INDUSTRIELLE STEUERUNGSSYSTEME

Inhaltsverzeichnis

Abbildungen

1.0 ANWENDUNGSBEREICH

Dieses Datenblatt enthält Schadenverhütungsempfehlungen für industrielle Steuerungssysteme (Industrial Control Systems, ICS). Dabei wird ein Systemansatz für die Bewertung von standortweiten ICS verfolgt, der auch ICS-Kommunikationsnetzwerke und Cyberrisiken berücksichtigt. Dieses Datenblatt enthält Lösungen zur Risikoreduzierung in Bezug auf Sachschutz und Geschäftskontinuität.

In diesem Dokument bedeutet der Begriff „industrielle Steuerungssysteme“ oder „ICS“ die Kombination von Hardwaresystemen und Softwareprogrammen, mit denen Prozesse, Produktion, Fertigung und dazugehörige Aktivitäten an Industrie- und Nicht-Industriestandorten kontrolliert, geschützt und überwacht werden. Die folgende Liste (nicht abschließend) enthält Beispiele von Hardwareressourcen, die an das ICS-Netzwerk angeschlossen sein können:

- Überwachung, Steuerung und Datenerfassung (SCADA)
- Prozessleitsystem (DCS), einschließlich Datenerfassungs- und Archivierungssystemen
- Speicherprogrammierbare Steuerung (SPS)
- Programmable Automation Controller (PAC)
- Gateway für Fremdgeräte
- Fernsteuerungs-Terminal (RTU)
- Netzwerkgeräte, einschließlich Netzwerk-Switches, Firewalls, Router usw.
- Intelligente Feldgeräte (z. B. intelligente Zähler, Armaturen, Relays und Prozesstransmitter)
- Gerätebus
- Mensch-Maschine-Schnittstelle (HMI)
- Engineeringstation
- Industrielle Schaltschränke, darunter Geräte- und Messtechnikschränke, E/A-Schränke (Ein- und Ausgabe) usw.
- Gebäudeleittechnik
- Intelligente Geräte oder industrielles Internet der Dinge (IIoT)

Dieses Datenblatt enthält allgemeine Richtlinien für ICS. Wenn für bestimmte Anlagen oder Prozesse spezifischere Datenblätter vorliegen, so haben die Angaben in diesen Datenblättern Vorrang.

Folgende Themen werden in diesem Datenblatt nicht behandelt:

- Detaillierte Auslegung oder detaillierter Betrieb von ICS-Anlagen oder Kommunikation/Netzwerken
- Leistung, Kompatibilität oder Funktionalität von Software
- Auslegung, Betrieb, Inspektion, Prüfung und Instandhaltung von sicherheitsgerichteten Steuerungen (SIS) (siehe FM Datenblatt zur Schadenverhütung 7-45, *Safety Controls, Alarms, and Interlocks*)
- IT-Systeme für den allgemeinen Geschäftsbetrieb (z. B. E-Mail-Programme, Programme mit Internetzugriff)

1.1. Gefahren

Wenn ICS nicht ordnungsgemäß verwaltet und instand gehalten werden, können aus kleineren Fehlfunktionen schwerwiegende Ausfälle werden, die dann zu Produktionsverlust und/oder potenziell erheblichen Sachschäden führen können. Es gibt verschiedene Faktoren, die zu einem Ausfall der Steuerungssysteme führen können. Beispiele hierfür sind böswillige Cyberangriffe, aber auch eine fehlende Planung von Notfall- und Wiederherstellungsmaßnahmen, die nach einem Cybervorfall greifen sollten.

1.2 Änderungen

Juli 2024. Zwischenrevision. Vornahme redaktioneller Änderungen

2.0 SCHADENVERHÜTUNGSEMPFEHLUNGEN

2.1 Einführung

Je nach Branche funktioniert jedes ICS unterschiedlich. ICS sind komplexe Systeme, bestehend aus Steuerungen, Logiksystemen, Motoren, Pumpen, Aktoren, Überwachungsanlagen, Sensoren usw., die alle über Kommunikationsnetzwerke miteinander verbunden sind.

Es ist wichtig, dass die für die standortweiten ICS verantwortlichen Mitarbeitenden über umfassende Kenntnisse des Gesamtsystems, der Betriebsanforderungen und erforderlichen Schutzmaßnahmen, der Kommunikationsnetzwerke sowie Softwareanforderungen verfügen, um Risiken und Gefahren in Bezug auf die standortweiten ICS identifizieren zu können.

2.2 Bauweise und Standort

2.2.1 Prozessleitwarten und dazugehörige wichtige Anlagenräume sollten außerhalb von Bereichen eingerichtet werden, in denen Explosionsgefahren vorliegen. Wenn dies nicht umsetzbar ist, sollte eine druckbeständige Bauweise gemäß FM Datenblatt zur Schadenverhütung 1-44, *Damage-Limiting Construction*, gewählt werden. Dabei gilt die Annahme, dass die Außenfläche der Leitwarte Überdruck ausgesetzt ist. Für die Stoßfestigkeit von Fenstern wird Verbundglas gemäß ANSI Z97.1 empfohlen (ASTM E1886 und E1996 oder FBC TAS 201 und 203 sind akzeptable Alternativen). Um dem Überdruck standzuhalten, wird für Fenster Verbundglas gemäß ASTM E1300 empfohlen.

2.2.2 Prozessleitwarten und dazugehörige Anlagenräume sollten so eingerichtet werden, dass sie nicht durch korrosive oder brennbare Flüssigkeiten, brennbare Gase oder mechanische Anlagen wie Kräne gefährdet werden.

2.2.3 Für aufgeständerte Prozessleitwarten und dazugehörige Anlagenräume, die einer Brandgefahr ausgesetzt sind, sollten Tragelemente aus Stahl entsprechend dem vorliegenden Risiko mit einer Feuerwiderstandsdauer von mindestens 1 Stunde vorgesehen werden.

2.2.4 Prozessleitwarten, Leitzentralen und zugehörige Räume mit industrieller Mess- und Regelungstechnik (z. B. E/A-Räume) und/oder industrielle Schaltschränke sollten eine nicht brennbare Bauweise aufweisen. Dies schließt unter anderem abgehängte Decken, Doppelböden, Trennwände, Inneneinrichtungen, Dämmmaterial für Rohre und RLT (Raumlufttechnik) sowie RLT-Filter ein.

Werden Kunststoffmaterialien eingesetzt, so sollte es sich dabei um FM Approvals anerkannte Materialien handeln oder solche, die den Status „Specification Tested“ erhalten haben, gemäß den folgenden Richtlinien:

A. FM Approval Standard 4882, *Class 1 Interior Wall and Ceiling Materials or Systems for Smoke Sensitive Occupancies*

B. FM Approval Standard 4884, *Panels Used in Data Processing Center Hot and Cold Aisle Containment Systems*

C. ANSI/FM Approval Standard 4910, *Cleanroom Materials Flammability Test Protocol*

2.2.5 Zwischen Prozessleitwarten und benachbarten Bereichen, einschließlich Anlagenräumen und Niederspannungs-Schaltanlagenräumen, sollte eine Abtrennung mit einer Feuerwiderstandsdauer von mindestens einer (1) Stunde eingesetzt werden. Diese Empfehlung gilt nicht für Stand-alone-Anlagen, die sich außerhalb der Prozessleitwarte befinden.

2.2.6 Werden redundante Prozessleitsysteme bereitgestellt, sollten die jeweiligen Steuerungen, Anlagen und Kabel in einem eigenen Brandabschnitt untergebracht werden.

2.2.7 Umkleideräume, Kantinen, Küchen, Besprechungsräume, Büros usw. sollten in einem eigenen Brandabschnitt eingerichtet werden.

2.2.8 Öffnungen in Böden und Wänden, durch die Rohre und Kabel verlaufen, sollten mit einem FM Approvals anerkannten oder gelisteten Dichtungsmaterial abgeschottet sein, dessen Feuerwiderstandsdauer der der Wände bzw. Böden entspricht.

2.2.9 Regenfallrohre, Betriebswasser- und andere Flüssigkeitsleitungen sollten um Prozessleitwarten und die dazugehörigen Anlagenräume herum verlegt werden. In mehrstöckigen Gebäuden sollte der darüber liegende Boden flüssigkeitsdicht abgedichtet werden. Wenn Rohrleitungen nicht um diese Bereiche herum verlegt werden können, sollten Ummantelungen (z. B. konzentrische Rohre) oder eine Auffangwanne sowie FM Approvals anerkannte Leckagemelder mit Alarmmeldungen vorgesehen werden, die an einer ständig besetzten Zentrale auflaufen. Weitere Details sind FM Datenblatt zur Schadenverhütung 1-24, *Protection Against Liquid Damage*, zu entnehmen.

2.2.10 Wenn sich Wasser oder andere Flüssigkeiten in Doppelböden ansammeln könnten, sollten Bodenabflüsse installiert werden.

2.2.10 Für industrielle Schaltschränke, einschließlich Türen und/oder Zugangsklappen, sollten nicht brennbare Baumaterialien verwendet werden. Es sollten anerkannte internationale Standards eingehalten werden.

2.3 Schutzmaßnahmen

2.3.1 Prozessleitwarten, die dazugehörigen Anlagenräume und industrielle Schaltschränke sollten gemäß FM Datenblatt zur Schadenverhütung 1-20, *Protection Against Exterior Fire Exposure*, gegen externe Brandgefahren geschützt werden.

2.3.2 Prozessleitwarten, Prozessleitzentralen und zugehörige Anlagenräume sollten mit FM Approvals anerkannten Rauchmeldern ausgestattet werden, die den Alarm an einen ständig besetzten Platz/eine ständig besetzte Stelle weiterleiten.

2.3.3 Wenn für geschäftskritische Systeme und/oder Sicherheitssteuerungssysteme eine höhere Branderkennungsstufe wünschenswert ist, sollte ein System zur Brandfrühesterkennung (*VEWFD – Very early warning fire detection*) im Anlagenraum und/oder innerhalb der industriellen Schaltschränke installiert werden, das den Alarm an eine ständig besetzte Stelle weiterleitet. Als Systeme zur Brandfrühesterkennung sollten je nach Bedarf FM Approvals anerkannte Rauchansaugsysteme oder intelligente, hochempfindliche punktförmige Brandmelder für die jeweilige Konstellation genutzt werden.

2.3.4 In Doppelböden und über Deckenbereichen mit vorhandenen Kabeln sollten FM Approvals anerkannte Rauchmelder installiert werden.

2.3.5 Es sollten Rauchmelder gemäß FM Datenblatt zur Schadenverhütung 5-48, *Automatic Fire Detection*, installiert werden.

2.3.6 Prozessleitwarten, Leitzentralen und Räume mit industrieller Mess- und Regelungstechnik sollten wie folgt mit Brandschutz ausgestattet werden:

2.3.6.1 Räume mit brennbarer Bauweise

A. Es sollte eine automatische Nass- oder vorgesteuerte Sprinkleranlage mit automatischen schnellansprechenden Sprinklern installiert werden. Anforderungen an die Auslegung, den Hydrantenbedarf und die Betriebsdauer sind dabei FM Datenblatt zur Schadenverhütung 3-26, *Anlagentechnischer Brandschutz in Nichtlager-Nutzungsarten*, zu entnehmen.

B. Es sollte eine automatische FM Approvals anerkannte Sprühnebelanlage installiert werden, die speziell für EDV-Räume gelistet ist. Bei der Installation sollten FM Datenblatt zur Schadenverhütung 4-2, *Water Mist Systems*, sowie das im FM Approval Listing genannte Auslegungs-, Installations-, Betriebs- und Instandhaltungshandbuch des Herstellunternehmens befolgt werden. Die Wasserversorgung sollte in der Lage sein, den Bedarf der Sprühnebelanlage für eine Dauer von 60 Minuten zu decken.

Für die vorstehenden Buchstaben A und B gilt Folgendes:

- Bei Prozessleitwarten und Leitzentralen mit einer Deckenhöhe von bis zu 9 m findet Brandgefahrenklasse 1 (HC-1) Anwendung.
- Bei Räumen mit industrieller Mess- und Regelungstechnik oder Prozessleitwarten und Leitzentralen mit einer Deckenhöhe von mehr als 9 m findet Brandgefahrenklasse 2 (HC-2) Anwendung.

2.3.6.2 Räume mit nicht brennbarer Bauweise

Es sollte eine Halocarbon- oder Inertgasanlage (sog. Clean-Agent-Löschanlage) bereitgestellt werden, die nach den Anweisungen des Herstellunternehmens und nach FM Datenblatt zur Schadenverhütung 4-9, *Halocarbon and Inert Gas (Clean Agent) Fire Extinguishing Systems*, ausgelegt und installiert wird. Automatische Nasssprinkleranlagen, automatische vorgesteuerte Sprinkleranlagen oder Sprühnebelanlagen (gemäß Abschnitt 2.3.6.1 oben) sind ebenfalls akzeptabel.

