer der Passwörter: Wiederverwendung früherer Passwörter wird unterbunden und die Gültigkeit ist begrenzt.**

Woran man es festmacht: Konfigurationsauszug mit Passworthistorie, zum Beispiel Wiederverwendung der letzten fünf Passwörter gesperrt, und der eingestellten maximalen Gültigkeit. Erweiterung, ab SL 3 gefordert.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SR 1.7 RE 2 **Die Begrenzung der Passwortlebensdauer gilt nicht nur für Personen, sondern für alle Konten, also auch für Dienst-, Wartungs- und Gerätekonten.**

Woran man es festmacht: Wechselplan für technische Konten mit letztem und nächstem Wechseldatum je Konto, dazu Wechselnachweise, etwa Änderungsprotokoll oder Ticket. Erweiterung, erst ab SL 4 gefordert.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SR 1.8 **Werden Zertifikate eingesetzt, stammen sie aus einer geordneten Zertifikatsverwaltung mit festgelegten Regeln für Beantragung, Ausstellung, Gültigkeitsdauer, Erneuerung und Sperrung.** Dokument

Woran man es festmacht: Zertifikatsrichtlinie oder eine kurze schriftliche Regelung mit Zuständigkeit, Laufzeiten und Sperrweg, dazu ein Bestandsverzeichnis der ausgestellten Zertifikate mit Ablaufdatum. Ein kleiner Betrieb führt eine Tabelle mit Zertifikat, Gerät, Ablaufdatum und Erinnerungstermin, das verhindert stillen Anlagenstillstand durch abgelaufene Zertifikate. Ab SL 2 gefordert.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SR 1.9 **Bei Anmeldung mit Schlüsselpaaren prüft das System die Gültigkeit des Zertifikats vollständig: Vertrauenskette, Gültigkeitszeitraum, Sperrstatus und den Nachweis, dass der Gegenüber den privaten Schlüssel tatsächlich besitzt. Der Bezug zwischen Zertifikat und Konto ist eindeutig.**

Woran man es festmacht: Konfigurationsauszug mit aktivierter Sperrprüfung, etwa CRL oder OCSP, Testprotokoll einer abgelehnten Anmeldung mit abgelaufenem oder gesperrtem Zertifikat, sowie die Zuordnungstabelle Zertifikat zu Konto. Ab SL 3 gefordert, auf SL 1 und SL 2 nicht verlangt.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 1.9 RE 1 **Die privaten Schlüssel liegen ausschliesslich in einem Hardwarespeicher, aus dem sie sich nicht auslesen lassen, und werden dort auch verwendet.**

Woran man es festmacht: Datenblatt oder Zertifizierungsnachweis des eingesetzten Sicherheitsbausteins und Konfigurationsauszug, der die Schlüsselerzeugung im Baustein zeigt, sodass der private Schlüssel den Baustein nie verlässt. Erweiterung, erst ab SL 4 gefordert.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 1.10 **Während der Anmeldung gibt das System keine verwertbaren Hinweise preis. Eingegebene Passwörter erscheinen verdeckt und Fehlermeldungen verraten nicht, ob Kennung oder Passwort falsch war.**

Woran man es festmacht: Bildschirmfoto der Anmeldemaske mit maskierter Eingabe und Bildschirmfoto der Fehlermeldung nach einem Fehlversuch. Bei Geräten, die dies technisch nicht können, etwa ältere Bedienpanels, eine kurze Notiz zur Ausgleichsmaßnahme, zum Beispiel Zugangsbeschränkung des Aufstellorts. Ab SL 1 gefordert.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 1.11 **Die Zahl aufeinanderfolgender Fehlversuche ist begrenzt und die Reaktion darauf ist einstellbar, zum Beispiel zeitliche Sperre. Die gewählte Reaktion behindert die sicherheitsgerichtete Bedienung der Anlage nicht.**

Woran man es festmacht: Konfigurationsauszug mit Grenzwert, zum Beispiel Sperre nach <= 5 Fehlversuchen, und Sperrdauer, dazu eine kurze Bewertung, warum die Sperre den Notbetrieb oder das sichere Abfahren der Anlage nicht blockiert. An Bedienplätzen mit Sicherheitsfunktion ist eine Zeitsperre einer dauerhaften Kontosperre vorzuziehen. Ab SL 1 gefordert.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 1.12 **Vor der Anmeldung lässt sich ein Nutzungshinweis anzeigen, der auf die Regeln zur Nutzung und Überwachung des Systems hinweist. Text und Anzeige sind vom Betreiber einstellbar.**

Woran man es festmacht: Bildschirmfoto des angezeigten Hinweistextes und der freigegebene Wortlaut mit Datum der Freigabe. Kleine Betriebe stimmen den Wortlaut kurz mit der Personalvertretung oder der Geschäftsführung ab, ein Absatz genügt. Ab SL 1 gefordert.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 1.13 **Zugriffe aus nicht vertrauenswürdigen Netzen, etwa Fernwartung durch Lieferanten, sind auf festgelegte Wege beschränkt, werden überwacht und lassen sich jederzeit unterbrechen.**

Woran man es festmacht: Verzeichnis der Fernzugänge mit Zweck, Gegenstelle, Ansprechpartner und dem genutzten Weg, dazu Verbindungsprotokolle und der Nachweis der Trennmöglichkeit, zum Beispiel Schlüsselschalter, Firewall-Regel oder abschaltbarer Fernwartungsrouter. Ab SL 1 gefordert.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 1.13 RE 1 **Jede einzelne Sitzung aus einem nicht vertrauenswürdigen Netz wird vor dem Verbindungsaufbau ausdrücklich von einer zuständigen Person freigegeben, eine dauerhaft offene Verbindung genügt nicht.**

Woran man es festmacht: Freigabeaufzeichnungen je Fernwartungssitzung mit Zeitpunkt, Anlass, freigebender Person und Dauer, technisch etwa über Schlüsselschalter am Zugangsrouter oder über ein Freigabeportal. Im kleinen Betrieb reicht ein Fernwartungsbuch am Schaltschrank, das der Instandhalter je Sitzung abzeichnet. Erweiterung, ab SL 2 gefordert und damit nie schon auf SL 1.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

6 FR 2: Nutzungskontrolle (Rechte, Sitzungen, Protokollierung) 24

SR 2.1 **Das System setzt die vergebenen Nutzungsrechte technisch durch: Jeder angemeldete Mensch, jedes Gerät und jeder Softwareprozess erhält genau die Zugriffe, die ihm zugewiesen wurden, und der Versuch darüber hinaus wird abgewiesen.**

Woran man es festmacht: Rechtekonzept mit Zuordnung von Konten zu Rechten, dazu ein Screenshot oder Konfigurationsauszug pro Leitsystem, HMI und Engineering-Station, der die aktiven Rechte zeigt. Zusätzlich ein Testprotokoll, in dem ein Konto mit geringen Rechten eine gesperrte Aktion versucht und abgewiesen wird. Ab SL 1 gefordert. Ein kleiner Betrieb kommt mit zwei bis drei Rollen aus, etwa Bedienen, Instandhalten, Projektieren, und dokumentiert diese auf einer Seite.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 2.1 RE 1 **Die Durchsetzung der Nutzungsrechte gilt nicht nur für menschliche Bediener, sondern ebenso für Softwareprozesse und Geräte, die selbsttätig auf das System zugreifen.**

Woran man es festmacht: Liste der technischen Konten und Dienstkonten, etwa OPC-UA-Clients, Historian-Anbindungen, Backup-Dienste, jeweils mit dem zugewiesenen Rechtesatz. Auszug aus der Rechteverwaltung, der belegt, dass diese Konten nicht als Administrator laufen. Erweiterung, ab SL 2 gefordert, nicht auf SL 1.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 2.1 RE 2 **Rechte werden nicht einzeln an Personen vergeben, sondern über Rollen, und die Zuordnung von Rolle zu erlaubten Aktionen ist nachvollziehbar festgehalten.** Dokument

Woran man es festmacht: Rollen-Rechte-Matrix als Tabelle: Zeilen sind die Rollen, Spalten die Aktionen wie Sollwert ändern, Programm laden, Alarm quittieren, Konto anlegen. Dazu die Zuordnungsliste Person zu Rolle. Erweiterung, ab SL 2 gefordert. Eine gepflegte Tabellenkalkulation mit Änderungsdatum reicht als Nachweis vollständig aus.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 2.1 RE 3 **Für eng begrenzte Ausnahmefälle kann eine berechtigte Aufsichtsperson eine Rechtebeschränkung zeitlich befristet aufheben, und jede solche Aufhebung wird protokolliert.**

Woran man es festmacht: Verfahrensbeschreibung für die Ausnahmefreigabe mit Angabe, wer sie erteilen darf und wie lange sie gilt, dazu Protokolleinträge bereits erfolgter Freigaben aus dem Systemlog. Erweiterung, ab SL 3 gefordert.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 2.1 RE 4 **Für besonders kritische Eingriffe ist die Freigabe durch zwei voneinander unabhängige berechtigte Personen erforderlich, bevor die Aktion ausgeführt wird.**

Woran man es festmacht: Liste der Aktionen, die dem Vieraugenprinzip unterliegen, etwa Änderung von Sicherheitsparametern oder Laden eines neuen Steuerungsprogramms, sowie Konfigurationsnachweis und Protokolleinträge mit beiden Freigebenden. Erweiterung, nur ab SL 4 gefordert.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 2.2 **Die Nutzung drahtloser Verbindungen im Automatisierungsnetz ist an eine ausdrückliche Berechtigung gebunden, und nur freigegebene Teilnehmer dürfen über Funk Daten austauschen oder eingreifen.**

Woran man es festmacht: Verzeichnis aller Funkstrecken, etwa WLAN-Zugangspunkte, Bluetooth-Kopplungen, Mobilfunk-Router, jeweils mit Zweck und freigegebenen Teilnehmern. Dazu die Konfiguration der Zugangskontrolle am Zugangspunkt. Ab SL 1 gefordert. Wer kein Funk im Prozessnetz betreibt, hält genau das schriftlich fest und belegt es mit einer Konfigurationsansicht, die Funk deaktiviert zeigt.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 2.2 RE 1 Unberechtigte drahtlose Geräte im Umfeld des Automatisierungsnetzes werden erkannt und gemeldet.

Woran man es festmacht: Aufzeichnung einer Funküberwachung oder ein wiederkehrender Funkscan mit Datum, Ergebnisliste und Vermerk zu jedem unbekannten Gerät. Meldeweg an die zuständige Stelle ist benannt. Erweiterung, ab SL 2 gefordert, nicht auf SL 1. Ein kleiner Betrieb kann einen quartalsweisen Scan mit einem Notebook durchführen und das Ergebnis als Protokoll ablegen.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 2.3 Die Verwendung tragbarer und mobiler Geräte am System, etwa Servicenotebooks, USB-Speicher oder Tablets, ist geregelt und technisch beschränkt auf ausdrücklich zugelassene Geräte.

Woran man es festmacht: Regelung zur Gerätenutzung, Liste der zugelassenen Servicegeräte mit Kennung, sowie Nachweis der technischen Sperre, etwa deaktivierte oder auf bestimmte Geräte beschränkte USB-Anschlüsse an HMI und Engineering-Station. Ab SL 1 gefordert. Ein kleiner Betrieb arbeitet mit zwei gekennzeichneten Service-Sticks, die nur an einer Schleusenstation beschrieben werden.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 2.3 RE 1 Vor dem Anschluss wird der Sicherheitszustand eines tragbaren oder mobilen Geräts geprüft, und Geräte, die den Vorgaben nicht entsprechen, werden am Zugriff gehindert.

Woran man es festmacht: Prüfkriterien für den Gerätezustand, etwa aktueller Schadsoftwareschutz und Patchstand, dazu Prüfprotokolle je Servicegerät und der Nachweis der technischen Durchsetzung, etwa über eine Schleusenstation oder eine Netzzugangskontrolle. Erweiterung, ab SL 3 gefordert.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 2.4 Für nachladbaren, auf dem System ausgeführten Code, etwa Skripte in Bedienoberflächen oder aktive Inhalte in Berichten, ist festgelegt, welche Arten zulässig sind, und nicht zugelassene Arten werden an der Ausführung gehindert.

Dokument

Woran man es festmacht: Festlegung, welcher nachladbare Code auf welchen Systemen erlaubt ist, dazu Konfigurationsnachweise der Sperre, etwa Skriptausführung im HMI-Browser deaktiviert, Makros in Auswertungsdateien blockiert. Ab SL 1 gefordert. Eine einseitige Festlegung mit den drei bis vier tatsächlich vorhandenen Fällen genügt.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 2.4 RE 1 Vor der Ausführung von nachladbarem Code wird geprüft, ob er aus der erwarteten Quelle stammt und unverändert ist.

Woran man es festmacht: Konfigurationsnachweis der Signaturprüfung oder Prüfsummenkontrolle, dazu ein Testprotokoll, in dem manipulierter oder unsignierter Code abgewiesen wird. Erweiterung, ab SL 3 gefordert.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 2.5 Eine Sitzung wird nach einer festgelegten Zeit ohne Bedienhandlung gesperrt und erst nach erneuter Anmeldung wieder freigegeben, ohne dass die Anzeige sicherheitsrelevanter Prozessinformationen dadurch verloren geht.

Woran man es festmacht: Konfigurationsauszug mit der eingestellten Sperrzeit je Arbeitsplatz sowie eine Begründung für Arbeitsplätze in ständig besetzten Warten, an denen die Sperre bewusst anders eingestellt ist. Ab SL 1 gefordert. Sichtnachweis: Bildschirmfoto der Sperrmaske mit weiterhin sichtbarer Alarmzeile.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 2.6 **Sitzungen aus der Ferne werden nach einer festgelegten Zeit ohne Aktivität oder auf Anforderung des Betreibers beendet, sodass keine offene Fernverbindung unbeaufsichtigt bestehen bleibt.**

Woran man es festmacht: Konfiguration des Fernzugangs mit Zeitgrenze für Untätigkeit, Protokolleinträge beendeter Fernsitzungen sowie die Beschreibung, wie der Betreiber eine laufende Fernwartung sofort trennen kann, etwa über einen Schlüsselschalter oder eine Freigabe je Sitzung. Ab SL 2 gefordert, nicht auf SL 1.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 2.7 **Die Zahl gleichzeitig offener Sitzungen je Konto oder Rolle ist begrenzt, und darüber hinausgehende Anmeldeversuche werden abgewiesen.**