Für Halocarbon- oder Inertgasanlagen (Clean-Agent-Löschanlagen) sollte sichergestellt werden, dass die folgenden Voraussetzungen erfüllt sind:

1. Es gibt eine Brandfrühesterkennung oder eine automatische Stromabschaltung des Raums und der Anlagen (mit Ausnahme von Notbeleuchtung) nach Raucherkennung, sofern mithilfe einer Prozessgefahrenanalyse (PGA) oder einer ähnlichen Analyse nachgewiesen worden ist, dass die gesteuerten Anlagen (d. h. Prozessanlagen) bei einer automatischen Stromabschaltung nicht beschädigt werden und/oder eine Gefahrensituation hervorrufen.
   a. Bei einer automatischen Stromabschaltung sollte für die Installation FM Datenblatt zur Schadenverhütung 5-32, *Data Centers and Related Facilities*, Abschnitt *Power Isolation of Data Processing Equipment and HVAC Systems*, befolgt werden.
   b. Die Verzögerungsdauer für die Stromabschaltung sollte so gewählt werden, dass es möglich ist, den Prozess in einen sicheren Zustand zu versetzen. Die Verzögerungsdauer sollte zudem die Haltezeit der Halocarbon- oder Inertgasanlage (Clean-Agent-Löschanlage) mit einem Sicherheitsfaktor von 2 nicht überschreiten.
2. Es gibt eine Brandfrühesterkennung mit einem Überwachungsalarm/-signal, die dem Bedienpersonal oder den Verantwortlichen ausreichend Zeit für eine Untersuchung gibt, bevor die Clean-Agent-Löschanlage Löschmittel beaufschlagt.
3. Die Anlageneinhausungen bestehen aus Metall.
4. Die Nutzung von Papier und anderen brennbaren Materialien ist in diesem Raum auf ein Minimum begrenzt.
5. Im Raum werden keine Verpackungsmaterialien oder Kunststoffkassetten gelagert. **Hinweis:** Diese Vorgabe umfasst alle brennbaren Medien (z. B. Bandspulen).
6. Für Belüftungssysteme, die mit Rück- oder Zuluft arbeiten, sind Abschaltvorrichtungen und/oder Schutzklappen vorhanden.

2.3.7 Die Prozesssteuerungssysteme am Standort sollten geschützt werden. Bei der Wahl der Schutzvorkehrungen sollten die Kritikalität des physischen Prozesses und die möglichen Auswirkungen eines brandbedingten Ausfalls des Prozesssteuerungssystems berücksichtigt werden. Siehe Abschnitt 3.1, *Brandschutz für industrielle Schalttechnik*. Eine der folgenden Alternativen sollte umgesetzt werden (A oder B):

A. Nicht brennbare Schränke mit Unterteilung in einzelne Abschnitte, um den Brandschaden auf einen möglichst kleinen Bereich zu begrenzen.

B. Halocarbon- oder Inertgasanlage (Clean-Agent-Löschanlage) im Raum, vorausgesetzt, die Schränke sind belüftet und/oder so aufgebaut, dass die Beaufschlagung direkt in den Innenraum der Schränke erfolgen kann. Die Empfehlungen im vorstehenden Abschnitt 2.3.6.2 sollten befolgt werden.

2.3.8 In allen Gebäudebereichen neben den Leitwarten und -zentralen (einschließlich Büro-, Aufenthalts-, Akten-, Konferenz- und Schulungsräumen, zugangsbeschränkten Bereichen, Toiletten etc.) sollte automatischer Sprinklerschutz gemäß FM Datenblatt zur Schadenverhütung 3-26, *Anlagentechnischer Brandschutz in Nichtlager-Nutzungsarten*, entsprechend der für die entsprechende Nutzungsart einschlägigen Brandgefahrenklasse installiert werden.

2.3.9 Brandschutzanlagen sollten gemäß FM Datenblatt zur Schadenverhütung 2-0, *Installationsrichtlinien für automatische Sprinkleranlagen*, und dem anwendbaren Datenblatt für die Objektschutzanlage installiert werden.

2.3.10 Rechenzentren für Prozessleitwarten sollten gemäß FM Datenblatt zur Schadenverhütung 5-32, *Data Centers and Related Facilities*, geschützt werden. Es sollte eine Prozessgefahrenanalyse durchgeführt werden, bevor die automatische Abschaltung zugelassen wird.

2.3.11 Notstromgeneratoren sollten gemäß FM Datenblatt zur Schadenverhütung 5-23, *Design and Protection for Emergency and Standby Power Systems*, geschützt werden.

2.3.12 Kabelbündel und -trassen sollten gemäß FM Datenblatt zur Schadenverhütung 5-31, *Cables and Bus Bars*, geschützt werden.

2.3.13 Zum Schutz elektrischer Anlagen sollten für spannungsführende elektrische Anlagen geeignete Kohlendioxid- oder Clean-Agent-Handfeuerlöscher (Klasse C) gemäß FM Datenblatt zur Schadenverhütung 4-5, *Portable Extinguishers*, bereitgestellt werden.

2.3.13.1 In Bereichen mit elektrischen Anlagen sollten keine Pulverlöscher verwendet werden.

2.3.13.2 Für gewöhnliche brennbare Materialien sollten Handfeuerlöscher bereitgestellt werden, die entsprechend ihrem Typ oder ihrer Kombination verschiedener Typen gemäß FM Datenblatt zur Schadenverhütung 4-5, *Portable Extinguishers*, geeignet sind.

2.3.14 Es sollte ein Einsatzplan für die Brandbekämpfung und Elektromaßnahmen in Prozessleitwarten, Leitzentralen, zugehörigen Räumen mit industrieller Mess- und Regelungstechnik und/oder industriellen Schaltschränken erarbeitet werden.

2.3.14.1 Es sollte sichergestellt werden, dass Elektrofachkräfte zur selben Zeit wie die Feuerwehr eingreifen können und dass sie entsprechend geschult und damit in der Lage sind, die sichere Stromabschaltung oder Stromisolierung der betroffenen Prozesssteuerschränke sicherzustellen und Löscharbeiten einzuleiten.

2.3.14.2 Ist eine Stromabschaltung aller elektrischen Betriebsmittel in den Räumen mit industrieller Mess- und Regelungstechnik und den industriellen Schaltschränken nicht möglich, sollte sichergestellt werden, dass nach einem Feueralarm geschultes Personal zur Verfügung steht, das in der Lage ist, die Brand-/Rauchsituation im betroffenen Bereich fachlich einzuordnen und den Einsatzplan mittels einer lokalen, regionalen oder vollständigen manuellen Stromisolierung umzusetzen.

2.4 Menschlicher Faktor

2.4.1 Änderungsmanagement

2.4.1.1 Die ICS-Management- und ICS-Sicherheitsprogramme sollten in Verbindung mit dem Änderungsmanagement-Programm verwaltet werden.

2.4.2 ICS-Management

Verpflichtung auf Leitungsebene ist die Grundlage für erfolgreiche ICS-Aufsicht- und ICS-Managementprogramme. Die Verpflichtung auf Leitungsebene hilft dabei, sicherzustellen, dass alle Bereiche der ICS die erforderliche Aufmerksamkeit, die nötigen finanziellen Mittel und das erforderliche Personal erhalten.

2.4.2.1 ICS-Aufsicht-Team

2.4.2.1.1 Organisationen sollten ein ICS-Aufsicht-Team aus Personen auf Gesamtunternehmens- und Standortebene bilden, das für die Überwachung der Umsetzung von Cybersicherheitsrichtlinien im Zusammenhang mit den ICS zuständig ist.

2.4.2.2 Geräteverwaltung

2.4.2.2.1 Es sollte ein Programm zur Inspektion, Prüfung und Instandhaltung der ICS ausgearbeitet und eingeführt werden. Richtlinien zur Ausarbeitung eines Programms zur Integrität von Anlagen sind FM Datenblatt zur Schadenverhütung 9-0, *Integrität von Anlagen*, zu entnehmen. Je nach Bedarf sollte ein Programm zur Geräteverwaltung folgende Punkte enthalten:

A. Es sollte ein Inventar der mit dem ICS-Netz verbundenen Hardware unter Angabe des Herstellunternehmens, der Modellnummer und der installierten Firmware, Software und Anwendungen einschließlich der Versionsnummern geführt werden.

B. Es sollte sichergestellt werden, dass die Inventarliste eine Kritikalitätseinstufung der ICS-Anlagen enthält, um Sicherheitsmaßnahmen zu priorisieren und erforderliche Sicherheitsupdates zu pflegen.

C. Pläne und Dokumentation zu ICS sollten aufbewahrt werden, z. B. Schaltpläne, Netzwerkpläne und gegebenenfalls Rohrleitungs- und Instrumentierungsdiagramme (R&I-Fließbild). Diese Dokumente sollten stets auf den neuesten Stand gebracht werden, wenn Änderungen an den ICS vorgenommen werden.

D. Inventarlisten, Pläne und Dokumentationen mit ausführlichen Informationen zur Auslegung und Funktionsweise der ICS sollten an einem überwachten Ort mit Zugangsbeschränkungen aufbewahrt werden. Nur im Bedarfsfall sollte Zugang gewährt werden. Handelt es sich dabei um digitale Dokumente, so sollten diese mit Passwörtern gesichert werden. Entsprechende Sicherungskopien sollten daneben in einem vertrauenswürdigen Netzwerk gespeichert werden. Die Dateien sollten nach Möglichkeit verschlüsselt werden. Alle Netzwerke außerhalb der ICS-/OT-Umgebung sollten als nicht vertrauenswürdige Netzwerke eingestuft werden, einschließlich des lokalen IT-Netzwerks.

2.4.2.3 Lieferkettenmanagement

2.4.2.3.1 Je nach Bedarf sollte ein Programm zum Lieferkettenmanagement folgende Punkte enthalten:

A. Die Vergabeunterlagen für den Lieferanten sollten Anforderungen zur Cybersicherheit für Systeme/Anwendungen oder Geräte enthalten. Vor Vertragsunterzeichnungen/-verlängerungen sollten vom Unternehmen genehmigte Anbieter (auch Drittanbieter) in Bezug auf ihre Sicherheitsrichtlinien und -verfahren neu bewertet werden.

2.4.3 ICS-Sicherheit

Die Verfügbarkeit der ICS ist für alle Prozesse kritisch. Eine effektive Strategie zur ICS-Sicherheit kann eine wichtige Rolle bei der Aufrechterhaltung dieser Verfügbarkeit spielen.

2.4.3.1 Zugangsverwaltung

2.4.3.1.1 Je nach Bedarf sollte ein Programm zur Zugangsverwaltung folgende Punkte enthalten:

A. Für die Zugangskontrolle zu ICS sollten ICS-Benutzeranmeldeinformationen (d. h. rollenbasierter Zugang zur Mensch-Maschine-Schnittstelle/zur Bedienstation und zu Engineeringstationen) verwendet werden. Der Zugang zu Engineeringstationen sollte zudem auf die Mitarbeitenden beschränkt werden, die zu Prozessänderungen berechtigt sind. Bei der Umsetzung des kontrollierten Zugangs zu ICS sollte Folgendes beachtet werden:

1. Für Mensch-Maschine-Schnittstellen (HMI) / Bedienstationen (ohne Möglichkeit zur Änderung der Einstellpunkte von Verriegelungen und der Alarme von Sicherheitsvorrichtungen) können gemeinsame Benutzeranmeldeinformationen verwendet werden.
2. Engineeringstationen erfordern eindeutige benutzerspezifische Anmeldedaten und Passwörter, die bei jedem Zugang zum System eingegeben werden. Das Auto-Log-out bei Inaktivität der Engineeringstation sollte nach höchstens etwa 30 Minuten erfolgen.
3. Benutzeranmeldeinformationen für den ICS-Zugang werden unabhängig von denen für IT-Systeme verwaltet. ICS-Benutzeranmeldeinformationen sollten in einem aktuellen Benutzerverzeichnis in der OT-Umgebung aufbewahrt werden. Zugriffsberechtigungen sollten in regelmäßigen Abständen überprüft werden. Für Personen, die keinen Zugang mehr benötigen, sollten die Zugangsdaten entfernt werden. Lokale Zugänge ohne Einbindung in ein Netzwerk können unter Umständen eine akzeptable Alternative darstellen.

B. Für alle Systeme, Hardware und Software sollten werkseitig eingestellte Standardbenutzernamen und -passwörter geändert werden. Passwörter sollten in regelmäßigen Abständen und bei großen Änderungen und/oder dem Wechsel von zuständigen Mitarbeitenden oder Lieferanten geändert werden. Die Verwendung allgemeiner Benutzernamen und schwacher Passwörter sollte vermieden werden.

C. Drahtlose Kommunikationskanäle sollten durch Authentifizierung und Verschlüsselung geschützt werden.

D. Für tragbare Geräte, die an die ICS angeschlossen werden, sollten die folgenden Vorsichtsmaßnahmen getroffen werden:

1. Vor Gewährung des Zutritts zum Standort sollte eine ICS-Cybersicherheitsschulung für Fachfirmen und andere Besucher, die den Standort vorübergehend betreten, durchgeführt werden. Diese Schulung sollte eine Einführung in die Regeln und Verfahren am Standort gemäß Abschnitt 2.4.3.1.1, D.2 bis D.5, beinhalten.
2. Bei Geräten, die in einer ICS-Umgebung verwendet werden, wie z. B. Laptops (einschließlich Laptops, Tablets etc. von Dritten), sollten Drahtlosverbindungen deaktiviert sowie Sicherheits-Patches und Antivirensoftware ständig aktualisiert bzw. überprüft werden. Außerdem sollte vor jeder Verbindung mit den ICS ein Virenscan durchgeführt werden.
3. Bei Speicherkarten, USB-Sticks, externen Festplatten usw. sollte vor dem Anschluss an die ICS jedes Mal ein Sicherheitsscan durchgeführt werden.
4. Verbindungen von Mobiltelefonen oder anderen Geräten, die über die Anbindung an ein Mobilfunknetz verfügen, mit den ICS sollten nicht erlaubt sein.
5. Nicht genutzte Schnittstellen (USB, RJ45-Steckverbindungen, serielle Schnittstellen etc.) an Anlagen, die an die ICS angeschlossen sind, sollten möglichst deaktiviert werden.

2.4.3.2 Konfigurationsmanagement

2.4.3.2.1 Je nach Bedarf sollte ein Konfigurationsmanagement-Programm folgende Punkte enthalten:

A. Ausstattung/Funktionen sollten für alle an die ICS angeschlossenen digitalen Geräte auf ausschließlich solche Ausstattung/Funktionen beschränkt werden, die zur Unterstützung des Betriebs der ICS notwendig sind. Dies umfasst u. a. Feldgeräte mit mehreren Einstellungen, die digital kommunizieren; Steuerungen, die sowohl die Basis-Prozessleitung als auch die Sicherheitssteuerung durchführen; Überwachungsgeräte, Mensch-Maschine-Schnittstellen und Engineeringstationen; Datenerfassungs- und Archivierungssysteme; Server; Netzwerkausrüstung wie Gateways, Switches und Router sowie Netzwerkschutzvorrichtungen wie Firewalls einschließlich aller in einer ICS-DMZ installierten Geräte.