Woran man es festmacht: Konfigurationsauszug mit der festgelegten Obergrenze je Rolle, etwa <= 1 gleichzeitige Sitzung für projektierende Konten, dazu ein Testprotokoll des abgewiesenen zweiten Anmeldeversuchs. Ab SL 3 gefordert.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 2.8 **Sicherheitsrelevante Ereignisse werden aufgezeichnet, und jeder Eintrag benennt mindestens Zeitpunkt, Quelle, auslösendes Konto, Art des Ereignisses und Ergebnis.** Dokument

Woran man es festmacht: Festlegung der aufzuzeichnenden Ereignisarten, etwa Anmeldung, fehlgeschlagene Anmeldung, Rechteänderung, Programmänderung, Konfigurationsänderung, dazu ein realer Ausschnitt der Protokolldatei, der die genannten Felder zeigt. Ab SL 1 gefordert. Ein kleiner Betrieb sammelt die Protokolle von Leitsystem, HMI und Firewall in einem Ordner mit fester Aufbewahrungsfrist.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 2.8 RE 1 **Die Protokolle der einzelnen Komponenten laufen an einer zentralen Stelle zusammen und ergeben eine gemeinsame, systemweit auswertbare Aufzeichnung.**

Woran man es festmacht: Architekturskizze der Protokollsammlung mit allen angebundenen Quellen, dazu eine Auswertung, die Ereignisse aus mindestens zwei Komponenten in einer Zeitleiste zeigt. Erweiterung, ab SL 3 gefordert.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 2.9 **Für die Protokollaufzeichnung ist ausreichend Speicher vorgesehen, damit Ereignisse über den festgelegten Aufbewahrungszeitraum erhalten bleiben und nicht ungewollt überschrieben werden.**

Woran man es festmacht: Berechnung oder Abschätzung des Speicherbedarfs aus täglichem Protokollvolumen mal Aufbewahrungsdauer, dazu die eingestellte Speichergrösse und die Auslagerungsregel. Ab SL 1 gefordert. Praktisch reicht ein täglicher Kopiervorgang auf eine getrennte Ablage mit dokumentierter Aufbewahrungsfrist.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 2.9 RE 1 **Beim Erreichen einer festgelegten Füllstandsschwelle des Protokollspeichers wird eine Warnung an die zuständige Stelle ausgegeben, bevor Speicherplatz vollständig aufgebraucht ist.**

Woran man es festmacht: Konfigurationsauszug der Schwelle, etwa Warnung ab >= 80 Prozent Belegung, sowie ein Beispiel der ausgelösten Meldung und der Empfängerliste. Erweiterung, ab SL 3 gefordert.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 2.10 **Fällt die Protokollierung aus oder läuft der Protokollspeicher voll, reagiert das System auf eine vorher festgelegte Weise und die zuständige Stelle wird informiert, ohne dass der sichere Betrieb der Anlage gefährdet wird.**

Woran man es festmacht: Festgelegte Reaktion je Fehlerfall, etwa ältere Einträge überschreiben und melden statt Anlagenstopp, mit Begründung aus der Prozesssicht. Nachweis über eine ausgelöste Testmeldung und den zugehörigen Protokolleintrag. Ab SL 1 gefordert.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 2.11 **Jede Protokollaufzeichnung trägt einen Zeitstempel aus einer benannten Zeitquelle, sodass sich Ereignisse verschiedener Komponenten zeitlich zueinander einordnen lassen.**

Woran man es festmacht: Angabe der verwendeten Zeitquelle je Komponente und ein Protokollausschnitt mit sichtbarem Zeitstempel samt Zeitzonenangabe. Ab SL 2 gefordert, nicht auf SL 1.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 2.11 RE 1 **Die Uhren aller beteiligten Komponenten werden gegen eine gemeinsame Zeitquelle abgeglichen, sodass die Abweichung innerhalb einer festgelegten Grenze bleibt.**

Woran man es festmacht: Konfiguration des Zeitabgleichs, etwa NTP-Server und Abgleichintervall, dazu ein Prüfprotokoll mit den gemessenen Abweichungen je Komponente gegen die festgelegte Grenze, etwa <= 1 Sekunde. Erweiterung, ab SL 3 gefordert.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 2.11 RE 2 **Die Zeitquelle selbst ist gegen Manipulation geschützt, und ein unplausibler oder veränderter Zeitbezug wird erkannt und gemeldet.**

Woran man es festmacht: Beschreibung der Absicherung der Zeitquelle, etwa authentisierter Zeitabgleich, Beschränkung auf eine interne Quelle, Überwachung auf Zeitsprünge, dazu Meldungen oder Protokolleinträge einer erkannten Abweichung. Erweiterung, nur ab SL 4 gefordert.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 2.12 **Für festgelegte kritische Handlungen lässt sich nachträglich zweifelsfrei belegen, wer sie ausgelöst hat, sodass die handelnde Person dies nicht glaubhaft abstreiten kann.** Dokument

Woran man es festmacht: Liste der Handlungen, für die dieser Nachweis gilt, etwa Rezeptänderung, Freigabe einer Charge, Änderung von Grenzwerten, dazu die zugehörigen Aufzeichnungen mit eindeutiger Personenkennung und der Nachweis, dass Gruppenkonten hierfür ausgeschlossen sind. Ab SL 3 gefordert.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 2.12 RE 1 **Der zweifelsfreie Nachweis der handelnden Person gilt nicht nur für ausgewählte kritische Handlungen, sondern für alle Nutzer und alle von ihnen ausgelösten Aktionen.**

Woran man es festmacht: Nachweis, dass jedes Konto personengebunden ist und keine geteilten Anmeldungen mehr bestehen, dazu ein Protokollausschnitt beliebiger Aktionen, in dem durchgängig eine eindeutige Personenkennung steht. Erweiterung, nur ab SL 4 gefordert.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

7 FR 3: Systemintegrität, Schutz von Daten, Software und Sitzungen vor unbefugter Veränderung 19

SR 3.1 **Das Automatisierungssystem erkennt, wenn Informationen während der Übertragung über einen Kommunikationskanal verändert wurden, und zwar für Steuerdaten, Konfigurationsdaten und Verwaltungsverkehr gleichermaßen. Der Schutz gilt auch für Verbindungen, die das System verlassen oder ungesicherte Netzsegmente durchqueren.**

Woran man es festmacht: Netz- und Protokollübersicht mit Angabe, welcher Kanal welchen Integritätsschutz nutzt (Prüfsumme, Message Authentication Code, signierte Telegramme), Konfigurationsauszug der Feldbus- oder OPC-UA-Sicherheitseinstellungen und ein Testprotokoll, in dem ein manipuliertes Telegramm nachweislich verworfen wurde. Ein kleiner Betrieb dokumentiert das in einer Tabelle je Verbindung mit Spalten Quelle, Ziel, Protokoll, Integritätsmechanismus und weist die Wirksamkeit einmalig mit einem Mitschnitt nach. Ab SL 1 gefordert.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 3.1 RE 1 **Der Integritätsschutz der Übertragung beruht auf kryptografischen Verfahren, sodass eine gezielte Manipulation durch einen Angreifer mit eigenen Mitteln nicht unerkannt bleibt. Eine einfache Prüfsumme gegen Übertragungsfehler genügt hier nicht.**

Woran man es festmacht: Liste der eingesetzten kryptografischen Verfahren und Schlüssellängen je Kanal, Verweis auf die zugrunde liegende Schlüsselverwaltung und Konfigurationsauszüge (zum Beispiel TLS-Cipher-Suiten, OPC-UA-SecurityPolicy, IPsec-Profile). Kleine Betriebe nutzen die Werkseinstellungen sicherer Profile ihrer Steuerungen und legen einen Screenshot der aktiven Einstellung ab. Erweiterung, gefordert ab SL 3.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 3.2 **Es bestehen Schutzmechanismen gegen Schadsoftware, die verhindern, dass unerwünschter Programmcode auf Systemkomponenten ausgeführt wird, und die einen Fund melden. Die Mechanismen sind so gewählt, dass sie den bestimmungsgemäßen Betrieb der Anlage nicht stören, und sie werden aktuell gehalten.**

Woran man es festmacht: Übersicht je Komponente, welcher Mechanismus greift (Virenschutz, Anwendungs-Whitelisting, gehärtetes Betriebssystem ohne Ausführungsrechte), Nachweis der Aktualisierung von Signaturen oder Whitelists sowie Meldungen aus dem Schutzsystem. Wo kein Virenschutz möglich ist, etwa auf einer Steuerung, wird die kompensierende Maßnahme begründet festgehalten. Kleine Betriebe fahren mit Whitelisting auf dem Bedien-PC und einer schriftlichen Regel für USB-Medien gut. Ab SL 1 gefordert.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 3.2 RE 1 **Der Schutz gegen Schadsoftware wirkt zusätzlich an den Übergangspunkten der Anlage, an denen Daten hinein oder hinaus gelangen, und nicht nur auf den Endgeräten selbst.**

Woran man es festmacht: Liste aller Ein- und Ausgangspunkte (Fernwartungszugang, Datenschleuse, Wechselmedien, Übergabe zum Büronetz, E-Mail-Weg für Programmstände) mit dem jeweils dort wirkenden Prüfmechanismus sowie Protokolle der geprüften Übergaben. Kleine Betriebe richten einen einzigen Übergabe-PC mit Virenprüfung als Schleuse ein und halten das in einer Arbeitsanweisung fest. Erweiterung, gefordert ab SL 2.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 3.2 RE 2 **Die Schutzmechanismen gegen Schadsoftware werden von zentraler Stelle verwaltet, Aktualisierungen werden zentral verteilt und Funde laufen an einer Stelle zur Auswertung zusammen.**

Woran man es festmacht: Konfiguration der zentralen Verwaltungskonsole, Bericht über den Aktualisierungsstand aller angeschlossenen Komponenten und eine Auswertung der gemeldeten Funde über einen Zeitraum. Erweiterung, gefordert ab SL 3.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 3.3 **Die Sicherheitsfunktionen des Systems werden in geplanten Abständen sowie nach Änderungen daraufhin überprüft, dass sie tatsächlich wirken. Die Prüfungen werden so gelegt, dass sie den Betrieb der Anlage nicht gefährden, und die Ergebnisse werden festgehalten.** Dokument

Woran man es festmacht: Prüfplan mit Prüfgegenstand, Intervall und Zeitfenster, dazu die Prüfprotokolle mit Datum, Prüfer, Sollverhalten und beobachtetem Verhalten. Sinnvolle Einzelprüfungen sind: Anmeldung mit gesperrtem Konto scheitert, Virenschutz schlägt bei einer Testdatei an, Fernwartungszugang ist ohne Freigabe nicht erreichbar. Kleine Betriebe hängen die Prüfung an den ohnehin geplanten Wartungsstillstand und arbeiten eine feste Checkliste ab. Ab SL 1 gefordert.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 3.3 RE 1 **Die Überprüfung der Sicherheitsfunktionen läuft mit automatisierten Mitteln ab, sodass sie ohne manuellen Aufwand wiederholbar ist und ein einheitliches Ergebnis liefert.**

Woran man es festmacht: Skripte oder Prüfwerkzeuge samt Zeitplanung, deren Ausgabedateien sowie ein Vergleich mehrerer Läufe, der zeigt, dass Abweichungen erkannt werden. Erweiterung, gefordert ab SL 3.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 3.3 RE 2 **Die Überprüfung der Sicherheitsfunktionen ist auch im laufenden Betrieb möglich, ohne dass die Anlage dafür angehalten oder in einen Sonderzustand versetzt werden muss.**

Woran man es festmacht: Beschreibung des Prüfverfahrens mit Nachweis der Rückwirkungsfreiheit, etwa eine Analyse der Auswirkungen auf Zykluszeiten und Netzlast, sowie Prüfprotokolle aus dem Produktivbetrieb. Erweiterung, gefordert ab SL 4.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SR 3.4 **Unbefugte Veränderungen an Software, Firmware und Informationen im Ruhezustand werden erkannt. Das gilt für Steuerungsprogramme, Parametersätze, Rezepturen und Konfigurationsdateien gleichermaßen.**

Woran man es festmacht: Verzeichnis der schützenswerten Stände mit hinterlegten Prüfwerten oder Signaturen, Ergebnisse der Integritätsvergleiche und der dokumentierte Abgleich mit der Version aus der Versionsverwaltung. Kleine Betriebe legen den freigegebenen Programmstand mit gebildeter Prüfsumme auf einem schreibgeschützten Ablageort ab und vergleichen bei Verdacht oder nach Wartung. Ab SL 1 gefordert.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SR 3.4 RE 1 **Wird eine Verletzung der Integrität von Software oder Informationen festgestellt, meldet das System dies selbsttätig an eine zuständige Stelle, ohne dass jemand aktiv nachsehen muss.**

Woran man es festmacht: Konfiguration der Meldewege (Alarm auf der Leitwarte, E-Mail, Meldung an das Überwachungssystem), Empfängerliste mit Vertretungsregelung und mindestens ein Testalarm mit dokumentierter Reaktionszeit. Erweiterung, gefordert ab SL 3.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SR 3.5 **Eingaben, die das System aus Prozessdaten, Schnittstellen oder Benutzeroberflächen entgegennimmt, werden auf zulässige Syntax, zulässigen Wertebereich und zulässige Länge geprüft, bevor sie verarbeitet werden. Unzulässige Eingaben führen nicht zu unkontrolliertem Verhalten.**

Woran man es festmacht: Spezifikation der Grenzwerte und Formate je Eingang, Auszüge aus der Prüflogik in der Steuerung oder Applikation sowie Testfälle mit bewusst falschen Eingaben (zu großer Wert, falscher Datentyp, überlange Zeichenkette) und dem dokumentierten Verhalten des Systems. Kleine Betriebe legen die Plausibilitätsgrenzen je Messstelle in einer Tabelle ab und prüfen sie bei der Inbetriebnahme durch. Ab SL 1 gefordert.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SR 3.6 **Für den Fall einer Störung ist festgelegt, welchen Zustand die Ausgänge zur Anlage einnehmen, und das System nimmt genau diesen Zustand ein. Der festgelegte Zustand ist mit der funktionalen Sicherheit der Anlage abgestimmt.**

Woran man es festmacht: Festlegung je Ausgang oder Ausgangsgruppe (Wert halten, definierter Ersatzwert, sicherer Abschaltzustand) mit Begründung aus der Risikobetrachtung, Konfigurationsauszug der Steuerung und ein Nachweis aus dem Ausfalltest, etwa Kabelbruch oder Kommunikationsverlust, der das erwartete Verhalten zeigt. Ab SL 1 gefordert.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SR 3.7 **Das System behandelt Fehlerzustände so, dass der Betrieb kontrolliert bleibt und keine Informationen preisgegeben werden, die einem Angreifer nützen. Fehlermeldungen an die Bedienung bleiben knapp, während die technischen Einzelheiten nur in den internen Aufzeichnungen landen.**