B. Es sollte sichergestellt werden, dass das ICS-Aufsicht-Team sämtliche Änderungen an digitalen Geräten, die an die ICS angeschlossen sind, vor ihrer Einführung im Rahmen des Änderungsmanagements mit Blick auf Sicherheitsfragen analysiert, validiert und genehmigt.

C. Im Rahmen einer Systemüberwachung sollten mögliche unbefugte Änderungen an Geräten zur Basis- und Sicherheitssteuerung sowie OT-Netzwerkgeräten geprüft werden.

D. Es sollte sichergestellt werden, dass Logiksysteme, SPS oder Steuerungen, die im Rahmen des Basis-Prozessleitsystems und des Sicherheitssteuerungssystems verwendet werden, vor der Aktivierung des Systems und vor dem Betrieb der ICS auf die vom Herstellunternehmen empfohlene Betriebsart eingestellt werden (d. h. Run, Program, Remote o. Ä.). Im Rahmen der oben empfohlenen Systemüberwachung sollten auch Änderungen der Betriebsart geprüft werden.

2.4.3.3 Patch-Management

2.4.3.3.1 Je nach Bedarf sollte ein Patch-Management-Programm folgende Punkte enthalten:

A. Es sollte sichergestellt werden, dass im Patch-Management-Programm auch Support- und Kommunikationsanlagen wie z. B. Fernzugriffserver, Bastion Hosts, Datenerfassungs- und Archivierungssysteme, Virenschutz, Virtual Private Networks sowie weitere Netzwerkkomponenten wie Firewalls usw. berücksichtigt werden. Es sollten auch Geräte zur Instandhaltung der ICS wie Laptops oder Handgeräte sowie Geräte zur Sicherheitsüberprüfung von Mobilgeräten, z. B. USB-Sicherheitsschleusen, einbezogen werden.

B. Mitteilungen und Warnungen zu Schwachstellen der Cybersicherheit von System- und Geräteherstellunternehmen, ICS-Integratoren, staatlichen Stellen und anderen sollten aufmerksam verfolgt werden.

C. Nach Bekanntwerden von Cybersicherheitsrisiken sollte das ICS-Aufsicht-Team basierend auf der Kritikalität und Gefährdung festlegen, welche Maßnahmen zum Schutz der ICS am Standort erforderlich sind. So können zusätzliche Schutzmaßnahmen gegen Systemschwachstellen erforderlich sein, bis ein Software-Patch installiert werden kann.

D. Es sollte sichergestellt werden, dass das ICS-Aufsicht-Team vor dem Patch-Deployment Rücksprache mit dem ICS-Lieferanten hält. Wenn möglich sollte vor der Installation ein Test mittels einer Simulation oder in einem virtuellen System erfolgen.

E. Wenn für veraltete Anlagen und/oder Softwareprogramme kein Support mehr vom Herstellunternehmen verfügbar ist, sollten für diese zusätzliche Schutzmaßnahmen gegen Schwachstellen bei der Cybersicherheit ergriffen werden.

2.4.3.4 Netzwerksicherung

2.4.3.4.1 Es sollte ein sicherer Fernzugriff auf die ICS-/OT-Umgebung eingerichtet werden. Alle Netzwerke außerhalb der ICS-/OT-Umgebung sollten als nicht vertrauenswürdige Netzwerke eingestuft werden, einschließlich des lokalen IT-Netzwerks. Soweit anwendbar, sollten folgende Vorsichtsmaßnahmen umgesetzt werden:

A. Es sollte sichergestellt werden, dass für den Fernzugriff auf die ICS folgende Voraussetzungen erfüllt sind:

1. Bei einem Zugriff von einem internen Netzwerk (Verbindung vom Unternehmensnetzwerk aus), z. B. dem lokalen IT-Netzwerk, sollte eine Multi-Faktor-Authentifizierung (MFA) über einen Bastion Host in einer industriellen DMZ (siehe Abschnitt 2.4.3.4.2 B) verwendet werden.
2. Bei einem Zugriff von einem externen Netzwerk (Verbindung von außerhalb des Unternehmensnetzwerks) sollte ein sicheres Virtual Private Network (VPN) und die Multi-Faktor-Authentifizierung (MFA) über einen speziellen Pfad über Unternehmenssysteme zu einem Zwischensystem (Jump Host in der industriellen DMZ) verwendet werden, welches den Zugriff auf die ICS-/OT-Umgebung herstellt.
3. PCs oder andere persönliche externe Geräte sollten nicht für einen Fernzugriff auf die ICS-/OT-Umgebung verwendet werden.

B. Es sollten keine Fernverbindungen zu speziellen Sicherheitssteuerungssystemen zugelassen werden.

C. Es sollten keine dauerhaften Fernverbindungen zur ICS-/OT-Umgebung zugelassen werden. Die Fernüberwachung, -datenerfassung und -diagnose mit eingeschränktem Datenfluss in eine Richtung ist möglich und erfordert keine Zeitlimits für die Verbindung zu ICS.

D. Einwählmodems sollten durch sichere moderne Kommunikationsmethoden ausgetauscht werden. Wenn dies nicht möglich ist, sollten folgende Maßnahmen ergriffen werden:

1. Einwählmodems sollten abgeschaltet und/oder ausgesteckt werden, wenn sie nicht benutzt werden.
2. Es sollten zusätzliche Schutzmaßnahmen für aktive Einwählmodems getroffen werden (z. B. Rückrufeinstellung auf eine eigens dafür vorgesehene Telefonnummer, Filtern der Anrufer-ID, Deaktivierung der automatischen Rufentgegennahme).

2.4.3.4.2 Soweit anwendbar, sollten folgende Sicherheitsvorkehrungen für Netzwerke ergriffen werden:

A. Die ICS-/OT-Netzwerke sollten mithilfe einer industriellen demilitarisierten Zone (DMZ) von IT- oder anderen Unternehmensnetzwerken getrennt werden. Alle Kommunikationen zu und von ICS sollten über diese DMZ erfolgen.

B. Das Basis-Prozessleitsystem(BPCS)-Netzwerk sollte durch Isolation (vollständige Trennung (Air Gap) oder schnittstellenbasierte Architektur) oder Segmentierung (integrierte oder gemeinsame Architektur) von den Sicherheitssteuerungsnetzwerken getrennt werden. Weitere Richtlinien zu Sicherheitssteuerungssystemen sind FM Datenblatt zur Schadenverhütung 7-45, *Safety Controls, Alarms, and Interlocks (SCAI)*, zu entnehmen.

C. Firewall-Regeln (geöffnete Schnittstellen, zulässige Protokolle usw.) sollten regelmäßig von Mitarbeitenden mit Kenntnissen im Bereich Netzwerke und Cybersicherheit überprüft werden. Änderungen an den Firewall-Regeln werden von der ICS-/OT-Umgebung aus durchgeführt und über ein Änderungsmanagementverfahren (MOC) unter Kontrolle des ICS-Aufsicht-Teams verwaltet.

D. Wenn möglich sollte eine „Allowlist“ vertrauenswürdiger Anwendungen in der ICS-Umgebung verwendet werden. Bei der Implementierung dieser Lösung ist Achtsamkeit geboten.

E. Wenn möglich sollte die Netzwerküberwachung und Protokollierung von Aktivitäten (auch Angriffserkennungssystem, IDS) im ICS-Netzwerk zusammen mit Security Information und Event Management Software (SIEM) eingesetzt werden, um mögliche unbefugte Aktivitäten zu erkennen. Wenn möglich sollte das OT-Netzwerk über ein Security Operations Center (SOC) überwacht werden.

F. Es sollten Antiviren-Softwareprogramme für ICS und in der OT-Umgebung eingesetzt werden, einschließlich in SCADA-Systemen. Dabei sollte eng mit dem ICS-Lieferanten oder Dienstleister zusammengearbeitet werden. Bei der Auswahl und Implementierung von Antivirenlösungen sollte sorgfältig vorgegangen werden.

2.5 Betrieb und Instandhaltung

Die ordnungsgemäße Funktionsweise der ICS ist kritisch, um erhebliche Anlagen- und/oder Sachschäden sowie daraus resultierende langfristige Betriebsunterbrechungen zu vermeiden. Die Möglichkeit ICS-bezogener Ausfälle und langfristiger Unterbrechungen kann durch Überwachungs- und Meldeverfahren, geeignete Notfall-/Wiederherstellungspläne und ICS-Verfügbarkeitsplanung sowie entsprechend geschultes und erfahrenes Bedienpersonal, das die dokumentierten Standard- und Notfallanweisungen ordnungsgemäß umsetzt, minimiert werden.

2.5.1 ICS-Betrieb

2.5.1.1 Alarmmanagement

2.5.1.1.1 Die Systemüberwachung der ICS-Anlagen und OT-Netzwerkgeräte sollte einbezogen werden, sofern sie entsprechend der Empfehlung in Abschnitt 2.4.3.2.1 C zum Konfigurationsmanagement eine mögliche Option darstellt.

A. Die Systemüberwachung sollte bei nicht autorisierten Änderungen an den Konfigurationseinstellungen der ICS-Anlagen, einschließlich der Sicherheitssteuerungssysteme und der OT-Netzwerkgeräte, anschlagen und einen entsprechenden Alarm auslösen.

Hinweis: Die vorstehend genannten Alarme sind nicht für Anlagenführende bestimmt. Sie sollten stattdessen von hierarchisch übergeordneten Mitarbeitenden, die für die Überwachung von OT-Netzwerkgeräten und ICS-Anlagen zuständig sind, bearbeitet werden.

Weitere Richtlinien zum Alarmmanagement sind FM Datenblatt zur Schadenverhütung 10-8, *Operators,* zu entnehmen.

2.5.1.2 Notfallverfahren

2.5.1.2.1 Planung und Vorbereitung sind das A und O für erfolgreiche Notfallverfahrensanweisungen zur Cyber- und ICS-Sicherheit. Dazu gehört die Benennung von zuständigen Mitarbeitenden und bei Bedarf externem Beratungspersonal oder anderen Fachkräften mit den entsprechenden Kenntnissen, um auf einen Cyberangriff zu reagieren.

A. Es sollte sichergestellt werden, ob für den Umgang mit Cybervorfällen Rollen und Zuständigkeiten festgelegt sind.

B. Es sollten Informationen zu Anbietern eingeholt werden, die berechtigt/vertraglich verpflichtet sind, bei einem Cyberangriff Support zu leisten.

2.5.1.2.2 Je nach Bedarf sollten die Notfallverfahren zur Cyber- und ICS-Sicherheit folgende Punkte enthalten:

A. Es sollte sichergestellt werden, dass ein Verfahren vorhanden ist, um die Auswirkungen des Ausfalls des Systems zur Unternehmensressourcenplanung (ERP) oder des Produktionsleitsystems (MES) auf die ICS und die Produktion zu verringern

B. Es sollte sichergestellt werden, dass eine Anleitung zum Abschalten des Systems und/oder Prozesses (d. h. zum Überführen des Systems in einen sicheren Zustand) vorhanden ist, wenn sich die ICS-Steuerung verdächtig verhält oder nicht mehr funktioniert. Diese Anleitung sollte bekannte oder mutmaßliche Cybervorfälle erfassen, darunter Folgendes:

- Schwarzer Bildschirm/Bedienpaneel der Mensch-Maschine-Schnittstelle friert ein

- Ungeklärte Geräteabschaltung
- Ransomware-Meldungen auf Workstations
- Unerwartete Cursorbewegungen auf Workstations ohne Eingabe des Bedienpersonals
- Unbekannte Konfigurationsänderung
- Probleme bei der Konfiguration oder Kalibrierung eines Teils der ICS

C. Es sollte geprüft werden, ob Verfahren für den Betrieb von kritischen Anlagen im manuellen Betriebsmodus vorhanden sind.

D. Es sollte sichergestellt werden, dass Notfallverfahren regelmäßig (zumindest in theoretischen) Notfallsimulationsübungen geübt werden.

2.5.1.3 Verfügbarkeitsplanung

2.5.1.3.1Verfügbarkeitsplanung für Anlagen

Es sollte ein ICS-Verfügbarkeitsplan gemäß FM Datenblatt zur Schadenverhütung 9-0, *Integrität von Anlagen*, schriftlich ausgearbeitet und gepflegt werden. Anhang C des Datenblatts enthält Richtlinien zur Ausarbeitung und Pflege eines geeigneten ICS-Verfügbarkeitsplans. Auch die Richtlinien für eine Strategie zur Risikominderung bezüglich Ersatzteilen, Miet- und redundanter Anlagen sind diesem Datenblatt zu entnehmen.

Darüber hinaus sollten die folgenden Punkte bei der Verfügbarkeitsplanung für die ICS berücksichtigt werden:

A. Erforderliche Maßnahmen zur Bewältigung unbeabsichtigter Abschaltungen und zur Wiederherstellung nach ICS-Ausfall-Szenarios als Teil des Notfall- und Wiederherstellungsplans (siehe Abschnitt 2.5.1.4)

B. Erprobung und Einübung des Plans in einer Regelmäßigkeit, welche durch den Asset Owner und entsprechend der Gefährdung festgelegt wird

C. Basierend auf dem Hardware-Inventar (siehe Abschnitt 2.4.2.2.1), einschließlich der Kritikalität der Komponenten und des Lebenszyklusmanagements, Bewertung der Notwendigkeit und des Umfangs der Ersatzteilbevorratung für ICS-Komponenten

2.5.1.3.2 ICS-Verfügbarkeitspläne werden jährlich überprüft.

2.5.1.4 Notfall- und Wiederherstellungsplan

2.5.1.4.1 Im Rahmen der ICS-Verfügbarkeitsplanung sollten je nach Bedarf die folgenden Punkte in den Notfall- und Wiederherstellungsplan aufgenommen werden:

A. Bei unbeabsichtigten Abschaltungen sollten vor dem Neustart der ICS die Ursachen dieser Abschaltung ermittelt werden.

B. Beim Auftreten von unbeabsichtigten Abschaltungen sollten, soweit möglich, elektronische Aufzeichnungen für die forensische Untersuchung geführt werden.