Woran man es festmacht: Übersicht der Fehlerklassen mit dem jeweils vorgesehenen Systemverhalten, Beispiele der angezeigten Meldungen im Vergleich zu den zugehörigen internen Protokolleinträgen sowie ein Testnachweis, dass keine Pfadangaben, Kontonamen, Datenbankausgaben oder Versionsdetails auf der Bedienoberfläche erscheinen. Ab SL 1 gefordert.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SR 3.8 **Laufende Sitzungen sind gegen Übernahme und Einschleusen fremder Nachrichten geschützt. Eine Sitzung endet nach dem Abmelden oder nach einer festgelegten Zeit ohne Aktivität, und danach ist sie nicht wiederverwendbar.**

Woran man es festmacht: Konfiguration der Sitzungsverwaltung mit den eingestellten Zeitgrenzen für Leerlauf und Höchstdauer, Nachweis des Schutzmechanismus gegen Wiedereinspielen von Nachrichten sowie ein Testprotokoll, in dem eine mitgeschnittene Sitzung nach dem Abmelden nicht mehr funktioniert. Ab SL 2 gefordert.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SR 3.8 RE 1 **Sitzungskennungen verlieren mit dem Ende der Sitzung ihre Gültigkeit und werden vom System nicht erneut anerkannt, auch dann nicht, wenn sie von außen wieder vorgelegt werden.**

Woran man es festmacht: Konfigurationsauszug der Sitzungsverwaltung zur Ungültigkeitserklärung sowie ein Testprotokoll, in dem eine zuvor gültige Kennung nach dem Abmelden erneut gesendet und vom System abgewiesen wird. Erweiterung, gefordert ab SL 3.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SR 3.8 RE 2 **Für jede neue Sitzung wird eine eigene, nur einmal verwendete Kennung erzeugt. Kennungen werden nicht zwischen Sitzungen, Benutzern oder Geräten wiederverwendet.**

Woran man es festmacht: Beschreibung des Erzeugungsverfahrens und ein Nachweis aus dem Protokoll oder Mitschnitt, dass mehrere aufeinanderfolgende Anmeldungen unterschiedliche Kennungen erhalten. Erweiterung, gefordert ab SL 3.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SR 3.8 RE 3 **Sitzungskennungen werden mit anerkannten Zufallsverfahren erzeugt, sodass sie sich weder erraten noch aus vorhergehenden Kennungen ableiten lassen.**

Woran man es festmacht: Angabe des verwendeten Zufallszahlengenerators und seiner Entropiequelle, Herstellererklärung oder Prüfbericht dazu sowie eine statistische Auswertung einer Stichprobe erzeugter Kennungen. Erweiterung, gefordert ab SL 4.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SR 3.9 **Die sicherheitsrelevanten Aufzeichnungen und die Werkzeuge, mit denen sie ausgewertet werden, sind gegen unbefugten Zugriff, Veränderung und Löschung geschützt. Der Kreis derer, die Aufzeichnungen ändern oder entfernen dürfen, ist eng gefasst und benannt.** Dokument

Woran man es festmacht: Berechtigungskonzept für die Protokolldaten mit namentlicher Zuordnung, Konfiguration der Weiterleitung auf ein getrenntes Protokollsystem, Aufbewahrungsfristen sowie ein Testnachweis, dass ein normaler Bediener Einträge nicht löschen kann. Kleine Betriebe leiten die Protokolle auf ein separates Gerät weiter, auf das die Anlagenbediener keinen Schreibzugriff haben. Ab SL 2 gefordert.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SR 3.9 RE 1 **Die sicherheitsrelevanten Aufzeichnungen werden zusätzlich auf einem Medium abgelegt, das nachträgliches Überschreiben ausschließt, sodass ein einmal geschriebener Eintrag auch mit Verwaltungsrechten nicht mehr verändert werden kann.** Dokument

Woran man es festmacht: Beschreibung der eingesetzten Ablage (einmal beschreibbares Medium, revisionssicherer Speicher, fortgeschriebene Signaturkette), Nachweis eines erfolglosen Änderungsversuchs und die Regelung, wie die Medien aufbewahrt und wiedergefunden werden. Erweiterung, gefordert ab SL 3.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

8 FR 4: Vertraulichkeit der Daten 6

SR 4.1 **Das Automatisierungssystem schützt vertrauliche Informationen vor unbefugter Kenntnisnahme, sowohl während der Übertragung als auch bei ruhender Speicherung. Es ist festgelegt, welche Daten als vertraulich gelten, etwa Rezepturen, Parametersätze, Zugangsdaten, Konfigurationsdateien oder Diagnosedaten mit Personenbezug.** Dokument

Woran man es festmacht: Liste der schutzbedürftigen Datenarten mit Speicherort und Übertragungsweg, dazu die konkrete Schutzmaßnahme je Eintrag, zum Beispiel verschlüsselte Verbindung, verschlüsselter Datenträger oder eingeschränkte Freigabe. Ein kleiner Betrieb kommt mit einer einseitigen Tabelle aus: Datenart, wo sie liegt, wer sie sehen darf, womit sie geschützt ist. Gefordert ab SL 1.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 4.1 RE 1 **Für Informationen, die über nicht vertrauenswürdige Netze übertragen oder ausserhalb der geschützten Umgebung gespeichert werden, ist die Vertraulichkeit technisch durchgesetzt und nicht nur organisatorisch zugesagt.**

Woran man es festmacht: Konfigurationsauszug der eingesetzten Transportverschlüsselung oder Datenträgerverschlüsselung, zum Beispiel VPN-Profil für Fernwartung, TLS-Einstellungen der Leitsystem-Schnittstelle, Verschlüsselung der Backup-Medien. Ein Screenshot der aktiven Einstellung mit Datum genügt als Beleg. Gefordert ab SL 2, nicht ab SL 1, da es sich um eine Erweiterung handelt.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 4.1 RE 2 **Die Vertraulichkeit ist auch an den Grenzen zwischen Zonen durchgesetzt, sodass Informationen beim Übergang von einer Zone in eine andere nicht ungeschützt sichtbar werden.**

Woran man es festmacht: Zonen- und Übergangsplan mit Kennzeichnung, welche Übergänge verschlüsselt sind, dazu Konfiguration der Übergangskomponente wie Gateway, Firewall oder Datendiode. Aufzeichnung eines Mitschnitts oder einer Prüfung, die zeigt, dass am Übergang keine Klartextdaten anliegen. Gefordert ab SL 4.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 4.2 **Es ist geregelt, wie vertrauliche Informationen zuverlässig entfernt werden, wenn Geräte ausser Betrieb gehen, den Besitzer wechseln, zur Reparatur gehen oder wiederverwendet werden, sodass keine lesbaren Restdaten zurückbleiben.** Dokument

Woran man es festmacht: Verfahrensbeschreibung zur Aussonderung mit Löschverfahren je Geräteart und Löschprotokolle mit Geräte-Identifikation, Datum und ausführender Person. Ein kleiner Betrieb protokolliert das in einer Zeile pro Gerät in einer gemeinsamen Liste und legt Zertifikate externer Entsorger dazu. Gefordert ab SL 2.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 4.2 RE 1 **Gemeinsam genutzte Speicherbereiche werden vor der erneuten Zuteilung an einen anderen Nutzer oder Prozess bereinigt, sodass keine Inhalte des vorherigen Nutzers ausgelesen werden können.**