C. Es sollten geeignete Kopien in der jeweils aktuellsten Fassung von allen ICS-Konfigurationsdateien (z. B. die letzte bekannte verlässliche Konfiguration, Basis-Konfiguration) sowie Dokumenten, die erforderlich sind, um ein vollständig funktionierendes System sicherzustellen, angefertigt werden. Eine Historie der Sicherungsdateien sollte an einem physisch sicheren Ort aufbewahrt werden.

1. Handelt es sich bei den Sicherungsdateien um unveränderliche Dateien (zum Beispiel mit Überschreibungsschutz, Write Once/Read Many, zu Deutsch: einmal schreiben, vielfach lesen), so sollten folgende Schritte befolgt werden:
   a. Die unveränderlichen Sicherungsdateien sollten auf einem Laufwerk in einem vertrauenswürdigen Netzwerk gespeichert werden, das vom Netzwerk mit den ursprünglichen Daten getrennt ist.
   b. Bei Änderungen am System und nach Systemupdates sollten neue Sicherungsdateien erstellt werden.
   c. Vor Ablauf der Aufbewahrungsfrist der letzten unveränderlichen Datei sollten neue Sicherungsdateien erstellt werden.

2. Handelt es sich bei den Sicherungsdateien um Dateien, die nicht unveränderlich sind (also zum Beispiel überschrieben werden können), so sollten folgende Schritte befolgt werden:
    a. Mindestens eine Kopie aller Sicherungsdateien sollte offline an einem physisch sicheren Ort gelagert werden.
    b. Bei Änderungen am System und nach Systemupdates sollten neue Sicherungsdateien erstellt werden.

D. Die Serviceverträge mit Herstellunternehmen und/oder Anbietern sollten überprüft werden, um die Lieferzeit von Komponenten zu kennen und darauf basierend eine optimale Strategie zur Wiederherstellung und der Beschaffung von Ersatzteilen bei Anlagenausfällen zu erstellen.

E. Der Notfall- und Wiederherstellungsplan sollte regelmäßig in risikogerechten Intervallen, aber mindestens jährlich überprüft werden. Das Programm sollte bei Bedarf aktualisiert werden, um seine Effektivität zu wahren.

Weitere Richtlinien zur Notfall-Einsatz- und Wiederaufbauplanung sind FM Datenblatt zur Schadenverhütung 9-1, *Supervision of Property*, FM Datenblatt zur Schadenverhütung 10-1, *Einsatz- und Notfallplanung*, und FM Datenblatt zur Schadenverhütung 10-5, *Disaster Recovery Planning*, zu entnehmen.

Weitere Richtlinien zur Untersuchung von Vorfällen sind FM Datenblatt zur Schadenverhütung 10-8, *Operators*, und FM Datenblatt zur Schadenverhütung 7-43, *Process Safety*, zu entnehmen.

2.6 Schulungen

2.6.1 Im Rahmen des Schulungsprogramms für das Bedienpersonal am Standort sollte eine ICS-Sicherheitsschulung sowie ein Programm, das das Bewusstsein für Sicherheitsrichtlinien und -prozeduren schärft, eingeführt werden. Das Programm sollte Cybersicherheitsstandards und bewährte Praktiken der Branche beinhalten.

2.6.2 Das Bedienpersonal und zuständige Mitarbeitende, die mit den ICS arbeiten, sollten spezifische Schulungen absolvieren, bevor sie Zugriff auf die ICS erhalten. Systemadministrator*innen oder Mitarbeitende mit höheren/erweiterten Zugangsberechtigungen sollten zusätzliche Schulungen (d. h. rollenbasierte Schulungen) erhalten, um ihre Aufgaben erfüllen zu können

2.6.3 Für alle ICS-Mitarbeitenden sollten Erst- und Nachschulungen zur ICS-Cybersicherheit regelmäßig, mindestens jedoch jährlich abgehalten werden.

2.6.4 Das Notfallteam für den Brandfall sollte Schulungen im Umgang mit Bränden an Prozesssteuerungssystemen erhalten. FM Datenblatt zur Schadenverhütung 5-32, *Data Centers and Related Facilities*, Abschnitt 2.7.1, bietet hierzu weitere Hinweise.

Weitere Richtlinien zu Bedienpersonal sind FM Datenblatt zur Schadenverhütung 10-8, *Operators*, zu entnehmen.

2.7 Versorgungsanlagen

2.7.1 Es sollte eine unterbrechungsfreie Stromversorgung sowie eine Notstromversorgung sichergestellt werden, damit die ICS so lange betrieben werden können, bis eine sichere Stromabschaltung möglich ist. Eine unterbrechungsfreie Stromversorgung sollte für alle Hilfssysteme wie Instrumentenluft (wo verwendet) und RLT sichergestellt werden, die für die Dauer eines sicheren Herunterfahrens erforderlich ist.

2.7.2 Die Versorgungs- und Hilfssysteme für die ICS (z. B. Batterien, unterbrechungsfreie Stromversorgung, Generatoren und Klimaanlagen) sollten im Rahmen des Programms zur Integrität von Anlagen regelmäßig Inspektions- und Instandhaltungsmaßnahmen unterzogen werden. Weitere Richtlinien sind FM Datenblatt zur Schadenverhütung 5-28, *DC Battery Systems*, sowie FM Datenblatt zur Schadenverhütung 5-23, *Design and Protection for Emergency and Standby Power Systems*, zu entnehmen.

2.7.3 Es sollte ein zuverlässiges System für die Instrumentenluft bereitgestellt werden, falls pneumatische Steuerungen im Einsatz sind (z. B. ein unabhängiger Instrumentenluftkompressor mit N+1-Reserve oder ein entsprechend ausgelegter Luftbehälter).

2.7.4 Es sollte eine zuverlässige RLT-Anlage bereitgestellt werden, um die für den Normalbetrieb erforderlichen Umgebungsbedingungen für die ICS-Anlagen aufrechtzuerhalten. Diese Empfehlung gilt insbesondere für ICS-Anlagen, die kritisch für den Betrieb sind.

3.0 GRUNDLAGEN DER EMPFEHLUNGEN

3.1 Brandschutz für industrielle Schalttechnik

Es ist zu beachten, dass die Installation von automatischem Sprinklerschutz primär dazu dient, die Raumstruktur sowie benachbarte Belegungen zu schützen. In einem kleinen Raum kann es auch bei einem von einer Sprinkler- oder Sprühnebelanlage kontrollierten Brand zu einem Verlust sämtlicher darin befindlicher technischer Anlagen kommen. Geht es daher darum, diese technischen Anlagen an sich zu schützen, ist eine Halocarbon- oder Inertgasanlage (Clean-Agent-Löschanlage) möglicherweise die bessere Option.

Bei einem Brand an Prozesssteuerschränken mit einer geeigneten Unterteilung in einzelne Abschnitte beschränkt sich der Brand eher auf den Schrank, an dem der Brand ausgebrochen ist, sodass der Schaden an benachbarten Schränken begrenzt wird. Liegt hingegen keine Unterteilung in einzelne Abschnitte vor, so breitet sich ein Brand an Prozesssteuerschränken erfahrungsgemäß über die gesamte Einhausung hinweg aus. Die Auswirkungen eines Ausfalls der Prozesssteuertechnik hängen vom Umfang des Brandschadens, der Kritikalität des Prozesses, der Verfügbarkeit von Ersatzteilen etc. ab.

3.2 ICS-Management

Der Asset Owner oder die jeweils beauftragte Person sollten über eine Strategie zur Cybersicherheit verfügen, um die standortweiten ICS zu schützen.

3.2.1 ICS-Aufsicht

Angesichts der Komplexität der Automatisierung, des Zusammenwirkens verschiedener Systeme und Netzwerke sowie der Datenerfassung für analytische Geschäftszwecke ist eine neue Bedrohung für ICS-Anlagen aufgekommen: Cyberrisiken. Zur Sicherstellung der Aufrechterhaltung der Prozesse am Standort bedarf es der Festlegung einer Person, deren Aufgabe es ist, den Schutz der ICS vor Cyberrisiken sicherzustellen. Diese Person sollte auch über das entsprechende Wissen dazu verfügen, wie sich bestimmte Methoden, Produkte und Systeme, die zur Sicherstellung der Cybersicherheit eingesetzt werden, auf die Leistung der ICS auswirken können.

3.2.2 Geräteverwaltung

Um die ICS gegen Cyberangriffe widerstandsfähig zu gestalten, ist es erforderlich, dass Organisationen wissen, was an das ICS-Netzwerk angeschlossen ist. Ohne diese Kenntnisse kann das Team keine Geräte identifizieren, die Cyberrisiken für die ICS darstellen.

Die digitalen Geräte, die an das ICS-Netzwerk angeschlossen sind, sollten in der Geräteverwaltung erfasst werden. Dabei sollten Mensch-Maschine-Schnittstellen, Bedienstationen, Engineeringstationen, Netzwerk-Switches, Modems, Router, Firewalls, Anwendungsserver, Drucker, Prozessleitsysteme (DCS), speicherprogrammierbare Steuerungen (SPS) und andere logische Steuerungen sowie mit dem Netzwerk verbundene intelligente Feldgeräte berücksichtigt werden. Betriebssysteme (d. h. Geräte der Ebene 3 des Purdue Reference Model eines OT-Netzwerks) sollten ebenfalls in die Geräteerfassung einbezogen werden. Zu den gängigen Geräten dieser Ebene gehören zentrale Datenerfassungs- und Archivierungssysteme im Werk, Betriebsplanungssysteme, Alarm- und andere Anwendungsserver, betriebsspezifische IT-Dienste wie DHCP, LDAP, DNS sowie Dateiserver. Zudem sollten IIoT-Geräte (industrielles Internet der Dinge) und selbst grundlegende IoT-Geräte (Internet der Dinge) berücksichtigt werden, die unter Umständen fehlerhaft an das ICS-Netzwerk angeschlossen sind.

Mit einer effektiven Geräteverwaltung lassen sich Geräte erfassen, die an das ICS-Netzwerk angeschlossen sind. Hierzu gehören unter anderem Mensch-Maschine-Schnittstellen, SPS, Engineeringstationen, Netzwerkgeräte, Server usw. Außerdem sollten für jedes Gerät unbedingt Firmware, Software und Anwendungen ergänzt werden. Ohne diese zusätzlichen Informationen können die jeweils verfügbaren Funktionen und Services nicht ermittelt werden, was die ICS anfällig machen kann.

Viele Anbieter auf dem Markt bieten automatisierte Lösungen zur aktiven und passiven Geräteerkennung/Netzwerkabbildung. Statt manueller Praktiken zur Geräteverwaltung sollten nach Möglichkeit Lösungen zur passiven Geräteerkennung eingesetzt werden.

3.2.3 Lieferkettenmanagement

Ein effektives Programm zum Lieferkettenmanagement stellt sicher, dass Geräte und Software so von den Anbietern konfiguriert sind, dass sie den Sicherheitsanforderungen der Organisation entsprechen.

Vor der Installation von neuen digitalen Steuerungssystemen oder anderen digitalen Geräten oder Software und/oder Anwendungen in ICS sollte die Organisation sich vergewissern, dass die Geräte aus einer vertrauenswürdigen Quelle stammen – beginnend vom Entwickler über den Hersteller, den Lieferanten, den Versand und die Lagerung bis hin zu Inbetriebnahme und Abnahmeprüfung.

3.3 ICS-Sicherheit

3.3.1 Zugangsverwaltung

Nicht gesicherte Zugangspunkte gehören zu den größten Angriffsvektoren in ICS. Diese Zugangspunkte sind anfällig für vorsätzliche Cyberangriffe, aber auch unbeabsichtigte Cybervorfälle. Cyberkriminelle wissen, dass ICS in der Regel die Möglichkeit zur Fernwartung unterstützen, und suchen deshalb nach diesen einfachen Zugangspunkten, um das System zu schädigen. Der schlimmste Fall wäre, wenn ein Zugangspunkt für einen längeren Zeitraum kompromittiert wird, sodass Dritte unbefugt Zugang zu ICS haben und wertvolle Informationen zu den ICS und den Prozessen am Standort erhalten, wodurch sie einen Cyberangriff sorgfältiger planen und ausführen können.

3.3.2 Konfigurationsmanagement

Digitale/elektronische Geräte sind mit Firmware und/oder Software ausgestattet, die viele Optionen und Funktionen für eine effektive Leistung und/oder Kommunikation bieten. Um die Möglichkeiten für Cyberangriffe zu reduzieren, werden diese Geräte „gehärtet“ (z. B. basierend auf ihrer Kritikalität oder dem Ergebnis einer Cyber-Prozessgefahrenanalyse (PGA)), um nur die Optionen und Funktionen zu nutzen, die für den Betrieb der ICS erforderlich sind.

Nachdem die gewünschte Konfiguration erfolgt ist und das System ordnungsgemäß funktioniert, sollten diese Einstellungen als Basis-Konfiguration oder zuletzt bekannte zuverlässige Konfiguration gespeichert werden. Bei Störungen durch physische Schäden oder Firmware-/Softwarekorruption kann diese Basis-Konfiguration zur Wiederherstellung des Systems verwendet werden.

Nachdem die Konfiguration von Sicherheits-SPS oder anderen Steuerungen erfolgt ist, sollten die SPS oder Steuerungen auf die vom Herstellunternehmen empfohlene Betriebsart eingestellt werden (Run, Program, Remote o. Ä.). Diese Konfiguration wird dann samt Einstellungen und Betriebsart durch Entfernen des physischen Schlüssels oder eine entsprechende Einstellung des digitalen Schlüssels gesichert. Dies unterstützt eine geregelte Zugangskontrolle, da so nur Personen Zugriff haben, die zur Anpassung der Sicherheitseinstellungen berechtigt sind.

Durch die Überwachung der Konfigurationseinstellungen können unbefugte Änderungen an ICS identifiziert werden. Durch diese Überwachung können interne oder externe Bedrohungen für die ICS erkannt und möglicherweise verhindert werden.

3.3.3 Patch-Management

Beim Patch-Management handelt es sich um das Aufspielen von Software-, Treiber- und Firmware-Updates, um mögliche Schwachstellen zu schließen. Patches sollten im Hinblick auf deren mögliche Auswirkungen auf den Prozess bewertet werden.

Vor dem Einspielen eines Patch sollte die Authentizität und Integrität der Software geprüft werden, um sicherzustellen, dass sie in ursprünglicher Form vorliegt und nicht geändert wurde. Die Quelle der Software ist ebenfalls kritisch. Vor dem Herunterladen von Software sollte unbedingt die Vertrauenswürdigkeit der Quelle bestätigt werden.

Wenn ein Patch keine Vorteile für die Cybersicherheit oder Leistung bringt, ist er unter Umständen nicht notwendig. Der Asset Owner sollte mit dem ICS-Lieferanten bei der Bereitstellung von Patches für das ICS-/OT-Netzwerk zusammenarbeiten.

3.3.4 Sicherheitsvorkehrungen für Netzwerke

Mit neuen technologischen Entwicklungen wie Industrie 4.0 weisen ICS/OT-Umgebungen eine nie da gewesene Vernetzung auf. Dadurch ergibt sich für ICS/OT-Umgebungen eine deutliche Steigerung der Gefährdung durch Cyberangriffe.

Lieferantensupport erfolgt zunehmend über Fernzugriff. Auch ist Fernzugriff praktisch für Mitarbeitende, um bequem von extern auf die ICS-/OT-Umgebung zuzugreifen. Kommunikationsvorgänge von externen Standorten, die Zugang zur ICS-/OT-Umgebung erfordern, sollten über eine sichere VPN-Verbindung mit Multi-Faktor-Authentifizierung (MFA) über eine DMZ auf einen Fernzugriffserver/Bastion Host mit Zugang zur ICS-/OT-Umgebung erfolgen. Kommunikationsvorgänge innerhalb der Unternehmensumgebung, die Zugang zur ICS-/OT-Umgebung erfordern, sollten gesichert durch eine Multi-Faktor-Authentifizierung (MFA) über eine DMZ, also geroutet über einen Fernzugriffserver/Bastion Host mit Zugang zur ICS-/OT-Umgebung, erfolgen.

Eine industrielle DMZ (demilitarisierte Zone) ist ein Perimeternetzwerk, das eine zusätzliche Sicherheitsbarriere zum Schutz vor nicht vertrauenswürdigem Datenverkehr für das unternehmensinterne OT-Netzwerk bietet. Eine demilitarisierte Zone (DMZ) bezeichnet einen Bereich, der ein vertrauenswürdiges Netzwerk abschirmt und einen sicheren Zugriff auf Ressourcen von nicht vertrauenswürdigen Netzwerken wie dem Internet ermöglicht. Dadurch werden Ressourcen, auf die Benutzer über nicht vertrauenswürdige Bereiche zugreifen müssen, vom sicheren Netzwerk abgeschirmt. Eine industrielle DMZ bietet Dienste, die eine Verbindung mit dem IT- und dem OT-Netzwerk erfordern, z. B. Fernzugriff, Patching, Antivirenprogramme, Datenerfassungs- und Archivierungssysteme, Produktionsleitsysteme und Dateiübertragungen.

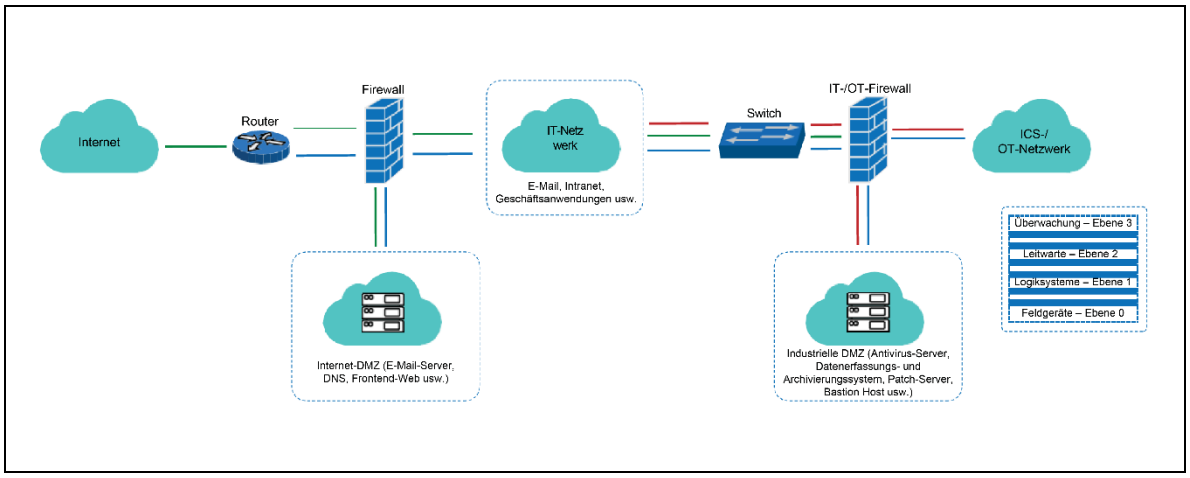

Abbildung 3.3.4: Beispiel für einen Kommunikationspfad mit Unternehmens-/Internet-DMZ und ICS-/industrieller DMZ

Angriffserkennungssysteme (IDS) sind Netzwerk-Sicherheitssysteme, die den Netzwerkverkehr und Geräte überwachen, um schadhafte Aktivitäten zu identifizieren. Alarme von den ICS sollten an zur weiteren Untersuchung an ein Security Operations Center (SOC) weitergeleitet werden.

Signaturbasierte Angriffserkennungssysteme konzentrieren sich auf die Suche nach Signaturen (d. h. Mustern), um Angriffe zu erkennen. Zur Identifizierung aktueller Angriffsmuster sind regelmäßige Aktualisierungen dieser Signaturen erforderlich.

Anomaliebasierte Angriffserkennungssysteme (IDS) konzentrieren sich zur Angriffserkennung auf unerwartete Aktivitätenmuster, zum Beispiel einen plötzlichen Anstieg der Netzwerkaktivitäten, mehrere fehlgeschlagene Login-Versuche, ungewöhnliche und als verdächtig eingestufte Netzwerk-Port-Aktivitäten usw. Diese Alarme werden regelmäßig an das Security Operations Center (SOC) übergeben.

3.4 Beispiele für Schadenfälle

3.4.1 Angriff auf die ukrainische Stromversorgung

Schadsoftware „Crashoverride“. Einer der größten Angriffe auf ICS fand am 23. Dezember 2015 in der Ukraine statt. Dabei waren ungefähr 225.000 Kunden von mehreren ungeplanten Stromausfällen betroffen. Die Ausfälle wurden durch Cyberangriffe aus der Ferne in drei örtlichen Stromversorgungsunternehmen verursacht. Während die Stromversorgung wiederhergestellt wurde, konnten die betroffenen Unternehmen nur unter eingeschränkten Bedingungen arbeiten.

Angaben zufolge war der Cyberangriff abgestimmt und erfolgte koordiniert nach sorgfältiger Erkundung der betroffenen Netzwerke. Einigen Berichten zufolge erfolgte dieser Angriff über einen Zeitraum von sechs Monaten. Laut Berichten fanden die Cyberangriffe in den jeweiligen Unternehmen in Abständen von 30 Minuten statt. Es waren mehrere Werke betroffen. Während des Angriffs wurden von mehreren externen Stellen ohne Berechtigung verschiedene Leistungsschalter aus der Ferne betätigt. Dabei wurden entweder bereits vorhandene Remote-Administrationswerkzeuge auf Betriebssystemebene oder Client-Software der ICS-Komponenten verwendet, auf die über VPN-Verbindungen (Virtual Private Network) zugegriffen wurde. Angaben zufolge verschafften sich die externen Stellen vor dem Cyberangriff gültige Benutzeranmeldeinformationen, um einen Fernzugriff zu ermöglichen.

Nach Meldungen der drei Stromversorgungsunternehmen wurden während des Cyberangriffs mehrere Systeme durch die Verwendung der Schadsoftware „KillDisk“ gelöscht. Die Schadsoftware löscht ausgewählte Dateien in Systemen und beschädigt das Startprogramm des Systems, wodurch es nicht mehr betrieben werden konnte. Zudem wurden Windows-basierte Mensch-Maschine-Schnittstellen in Fernsteuerungs-Terminals von KillDisk überschrieben. Mehrere Seriell-zu-Ethernet-Geräte an Unterstationen wurden durch Beschädigungen der Firmware außer Betrieb gesetzt. Die unterbrechungsfreie Stromversorgung wurde über die Fernverwaltungsschnittstelle getrennt, was die erwartete Wiederherstellung der Systeme verzögerte.

Alle drei Unternehmen berichteten, dass ihre Systeme mit der Schadsoftware „BlackEnergy“ infiziert waren. Es ist allerdings nicht sicher, ob dies eine Rolle beim Cyberangriff spielte. Angaben zufolge wurde die Schadsoftware über Spear-Phishing-E-Mails mit schadhaften Anhängen eingeführt. Es ist möglich, dass mithilfe von BlackEnergy gültige Benutzeranmeldeinformationen abgerufen wurden. Das ist jedoch nicht bestätigt. Es hätte auch ein beliebiger Remote-Access-Trojaner (RAT) verwendet werden können.

Nach den Angriffen konnten die Unternehmen die Leistungsschalter nicht aus der Ferne zurücksetzen. Es musste Bedienpersonal entsendet werden, um die Schalter manuell zu betätigen. Das führte zu einem Stromausfall über eine Dauer von 4 bis 6 Stunden. Es ist anzumerken, dass als Folge dieses Vorfalls keine Beschädigungen der Stromerzeugungsanlagen gemeldet wurden.

3.4.2 TRISIS

Im Dezember 2017 stellten Sicherheitsexperten einen Schadsoftwareangriff auf sicherheitsgerichtete Steuerungen (SIS) und Prozessleitsysteme (DCS) an einem großen Industriestandort im Nahen Osten fest. Cybersicherheitsorganisationen bezeichnen diese Schadsoftware als TRITON oder TRISIS. Das Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) des Department of Homeland Security nennt sie HATMAN. Die Schadsoftware beschädigte Mensch-Maschine-Schnittstellen und die Triconex-/Tricon-Sicherheitssteuerungen von Schneider Electric. Ein Angreifer konnte die Speicherinhalte der Steuerung lesen und ändern (d. h., vorhandene Programme über einen Netzwerk-Fernzugriff überschreiben).

Auf Grundlage der verfügbaren Informationen erhielten die Angreifer Fernzugriff auf eine SIS-Engineeringstation und konnten die Schadsoftware installieren: eine Windows-PC-basierte ausführbare Datei kommunizierte mit der Sicherungssteuerung (Triconex) und eine schadhafte binäre Komponente wurde in die Steuerung geladen. Das FireEye-Cybersicherheitsunternehmen Mandiant untersuchte den Vorfall und berichtete [1], „dass die Schadsoftware Lese-/ und Schreibzugriff auf Programme hatte sowie den Zustand der Steuerung abfragen konnte. Zudem konnte sie über ein TriStation-Protokoll – ein firmeneigenes Protokoll, über das die TriStation-Software (Tricon-Programmierungssoftware) mit Triconex-Sicherheitssystemen kommuniziert – mit der Steuerung kommunizieren. Anscheinend war der Angreifer mit dem Triconex-System vertraut und hatte die Schadsoftware vor dem Angriff getestet.“

Nach der Analyse von Mandiant gibt es Belege, dass die Angreifer außerdem Zugang zum Prozessleitsystem (DCS) des Werks erlangt hatten, sich aber entschieden, das Sicherheitssystem zu manipulieren. Versehentlich verursachten die Angreifer eine Systemabschaltung, als sie versuchten, die Steuerungen umzuprogrammieren, um Sachschaden anzurichten. Das System wechselte aufgrund einer fehlgeschlagenen Validierungsprüfung zwischen den Prozessoren in einen Fail-safe-Zustand, woraufhin es heruntergefahren und der Verantwortliche alarmiert wurde. Hätten die Angreifer die Kontrolle über DCS und SIS erlangt, hätten sie möglicherweise schwere Schäden anrichten können, so Mandiant.

Nach Angaben von ICS-CERT und Dragos fehlt dem in älteren Steuerungen verwendeten TriStation-Protokoll (das bei diesem Vorfall angegriffen wurde) eine Authentifizierungs- oder Verschlüsselungsmethode für Backdoor-Konten, die im Notfall den Administratorzugriff und die Kontrolle über das Gerät ermöglichen. Neuere Versionen des Triconex-Systems verfügen allerdings über einen solchen Authentifizierungsfaktor für diese Konten und sind deshalb weniger anfällig für solche Angriffe. In einer Sicherheitsmitteilung bestätigte Schneider Electronic diese Schwachstelle und entwickelte ein Tool, mit dem die Schadsoftware in einer Tricon-Steuerung erkannt und entfernt werden kann. Unternehmensangaben zufolge befand sich der Hardware-Schlüsselschalter, mit dem die Steuerung manuell betätigt werden kann, noch im Betriebsmodus „Program“. Das ist inakzeptabel, wenn die Steuerung nicht programmiert wird.