Woran man es festmacht: Herstellerangabe oder Konfigurationsnachweis zur Bereinigung wiederverwendeter Speicher- und Pufferbereiche, ergänzt um ein Prüfprotokoll aus dem Abnahme- oder Wartungstest. Wo die Komponente das nicht kann, dient die dokumentierte Ausgleichsmaßnahme als Beleg, etwa keine Mehrfachnutzung des Gerätes durch verschiedene Rollen. Gefordert ab SL 3, nicht ab SL 1, da es sich um eine Erweiterung handelt.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 4.3 **Wo kryptografische Verfahren eingesetzt werden, entsprechen Algorithmen, Schlüssellängen und der Umgang mit Schlüsseln dem anerkannten Stand der Technik, und es ist geregelt, wie Schlüssel erzeugt, verteilt, gespeichert, gewechselt und zurückgezogen werden.** Dokument

Woran man es festmacht: Übersicht der eingesetzten Verfahren je System mit Algorithmus, Schlüssellänge und Gültigkeitsdauer, dazu die Regelung zur Schlüsselverwaltung und Aufzeichnungen über Schlüsselwechsel und Zertifikatserneuerungen. Als Massstab dienen öffentliche Empfehlungen, etwa die technischen Richtlinien des BSI. Ein kleiner Betrieb führt eine Zertifikatsliste mit Ablaufdatum und einer Erinnerung >= 30 Tage vor Ablauf. Gefordert ab SL 1.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

9 FR 5: Eingeschränkter Datenfluss, Zonen und Conduits 11

SR 5.1 **Das System kann in abgegrenzte Zonen aufgeteilt werden, und der Datenverkehr zwischen diesen Zonen läuft ausschliesslich über definierte Übergänge. Die Aufteilung folgt einem nachvollziehbaren Schnitt, etwa nach Schutzbedarf, Verantwortung oder Funktion der Anlagenteile.**

Dokument

Woran man es festmacht: Netzplan mit eingezeichneten Zonen und den Übergängen dazwischen, Liste der Zonen mit jeweiliger Begründung des Schnitts, Konfiguration der trennenden Komponenten wie VLAN-Definitionen oder Firewall-Interfaces. Ein kleiner Betrieb kommt mit einer einseitigen Skizze aus, auf der Büro, Maschinennetz und Fernwartungszugang als drei Kästen mit den Verbindungen dazwischen stehen, plus einem Screenshot der VLAN-Konfiguration des Switches.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 5.1 RE 1 **Die Trennung der Zonen ist physisch ausgeführt, also über eigene Netzkomponenten und eigene Verkabelung, und beruht nicht allein auf einer logischen Konfiguration innerhalb gemeinsam genutzter Geräte. Abschnitt 9.1 in dieser Liste, gefordert ab SL 2. Erweiterungen dieser Norm sind nie bereits ab SL 1 verpflichtend.**

Woran man es festmacht: Inventar der Netzkomponenten mit Zuordnung, welcher Switch oder Router welche Zone bedient, Fotos oder Schrankplan der getrennten Verteilungen, Kabelkennzeichnung. Kleine Betriebe belegen das mit zwei getrennten, klar beschrifteten Switches statt eines geteilten Geräts und einem Foto des Schaltschranks in der Anlagendokumentation.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 5.1 RE 2 **Das Automatisierungsnetz kann ohne Netze ausserhalb der Automatisierung betrieben werden. Fällt die Büro-IT oder eine externe Anbindung aus, laufen Steuerung und Überwachung der Anlage weiter. Gefordert ab SL 3.**

Woran man es festmacht: Abhängigkeitsliste der im Automatisierungsnetz genutzten Dienste wie Zeitserver, Namensauflösung, Verzeichnisdienst oder Lizenzserver mit Angabe, wo diese betrieben werden, sowie ein Testprotokoll eines Trennversuchs, bei dem die Verbindung zur Büro-IT gezogen wurde. Ein kleiner Betrieb notiert das Ergebnis eines solchen Versuchs im Wartungsprotokoll: Uplink gezogen, Anlage lief weiter, nur die Berichte im Büro fehlten.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 5.1 RE 3 **Zonen mit besonders kritischen Funktionen, etwa Sicherheits- oder Schutzfunktionen, sind sowohl logisch als auch physisch von den übrigen Zonen abgesetzt. Gefordert ab SL 4.**

Woran man es festmacht: Kennzeichnung der kritischen Zonen im Zonenplan mit Begründung der Einstufung, Nachweis eigener Netzkomponenten und eigener Verkabelung für diese Zonen, Konfiguration der Übergänge mit Nachweis, dass kein gemeinsamer Pfad besteht.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 5.2 **An den Zonenübergängen wird der Datenverkehr kontrolliert, überwacht und nach festgelegten Regeln durchgelassen oder blockiert. Es gibt keinen Weg zwischen zwei Zonen, der an dieser Kontrolle vorbeiführt.**

Woran man es festmacht: Regelwerk der Firewall oder des Übergangsgeräts im Export, Protokolle der geblockten und erlaubten Verbindungen, Nachweis, dass es keine Nebenwege gibt, etwa durch eine Prüfung auf zusätzliche Netzwerkkarten, Modems oder Mobilfunkrouter in Anlagenrechnern. Ein kleiner Betrieb belegt das mit dem Regel-Export der einen Firewall und einer kurzen Begehungsnotiz, dass in keinem Schaltschrank ein ungeplanter Router steckt.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 5.2 RE 1 **Das Regelwerk am Zonenübergang arbeitet nach dem Grundsatz, dass alles gesperrt ist, was nicht ausdrücklich freigegeben wurde. Jede Freigabe ist einzeln begründet und einem Zweck zugeordnet. Gefordert ab SL 2.**

Woran man es festmacht: Regelwerk mit sichtbarer Schlussregel, die den Rest verwirft, und eine Freigabeliste, in der zu jeder Regel Quelle, Ziel, Dienst, Zweck und verantwortliche Person stehen. Kleine Betriebe führen diese Liste als Tabelle mit fünf Spalten neben dem Firewall-Export und prüfen sie einmal im Jahr auf Regeln, die niemand mehr braucht.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 5.2 RE 2 **Das Automatisierungsnetz kann bewusst von allen äusseren Verbindungen abgekoppelt und im abgeschotteten Betrieb weitergefahren werden. Der Vorgang ist auslösbar, ohne die Anlage anhalten zu müssen. Gefordert ab SL 3.**

Woran man es festmacht: Beschreibung des Abkoppelvorgangs mit Angabe, wer ihn auslösen darf und wie, Nachweis der technischen Umsetzung, etwa ein Regelsatz für den Notbetrieb oder ein gekennzeichneter Trennschalter, sowie das Protokoll einer Übung, bei der die Abkopplung tatsächlich getestet wurde. Ein kleiner Betrieb hält die Übung einmal im Jahr im Rahmen der Wartung ab und notiert Datum, Dauer und Auffälligkeiten.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SR 5.2 RE 3 **Fällt das Gerät am Zonenübergang aus oder verliert es seine Regeln, sperrt es den Verkehr, statt ihn durchzulassen. Der Ausfall darf keine offene Verbindung hinterlassen. Gefordert ab SL 4.**