Triconex-Systeme gelten auf dem Markt als hochwertige Sicherheitssysteme. Tricon basiert auf der TMR-Technologie (Triple Modular Redundant). Bei dieser Technologie werden drei isolierte, parallele Steuerungssysteme und umfassende Diagnosetools in ein System integriert. Das Tricon-System bietet einen fehlerfreien Betrieb mit hoher Integrität und ununterbrochenen Prozessen ohne singuläre Schwachstelle. Das TMR-Prinzip wird auf Eingaben, Ausgaben und Logik angewendet. Aufgrund der Größe und Kosten werden solche Systeme hauptsächlich für kritische Anlagen wie Turbinensteuerungen (Überdrehzahlkontrolle) und manchmal als Prozessleitsystem (DCS) verwendet. Auch wenn diese Schadsoftware speziell auf Triconex-Systeme ausgerichtet wurde, warnen Cybersicherheitsunternehmen, dass Angreifer die Funktionen und Methodik anpassen und Sicherheitssysteme anderer Anbieter angreifen könnten. Die Auffassung, dass das Sicherheitssystem selbst bei einer Manipulation des Prozessleitsystems Schaden verhindert, wurde durch diesen Vorfall widerlegt.

4.0 VERWEISE

4.1 FM

FM Datenblatt zur Schadenverhütung 1-20, *Protection Against Exterior Fire Exposure*
FM Datenblatt zur Schadenverhütung 1-44, *Damage-Limiting Construction*
FM Datenblatt zur Schadenverhütung 2-0, *Installationsrichtlinien für automatische Sprinkleranlagen*
FM Datenblatt zur Schadenverhütung 3-26, *Anlagentechnischer Brandschutz in Nichtlager-Nutzungsarten*
FM Datenblatt zur Schadenverhütung 4-5, *Portable Extinguishers*
FM Datenblatt zur Schadenverhütung 4-9, *Halocarbon and Inert Gas (Clean Agent) Fire Extinguishing Systems*
FM Datenblatt zur Schadenverhütung 5-11, *Lightning and Surge Protection for Electrical Systems*
FM Datenblatt zur Schadenverhütung 5-23, *Design and Protection for Emergency and Standby Power Systems*
FM Datenblatt zur Schadenverhütung 5-28, *DC Battery Systems*
FM Datenblatt zur Schadenverhütung 5-31, *Cables and Bus Bars*
FM Datenblatt zur Schadenverhütung 5-32, *Data Centers and Related Facilities*
FM Datenblatt zur Schadenverhütung 7-43, *Process Safety*
FM Datenblatt zur Schadenverhütung 7-45, *Safety Controls, Alarms, and Interlocks (SCAI)*
FM Datenblatt zur Schadenverhütung 9-0, *Integrität von Anlagen*
FM Datenblatt zur Schadenverhütung 9-1, *Supervision of Property*
FM Datenblatt zur Schadenverhütung 10-1, *Einsatz- und Notfallplanung*
FM Datenblatt zur Schadenverhütung 10-5, *Disaster Recovery Planning*
FM Datenblatt zur Schadenverhütung 10-8, *Operators*

4.2 Sonstige

International Society for Automation (ISA). ISA/IEC 62443 – Reihe von Normen und technischen Berichten

National Institute of Standards and Technology (NIST). *Guide to Industrial Control Systems (ICS) Security*. NIST SP 800-82, Revision 2

North American Electric Reliability Corporation (NERC). CIP Reliability Standards

Electric Power Research Institute (EPRI), *Generation Cyber Security*

US Department of Homeland Security, National Cybersecurity and Communications Integration Center (NCCIC), ICS-CERT

ANHANG A – BEGRIFFSDEFINITIONEN

Allowlist: Eine Liste diskreter Entitäten wie Hosts oder Anwendungen, die als vertrauenswürdig bekannt sind und deren Verwendung in einer Organisation und/oder einem Informationssystem freigegeben wurde. Beispiel: Im Rahmen der Härtung werden nur bestimmte Anwendungen und Dienste auf einem Host zugelassen.

Angreifer: Person, die Computer-Software und -Hardware erstellt und/oder modifiziert, um eine Straftat zu begehen oder sich finanzielle Vorteile zu verschaffen. Angreifer versuchen in der Regel, sich Zugang zu Computersystemen zu verschaffen, um Benutzernamen und Passwörter zu erhalten.

Angriffserkennungssystem: Ein Sicherheitssystem, das Netzwerk- und Systemereignisse überwacht und analysiert, um unbefugte Zugriffsversuche auf Systemressourcen zu ermitteln und in Echtzeit oder Fast-Echtzeit diesbezügliche Warnungen auszugeben. Ein Angriffserkennungssystem kann unbefugten Datenverkehr zwar erkennen und entsprechende Warnungen ausgeben, es kann ihn aber nicht sperren oder zurückweisen.

Angriffsvektor: Eine Methode oder ein Mittel, das ein böswilliger Akteur nutzt, um auf Daten oder das Computernetzwerk einer Organisation zuzugreifen oder diese zu beschädigen. Beispiele für Angriffsvektoren sind Denial of Service (DoS), Schadsoftware, physischer Zugang, Ransomware und Social Engineering.

Antivirensoftware: Software, die einen Computer vor Viren und Schadsoftware schützt. Wenn schädlicher Code entdeckt wird, versucht die Antivirensoftware, betroffene Dateien, Verzeichnisse oder Datenträger zu bereinigen, löschen oder unter Quarantäne zu stellen.

Authentifizierung: Prüfung einer Angabe, z. B. die Identität eines Benutzers des Computersystems. Im Gegensatz zur Identifizierung, also die Angabe der Identität einer Person oder eines Gegenstands, ist die Authentifizierung der Überprüfungsprozess der Identität. Ein Passwort, das ein Benutzer bei der Anmeldung eingibt, ist eine typische Authentifizierung.

Basiskonfiguration: Spezifikation oder Produkt, die bzw. das formal überprüft und bestätigt wurde, anschließend als Grundlage für künftige Entwicklungen dient und nur durch ein formales Veränderungsmanagement geändert werden kann.

Basis-Prozessleitsystem (BPCS): Über das Basis-Prozessleitsystem (BPCS) werden Anlagen, Produktion und Prozesse an einem Standort verwaltet. Auf der Grundlage einer oder mehrerer vorhandener Bedingungen nutzt das Basis-Prozessleitsystem Feedback von Regelkreisen, um eine bestimmte Bedingung, Ausgabe oder einen bestimmten Prozess zu automatisieren und aufrechtzuerhalten. Basis-Prozessleitsysteme können an alle Prozessanforderungen angepasst werden – von sehr großen und komplexen Systemen wie Stromerzeugungsanlagen oder chemischen Verarbeitungsanlagen bis hin zu sehr einfachen Systemen mit jeweils einer Ein- und Ausgabe wie Bewegungsmeldern oder Beleuchtungsanlagen.

Bedienstation: Eine Bedienstation stellt eine dynamische Ansicht aller Prozesse im Werk dar, die für den Betrieb von Steuerungssystemen erforderlich sind. Sie stellt Steuerungsgrafiken, Analysen, Trends, Alarme sowie Statusanzeigen bereit.

Benutzeranmeldeinformationen: Benutzeranmeldeinformationen bestehen mindestens aus einem Benutzernamen und Passwort, können aber auch physische oder biometrische Merkmale wie einen Fingerabdruck beinhalten. Benutzeranmeldeinformationen dienen der Authentifizierung eines Benutzers, wenn er sich an ICS anmeldet. Unter Umständen sind den Benutzeranmeldeinformationen eines Benutzers bestimmte Zugangsberechtigungen zugeordnet. Anmeldeinformationen für einen Standardnutzer können Zugang zu einer Bedienstation gewähren, während ein höherer Zugriffslevel für einen anderen Benutzer Zugriff auf eine Engineeringstation gewähren kann.

Benutzerverzeichnis: System, in dem Informationen zu Nutzern/Mitgliedern einer bestimmten Domäne hinterlegt sind, um die Authentifizierung und Berechtigungen zentral zu verwalten. Ein häufig verwendetes Benutzerverzeichnis in IT- und OT-Netzwerken ist Microsoft Active Directory.

Betriebssystem (OS): Die grundlegende Software, die eine Interaktion mit einem Computer ermöglicht. Das Betriebssystem steuert den Computerspeicher, Kommunikationen und Funktionen zur Aufgabenverwaltung.

Böswilliger Akteur: Entität, die teilweise oder gänzlich für einen Vorfall verantwortlich ist, der die Sicherheit einer Organisation beeinträchtigt. Beispiele hierfür sind: Hacktivismus, Insider-Bedrohungen, staatliche Akteure und organisiertes Verbrechen.

Datendiode/Einweg-Gateway: Siehe „Einweg-Datendiode“ unten.

Datenerfassungs- und Archivierungssystem: Ein ICS-Datenerfassungs- und -Archivierungssystem ist ein spezielles Softwaresystem, das Datenpunkte, Alarmereignisse, Batch-Datensätze und andere Informationen aus industriellen Geräten und Systemen sammelt und diese in einer speziell dafür angelegten Datenbank speichert (d. h. eine zentrale Datenbank, die Datenanalysen durch statistische Prozesskontrolltechniken unterstützt).

Demilitarisierte Zone (industrielle DMZ):

1. Eine Schnittstelle an einer Routing-Firewall, ähnlich der Schnittstellen auf der durch die Firewall geschützten Seite. Datenverkehr zwischen der DMZ und anderen Schnittstellen auf der geschützten Seite der Firewall läuft weiterhin durch die Firewall und es können für diesen Verkehr auch Firewall-Schutzrichtlinien gelten.
2. Ein Host oder Netzwerk, das sich als „neutrale Zone“ zwischen dem privaten Netzwerk einer Organisation und dem Internet befindet. Die meisten industriellen DMZ befinden sich zwischen der IT- und der OT-Umgebung eines Unternehmens.
3. Segment eines Perimeternetzwerks, das sich logisch zwischen internen und externen Netzwerken befindet. Zweck ist die Umsetzung von Richtlinien bezüglich des internen Netzwerks für den externen Austausch von Informationen und der eingeschränkte Zugriff auf zugängliche Informationen durch externe, nicht vertrauenswürdige Quellen sowie die Abschirmung interner Netzwerke vor Angriffen von außen.

Ein-/Ausgabegerät: Allgemeiner Begriff für das Gerät, das zur Kommunikation mit einem Computer oder Steuerungssystem verwendet wird.

Einweg-Datendioden und Einweg-Gateways: Hardware-basierte Geräte mit zwei Knoten oder Stromkreisen (einer, der nur sendet, und einer, der nur empfängt), die einen Datenfluss von einer Quelle an ein Ziel nur in eine Richtung zulassen. Auf der einen Seite wird eine Leuchtdiode (LED) als Datenübermittler verwendet, auf der anderen eine Empfangsdiode. So ist es physisch unmöglich, Daten in die andere Richtung weiterzuleiten. Das können Softwarelösungen sein (z. B. über eine Firewall-Einstellung) oder sogar eine Schalter- oder Router-Konfiguration als Einweg-Gateway. Ein „echter“ Einweg-Gateway verwendet allerdings eine oder mehrere Einweg-Datendiode(n). Auszug aus NIST 800-82: Einweg-Gateways sind eine Kombination aus Hardware und Software. Die Hardware lässt den Datenfluss von einem Netzwerk in ein anderes zu, kann aber physisch keine Informationen zurück in das Quellnetzwerk senden. Die Software repliziert Datenbanken und bildet Protokollserver und Geräte nach.

Einweg-Kommunikation: Strategien, mit denen sichere Einweg-Kommunikationen von Geräten oder über mehrere Netzwerke/Schutzzonen hinweg gewährleistet werden. Hierzu gehören:

1. Ausschließliches Senden eines analogen Signals (Stromstärke oder Spannung) an ein/von einem Gerät anstelle des Sendens von digitalen Daten
2. Verwendung einer Einweg-Datendiode/ eines Einweg-Gateways
3. Verwendung von Regeln in einer Firewall oder DMZ, um Daten netzwerkübergreifend weiterzuleiten

Engineeringstation: Die Engineeringstation ist eine zuverlässige High-Performance-Computerplattform zur Konfiguration, Pflege und Analyse der Anwendungen und weiteren Anlagen des Steuerungssystems. Normalerweise enthält sie anbieterspezifische Software für die Programmierung von Geräten und die Projektdateien, die zur Programmierung von Geräten, einschließlich SPS und Mensch-Maschine-Schnittstellen, verwendet werden.

Feldgerät: Gerät, das an der Feldseite eines ICS angeschlossen ist. Zu Feldgeräten gehören unter anderem Fernsteuerungs-Terminals (RTU), speicherprogrammierbare Steuerungen (SPS), Aktoren, Sensoren, Mensch-Maschine-Schnittstellen (HMI) und dazugehörige Kommunikationen.

Fernsteuerungs-Terminal (RTU): Einheit zur Unterstützung von Fernstationen für Prozessleitsysteme (DCS) und für Systeme zur Überwachung, Steuerung und Datenerfassung (SCADA). RTUs sind Feldgeräte, mit denen Parameter überwacht werden. Sie kommunizieren über Fernkommunikationsfunktionen (z. B. Modem, Mobilfunk, Funkschnittstellen oder andere Kommunikationstechnologien zur Fernübertragung) mit einer übergeordneten Steuerung. Manchmal werden SPS als Feldgeräte implementiert, die als RTU dienen. In diesem Fall wird ein SPS häufig als RTU bezeichnet. Sie werden häufig an Standorten installiert, an denen sich der Zugang zur Stromversorgung schwierig gestaltet, und können mit Solarenergie versorgt werden.

Fernzugriff: Zugriff auf die Sicherheitszone eines Informationssystems, der von außen durch einen Benutzer (oder ein Informationssystem) erfolgt (Quelle: NIST SP 800-53.) Verwendung von Systemen innerhalb der Sicherheitszone, wobei der Zugang zum System von einem anderen geografischen Standort erfolgt. Die Berechtigungen entsprechen denen bei einem Zugang vor Ort. Beispiele für Geräte für einen Fernzugriff:

1. Modems modulieren und demodulieren bidirektional Daten. Im Wesentlichen wandeln sie analoge elektrische Signale von außerhalb des Netzwerks in digitale Einsen und Nullen um, damit sie vom Router verarbeitet werden können, und umgekehrt.
2. Router sind einem Modem nachgeschaltet. Sie sind über eine öffentliche IP-Adresse an ein WAN oder das Internet angeschlossen. Sie verteilen und transportieren Netzwerkdaten und priorisieren die Daten dabei, um die am besten geeignete Route für jede Übertragung zu wählen.
3. Über Fernzugriffserver lassen sich Fernverbindungen von außerhalb des LAN verwalten. Sie werden gemeinhin als Bastion Host oder Jump Host bezeichnet.

Fernzugriffserver: Server, über den sich eine Fernverbindung von außerhalb des LAN verwalten lässt. Server dieser Art werden gemeinhin als Bastion Host oder Jump Host bezeichnet.

Firewall: Eine Firewall ist ein System zur Netzwerksicherung, das den ein- und ausgehenden Netzwerkdatenverkehr überwacht und basierend auf definierten Sicherheitsregeln entscheidet, ob ein bestimmter Datenfluss zugelassen oder gesperrt wird.

Gateway: Ein Übergabemechanismus, der zwei oder mehr Computernetzwerke mit ähnlichen Funktionen, aber unterschiedlichen Implementierungen verbindet. Ein Gateway ermöglicht die Kommunikation von Host-Computern in einem Netzwerk mit Hosts eines anderen Netzwerks.

Gerät: Physisches oder logisches Objekt, das einer Organisation entweder gehört oder für das ihr die Obhutspflicht obliegt und das einen empfundenen oder tatsächlichen Wert für die Organisation hat.

Gestaffelte Verteidigung (Defense in Depth): Konzept zum Schutz von IT- und OT-Umgebungen durch ein mehrschichtiges System ineinandergreifender Sicherheitskontrollen.

Härtung: Sicherheitsmaßnahme, bei der nicht benötigte Funktionen, Schnittstellen und Dienste entfernt oder deaktiviert werden sowie Cybersicherheitskontrollen angewendet werden, um eine unbefugte Verwendung zu vermeiden. Bei der Härtung lässt sich folgende Unterscheidung treffen:

1. Physische Härtung: Deaktivierung durch physische Maßnahmen: Entfernung nicht benötigter Kommunikationsschnittstellen, Sperrung des Zugangs zu den Schnittstellen und Laufwerken usw.
2. Logische Härtung: Deaktivierung von nicht verwendeten Netzwerk- und Kommunikationsprotokollen, Treibern für nicht verwendete Peripheriegeräte, Webservern usw. Im Anschluss Anwendung von Cybersicherheitskontrollen wie der Aktivierung von Passwortschutz zum Aktualisieren von Firmware und Laden von Programmen, Aktivierung von Protokollen und Alarmen und Aktivierung von Sicherheitstechnologien wie Antivirenprogrammen oder Allowlisting-Software, die mit dem Gerät geliefert wurden.

Industrielle Schaltschränke: Eine Baugruppe mit zwei oder mehr Steuer- und Stromkreiskomponenten. Zu den Steuerkreiskomponenten zählen speicherprogrammierbare Steuerungen (SPS), Ein- und Ausgangsmodule, Motorantriebe und Kommunikationsmodule. Zu den Stromkreiskomponenten zählen Stromquellen, USV-Anlagen (unterbrechungsfreie Stromversorgung), Relais, Transformatoren und Spannungs-/Stromwandler. Üblicherweise werden industrielle Schaltschränke mit einer Spannung von 600 V oder weniger betrieben, wobei nach der Norm UL 508A und den IEC-Standards Spannungen bis maximal 1.000 Volt zulässig sind.

Industrielle Schalttechnik: Siehe industrielle Schaltschränke.

Industrielle Steuerungssysteme (ICS):

1. Allgemeiner Begriff, unter dem verschiedene Arten von Steuerungssystemen, darunter Systeme zur Überwachung, Steuerung und Datenerfassung (SCADA) sowie Prozessleitsysteme (DCS), und weitere Steuerungssystemkonfigurationen wie speicherprogrammierbare Steuerungen (SPS) sowie Sicherheits-Logiksysteme, die häufig in Industriebranchen und kritischen Infrastrukturen eingesetzt werden, zusammengefasst werden. ICS bestehen aus verschiedenen Steuerungskomponenten (z. B. elektrische, mechanische, hydraulische, pneumatische), die zusammenarbeiten, um ein bestimmtes Ziel zu erreichen (z. B. Fertigung, Generierung und Transport von Materie oder Energie).
2. Zusammenstellung von Personal, Hardware und Software, die den sicheren und zuverlässigen Betrieb eines industriellen Prozesses betreffen oder beeinflussen kann.

Insider-Bedrohung: Bedrohungen, die – absichtlich schadhaft oder unabsichtlich – von Personen innerhalb der Organisation ausgehen, z. B. unzufriedene Mitarbeitende, ehemaliges Personal, Vertrags- und Geschäftspartner*innen, die über interne Informationen zu den Sicherheitsvorkehrungen, Daten und Computersystemen der Organisation verfügen.

Integrität: Eigenschaft eines Systems, die Folgendes widerspiegelt: die logische Fehlerfreiheit und Zuverlässigkeit des Betriebssystems, die logische Vollständigkeit der Hardware und Software, die die Schutzmechanismen bereitstellt, sowie die Konsistenz von Datenstrukturen und gespeicherten Daten.

1. Intelligentes elektronisches Gerät (IED): Alle Geräte mit einem oder mehreren Prozessoren, die Daten von einer externen Quelle empfangen, dorthin senden und steuern können, z. B. elektronische Multifunktionsmessgeräte, digitale Relais, Steuerungen.

Isolation: Vollständige Trennung eines Netzwerks von anderen Netzwerken (Air Gap). Sicherheitsgerichtete Steuerungen (SIS) an großen Standorten sind isoliert, da sie nicht über das ICS-Netzwerk gesteuert werden, welches das Basis-Prozessleitsystem (BCPS) steuert.

IT-Netzwerk: Ein Netzwerk, das in der Regel zur Durchführung von Geschäftstätigkeiten verwendet wird und in dem mit Computern Daten erstellt, geändert, gespeichert, abgerufen und übertragen werden.

Konfigurationsmanagement (CM): Richtlinien und Anweisungen für Steuerungsmodifikationen an Hardware, Firmware, Software und Dokumentation, um sicherzustellen, dass das Informationssystem gegen unsachgemäße Modifikationen vor, während und nach der Systemimplementierung geschützt ist.

Leitzentrale: Siehe Prozessleitwarte.

Local Area Network (LAN): Kommunikationsnetzwerk, das dazu dient, Computer und weitere intelligente Geräte in einem begrenzten geografischen Bereich (in der Regel unter 10 Kilometer) miteinander zu verbinden.

Lösungen zur Geräteerkennung:

1. Passive Überwachung: Unbemerkte, nicht intrusive Überwachungstechnologie, mit der Datenverkehr aus einem Netzwerk erfasst wird, indem der Verkehr kopiert wird, häufig über einen SPAN-Port (Switched Port Analyzer), Port-Spiegelung (Port Mirroring) oder einen Netzwerk-TAP (Test Access Point). Auf OT-Netzwerke spezialisierte Angriffserkennungssysteme (IDS) verwenden diese Technik zur Geräteerkennung sowie zur Erkennung von unbefugten Aktivitäten.
2. Aktive Überwachung: Intrusive Überwachungstechnologie, die Abfragen in der systemeigenen Programmiersprache (Protokoll) der Steuerung durchführt, die von Herstellunternehmen zu Herstellunternehmen leicht unterschiedlich sein können. Bei der aktiven Überwachung werden ausführliche Informationen von der Steuerung abgerufen (IP- und MAC-Adressen, Firmwareversion, Backplane-Konfiguration usw.).

Mensch-Maschine-Schnittstelle (HMI):

1. Die Hardware oder Software, über die das Bedienpersonal mit einer Steuerung interagiert. Eine Mensch-Maschine-Schnittstelle kann eine physische Schalttafel mit Tasten und Anzeigeleuchten sein oder ein Industrie-PC mit einer farbigen Grafikanzeige, auf dem eine spezielle Software für die Mensch-Maschine-Schnittstelle betrieben wird.
2. Software- und Hardware, die es autorisierten Personen ermöglicht, Prozesse und/oder Geräte zu überwachen und zu steuern, zum Beispiel Darstellung des aktuellen Zustands oder der historischen Entwicklung, Vornahme steuerungsrelevanter Änderungen und manuelle Übernahme der Kontrolle im Notfall.

Multi-Faktor-Authentifizierung (MFA): Zu einer Multi-Faktor-Authentifizierung gehören mindestens zwei Authentifizierungsfaktoren, d. h. etwas, das die betreffende Person kennt, z. B. ein Passwort; etwas, das sie besitzt, z. B. ein zeitbasiertes oder statisches Token, oder etwas, das ihr eigen ist, z. B. ein Fingerabdruck. Die Zwei-Faktor-Authentifizierung ist eine Multi-Faktor-Authentifizierung mit genau zwei Faktoren.

OT-Netzwerk (Produktionsnetzwerk): Der Begriff Produktionsnetzwerk (OT) wird häufig synonym mit den Begriffen industrielles Steuerungssystem (ICS) oder Prozesssteuerungsnetzwerk (PCN) verwendet. Der Begriff dient zur Unterscheidung zwischen dem IT-Netzwerk und den vernetzten Steuerungssystemen der Anlagen oder Maschinen (OT). Ein ICS umfasst verschiedene Steuerungen und Instrumente zur Überwachung und Steuerung eines physischen Prozesses, wohingegen ein OT-Netzwerk aus den Computersystemen und der Infrastruktur besteht, über die industrielle Vorgänge (einschließlich der ICS) gesteuert werden.

Patch: Ein Software-Add-on, mit dem Bugs und Sicherheitslücken in Betriebssystemen oder Anwendungen behoben werden können. Wenn eine Software mit Patches auf dem aktuellen Stand gehalten wird, lassen sich Sicherheitsrisiken minimieren.

Phishing: Angriff auf die Sicherheit, bei dem Opfer dazu verleitet werden, Informationen preiszugeben, indem eine gefälschte E-Mail den Empfänger auffordert, eine Website aufzurufen, die wie eine legitime Quelle aussieht.

Physischer Zugang: Tatsächlicher praktischer Zugang am Standort auf Computer- und Netzwerk-Hardware oder andere Teile einer Netzwerkinstallation.

Produktionsleitsystem (MES): Ein computergeschütztes System mit Software, das in Produktions- und Fertigungsumgebungen eingesetzt wird, um Inventar- und andere Produktionsinformationen zu erfassen, ähnlich einem System zur Unternehmensressourcenplanung (ERP). Allerdings liegt der Fokus beim Produktionsleitsystem auf der Fertigung (z. B. Erfassung und Dokumentation von Daten zur Herstellung von Fertigerzeugnissen aus Rohstoffen).

Protokoll: Ein Protokoll ist ein System von Regeln, das von zwei Komponenten für den Datenaustausch genutzt wird, um diese Daten lesen zu können. Ein Protokoll ist nicht als „Sprache“ anzusehen, es handelt sich eher um die Grammatik und Syntax bei der Kommunikation dieser Sprache. In der ICS-Umgebung sind Protokolle häufig spezifisch für den jeweiligen Geräteanbieter. Sie sind oft hinsichtlich der Funktionalität und Zuverlässigkeit und nicht unbedingt hinsichtlich der Sicherheit optimiert. In der Regel werden sie in Klartext (unverschlüsselt) übermittelt. Das belegt die Notwendigkeit, das OT-Netzwerk von der IT-Umgebung zu trennen. Beispiele für ICS-Protokolle, die in der Industrie häufig zur Anwendung kommen, sind Modbus RTU, Modbus TCP, Profibus, Profinet, DNP3 und ControlNet. Auf der IT-Seite basieren Protokolle häufig auf TCP/IP (z. B. FTP, DNS, HTTP, HTTPS).

Prozessleitsystem (DCS): Ein Prozessleitsystem (DCS) ist ein automatisiertes Leitsystem, das Prozesse durch die Verteilung von Kontrollfunktionen über mehrere miteinander verbundene Komponenten steuert. Dabei werden statt einer einzelnen zentral positionierten Einheit mehrere verteilte Komponenten eingesetzt. Der Begriff „Prozessleitsystem(DCS)-Controller“ bezieht sich auf das physische Steuerungsgerät, wohingegen der Begriff „Prozessleitsystem“ das gesamte System, einschließlich Anwendungsservern, Mensch-Maschine-Schnittstellen (HMI) usw., umfassen kann.

Prozessleitwarte: Ein abgetrennter und/oder isolierter Raum, in dem das Personal Prozesse zentral oder remote überwacht und leitet. Die Prozessleitwarte befindet sich üblicherweise in einem separaten Raum, ist jedoch zur Überprüfung der Funktionsfähigkeit der Technik mit den Räumen, in denen die industrielle Schalttechnik untergebracht ist, verbunden. Systeme zur Prozessleitung sind in der Industrie weit verbreitet. Sie ermöglichen üblicherweise die Massenproduktion mit durchgängig laufenden Prozessen (z. B. bei Papier, Arzneimitteln, Chemikalien oder Stromerzeugung) sowie andere Industrieprozesse. In einigen Fällen sind Prozessleitwarten/Technikbereiche unbesetzt und werden remote betrieben.

Prozessleitzentrale: Siehe Prozessleitwarte.

Ransomware: Bösartige Software (Schadsoftware), die Vorgänge deaktiviert oder den Zugriff auf Daten blockiert, bis eine Zahlungsaufforderung erfüllt wird.

Räume mit industrieller Mess- und Regelungstechnik: Räume, in denen sich die Technik zur Prozesssteuerung befindet, darunter üblicherweise mehrere industrielle Schaltschränke sowie Netzwerkgeräte, die für die Funktionsfähigkeit physischer Prozesse benötigt werden.

Richtlinie: Regelwerk, das den Ablauf bestimmter Verfahren festlegt.

Rollenbasierte Zugriffskontrolle: Identitätsbasierte Zugangskontrolle, wobei die identifizierten und kontrollierten Systementitäten Funktionsbereiche in einer Organisation oder einem Prozess darstellen.

Router: Ein Gateway zwischen zwei Netzwerken auf Ebene 3 des OSI-Modells (Open Systems Interconnection), das Datenpakete zwischen den Netzwerken weiterleitet. Die gängigste Form von Routern wird mit IP-Paketen (Internet Protocol) betrieben.

SCADA-Steuerzentrale: Eine Steuerzentrale mit Computern, auf denen SCADA-Software installiert ist. Damit werden Anlagen an einem oder mehreren Orten in räumlicher Entfernung von der Steuerzentrale betrieben und überwacht. SCADA-Steuerzentralen sind üblicherweise dort eingerichtet, wo keine lokalen Systeme zur Prozesssteuerung wie Prozessleitsysteme (DCS) oder speicherprogrammierbare Steuerungen (SPS) vorhanden sind. Bei SCADA-Steuerzentralen läuft der Datenverkehr in beide Richtungen und es können betriebliche Änderungen an geografisch entfernt gelegenen Anlagen vorgenommen werden.

Schadsoftware: Ein Oberbegriff für bösartige Software wie Viren, Trojaner, Spyware und schadhafte aktive Inhalte.

Schwachstelle: Schwachstelle im Systemdesign, in der Ausführung, in der Betreibung oder der Verwaltung, die zur Verletzung der Systemintegrität oder der Sicherheitsrichtlinien ausgenutzt werden könnte.

Security Information und Event Management (SIEM): Anwendung, die es ermöglicht, Sicherheitsdaten aus Informationssystemkomponenten zu sammeln, Audit-Trails zu vereinheitlichen und Tests anhand einer Reihe von Korrelationsregeln zu protokollieren, und die bei Auslösung Ereignisse für eine Analyse erstellt sowie diese Daten über eine einzelne Schnittstelle als praktisch umsetzbare Informationen präsentiert.

Security Operations Center (SOC): Lösung, die Personen, Prozesse und Technologien umfasst, einschließlich SIEM-Lösungen, die unter anderem digitale Umgebungen überwachen (d. h. IT und OT), um diese zu schützen; auf Ereignisse reagieren, die zu Schadenfällen führen können; zu bekannten/unbekannten Bedrohungen recherchieren; auf Vorfälle reagieren sowie Informationen teilen.

Segmentierung: Unterteilung eines Netzwerks in kleinere abgetrennte Abschnitte, die aber weiterhin Teil des gesamten Netzwerks sind. Innerhalb von ICS wird eine Segmentierung in der Regel über Virtual Local Area Networks (VLANs) oder Hardware-Firewalls realisiert. Segmentierung dient dazu, die Verbreitung von Schadsoftware einzudämmen oder einen Angriff zu erschweren. Dabei ist jedoch zu beachten, dass ein VLAN keine akzeptable Lösung zur Trennung von IT- und OT-Netzwerken darstellt.

Sensor:

1. Ein Gerät, das einen Ausgabewert in Form von Spannung oder Stromstärke erzeugt, der für eine bestimmte zu messende physische Eigenschaft (z. B. Geschwindigkeit, Temperatur, Durchfluss) repräsentativ ist
2. Ein Gerät, das eine physische Menge misst und in ein Signal umwandelt, das von einem Beobachter oder Instrument gelesen werden kann
3. Ein Gerät, das auf eine Eingabemenge reagiert, indem es einen funktionsbezogenen Ausgabewert generiert, in der Regel ein elektrisches oder optisches Signal

Sicherheitssteuerungsnetzwerk: Netzwerk, das sicherheitsgerichtete Steuerungen für die Kommunikation von sicherheitsbezogenen Informationen verbindet.

Sicherheitssteuerungssystem: System, das zur Implementierung von einer oder mehreren Funktionen mit Sicherheitsanforderung verwendet wird. Es besteht aus einer Kombination von Sensoren, Logiksystemen und Aktoren.

Speicherprogrammierbare Steuerung (SPS): Speicherprogrammierbare Steuerungen (SPS) sind automatisierte Steuerungen, die komplexe Prozesse steuern können. Sie werden häufig in Systemen zur Überwachung, Steuerung und Datenerfassung (SCADA) sowie in Prozessleitsystemen (DCS) eingesetzt. SPS werden auch als Hauptsteuerungen in kleineren Systemkonfigurationen eingesetzt. SPS werden in fast allen industriellen Prozessen umfassend verwendet.

Standardpasswort: Standardpasswort eines Systems bei Auslieferung oder Erstinstallation. Benutzer sollten das Standardpasswort immer umgehend ändern.

Steuernetzwerk: Zeitkritisches Netzwerk, das in der Regel an Anlagen angeschlossen ist, die physische Prozesse steuern. Das Steuernetzwerk kann in Zonen unterteilt werden. Es können mehrere separate Steuernetzwerke in einem Unternehmen oder an einem Standort vorhanden sein.

System zur Unternehmensressourcenplanung (ERP): Software, die in Geschäftsumgebungen zum Einsatz kommt. Beispiele sind SAP und Oracle/PeopleSoft, Systeme zur Verwaltung von Produktionsaufträgen, der Lagerung sowie Transportinformationen zu abgeschlossenen Aufträgen.

Trennung: Geeignete Aufteilung verschiedener Netzwerke, die gegenseitig als nicht vertrauenswürdig eingestuft werden. Eine Trennung erfolgt in der Regel über Firewalls (und idealerweise eine formale DMZ) oder ein Einweg-Gateway. Die Trennung vom IT-Netzwerk ist für die Sicherheit des ICS-Netzwerks eine Schlüsseleigenschaft.

Überwachung, Steuerung und Datenerfassung (SCADA): Dient zur Steuerung verstreuter Anlagen, bei denen die zentrale Datenerfassung ebenso wichtig ist wie die Steuerung. SCADA-Systeme werden in Verteilernetzen verwendet, z. B. In

1. Wasserverteilungs- und Abwassersammelsystemen
2. Öl- und Erdgasleitungen
3. Stromversorgungs-Übertragungs- und Verteilernetzen
4. Bahnnetzwerken und anderen öffentlichen Transportsystemen

SCADA-Systeme kombinieren Datenerfassungssysteme mit Datenübertragungssystemen und Software für Mensch-Maschine-Schnittstellen und bieten so ein zentrales Überwachungs- und Steuerungssystem für zahlreiche Prozessein- und -ausgaben. SCADA-Systeme dienen zum Sammeln von Felddaten, ihrer Übertragung an eine zentrale Computeranlage sowie der Anzeige dieser Informationen für das Bedienpersonal in grafischer oder Textform. So kann das Bedienpersonal ein ganzes System von einem zentralen Standort nahezu in Echtzeit überwachen oder steuern. Je nach Differenziertheit und Einrichtung des Systems kann die Steuerung eines Systems, Vorgangs oder einer Aufgabe automatisch oder über Befehle des Bedienpersonals erfolgen.

Unbefugtes Gerät: Ein unbefugtes Gerät ist ein nicht zugelassenes Gerät, das nicht berechtigt ist, auf ein Netzwerk zuzugreifen und dort betrieben zu werden. Mit diesen unter Umständen mit böswilliger Absicht installierten Geräten könnten Sicherheitsvorkehrungen umgangen werden.

Unveränderliche Sicherungsdateien: Unveränderliche Sicherungsdateien sind Dateien, an denen keinerlei Änderungen vorgenommen werden können (Write Once, Read Many, zu Deutsch: einmal schreiben, vielfach lesen) und bei denen vor Ablauf der Aufbewahrungsfrist auch keine Löschung möglich ist. (Das Ablaufdatum dieser Aufbewahrungsfrist muss bei Erstellung der unveränderlichen Sicherungsdatei konfiguriert werden.) Da unveränderliche Dateien keine Änderungen oder Löschungen zulassen, kommt der Versionskontrolle eine sehr wichtige Bedeutung zu.

Verfahren: Schritte, die zur Durchführung einer bestimmten Aufgabe ausgeführt werden.

Verschlüsselung: Die Verschlüsselung von Daten, sodass sie für Personen unlesbar sind, die nicht über den „Schlüssel“ zur Entschlüsselung verfügen. Verschlüsselte Umwandlung von Klartext in sogenannten Ciphertext (Geheimtext), der die ursprüngliche Bedeutung der Daten verschleiert, damit sie nicht gelesen oder verwendet werden können.

Virtual Private Network (VPN): Sichere Verbindung zwischen einem öffentlichen Netzwerk (in der Regel das Internet) und einem privaten Netzwerk.

WAN-Lösungen: Ein Wide Area Network (WAN) ist ein Computernetzwerk, das sich über große Regionen, Länder oder sogar weltweit erstreckt. Es gibt verschiedene Möglichkeiten der Datenübertragung zwischen Netzwerken, die sich über einen geografischen Bereich erstrecken, verschiedene Verbindungsarten, mit denen diese WANs erstellt werden. Beispiele für verkabelte Lösungen: MPLS, T1 und permanente virtuelle Verbindungen. Zu den drahtlosen Kommunikationsdiensten gehören 4G und 5G, Wi-Fi und Satellitennetzwerke.

Wardialing: Ein Wardialer ist ein Computerprogramm, mit dem die Telefonnummern identifiziert werden, über die eine Verbindung zu einem Computer-Modem hergestellt werden kann. Das Programm wählt automatisch eine Reihe definierter Telefonnummern an und protokolliert und erfasst die Nummern, mit denen eine Verbindung zum Modem hergestellt werden kann, in einer Datenbank. Einige Programme können auch das spezifische Betriebssystem des Computers identifizieren und automatische Penetrationstests durchführen. In diesen Fällen durchsucht der Wardialer eine zuvor erstellte Liste mit gängigen Benutzernamen und Passwörtern, um Zugang zum System zu erhalten.

Zugriff/Zugang: Die Fähigkeit und Mittel, mit einem System zu kommunizieren oder anderweitig zu interagieren, um Systemressourcen zu nutzen. Dies kann physischer Zugang sein (Berechtigung, einen Bereich physisch zu betreten, Besitz eines physischen Schlüssels, eines PIN-Codes, einer Zugangskarte oder biometrischer Merkmale für den Zugang) oder logischer Zugriff (Berechtigung zur Anmeldung an einem System und einer Anwendung durch eine Kombination aus logischen und physischen Mitteln).

Zuverlässigkeit: Fähigkeit eines Systems, eine erforderliche Funktion unter festgelegten Bedingungen für einen angegebenen Zeitraum auszuführen.

ANHANG B – ANGABEN ZUR ÜBERARBEITUNG DES DOKUMENTS

Ziel des Anhangs ist die Darstellung der Änderungen an dem Dokument, die im Zuge der jeweiligen Veröffentlichung vorgenommen wurden. Die Nummerierung der einzelnen Abschnitte bezieht sich dabei auf die jeweils aktuelle Nummerierung zum Zeitpunkt der angegebenen Veröffentlichung (d. h., die Nummerierung der einzelnen Abschnitte kann sich je nach Version ändern).

Juli 2024. Zwischenrevision. Vornahme redaktioneller Änderungen

Januar 2024. Zwischenrevision. Vornahme geringfügiger redaktioneller Änderungen

Juli 2023. Zwischenrevision. Zu den wesentlichen Änderungen gehören:

A. Verbesserung und Klarstellung der Empfehlungen zum Brandschutz

   1. Verbesserung der Richtlinien zum Brandschutz für Belegungen und Anlagen

B. Aktualisierung der Empfehlungen zur ICS-Sicherheit

   1. Ergänzung von Richtlinien zu Verbindungen zu Remote-SCADA-Steuerzentralen

C. Ergänzung weiterer Begriffe in Anhang A – Begriffsdefinitionen

Januar 2023. Zwischenrevision. Folgende Änderungen wurden vorgenommen:

A. Klarstellung der Empfehlungen zum Brandschutz

B. Klarstellung der Empfehlungen zum ICS-Management

C. Klarstellung und Modifizierung der Empfehlungen zur ICS-Sicherheit, darunter:

   1. Modifizierung der Empfehlungen zur Konfiguration und Systemüberwachung für ICS und OT-Netzwerkgeräte, einschließlich der Sicherheitssteuerungssysteme

   2. Klarstellung der Empfehlungen zum Patch-Management

   3. Klarstellung der Empfehlungen zu Sicherheitsvorkehrungen für Netzwerke

D. Klarstellung und Modifizierung der Empfehlungen zum ICS-Betrieb, darunter:

   1. Klarstellung der Empfehlungen zum Alarmmanagement

2. Modifizierung hinsichtlich des Notfall- und Wiederherstellungsplans mit Blick auf akzeptable Arten von Sicherungsdateien

E. Ergänzung weiterer Begriffe in Anhang A – Begriffsdefinitionen

Juli 2022. Zwischenrevision. Vornahme geringfügiger redaktioneller Änderungen

Oktober 2021. Zwischenrevision. Aktualisierung des Verweises auf Batterietests (Abschnitt 2.7)

Juli 2021. Zwischenrevision. Aktualisierung und Präzisierung folgender Punkte:

A. ICS-Sicherheit

i. Zugangsverwaltung
ii. Konfigurationsmanagement
iii. Patch-Management
iv. Sicherheitsvorkehrungen für Netzwerke

B. ICS-Betrieb

i. Notfallverfahren

C. Empfehlung zur Bauweise und zum Brandschutz

Juli 2020. Zwischenrevision. Aktualisierung der Angaben zur Verfügbarkeitsplanung und zu Ersatzteilen

Oktober 2019. Erstveröffentlichung dieses Dokumentes