Woran man es festmacht: Herstellerangabe oder Konfigurationsnachweis zum Verhalten der Komponente bei Störung und Neustart, Testprotokoll eines gezielt herbeigeführten Ausfalls mit dem beobachteten Ergebnis, Abgleich mit der Risikobetrachtung der Anlage, weil ein sperrender Übergang je nach Prozess selbst Folgen haben kann.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SR 5.3 **Allgemeine Kommunikationsdienste zwischen Personen, etwa E-Mail, Messenger oder Videotelefonie, lassen sich auf Geräten und in Netzen der Automatisierung unterbinden. Der Umfang der Sperrung ist festgelegt und begründet.**

Woran man es festmacht: Festlegung, welche Dienste im Automatisierungsnetz unzulässig sind, dazu die technische Umsetzung: gesperrte Ports und Ziele im Regelwerk, entfernte oder blockierte Anwendungen auf Bedienrechnern, Nachweis über die Softwareliste der Geräte. Ein kleiner Betrieb erledigt das mit einer Anwendungssperre auf dem HMI-Rechner und der Regel, dass ausgehender Mail- und Web-Verkehr aus dem Maschinennetz blockiert ist.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SR 5.3 RE 1 **Solche Kommunikationsdienste zwischen Personen sind im Automatisierungsnetz vollständig unterbunden, nicht nur teilweise eingeschränkt oder auf einzelne Geräte begrenzt. Gefordert ab SL 2.**

Woran man es festmacht: Nachweis, dass die Sperre für alle Geräte der Zone gilt, etwa über eine Auswertung der installierten Software auf jedem Rechner der Zone und einen Verbindungstest von einem beliebigen Anlagenrechner aus. Kleine Betriebe belegen das mit einer Geräteliste, in der jede Zeile mit dem Prüfdatum abgehakt ist, und einem Screenshot des fehlgeschlagenen Verbindungsversuchs.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SR 5.4 **Daten und Funktionen der Anwendungen sind so getrennt, dass Prozesse mit unterschiedlichem Schutzbedarf oder unterschiedlichen Rechten nicht auf dieselben Bereiche zugreifen. Die Trennung ist im Systemaufbau vorgesehen und nicht dem Zufall der Installation überlassen.**

Woran man es festmacht: Übersicht der Anwendungen mit Angabe, welche Daten und Dienste sie nutzen und welche Konten dahinterstehen, Konfiguration getrennter Instanzen, Datenbanken, Verzeichnisse oder virtueller Maschinen, Berechtigungsliste je Bereich. Ein kleiner Betrieb löst das über getrennte Benutzerkonten und getrennte Datenordner für Engineering und Bedienung sowie eine Notiz, welche Anwendung auf welchen Ordner zugreift.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

10 FR 6: Zeitnahe Reaktion auf Ereignisse 3

SR 6.1 **Die im System gesammelten Ereignisaufzeichnungen sind für die dafür berechtigten Personen und Rollen les- und auswertbar, ohne dass der laufende Betrieb der Anlage gestört wird, und der Zugriff darauf ist selbst auf befugte Nutzer beschränkt.**

Woran man es festmacht: Rollen- und Rechtematrix, die zeigt, wer Protokolldaten einsehen darf, plus ein Screenshot oder Export einer tatsächlich abgerufenen Protokollansicht mit Zeitstempel. Ergänzend eine kurze Notiz, über welchen Weg der Abruf erfolgt, etwa Bedienoberfläche der Steuerung, Log-Server oder Dateiexport. Kleine Betriebe genügen mit einer einseitigen Übersicht je Anlage: wo liegt das Protokoll, wer hat Lesezugriff, wie wird es geholt. Ein Testabruf einmal im Jahr, im Wartungsprotokoll vermerkt, belegt, dass der Weg funktioniert. Gilt ab SL 1 für alle Sicherheitsstufen.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SR 6.1 RE 1 **Die Ereignisaufzeichnungen lassen sich über eine maschinelle Schnittstelle abrufen, so dass Auswertewerkzeuge sie ohne manuelles Abtippen weiterverarbeiten können, und die Daten liegen dabei in einem dokumentierten, gängigen Format vor.**

Woran man es festmacht: Beschreibung der genutzten Schnittstelle mit Formatangabe, etwa Syslog, OPC UA Alarms and Conditions, REST-Abruf oder CSV-Export, dazu ein Beispieldatensatz und die Konfiguration des empfangenden Systems. Belegen lässt sich das mit einem Auszug aus der SIEM- oder Log-Sammler-Konfiguration und einem Nachweis eingehender Datensätze. Ohne SIEM reicht ein Log-Sammler auf einem einfachen Server, der die Protokolle nachts per Skript abholt und ablegt; das Skript selbst plus ein Verzeichnislisting der eingesammelten Dateien ist der Nachweis. Als Erweiterung erst ab SL 3 gefordert, nicht ab SL 1.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SR 6.2 **Sicherheitsrelevante Vorgänge im System werden fortlaufend beobachtet, die Überwachung erkennt Angriffsversuche und Fehlverhalten und meldet sie zeitnah an eine benannte Stelle, und die dafür eingesetzten Werkzeuge, Meldewege und Zuständigkeiten sind festgelegt.**

Woran man es festmacht: Übersicht der Überwachungswerkzeuge je Zone, etwa Netzwerksensor, Antivirenmeldungen, Firewall-Alarme oder Integritätsprüfung, mit der Angabe, wer die Meldung erhält und in welcher Frist reagiert wird. Als Beleg dienen Alarmkonfigurationen, eine Liste ausgelöster Meldungen der letzten Monate und die Bearbeitungsvermerke dazu. Kleine Betriebe kommen ohne Rund-um-die-Uhr-Leitstelle aus: eine Sammelmailadresse oder ein Ticketpostfach, das die Alarme der vorhandenen Systeme bündelt, plus eine feste Regel, dass ein Benannter sie an jedem Arbeitstag sichtet, ist ausreichend und wird über die Postfachhistorie belegt. Ab SL 2 gefordert.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

11 FR 7: Ressourcenverfügbarkeit 13

SR 7.1 **Das System bleibt bei Überlast oder gezielten Überflutungsangriffen in einem definierten Betriebszustand, die wesentlichen Steuerungsfunktionen laufen weiter, und ein Ausfall einzelner Dienste reisst die Anlage nicht mit.**

Woran man es festmacht: Konfiguration der Schutzmechanismen (Rate Limiting, Verbindungsgrenzen, Broadcast Storm Control auf den Switches), Herstellerangaben zum Verhalten unter Last sowie Protokoll eines Lasttests oder eines realen Überlastereignisses mit Beobachtung der Steuerungsfunktion. Gefordert ab SL 1. Ein kleiner Betrieb belegt das mit den Screenshots der Switch- und Firewall-Einstellungen und einer kurzen Notiz, welche Funktion bei einem Test der wichtigsten Zelle weiterlief.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SR 7.1 RE 1 **Die Kommunikationslast, die einzelne Komponenten in das Netz einspeisen können, ist begrenzt, sodass eine fehlerhafte oder übernommene Komponente das Netzsegment nicht flutet.**

Woran man es festmacht: Portbezogene Bandbreiten- und Multicast-Grenzen auf den Netzkomponenten, Nachweis der Begrenzung je Anschluss sowie eine Messung der tatsächlichen Grundlast je Gerät. Gefordert ab SL 2, nicht ab SL 1. Ohne Managed Switches lässt sich diese Zeile nicht belegen, das ist dann der offene Punkt.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SR 7.1 RE 2 **Eine Überlastsituation im betrachteten System wirkt sich nicht auf benachbarte Systeme oder Netze aus, die Rückwirkung nach aussen ist technisch begrenzt.**

Woran man es festmacht: Segmentierungs- und Filterregeln an den Übergängen, Nachweis der Begrenzung ausgehenden Verkehrs sowie Testprotokoll, das zeigt, dass eine erzeugte Last im Zellennetz das Büro- oder Nachbarnetz nicht beeinträchtigt hat. Gefordert ab SL 3.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SR 7.2 **Die Beanspruchung von Rechenzeit, Arbeitsspeicher, Speicherplatz und Netzbandbreite ist so begrenzt, dass ein einzelner Prozess oder Dienst die für die Steuerung notwendigen Ressourcen nicht aufzehren kann.**

Woran man es festmacht: Konfiguration der Ressourcengrenzen (Kontingente, Prozessprioritäten, Speichergrenzen), Auswertung der Auslastungsüberwachung über einen repräsentativen Zeitraum sowie Schwellwerte, bei deren Überschreiten gewarnt wird. Gefordert ab SL 1. Kleine Betriebe nutzen die Bordmittel des Betriebssystems und ein einfaches Monitoring mit Speicherplatz- und CPU-Alarm per E-Mail.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SR 7.3 **Von Konfigurationen, Anwendungsdaten und Programmständen des Systems bestehen Sicherungen, die ohne Unterbrechung des laufenden Betriebs erstellt werden können und die vor unbefugtem Zugriff und Veränderung geschützt sind.** Dokument

Woran man es festmacht: Sicherungskonzept mit Umfang, Rhythmus und Aufbewahrungsdauer, Sicherungsprotokolle der letzten Läufe sowie Nachweis des Zugriffsschutzes auf die Sicherungsmedien (getrennte Ablage, Verschlüsselung, eigene Berechtigungen). Gefordert ab SL 1. Ein kleiner Betrieb sichert SPS-Projekte und HMI-Stände auf ein verschlüsseltes, nach der Sicherung physisch getrenntes Medium und hält Datum und Version in einer einfachen Liste fest.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SR 7.3 RE 1 **Die Brauchbarkeit der Sicherungen ist überprüft, es ist belegt, dass sich aus ihnen tatsächlich ein funktionsfähiger Stand zurückspielen lässt.**

Woran man es festmacht: Protokoll einer Rückspielprobe mit Datum, geprüftem Sicherungsstand, Zielsystem und Ergebnis, mindestens für die kritischen Komponenten. Gefordert ab SL 2, nicht ab SL 1. Kleine Betriebe prüfen einmal jährlich stichprobenartig ein SPS-Programm und ein HMI-Abbild auf einem Ersatzgerät und halten das Ergebnis in zwei Sätzen fest.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SR 7.3 RE 2 **Die Sicherung läuft automatisiert nach festgelegtem Zeitplan ab, ein fehlgeschlagener Lauf wird erkannt und gemeldet.**

Woran man es festmacht: Zeitplan des Sicherungsauftrags, Ausführungsprotokolle ohne Lücken sowie Nachweis der Fehlermeldung bei einem gescheiterten Lauf (Alarm, Ticket, Mail). Gefordert ab SL 3.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SR 7.4 **Nach Störung, Ausfall oder Angriff lässt sich das System in einen bekannten, sicheren Zustand zurückführen, die Wiederherstellung ist geübt und die Verantwortlichkeiten sind benannt.** Dokument

Woran man es festmacht: Wiederanlaufplan je kritischer Komponente mit Reihenfolge, benötigten Medien, Ansprechpartnern und Zielzeit, dazu das Protokoll der letzten Wiederanlaufübung. Gefordert ab SL 1. Ein kleiner Betrieb kommt mit einer einseitigen Wiederanlaufkarte pro Anlage aus, die im Schaltschrank hängt und beim Ersatzteiltausch mitgeprüft wird.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SR 7.5 **Bei Ausfall der regulären Stromversorgung geht das System in einen definierten Zustand über, entweder wird die Versorgung ersatzweise aufrechterhalten oder es erfolgt ein geordnetes Herunterfahren ohne Verlust des sicheren Zustands.**

Woran man es festmacht: Auslegung und Wartungsnachweis der unterbrechungsfreien Stromversorgung oder des Notstromgeräts, Prüfprotokoll des letzten Batterie- oder Lasttests sowie Beschreibung des Verhaltens beim Umschalten und beim Wiederkehren der Spannung. Gefordert ab SL 1. Kleine Betriebe prüfen die USV jährlich unter Last und halten Testdatum, Überbrückungszeit und Batteriealter fest.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 7.6 **Die Netz- und Sicherheitseinstellungen des Systems sind auf einen freigegebenen Sollstand festgelegt, Abweichungen vom Sollstand sind erkennbar und der aktuelle Stand ist jederzeit abrufbar.** Dokument

Woran man es festmacht: Freigegebene Sollkonfiguration je Geräteklasse (Härtungsvorgabe), aktuelle Konfigurationsstände der Geräte sowie Ergebnis eines Soll-Ist-Abgleichs mit Liste der Abweichungen und deren Begründung. Gefordert ab SL 1. Ein kleiner Betrieb legt die Konfigurationsexporte versioniert ab und vergleicht sie vor und nach jeder Änderung.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 7.6 RE 1 **Der aktuelle Stand der Sicherheitseinstellungen lässt sich maschinenlesbar ausgeben, sodass er automatisiert gegen den Sollstand geprüft werden kann.**

Woran man es festmacht: Beispielausgabe im maschinenlesbaren Format (Konfigurationsexport, strukturierte Datei, Schnittstellenabfrage) und das Skript oder Werkzeug, das den Abgleich gegen den Sollstand ausführt, samt Ergebnisbericht eines Laufs. Gefordert ab SL 3.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 7.7 **Das System ist auf die für den Betrieb notwendigen Funktionen beschränkt, nicht benötigte Dienste, Ports, Protokolle und Schnittstellen sind abgeschaltet oder entfernt.**

Woran man es festmacht: Liste der aktiven Dienste und offenen Ports je Komponente mit Begründung des Bedarfs, Nachweis der Deaktivierung der übrigen (Konfiguration, Portscan-Ergebnis) sowie Regelung für USB- und Wartungsschnittstellen. Gefordert ab SL 1. Kleine Betriebe nehmen einen einfachen Portscan pro Segment auf und begründen jede offene Position in einer Zeile.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR 7.8 **Ein aktuelles Verzeichnis aller Systemkomponenten mit Hersteller, Typ, Firmware- oder Softwarestand und Netzadresse ist vorhanden und wird bei Änderungen nachgeführt.** Dokument

Woran man es festmacht: Komponentenverzeichnis mit Stand und Verantwortlichem, Nachweis der Pflege über die Änderungshistorie sowie Abgleich gegen eine Netzaufnahme, um nicht erfasste Geräte zu finden. Gefordert ab SL 2, nicht ab SL 1. Ein kleiner Betrieb führt das Verzeichnis als Tabelle und aktualisiert es verbindlich bei jedem Gerätetausch und jedem Firmware-Update.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung