Bundesamt
für Sicherheit in der
Informationstechnik

ICS-Security-Kompendium

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-5599
E-Mail: ics-sec@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Zum Messen, Steuern und Regeln von Abläufen, beispielsweise zur Automation von Prozessen und zur Überwachung von großen Systemen, kommen in vielen Bereichen der Industrie sogenannte Industrial Control Systems (ICS; deutsch: industrielle Steuerungssysteme, Automatisierungssysteme) zum Einsatz. Diese finden häufig Verwendung in der produzierenden Industrie und in Branchen, die zu den kritischen Infrastrukturen (KRITIS) gezählt werden, z. B. Energie, Wasser, Ernährung oder Transport und Verkehr.

1.1 Motivation

ICS waren in der Vergangenheit physisch von anderen IT-Systemen und Netzen entkoppelt (engl. air gap) und damit vor äußeren Einflüssen geschützt. Daher war die IT-Security bei der Auswahl und Entwicklung zumeist proprietärer Software und Protokolle von untergeordneter Bedeutung.

Mit dem Einzug von IT-Systemen aus dem Büroumfeld und der zunehmenden Vernetzung der ICS auch über Netzgrenzen hinweg (z. B. in ein Unternehmensnetz) sind diese Systeme heute ähnlichen Gefährdungen ausgesetzt wie Systeme aus der klassischen Unternehmens-IT. Dass diese Gefährdungen real sind, beweisen verschiedene Vorfälle der jüngeren Vergangenheit.

Je nach Ziel der Angreifer unterscheidet sich die Vorgehensweise der Angreifer etwas. Bei Systemen, die direkt über das Internet erreichbar sind, werden gezielt Angriffe auf das System gestartet. Es werden also direkt Schwachstellen ausgenutzt. Diese können ggf. das Betriebssystem, Serveranwendungen oder Webanwendungen betreffen.

Bei vielen in den letzten Jahren bekannt gewordenen Angriffen dienen Spear-Phishing-Attacken als Einstieg in das Unternehmen. Auf diese Weise wird ein Art „Brückenkopf“ auf einem Rechner in dem Unternehmen errichtet. Von diesem wird das Netzwerk ausgekundschaftet und weitere Systeme infiziert. Haben die Angreifer das eigentliche Zielsystem erreicht, ziehen sie von dort die gesuchten Informationen ab oder nehmen die Manipulation vor. Wenn der Angreifer sein Ziel erreicht hat, wird er zudem versuchen, seine Spuren zu verwischen, um unentdeckt zu bleiben.

Dadurch wird deutlich, das die Sicherheitskonzeption von Systemen zur Prozesssteuerung zu überdenken und ggf. der aktuellen Gefährdungslage anzupassen ist.

In Tabelle 1 sind beispielhaft typische, in jüngerer Vergangenheit bei ICS-Sicherheits-Audits festgestellte Beobachtungen aufgeführt, welche Rückschlüsse auf die aktuelle Gefährdungslage zulassen.

ICS-Komponente	Sicherheitsrelevante Beobachtungen
Netz	• Anbindung unbekannter Systeme zur Datensicherung
Firewall/ Router	• Regeln nicht ausreichend restriktiv • undokumentierte Regeleinträge • offenbar nicht mehr benötigte Datenflüsse • Bypass im Routing • IP-Forwarding auf Servern
Modems	• ungeschützter Zugang • Anschluss nicht dokumentiert • ständige Verbindung (always-on)
Fernwartung	• Anschluss direkt in Feldebene

ICS-Komponente	Sicherheitsrelevante Beobachtungen
Betriebssysteme/ Härtung	• Betriebssystemkomponenten nicht gehärtet • nicht benötigte Dienste angeboten • Nicht-unterstütze neue Betriebssystem- Version und fehlende Patches
Funkverbindungen	• fehlende Verschlüsselung • veraltete Netzelemente
Industrie-Switche	• fehlende Robustheit gegen unerwartete bzw. nicht-standardkonforme Kommunikation • Backdoors (z. B. hardcodierte Passwörter)
veraltete Netzelemente	• Administrativer, webbasierter Zugang ohne Absicherung (z. B. SSL) Fehlende Protokollunterstützung (z. B. nur 'telnet'-Zugang)

Tabelle 1 Festgestellte Auditergebnisse zur aktuellen Gefährdungslage

Entgegen der klassischen IT haben ICS abweichende Anforderungen an die Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit. Dies äußert sich beispielsweise in längeren Betriebszeiten und seltenen Wartungsfenstern. Zudem sind insbesondere die Echtzeitanforderungen zu nennen, die für die Steuerung häufig unerlässlich sind. Hinzu kommen Gewährleistungsansprüche. Etablierte Schutzmaßnahmen aus dem Büroumfeld sind dabei nur bedingt auf ICS übertragbar.

1.2 Ziele

Vor diesem Hintergrund hat das ICS-Security-Kompendium folgende Ziele:

- Das Kompendium stellt ein Grundlagenwerk für die IT-Security in ICS dar. Es ermöglicht sowohl IT-Security- als auch ICS-Experten den einfachen Zugang zur IT-Security in ICS, und erläutert die zur Erfassung dieses Themas notwendigen Grundlagen der IT-Security, der ICS-Abläufe und der relevanten Normen und Standards.
- Es wurde ein konkreter Zusammenhang zum IT-Grundschutz erarbeitet. Nachdem auf Basis vorhandener Standards und Normen architektonische, technische und organisatorische Sicherheitsmaßnahmen für ICS entwickelt wurden, wird insbesondere aufgezeigt, welche Erweiterungen nötig sind, um IT-Grundschutz im Bereich der ICS-Security anwenden zu können und welche Betrachtungen zusätzlich notwendig sind, wenn IT-Grundschutz auf ICS-Infrastruktur angewendet wird. Hierbei werden auch die Unterschiede und Lücken etablierter ICS-Standards und insbesondere des IT-Grundschutzes im Bereich ICS-Security aufgezeigt.
- Es werden veröffentlichte Standards und Best-Practices für die IT-Security von ICS vorgestellt, sowie eine Sammlung der wichtigsten Maßnahmen zusammengestellt.
- Eine konkrete praktikable Methodik zur Auditierung von ICS wird beschrieben.
- Letztlich gibt das Kompendium Hinweise zum aktuellen Handlungsbedarf und zu zukünftigen Themen für Forschung und Entwicklung im Bereich ICS.

Das ICS-Security-Kompendium bildet einen allgemeinen Rahmen für die verschiedenen Anwendungsbereiche industrieller Steuerungssysteme. Ein solches Grundlagenwerk kann natürlich nicht auf alle Spezifika der unterschiedlichen Industriesektoren detailliert eingehen. Daher ist das Kompendium als Aufforderung an die jeweiligen Verbände und Organisationen zu verstehen, auf dieser Grundlage eigene,

sektorenspezifische Ausprägungen oder Präzisierungen des Kompendiums zu erstellen und dabei die jeweils geltenden Besonderheiten im Detail zu erläutern. Nur so ist es möglich, die industriespezifischen Grundlagen passgenau für bestimmte Anwendungsbereiche darzustellen.

Die Durchführung einer wiederkehrenden (regelmäßigen bzw. anlassbezogenen) Risikoanalyse wird dabei als verpflichtend angesehen. Im Rahmen der Risikoanalyse sind dann insbesondere die in Kapitel 3 dargestellten Gefährdungen zu untersuchen und zu bewerten. Anschließend liegt es in der Verantwortung des Anlagenbetreibers, geeignete Sicherheitsmaßnahmen abzuleiten, welche die durch die identifizierten Gefährdungen gegebenen Risiken auf ein akzeptables Restrisiko reduzieren. Eine Hilfestellung können dabei die in Kapitel 5 dargestellten Best Practices liefern.

Dabei gilt es zusätzlich, die Umsetzbarkeit mit Blick auf die jeweiligen Rahmenbedingungen zu bewerten und ggf. alternative Sicherheitsmaßnahmen zu definieren. Beispielsweise können Anforderungen aus dem Bereich Safety die konkreten Umsetzungsmöglichkeiten einer Sicherheitsmaßnahme beschränken. Gerade hier sind die jeweiligen Verbände und Organisationen geeignet, um eine mögliche Umsetzung der Best-Practices aufzuzeigen. Daher sollten diese sektorspezifischen Ausprägungen insbesondere die Kapitel „Grundlagen von ICS“ und „Best-Practice Guide für Betreiber“ adressieren. Natürlich können auch weitere Inhalte wie beispielsweise die Darstellung der relevanten Schwachstellen oder der geltenden Normen und Standards speziell für den jeweiligen Sektor präzisiert werden. Hierdurch ergibt sich das Potenzial, branchenweite Empfehlungen oder Richtlinien zu erarbeiten, die den jeweils geltenden Anforderungen gerecht werden.

1.3 Adressatenkreis

Das Kompendium richtet sich primär an Betreiber und macht auf das Thema IT-Security aufmerksam. Die Implementierung von IT-Security in Form der erarbeiteten Best Practices führt zu einer Risikominderung in ICS.

Systemintegratoren und Hersteller von ICS-Komponenten sollten die Maßnahmen kennen und bei der Entwicklung und Planung neuer Komponenten und Anlagen berücksichtigen.

Eine weitere Zielgruppe sind Unternehmen, welche die IT-Security von Automatisierungssystemen prüfen und bewerten. Zudem dient es als Anregung für alle Personen, die sich in irgendeiner Weise mit der IT-Security von Automatisierungssystemen beschäftigen.

Hersteller und Integratoren werden in der Fortschreibung des Kompendiums stärker adressiert werden (vgl. Kapitel 8).

1.4 Inhalte

Kapitel 2 gibt eine Einführung in die Grundlagen von ICS. Es richtet sich an IT-Security-Experten (aus der klassischen Unternehmens-IT), die bisher nicht oder nur wenig mit ICS in Berührung gekommen sind.

In Kapitel 3 werden die Security-spezifischen Grundlagen von ICS erläutert. Diese bieten einen Zugang zum Thema IT-Security. Neben der allgemeinen Einführung in Schwachstellen und Angriffsvektoren erfolgt eine Erläuterung der Besonderheiten von ICS, die an ICS-Anwender und IT-Security-Experten gleichermaßen gerichtet ist.

Kapitel 4 gibt einen Überblick über nationale und internationale Organisationen und deren Standards und Quasi-Standards im Bereich der ICS-Security. Es soll alle Leser dabei unterstützen, die vorhandenen Veröffentlichungen einzuordnen.

Kapitel 5 definiert architektonische, technische und organisatorische Maßnahmen zum Schutz von ICS. Zudem erfolgt eine Gegenüberstellung der Best Practices zu etablierten Standards. Die Best-Practices adressieren in erster Linie Betreiber von ICS.

Aufbauend auf den zuvor beschriebenen Maßnahmen wird in Kapitel 6 eine Methodik für die Durchführung von Audits in ICS beschrieben.

In Kapitel 7 werden aktuelle Trends aus dem ICS-Umfeld betrachtet. Aus diesen Trends sind mögliche Projekte und notwendige Forschungsaktivitäten abgeleitet.

Kapitel 8 fasst die Ergebnisse der Studie zusammen und gibt einen Ausblick auf zukünftige Fortschreibungen.

Das Thema Industrie 4.0 wird in diesem Dokument nur am Rande betrachtet. Industrie 4.0 ist ein wichtiges Zukunftsprojekt der Bundesregierung und ein Innovationstreiber für die deutsche Industrie. Das vorliegende ICS-Security-Kompendium zielt jedoch in erster Linie darauf ab, die Sicherheit heutiger Anlagen zu verbessern. Bei heutigen Industrieanlagen handelt es sich allerdings nicht um Industrie 4.0 – lediglich in modernsten Anlagen sind Ansätze von Industrie 4.0 bereits umgesetzt. Insgesamt besteht allerdings der größte Handlungsbedarf bei Bestandsanlagen („Industrie 3.0“). Für Industrie 4.0 ist es aufgrund der fortschreitenden Forschung und Entwicklung noch nicht möglich, allgemein anwendbare Best-Practices zu definieren. Jedoch können und sollten die hier dargestellten Grundlagen auch bei der Umsetzung des Paradigmas Industrie 4.0 berücksichtigt und in geeigneter Weise ergänzt werden.

1.5 Safety & Security

Zu Beginn des Dokuments soll noch eine Abgrenzung zwischen den Begriffen Safety und Security erfolgen. Safety steht dabei für die funktionale Sicherheit der Maschine oder Anlage und adressiert damit den Schutz der Umgebung vor anormalen Betrieb. Security beschreibt den Schutz von IT-Systemen gegen absichtliche herbeigeführte oder ungewollte Fehler. Saftey-Systeme müssen ebenfalls gegen Angriffe geschützt werden.

2 Grundlagen von ICS

Dieses Kapitel gibt eine Einführung in die Grundlagen der ICS. Nach der Erläuterung der Anwendungsgebiete der ICS erfolgt eine Beschreibung einer typischen ICS-Architektur. Die auf dieser Architektur aufsetzende Nutzung von ICS-Komponenten sowie, die in ICS genutzten Kommunikationstechniken werden umrissen. Grundlage der Beschreibungen bildet dabei die herstellerunabhängige gängige Praxis aus Anwendersicht. Mit Rücksicht auf die Vielzahl unterschiedlicher Anwendungen von ICS erfolgt hier eine Betrachtung mit Fokus auf die IT-Security, weshalb die anwendungsspezifischen Details nur generisch angesprochen werden.

2.1 Begriffsbestimmung

Die Begriffe für Komponenten und Funktionen im Bereich der Automatisierungstechnik werden, im Bereich der internationalen Normung umfassend definiert (s. z. B. IEC 60050). Mit Rücksicht auf die in unterschiedlichen Branchen gebräuchliche Nomenklatur, wird im Folgenden eine Gegenüberstellung für die gängigen Begriffe geliefert.

- ICS (Industrial Control System)

  ICS ist ein Oberbegriff für Automatisierungslösungen zur Steuerung technischer Prozesse

- DCS (Distributed Control System), PLS (Prozessleitsystem)

  PLS werden meist für größere verfahrenstechnische Anlagen eingesetzt und bestehen üblicherweise aus einem Paket, das folgende Mechanismen beinhaltet:

  PNK zur Steuerung von Aktoren und Aufnahme der Messwerte, Alarmsystem, Anlagenvisualisierung, Kurvenaufzeichnung von analogen Messwerten, Benutzerverwaltung, Möglichkeiten des Engineering sowie eine zentrale Datenhaltung.

- SCADA (Supervisory Control and Data Acquisition)

  SCADA beschreibt das Steuern und überwachen technischer Prozesse mittels eines Computersystems. Dabei bezieht sich der Terminus gewöhnlich auf Systeme mit dezentraler Datenbasis (im Gegensatz zu PLS). Bei SCADA Lösungen werden die automatisierten Funktionen in RTU oder PLC abgebildet, während das Computer System für Bedienung, Archivierung und Auswertung des Prozessgeschehens verwendet wird.

- PLC (Programmable Logic Controller), SPS (Speicherprogrammierbare Steuerung), PNK (Prozessnahe Komponente); MTU (Main Terminal Unit), Controller

  Ein PLC ist ein Gerät, das zur Steuerung oder Regelung einer Maschine oder Anlage eingesetzt und auf digitaler Basis programmiert wird.

- Sensor, Messwertaufnehmer, Endschalter, Taster/Schalter, Initiator, Grenztaster

  Dies sind Komponenten zur Erfassung physikalischer Größen und deren Wandlung in ein Einheitssignal (4-20 mA, 24V, etc.). Die dabei eingesetzten Kommunikationsprotokolle werden als Feldbusse bezeichnet.

- Aktuator, Aktor

  Ein Aktor wandelt eine Steuergröße (elektrisches oder pneumatisches Signal) in die Stellgröße zum Beeinflussen des Prozessgeschehens um.

- Analytik, PAT (Process Analytical Technology)

  PAT dient der Optimierung, der Analyse und Kontrolle von Herstellungsprozessen in der chemischen Industrie.

- HMI (Human Machine Interface); BUB (Beobachtung- und Bedienkomponenten), ABK (Anzeige- und Bedienkomponente)

  Diese Komponenten dienen der Verwirklichung von Anzeige- und Bedienfunktionen. Funktional können sie typischerweise Standard-Bedienbilder, freie Grafiken, Rezepterstellungs- und Beobachtungswerkzeuge, Alarmbehandlung, Datenarchivierung und Auswertung, Systemdiagnosen, Systemdokumentation (technische Systeme und Produktionsprozess) und interaktive Betriebsunterstützung beinhalten.

- EWS (Engineering Workstation), ES (Engineering Station), Programmiergerät, Service Rechner

  Diese Komponenten ermöglichen die Konfiguration der ICS Komponenten.

- RTU (Remote Terminal Unit), RIO (Remote I/O)

- Automatisierungstechnische Komponente zur Erfassung und ggf. Verarbeitung von Prozessinformationen und Übertragung der Informationen an eine zentrale Verarbeitungseinheit.

- ABPNK

  Hierbei handelt es sich um Komponenten, bei denen die Funktionen von Anzeige- und Prozesssteuerungsfunktionen in einem Gerät vereinigt werden. Beispielhaft seinen in diesem Zusammenhang Panel PCs genannte, welche mit RTU verbunden werden und auf denen eine Automatisierungsfunktion betrieben wird (z.B. SoftPLC).

- SIL

  Beim Safety Integrity Level (gem. IEC 61508) handelt es sich um gestufte (4 Stufen), spezifische Qualitätsanforderungen an automatisierte Funktionen und deren funktionale Einbindung in den materiellen Produktionsprozess.

- GxP

  GxP bezeichnet zusammenfassend alle Richtlinien für „gute Arbeitspraxis“, welche insbesondere in der Medizin, der Pharmazie und der pharmazeutischen Chemie Bedeutung haben. Das "G" steht für "Gut(e)" und das "P" für "Praxis", das "x" in der Mitte wird durch die jeweilige Abkürzung für den spezifischen Anwendungsbereich ersetzt. Bezüglich ICS sind dabei insbesondere M (Manufacturing), AM (Automation), D (Dokumentation) und E (Engineering) von Bedeutung.

- Konfigurieren

  Unter Konfigurieren versteht man die Festlegung der anwendungsspezifischen Funktion eines ICS, wobei keine Programmierung im eigentlichen Sinne des Wortes vorgenommen wird, sondern die gewünschte Funktion unter Zuhilfenahme von vom Gerätehersteller „vorgefertigt“ zur Verfügung gestellter Module erfolgt. Diese werden typischerweise in sog. Bibliotheken (häufig auch Toolbox genannt) von den Systemherstellern angeboten.

- CIF (Control in the Field)

  Hierbei handelt es sich um eine Automatisierungsstrategie, bei der Automatisierungsfunktionen (z. B. Regler) in Feldgeräte (z. B. Stellungsregler von Regelventilen) implementiert werden. Die notwendigen Istwerte werden dabei direkt, vom jeweiligen Messwertaufnehmer per Feldbus, an den Regler geleitet.

2.2 Grundcharakteristika

ICS werden überall dort eingesetzt, wo Abläufe automatisiert werden. Sie werden für das Messen, Steuern, Regeln und Bedienen von industriellen Abläufen benutzt.

Beispiele hierfür sind die Verfahrens- und Prozesstechnik, die Fertigungsautomatisierung, die Ver- und Entsorgungsnetze (z. B. Strom, Wasser, Gas, Fernwärme), die Betriebstechnik (z. B. Schienen- und Straßenverkehr) und die Gebäudeautomation. Die individuellen Anforderungen an ICS werden unmittelbar durch die betrieblichen Anforderungen der materiellen Produktionsprozesse bestimmt. ICS werden in der Regel vertikal und horizontal integriert.

2.2.1 Vertikale Integration

Innerhalb der Wertschöpfungskette eines Betriebes gibt es zwischen dem Produktionsauftrag und der materiellen Produktion einen Geschäftsprozess, in dessen Rahmen

- Produktionsführung (in welchem Betrieb wird ein Produktionsauftrag abgewickelt),
- Betriebsführung (sind die für die Abwicklung eines Produktionsauftrages notwendigen Ressourcen verfügbar) und
- Prozessführung (befinden sich die technischen Parameter des Produktionsprozesses im richtigen Bereich)

bearbeitet werden. Nach Abschluss eines Produktionsauftrages wird ein entsprechender Produktionsbericht erstellt und archiviert. Die Details dieses Geschäftsprozesses können sich aufgrund individueller Anforderungen (z. B. im Bereich der pharmazeutischen Produktion) stark unterscheiden.

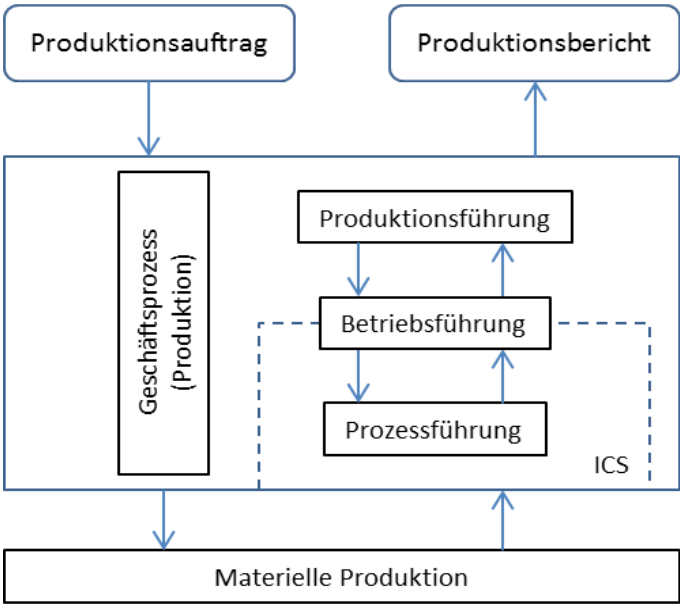


Abbildung 1: Vertikale Integration von Produktionsanlagen

2.2.2 Horizontale Integration

Typischerweise anzutreffende Produktionsprozesse beinhalten mehrstufig gegliederte Produktionsschritte. In vielen dieser Produktionsschritte sind ICS anzutreffen. Mit Rücksicht auf eine effiziente Produktion und die Einhaltung der qualitätsrelevanten Vorschriften ist zwischen den Produktionseinrichtungen (Anlagen, Lager usw.) ein Informationsaustausch erforderlich. Dieser Informationsaustausch kann in unterschiedlicher Weise erfolgen. Im Folgenden wird der Fokus jedoch auf Kommunikation im Sinne eines elektronischen Datenaustauschs gelegt.

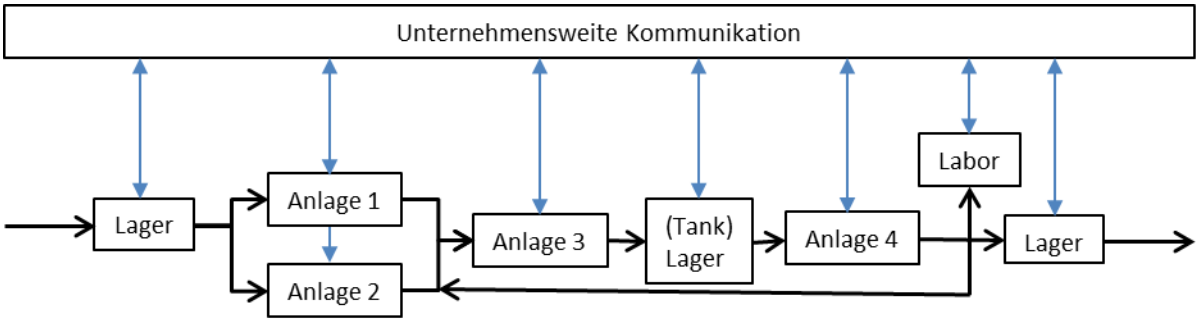


Abbildung 2: Horizontale Integration von Produktionsanlagen

Diese Struktur ist dem unternehmerischen Streben nach Qualität und Effizienz geschuldet. Sie liefert gleichzeitig den Rahmen für die technische Umsetzung des Geschäftsprozesses.

Bedingt durch diese Struktur und die zusätzlich vorhandene „starre" Anbindung an den jeweiligen materiellen Produktionsprozess ergibt sich für ICS eine andere Abfolge der Prioritäten, als die in der Office IT gebräuchliche. Bedingt dadurch können die im Bereich der Office IT gebräuchlichen Strategien nicht ohne Weiteres umgesetzt werden (vgl. Kapitel 2.2.8).

2.2.3 Lebenszyklus

Der Lebenszyklus von ICS wird aus dem der zugehörigen Produktionsanlagen abgeleitet. Dieser ist deutlich länger als die in der Office IT typischerweise anzutreffenden Zeiträume. Die Laufzeit beträgt zehn bis fünfzehn Jahre. Mitunter können es auch 20 Jahre sein. In der Office-IT sind es meist nur drei bis fünf Jahre.

2.2.4 Echtzeitverhalten

Regelkreise werden im Hinblick auf ihr Zeitverhalten optimiert. Kommt es aufgrund von (temporären) Modifikationen im Bereich der Software zu Änderungen am Zeitverhalten des ICS führt dies zu Störungen im materiellen Produktionsprozess. Dies kann dazu führen, dass z. B. mehr Ausschuss anfällt.

2.2.5 Funktionale Sicherheit

Es gibt viele Anwendungen, in welchen der Betrieb der Anlagen an behördliche Auflagen gebunden ist (z. B. Anlagensicherheit). In diesen Fällen bedürfen wesentliche Änderungen, worunter auch Softwareänderungen an den eingesetzten ICS fallen können, einem dedizierten Genehmigungsprozess.

Aufgrund des vorgeschriebenen Prüfprozesses sind hier beispielsweise die Möglichkeiten zum zeitnahen Einspielen von Sicherheitsupdates begrenzt bzw. nicht gegeben.

2.2.6 Physikalische Trennung

Im Bereich des Aufbaus von ICS ist es üblich, neben logischer Trennung einzelner Teilbereiche auch eine physikalische Trennung von Funktionseinheiten – speziell im Bereich der Infrastruktur – umzusetzen.

Beispiel:

Im Bereich der Office-IT ist es üblich, verschiedene logische Netzwerke auf einem Switch zu betreiben. Im Bereich der ICS ist dies, mit Rücksicht auf mögliche ungewollte Querverbindungen und deren potenzielle Auswirkung, ungebräuchlich. Werden unterschiedliche Netzwerksegmente trotzdem zusammengefasst, so ist dies im Rahmen einer Risikobewertung zu betrachten. Die Auswirkungen auf die Systemintegrität und Aspekte wie z. B. die Validierbarkeit eines ICS sind in diesen Fällen zu bewerten und zu dokumentieren.

2.2.7 Software

Im Gegensatz zur Office IT werden ICS über längere Zeiträume mit quasi gleicher Anwendersoftware betrieben. Änderungen finden im Rahmen vorprojektierter Möglichkeiten wie z. B. Änderung von Regler Parametern, Änderung von Grenzwerten, aber auch Erstellung von Rezepten statt.

2.2.8 Updates

Im Bereich der Office IT werden Systeme nach Bekanntwerden von Fehlern oder Schwachstellen schnellstmöglich (durch die Installation von Patches) nachgebessert.

Im Anwendungsbereich von ICS sind bei Softwareänderungen, auch während des Änderungsprozesses, neben den Funktionen die vorgegebenen Reaktionszeiten einzuhalten. Darüber hinaus sind grundsätzlich Prüfungen der Gesamtanordnung bestehend aus ICS und materiellem Produktionsprozess erforderlich. Die jeweilige Prüftiefe richtet sich nach der jeweiligen Applikation. So sind anwendungsspezifische (z. B. im Bereich der Pharmaproduktion) Prüfungen durchzuführen und zu dokumentieren, deren Abarbeitung eine Produktionsunterbrechung erzwingen. Updates können daher in der Regel nur im Rahmen von Wartungsaktivitäten in größeren Abständen eingebracht werden.

2.2.9 Hardware

Im Gegensatz zur Office IT werden ICS über längere Zeiträume mit gleicher Hardware (Gerätetypen) betrieben.

2.2.10 Normen

Im Bereich der ICS gibt es eine Vielzahl von Normen, welche stringente Anforderungen an ICS beinhalten (z. B. IEC 61508-3 im Bereich der Softwareentwicklung).

2.3 Hierarchische Gliederung von ICS

Eine typischerweise durch den Geschäftsprozess vorgegebene Hierarchie eines ICS gestaltet sich wie folgt:

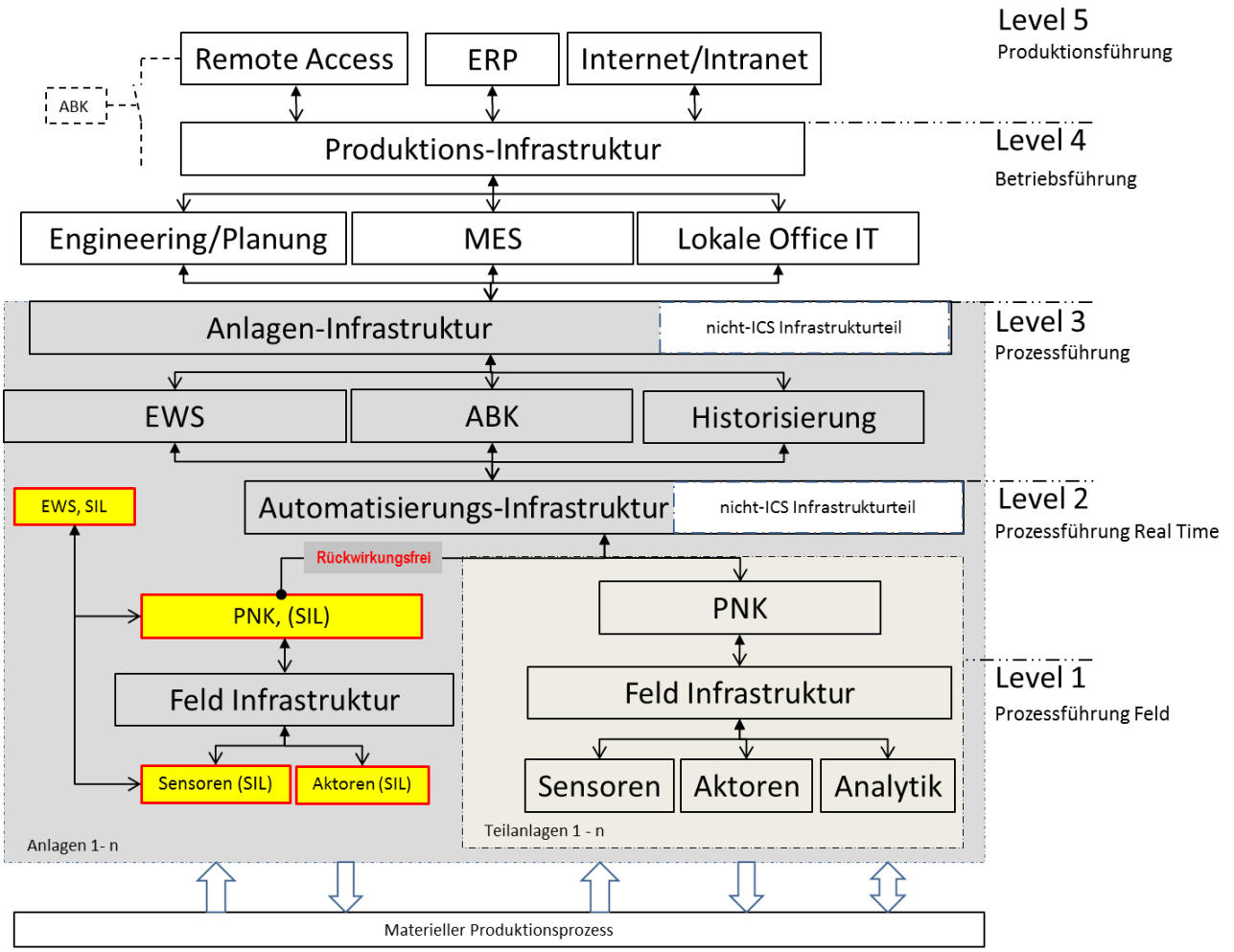


Abbildung 3: Hierarchische Gliederung eines ICS

2.3.1 Level 1: Prozessführung, Feld

In diesem Level befinden sich die Komponenten, welche zur Gewinnung von Informationen aus dem Bereich der materiellen Produktion erforderlich sind, bzw. die Einfluss auf das Geschehen im Bereich der materiellen Produktion nehmen (Endschalter, Messwertaufnehmer, Analysegeräte, Ventile, Stellglieder, Motoren usw.). Diese Komponenten interagieren einerseits direkt mit dem materiellen Produktionsprozess und andererseits, unter Zuhilfenahme ihrer zugehörigen Infrastruktur, mit den zugehörigen informationsverarbeitenden Einheiten oder ggf. auch untereinander (z. B. bei Umsetzung von CIF-Strategien). Die zugehörige Infrastruktur kann je nach Anwendung und eingesetzter Technologie verschiedene Komponenten enthalten. Beispielhaft seien an dieser Stelle genannt:

- Remote I/O (ggf. mit Signalvorverarbeitung, dann spricht man von RTU),
- Interface-Bausteine zur Signalkonditionierung,
- Switches bei Verwendung von Feldbus Lösungen.

Die Prozessdatensignalübertragungen im Level 1 erfolgen in Echtzeit. Eine Störung der Signalübertragung führt, sofern keine physikalische (z. B. 2 von 3 Verschaltung bei Messwertaufnehmern) oder logische (z. B. Ersatzwertaufschaltung bei Messwertstörung) Redundanz vorhanden ist, zu einer unmittelbaren Störung im materiellen Produktionsprozess.

Bei der Verwendung von Feldbussen oder HART fähigen Geräten besteht zusätzlich die Möglichkeit, Diagnose- und Konfigurationsdaten zu übermitteln.

2.3.2 Level 2: Prozessführung, Realtime

In diesem Level befinden sich die Komponenten, welche zur Signalverarbeitung im Sinne der Darstellung der automatisierten Funktionen erforderlich sind (z. B. Endlage erreicht: Antriebsmotor AUS oder Füllstand HOCH: Pumpe AUS). Diese Komponenten werden typischerweise in Abhängigkeit der zu automatisierenden Teilanlagenkonfiguration ausgelegt. In Abhängigkeit vom eingesetzten Automatisierungsprodukt und der Größe der zu automatisierenden (Teil-) Anlage werden einzelne Geräte oder Netzwerke mit Gruppen von Automatisierungs-Produkten eingesetzt.

Die technische Ausgestaltung ist darüber hinaus im Detail sehr stark von der gewählten konzeptionellen Lösung abhängig.

Prinzipiell sind drei Varianten anzutreffen:

1. Die Informationen aus der Feldebene werden ohne Vorverarbeitung eingelesen und verarbeitet; Stellbefehle werden direkt an die Aktoren übermittelt. So erfolgt z. B. die Überwachung der Stellungsrückmeldungen eines Ventils hinsichtlich:
   - des statischen Zustands wie AUF/ZU dürfen nicht gleichzeitig anstehen und
   - des logischen Ablaufs wie innerhalb 1 Sekunde nach Absteuerung muss die Rückmeldung ZU anstehen.
2. Es erfolgt im Feld eine Signalvorverarbeitung (z. B. die Laufzeitüberwachung eines Ventils) innerhalb einer RTU, die Level 2 Komponenten erhält lediglich die resultierenden Informationen wie z. B. das Ventil ist auf und hat eine Laufzeitstörung.
3. Automatisierungsfunktionen, wie z. B. Regelungen werden in Feldgeräten wie z. B. Stellungsreglern an Regelventilen (Positioner) implementiert. Die zugehörigen Ist-Werte werden von den entsprechenden Messwertaufnehmern direkt (z. B. per Feldbus) an die Positioner gesendet (CIF).

Die Verarbeitung dieser Informationen erfolgt deterministisch, d. h. für eine ordnungsgemäße Gesamtfunktion muss eine vordefinierte Reaktionszeit sichergestellt werden. Ein nicht Einhalten dieser Anforderung führt zu einer unmittelbaren Störung im materiellen Produktionsprozess.

Eine Sonderstellung im Bereich der Level 1 und Level 2 Anwendungen nehmen die Systeme zur Reduzierung des Betriebsrisikos ein, sofern an diese besondere Zuverlässigkeitsanforderungen gestellt werden (z. B. SIL). In Abhängigkeit von der branchenspezifischen Anwendung werden an diese Systeme Zusatzanforderungen bis hin zur physikalischen Abtrennung der Systeme (vgl. IEC/EN 61511-1 Abs. 9.5.1) gestellt.

Eine besondere Betrachtung ist außerdem für Komponenten erforderlich, bei deren Betrieb spezifische Qualitätsanforderungen zur erfüllen sind, wie beispielsweise GMP (Good Manufacturing Practice) oder GAMP (Good Automation Practice) Anforderungen. In diesen Fällen sind ggf. spezifische Risikoanalysen auszuführen und zu dokumentieren.

2.3.3 Level 3: Einrichtungen zur Prozessführung

Im Level 3 sind die Einrichtungen angesiedelt, die für die Prozessführung notwendig sind, die jedoch keine Daten in Echtzeit verarbeiten. Beispielhaft sind in diesem Zusammenhang zu nennen:

- HMI/BUB,
- produktbezogene Engineering- und Wartungsstationen
- Messwert- und Prozessdatenarchivserver usw.

Diese Komponenten sind für die Prozessführung wichtig, ihr Verhalten ist jedoch sowohl hinsichtlich des Zeitverhaltens als häufig auch bezüglich ihrer Verfügbarkeit weniger kritisch als das der Level 1 und 2 Komponenten. Dies begründet sich zum einen dadurch, dass z. B. im Bereich der Bedienstationen häufig inhärente Redundanzen verfügbar sind, da z. B. mehrere Bedienstationen vorhanden sind, sodass der Ausfall einer Bedienstation zu einem Komfortverlust, nicht jedoch zu einer unmittelbaren Störung im materiellen Produktionsprozess führt. Gleiches gilt für Archivserver, bei denen ein kurzer Ausfall von den meisten Automatisierungssystemen toleriert wird, da Prozessdaten in den Realtime-Komponenten so lange gespeichert werden, bis sie archiviert wurden.

Ungeachtet dieser Umstände werden Level 3 Komponenten bzgl. Softwareupdates restriktiv behandelt, da sowohl die Interaktion zwischen den Level 3 Komponenten und den Level 1 und 2 Komponenten als auch die Interaktion der Level 3 Komponenten untereinander für eine ordnungsgemäße Führung des materiellen Produktionsprozesses zwingend erforderlich ist und ein potenzieller Fehler auf Ebene der eingesetzten Software alle Level 3 Komponenten gleichzeitig betreffen kann.

2.3.4 Level 4: Betriebsführung

Die im Level 4 angesiedelten Komponenten übernehmen die Funktionen der Betriebsführung. Diese lassen sich typisch in folgende Kategorien gliedern:

1. Manufacturing Execution System (MES)

   Die MES bilden in der Betriebsführung den Datentransfer zwischen Automatisierungstechnik einerseits und betriebswirtschaftlicher Datenverarbeitung andererseits ab. Dieser Datentransfer beinhaltet neben den eigentlichen Kommunikationsvorgängen auch eine Datenaggregierung. Diese ist notwendig, da die Einrichtungen in Level 3 die Prozessdaten in Sekundenintervallen verarbeiten, während im Level 4 eine Datenverarbeitung in wesentlich größeren Zeitintervallen erfolgt (z. B. tageweise).

2. Engineering/Planung

   Im Level 4 sind systemunabhängige Engineering- und Planungswerkzeuge angesiedelt, die notwendig sind, um technische Dokumentation zu erstellen und zu pflegen (Schaltpläne, Bauzeichnungen, Prozessbeschreibungen usw.).

3. Lokale Office IT

   Im Level 4 ist darüber hinaus die produktionsnahe Office IT angesiedelt, welche einerseits vom Betriebspersonal für nicht produktionsbezogene Aktivitäten benutzt wird (Email, Dokumente verfassen, außerordentlich Analysen etc.) andererseits haben diese Komponenten häufig lesenden Zugriff auf Level 3 Komponenten um z. B. Prozessdaten aus dem Archivserver zu extrahieren, um diese speziellen Analysen zuzuführen oder um Anlagenbedienbilder auf Arbeitsplatzrechnern darzustellen.

2.3.5 Level 5: Produktionsführung

Im Level 5 sind die Softwarelösungen angesiedelt, mit deren Hilfe die umfassende unternehmensweite Betriebsorganisation unterstützt wird.

Typischerweise werden im Level 5 folgende Funktionen angesiedelt:

- ERP Anbindung

Über diesen Weg werden Produktionsaufträge und Produktionsberichte übermittelt. Darüber hinaus wird er häufig auch für die Übermittlung performancerelevanter Vergleichsdaten genutzt. Im Normalfall kommuniziert das ERP mit dem MES (Level 4).

- Internet/Intranet Zugang

  Aus Sicht des ICS stellen Internet und Intranet eine gleichrangige, nicht vertrauenswürdige Umgebung dar. Für die Bearbeitung der Aufgaben im Level 4 ist eine derartige Anbindung meist jedoch erforderlich.

- Remote Access Einrichtungen

  Zu Wartungszwecken werden häufig spezifische Zugänge verwendet. Diese benutzen technologisch in der Regel das Internet (wobei auch Telefonverbindungen wie Internetverbindungen anzusehen sind). Diese Verbindungen unterscheiden sich von den vorgenannten Verbindungen dadurch, dass sie normalerweise nicht permanent benötigt werden.

2.3.6 Ausnahmen

Ungeachtet der hier beschriebenen hierarchischen Struktur gibt es Anwendungen, in denen die hier postulierte Hierarchie nicht umgesetzt werden kann.

Beispielhaft seinen genannt

- ABPNK

  Bei ABPNK handelt es sich um Geräte, welche Signalverarbeitung, Beobachtung und Bedienung und Anschaltung des materiellen Produktionsprozesses in einem Gerät vereinigen. Projiziert man diese Funktion auf das hier beschriebene hierarchische Modell, sind diese Geräte somit in den Levels 1 bis 3 angesiedelt. In der Praxis werden diese Geräte, sofern sie z. B. Package Units steuern, üblicherweise auf Level 2 in das ICS eingebunden. Steuern sie hingegen autonome Systeme z. B. im Bereich kleinerer Anwendungen, werden diese Systeme als eigenständige ICS betrieben.

- Spezifische Qualitätsmessungen

  In verschiedenen Anwendungen werden Sensoren, welche qualitätsrelevante Daten aufzeichnen, unter Umgehung des Levels 2 direkt an registrierende Systeme, welche auf Level 3 angesiedelt sind, angeschaltet. Da in diesen Fällen spezifische Anforderungen zu erfüllen sind, werden für diese Anwendungen meist logisch und physikalisch separierte Netzwerke aufgebaut.

2.4 Prozessleitsystem vs. SCADA

Die Verwirklichung der hier vorgestellten Automatisierungsfunktionen kann prinzipiell sowohl mit PLS als auch mit sog. SCADA Lösungen verwirklicht werden.

PLS und DCS sind dadurch gekennzeichnet, dass sie über eine zentrale Datenhaltung für alle Parameter verfügen. Alle Komponenten eines Prozessleitsystems greifen auf diese Daten zu. Die für den Betrieb des Prozessleitsystems notwendigen Kommunikationsvorgänge werden automatisch nach Maßgabe der individuellen Konfiguration etabliert, ohne dass der Anwender sich darum kümmern muss. Das Engineering für Prozessleitsysteme erfolgt von zentraler Stelle unter Verwendung eines integrierten Engineering-Werkzeuges.

SCADA Lösungen sind heterogen aufgebaut. Sie bestehen aus unterschiedlichen Komponenten, zwischen denen es üblicherweise keine vorkonfigurierten Kommunikationskanäle gibt. Alle für die Verwirklichung einer Automatisierungsaufgabe notwendigen Kommunikationsvorgänge müssen individuell geplant und konfiguriert werden. Für das Engineering der einzelnen Komponenten sind u. U. verschiedene Engineering Werkzeuge erforderlich.

Aus Sicht des Anlagenbetreibers können mit beiden Lösungen gleichwertige Applikationen realisiert werden. Die für die Erstellung einer bestimmten Lösung notwenigen Arbeiten unterscheiden sich jedoch drastisch. Dies lässt sich an folgendem Beispiel verdeutlichen:

In einem System soll aus einem bestehenden Analogeingang ein zusätzlicher Alarm generiert werden.

Arbeiten in einem SCADA System	Arbeiten in einem PLS
• Öffnen des Konfiguration Tools der Quell SPS (der SPS die den Analogwert verarbeitet) • Einfügen und Konfigurieren eines Alarmbausteins • Test des Alarmbausteins • Definition einer Kommunikationsvariablen für den Alarm • Zuordnung der Kommunikationsvariablen zu einem Kommunikationsvorgang • Neuladen der SPS Applikation • Öffnen des Konfigurationstools der SCADA Lösung • Definition einer Kommunikationsvariablen • Zuordnung der Kommunikationsvariablen zu einem Kommunikationsvorgang • Festlegen des Meldetextes • Test der Datenübertragung	• Öffnen des zentralen Engineering Tools • Aufruf der Messstelle • Einschalten der Alarmfunktion • Nachführen der Dokumentation

Tabelle 2: Vergleich SCADA-System und PLS

Diesem Vorteil bzgl. des Bedienungskomforts steht ein bei gleichem Anlagenumfang u. U. deutlich höherer Einstandspreis des PLS gegenüber.

2.5 Kommunikationsvorgänge

Die für den Betrieb von ICS erforderlichen Kommunikationsvorgänge können mit vielen verschiedenen, im Ergebnis vergleichbaren, technologischen Lösungen realisiert werden. Darüber hinaus ist dieses Feld einem intensiven Entwicklungsprozess unterworfen. Aus diesem Grund werden im Folgenden wesentliche technische Anforderungen und keine individuellen Lösungen betrachtet.

Basis der Betrachtung ist die Systemdarstellung gem. Abbildung 3. Als Unterscheidungskriterium wird der Level, auf dem ein Kommunikationsvorgang stattfindet, verwendet. Zunächst werden Kommunikationsvorgänge innerhalb des individuellen Levels betrachtet.

2.5.1 Kommunikationsvorgänge in Level 1

Grundsätzlich besteht für die Kommunikation auf Level 1 die Notwendigkeit, Prozessdaten unter Einhaltung deterministischer Bedingungen zu übertragen. Zusätzlich müssen im Anforderungsfall Diagnose- und Konfigurationsdaten übermittelt werden. Darüber hinaus sind abhängig von spezifischen Anforderungen (z. B. SIL) Verfälschungssicherungen und (z. B. Fernwirktechnik) Verschlüsselungen notwendig. Grundsätzlich stehen drei verschiedene Varianten zur Verfügung:

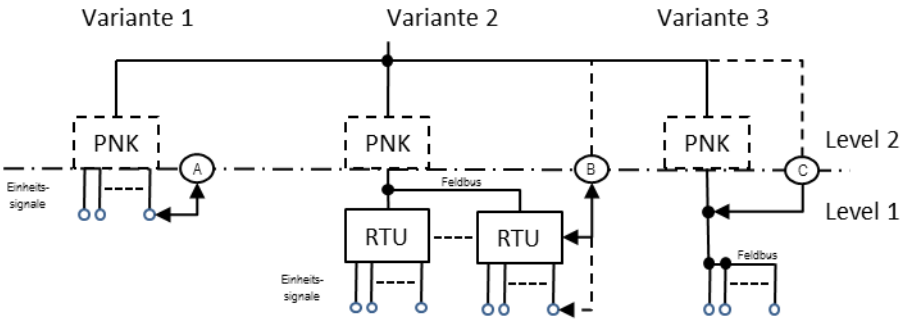


Abbildung 4: Anschaltung von Feldsignalen

- Variante 1
  - Die Feldgeräte werden unter Verwendung von Einheitssignalen im Rahmen einer Punkt-zu- Punkt Verdrahtung mit den PNK verbunden.
  - Wartungsgeräte werden typisch gem. A angeschlossen.
- Variante 2
  - Die Feldgeräte werden unter Verwendung von Einheitssignalen mit den RTU verbunden, diese kommunizieren mittels Feldbus mit den zugehörigen PNK.
  - Wartungsgeräte werden typisch gem. B angeschlossen, wobei der Anschluss der Feldgeräte möglicherweise an der RTU (z. B. bei EX Anwendungen) erfolgt.
  - Besondere Beachtung erfordern Lösungen, bei denen der Wartungsanschluss zu Kommunikationsverbindungen zwischen Level 2 und Level 1 führt (z. B. HART Multiplexer).
- Variante 3
  - Die Feldgeräte werden mittels Feldbus mit den PNK verbunden.
  - Wartungsgeräte werden typisch gem. C angeschlossen, wobei der Anschluss möglicherweise an der PNK (z.B. bei EX Anwendungen) erfolgt.
  - Besondere Beachtung erfordern Lösungen, bei denen der Wartungsanschluss zu Kommunikationsverbindungen zwischen Level 2 und Level 1 führt (z. B. Feldbusüberwachungssysteme).

Im Bereich der Feldbusse existiert eine Vielzahl unterschiedlicher Produkte. Gemäß IEC 61158 stehen folgende Feldbus Systeme zur Verfügung:

- FOUNDATION Fieldbus,
- CIP (Common Industrial Protocol),
- PROFIBUS und PROFINET,
- P-NET,
- WorldFIP,
- INTERBUS,
- SwiftNet,
- CC-Link,
- HART[1],

1 Bei dem HART Protokoll handelt es sich grundsätzlich nicht um einen Feldbus in eigentlichen Sinne, da hier auf konventionelle, Punkt-zu-Punkt verdrahtete 4-20 mA Signale digitale Kommunikation aufgeprägt wird, bzw. parallel dazu benutzt wird.

- VNET/IP,
- TCnet,
- EtherCAT,
- ETHERNET Powerlink,
- EPA (Ethernet for Plant Automation),
- Modbus (RTU bzw. ASCII aber auch TCP),
- SERCOS,
- RAPIEnet,
- SafetyNet p
- MECHATROLINK.

Zusätzlich gibt es eine Variante (Multidrop), bei der eine busähnliche Funktion geschaffen werden kann. Darüber hinaus gibt es eine drahtlos arbeitende Variante (Wireles HART), die speziell für den Aufbau verschlüsselter drahtloser Netzwerke für die Messdatenübertragungen verfügbar ist. Details hierzu sind in IEC 62591:2010 festgelegt.

Bzgl. der Anforderungen an Feldbusses gibt es zwischen der Fertigungstechnik und der Verfahrenstechnik grundlegende Unterschiede.

Fertigungstechnik	**Verfahrenstechnik**
Viele Binärsignale	Viele Analogsignale
Kein zeitlicher Einfluss d. Konfigurationsarbeiten auf d. Datenübertragung	Explosionsschutz
Schnelle Datenübertragung	Hohe Verfügbarkeit
	Energieübertragung per Buskabel

Tabelle 3: Unterschiede zwischen Fertigungs- und Verfahrenstechnik

2.5.2 Kommunikationsvorgänge in Level 2

Auf Level 2 eines ICS finden sich sowohl Realtime-Verbindungen (z. B. zwischen den PNK) als auch Verbindungen, die nicht übertragungszeitkritisch sind (z. B. Engineering-Zugriffe). Es kommen deshalb häufig Protokolle mit unterschiedlichen Stacks (z. B. bei neuen Systemen Industrial Ethernet) zum Einsatz. Typischerweise kommen die Schichten 1,2 und 7 des OSI-Schichtenmodells zur Anwendung. Bei Prozessleitsystemen werden die Funktionen der Schicht 7 üblicherweise nicht offen gelegt.

Als Softwareschnittstelle kommen z. B. OPC (OLE for process control) bzw. OPC UA (Unified Architecture) oder DDE (Dynamic Data Exchange) zum Einsatz.

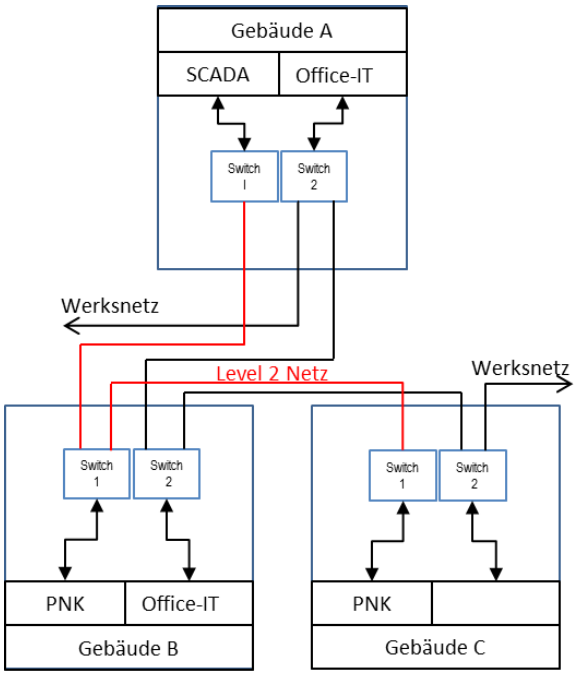
Mit Rücksicht auf die Konsequenzen eines Ausfalls der Level 2 Kommunikation finden sich hier häufig redundante Strukturen.

Für die Kommunikation zwischen PNK, die besonderen Anforderungen genügen müssen (z. B. SIL) kommen zusätzlich spezifische Sicherungsverfahren zum Einsatz, die es erlauben zufällige Übertragungsfehler an den Daten zu erkennen (z. B. CRC Checksummen).

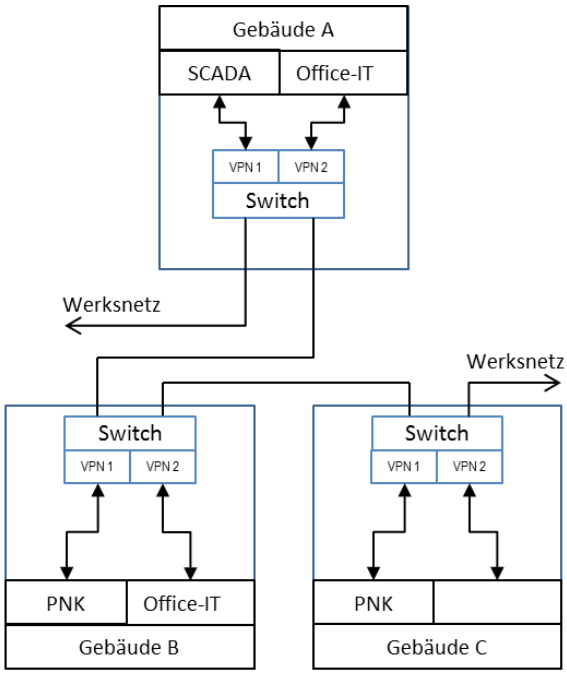
Speziell bei SCADA Lösungen werden häufig die gleichen Protokolle wie im Level 1 verwendet.

Besondere Betrachtungen machen Anlagen nötig, bei denen für die hier beschriebene Kommunikation Übertragungsmedien und zugehörige Infrastruktur verwendet werden, die nicht exklusiver Bestandteil des ICS sind. Dies gilt insbesondere für Fernwirkanlagen bzw. ICS, mit denen geografisch getrennt angeordneten Teilanlagen betrieben werden (z. B. Gas- Strom- und Wasser/Abwasserversorgung).

Darüber hinaus sind aber auch Anwendungen, bei denen Switches, Router und Lichtwellenleiter als Bestandteil eines Level 5 IT Werksnetzes, welche für die Level 2 Kommunikation zum Einsatz kommen sollen, einer spezifischen Betrachtung zu unterziehen.



Level 2 Kommunikation separiert



Level 2 Kommunikation integriert

Abbildung 5: Gegenüberstellung Kommunikationskonzepte

In diesen Fällen ist eine gesonderte Betrachtung der aus dieser Architektur resultierenden Risiken erforderlich.

Separierte Level 2 Kommunikation	Integrierte Level 2 Kommunikation
• Getrennte Kommunikations-Infrastruktur • Änderungen an Office-IT-Switches haben keinen Einfluss auf ICS • Keine ungewollte Querkommunikation • Getrenntes Patch Management für Switche möglich • Lebenszyklus der Office-IT-Switches hat keinen Einfluss auf ICS • Ggf. sinnvolle Redundanzen können umgesetzt werden	• Gemeinsame Kommunikations-Infrastruktur • Änderungen an Office-IT-Switches müssen bzgl. Auswirkungen auf ICS bewertet werden (Daten, Übertragungszeiten, usw.) • Möglichkeiten der Kommunikation zwischen den verschiedenen VPN müssen bewertet werden • Patchmanagement muss z. B. bei GMP Anforderungen bewertet werden • Lebenszyklus der Office-IT-Switches hat Einfluss auf ICS • Redundanzforderungen lassen sich ggf. nicht vollständig umsetzen.

Tabelle 4: Gegenüberstellung separierter und integrierter Level 2 Kommunikation

Prinzipiell sind auch drahtlose Übertragungsprotokolle auf Level 2 anwendbar, wie sie z. B. mit WLAN gem. IEEE 802.11 verfügbar sind. Diese Lösungen sind jedoch mit Rücksicht auf die besonderen Anforderungen industrieller Umgebungen (z. B. EMV, Störungen durch Stahl Konstruktionen etc.), ungeachtet möglicher IT-Security-Risiken, für diese Anwendungsbereiche kritisch zu bewerten.

2.5.3 Kommunikationsvorgänge in Level 3

Über das Level 3 einer ICS Anwendung wird der Datentransfer zwischen dem eigentlichen ICS und den übergeordneten Funktionen bzw. Stationen abgewickelt. Level 3 bildet den äußeren Perimeter der eigentlichen ICS Anwendung (ausgenommen Sonderfälle mit integrierter MES Funktionalität). Die Datenübertragung erfolgt typischerweise unter Verwendung von Ethernet Technologie. Typisch kommen die Schichten 1, 2, 3, 4 und 7 des OSI-Schichtenmodells zur Anwendung.

Als Softwareschnittstellen kommen Funktionen wie:

- DDE zum Zugriff auf vordefinierte Datenbereiche
- OLE (Object Linking and Embedding) zum Zugriff auf (externe) Software Elemente
- ODBC (Open Data Base Connection) zum Zugriff auf Datenbanken

Drahtlose Übertragungsprotokolle kommen auf Level 3 zur Anwendung. Beispielhaft sei hier die Verbindung zwischen an das ICS angeschlossenen Wartungsrechnern und Handheld Computern genannt, die zu Wartungszwecken benutzt werden. Eingesetzt werden typischerweise z. B. WLAN gem. IEEE 802.11.

2.5.4 Kommunikationsvorgänge in Level 4

Im Level 4 kommt die gesamte Bandbreite der Kommunikationstechnologie zum Einsatz.

Für den Betrieb von ICS hat Level 4 bzw. die dort implementierten Funktionen besondere Bedeutung, als hier die nach außen wirksamen Schutzfunktionen angesiedelt sind. Die Systeme auf Level 4 werden bei vielen Anwendern von der IT-Abteilung des jeweiligen Anlagenbetreibers administriert. Hinsichtlich des Schutzbedarfs bestehen Anforderungen, wie im Bereich der Office-IT üblich. Für die Anwendungen auf Level 4 sind die typischen IT-Security Strategien aus dem Bereich der Office-IT anwendbar.

Auf Level 4 werden die IT-Security-Funktionen etabliert, die ein ICS gegen Bedrohungen von außen schützen, welche externe Kommunikationsvorgänge als Basis benutzen.

2.5.5 Kommunikationsvorgänge in Level 5

Für Level 5 werden keine ICS Anforderungen formuliert.

Einzige Ausnahme hiervon bilden exklusiv für das jeweilige ICS geschaltete Wartungszugänge (Remote Access). Für diese Anwendungen kommt die gesamte Bandbreite der verfügbaren Technologie bis hin zu GSM, UMTS und LTE mit Übertragungsgeschwindigkeiten von knapp 100 KBit/s bis hin zu einem GBit/s zum Einsatz.

3 Gefährdungen der IT-Security

Die Sichtweise auf die Sicherheit von ICS hat sich in der jüngeren Vergangenheit gewandelt. Die Installationen waren lange Zeit abgeschottete Systeme basierend auf proprietären Technologien ohne Vernetzung mit Fremdsystemen. Eine Vernetzung mit dem Internet oder vorhandenen Bürokommunikationsnetzen wurde nicht in Betracht gezogen oder war aufgrund technologischer Barrieren nicht realisierbar.

Durch den verstärkten Einsatz von Software und Protokollen aus der Office-IT sowie die zunehmende Vernetzung und gemeinsame Nutzung von Ressourcen (vgl. 2.5) sind ICS den gleichen Gefährdungen ausgesetzt, wie dies bereits in der Office-IT der Fall ist. Aufgrund von anderen Rahmenbedingungen sind hier jedoch nicht immer die gleichen Lösungsmöglichkeiten gegeben.

Zu diesen Rahmenbedingungen zählen u. A.:

- die hohen Verfügbarkeitsanforderungen, die das Einspielen von Updates wie in der Office-IT erschweren (vgl. 2.2.4)
- die lange Lebensdauer (vgl. 2.2.6 und 2.2.9)
- die Tatsache, dass bei der Konzeption der eingesetzten Protokolle in der Vergangenheit Aspekte der IT-Security nicht berücksichtigt wurden. Ausnahmen bilden hier nur in jüngster Zeit verabschiedete Protokollspezifikationen.
- Vorgaben für Genehmigungen und Betrieb der Anlagen oder Komponenten (z. B. SIL)

Kategorie	klassische Unternehmens-IT	ICS
Performance	• keine garantierten Abarbeitungszeiten • hohe Latenz u. U. akzeptabel	• garantierte Abarbeitungszeiten • Latenz ist zum Teil hart begrenzt
Verfügbarkeit	• Rebooten produktiver Systeme nicht ungewöhnlich • Kurzfristig anberaumte Wartungsvorgänge (z. B. Patch) • Wartungsausfälle verursachen geringe Kosten	• Reboot im produktivem Umfeld nicht akzeptabel • Wartungszyklen nur mit langem Vorlauf • Wartungsausfälle verursachen hohe Kosten
Beurteilung von Risiken	• Vertraulichkeit und Integrität von Daten stehen im Vordergrund • Wesentliche Risiken betreffen die nachhaltige Störung von Geschäftsprozessen	• Schutz von Mensch und Umwelt stehen im Vordergrund • Wesentliche Risiken betreffen den unzureichenden Schutz von Menschen und die Zerstörung von Produktionskapazitäten. Auswirkungen auf die Umwelt sind möglich
Systemressourcen / Dediziertheit	• Systeme verfügen über freie Ressourcen, die beispielsweise die Installation von IT-Security-Tools auf dem System erlauben	• Installation von fremden Softwarekomponenten auf den Systemen nicht oder erst nach Freigabe vorgesehen, z. B. Virenschutzprogramme, Programme für Videoanbindung

Kategorie	klassische Unternehmens-IT	ICS
Lebenszeit der Komponenten	• wenige Jahre	• bis zu 20 oder 25 Jahre

Tabelle 5 Eigenschaften und Schutzziele von klassischer Unternehmens-IT und ICS im Vergleich

Im Folgenden werden einige für ICS relevante Gefährdungen in Bezug auf die IT-Sicherheit aufgeführt. Diese treten in der Unternehmens-IT ebenfalls auf. Für vertiefende Informationen werden Hinweise zu den Gefährdungen aus dem IT-Grundschutz gegeben.

Dabei ist zu beachten, dass dies keine Auflistung nach Wichtigkeit darstellt. Eine Bewertung von Schwachstellen erfolgt in Verbindung mit einer Risikoanalyse, die auch die potenziell gefährdeten Menschen und Objekte berücksichtigen muss.

3.1 Organisatorische Gefährdungen

3.1.1 Unzureichende Regelungen zur IT-Security

Das Thema IT-Security bedarf einer ganzheitlichen Betrachtung. Wenn Zuständigkeiten für Erfassung und Aktualisierung von informationstechnischen Abläufen nicht geregelt sind, veraltet die Dokumentation oder es wird gar keine erstellt. Auch die Einbeziehung der Fachabteilungen ist für eine vollständige Erfassung und Umsetzung notwendig.

Regelungen zum Thema IT-Security beeinflussen viele Bereiche von der Beschaffung neuer Komponenten über die Einstellung neuen Personals bis hin zum Betrieb und der Entsorgung von Geräten (vgl. [BSI GS] G 2.1).

Durch unterschiedliche Kenntnisse im Bereich IT-Security oder ICS kann es zu Umsetzungsproblemen kommen. Auf der einen Seite können vonseiten der Office-IT-Security Vorgaben gemacht werden, die im Bereich ICS aufgrund der Technik nicht umsetzbar sind. Auf der anderen Seiten können bestimmte IT-Security-Aspekte den ICS-Experten nicht bekannt sein. Auf diese Weise kommt es zu Reibungsverlusten in der Kommunikation und der Umsetzung.

Das alleinige Erstellen von Regelungen hilft jedoch nichts, wenn diese nicht angemessen an die Mitarbeiter kommuniziert ([BSI GS] G 2.2) und kontrolliert ([BSI GS] G 2.4) werden.

3.1.2 Unzureichende Dokumentation

Die Dokumentation deckt ein weites Feld ab ([BSI GS] G 2.27). Hierzu gehören u. A. ein aktuelles Abbild der Netzwerkverkabelung ([BSI GS] G 2.12) sowie des gesamten Informationsverbundes ([BSI GS] G 2.136) mit allen Komponenten, auf den einzelnen Komponenten betriebenen Dienste und der Freigaben in der Firewall.

Die Dokumentation bildet zudem die Grundlage für eine Risikoanalyse und die Umsetzung der Maßnahmen zur IT-Security.

Bei einer unzureichenden Dokumentation kann sich im Schadensfall, beispielsweise durch den Ausfall von Hardware bzw. Fehlfunktionen von Programmen, die Fehlerdiagnose und -behebung erheblich verzögern oder völlig undurchführbar sein.

Durch fehlende Dokumentation kann zudem, ein trügerisches Gefühl der Sicherheit erwachsen. So werden Entscheidungen getroffen oder Aussagen gemacht, die auf einem falschen Informationsstand beruhen. Dies kann beispielsweise die Vernetzung von Office- und ICS-Netz betreffen, sodass dort eine klare Trennung angenommen wird, obwohl es Verbindungen zu einzelnen Komponenten gibt.

3.1.3 Unvollständige Absicherung der Fernwartungszugänge

ICS werden oftmals aus der Ferne über Fernwartungszugänge überwacht oder betrieben. Als Übertragungsmedium werden unterschiedliche öffentliche und private Netze verwendet, wie z. B. das Telefonienetz, Funknetz, Mobilfunknetz und zunehmend das Internet (vgl. 2.5.2, 2.5.4, 2.5.5). Sind diese Zugänge unzureichend geplant, falsch konfiguriert oder werden nicht überwacht ([BSI GS] G 2.128, G 2.129, G 2.130, G 2.131)), so können Angreifer u. U. unbefugt über diese Zugangsmöglichkeiten auf einzelne ICS und die ICS-Infrastruktur zugreifen und so Sicherheitsmechanismen am Perimeter umgehen.

Neben Fernwartungszugängen an zentraler Stelle können Fernwartungszugänge auf Level 2 oder 3 (vgl. 2.5.2, 2.5.3) stattfinden und so direkt an der Steuerung angesiedelt sein. Bestehende Sicherheitsmechanismen zum Schutz des ICS-Netzes können so umgangen werden (z. B. Modem-Einwahl-Möglichkeit ohne Sicherheitsmechanismen wie einer Authentisierung). Insbesondere in Bestandsanlagen kommen ungesicherten Modem-Verbindungen vor, sodass ein Angreifer hierüber möglicherweise das ICS angreifen könnte.

3.1.4 Einsatz von Standard-IT-Komponenten mit bereits identifizierten Schwachstellen

Neben ICS-spezifischen IT-Komponenten werden zunehmend Komponenten, Technologien und Software aus der Office-IT in ICS-Lösungen eingesetzt. Diese Komponenten, sogenannte commercial off-the-shelf (COTS) Produkte, weisen (wie fast jede Software) Schwachstellen auf. Diese sind oftmals dokumentiert und öffentlich bekannt.

Darüber hinaus sind häufig entsprechende Angriffswerkzeuge frei verfügbar, die auch von nicht versierten Angreifern benutzt werden können. Da diese Produkte weit verbreitet sind, besteht für Angreifer auch ein großes Interesse daran, weitere Schwachstellen in diesen Produkten ausfindig zu machen. Somit werden durch den Einsatz von COTS-Produkten alte und neue Schwachstellen aus der Office-IT in die ICS-Umgebung überführt (vgl. ([BSI GS] G 0.28).

Aufgrund des hohen Verbreitungsgrads besteht für COTS-Produkte beispielsweise nicht nur das Interesse von Angreifern neue Schwachstellen aufzudecken, sondern auch speziell zugeschnittene Schadprogramme für diese Produkte zu entwickeln. Darüber hinaus ist es entgegen dem Vorgehen in der klassischen Office-IT nicht immer möglich, einen Virenschutz im ICS-Netz zu betreiben und daher schwieriger, einen Schutz vor Schadprogrammen umzusetzen.

Typische Bereiche, in denen COTS-Produkte zum Einsatz kommen, sind beispielsweise Bedien- und Engineeringsysteme oder Router, Switche und Modems.

3.1.5 Fehlende Überwachung der unterstützenden Infrastruktur

Das Überwachen von Zuständen in der Produktion ist eine wesentliche Funktion von ICS-Lösungen. So werden gewöhnlich die Produktion betreffende Warnungen (z. B. bei unterschrittenen Füllständen) und technische Parameter (z. B. Temperaturen, Ventilstellungen) abgebildet. Dagegen fehlt es häufig an einer angemessenen Überwachung der unterstützenden IT-Infrastruktur (vgl. [BSI GS] G 2.22, G 2.160).

Werden ungewöhnliche oder security-relevante zu überwachende Ereignisse von ICS nicht oder unzureichend überwacht, so können beispielsweise Angriffsversuche, Engpässe in der Netzarchitektur oder absehbare Ausfälle nicht frühzeitig erkannt werden. Zu diesen Ereignissen zählen erfolglose und erfolgreiche Authentisierungen, eine erhöhte Auslastung des Netzes an Knotenpunkten und fehlerhafte Leseversuche von einer Festplatte.

Darüber hinaus kann auch eine mangelhafte, unübersichtliche Darstellung der Ereignisse dazu führen, dass Warnungen und Fehler verspätet erkannt werden.

3.1.6 Abhängigkeiten des ICS-Netzes von IT-Netzen

ICS-Netze werden mittlerweile nicht mehr durchgängig autark betrieben. Bestehen Abhängigkeiten zu anderen Systemen, Netzen oder Diensten, so wirken sich Ausfälle oder Sicherheitsvorfälle außerhalb des ICS-Netzes auch indirekt auf die ICS-Umgebung aus (vgl. 2.5.2).

Insbesondere wenn diese Systeme und Netze nicht unter der Kontrolle des ICS-Betreibers stehen, kann dies zu starken Beeinträchtigungen in der Produktion und der Verfügbarkeit der ICS-Installation führen. Darüber hinaus kann der Vorfall oder Fehler u. U. nur mit eingeschränkten Möglichkeiten behoben werden.

Beispiele für Abhängigkeiten zu anderen Systemen und Netzen sind Internetanbindungen (sowohl drahtgebunden als auch über Mobilfunk), gemeinsam genutzte Infrasstrukturkomponenten (vgl. 2.5.2) oder auch die zunehmende Nutzung von Cloud-Diensten.

3.1.7 Magelnde Awareness

Die Mitarbeiter tragen stark zur IT-Security in einem Unternehmen bei. Wenn diese nicht für die Bedrohungen sensibilisiert sind, stellen sie ein hohes Risiko dar. Beispiele hierfür sind die Auswahl schlechter Passwörter oder auch das Öffnen von Anhängen an E-Mails.

So wird durchaus die Meinung vertreten, dass das interne Netz bereits sicher ist und dort folglich keine Risiken vorhanden sind. Man wiegt sich so in einer trügerischen Sicherheit. Durch den sorglosen Umgang mit der eingesetzten IT werden ggf. Sicherheitsmaßnahmen umgangen oder ignoriert und damit wird den Angreifern das Leben einfacher gemacht.

3.2 Menschliche Fehlhandlungen

3.2.1 Unzureichende Absicherung oder zu weitreichende Vernetzung

Werden unnötige Kommunikationskanäle in das ICS-Netz eingerichtet, kann ein Angreifer diese ggf. unzureichend gesicherten Zugriffswege nutzen, um auf das ICS zuzugreifen und Systeme zu kompromittieren (vgl. [BSI GS] G2.60, G 3.29).

Wenn z. B. ein Mitarbeiter zur Überwachung eines ICS von dem Büroarbeitsplatz aus eine Datenverbindung von seinem Arbeitsplatzrechner in das ICS-Netz einrichtet, so wird damit das Office-Netz (z. B. mit Verbindung zum Internet) mit dem ICS-Netz gekoppelt ([BSI GS] G 3.78). Somit ist das ICS-Netz denselben Bedrohungen ausgesetzt wie das Office-Netz (z. B. Angriffe und Schadprogramme aus dem Internet).

Es sind neben den zuvor genannten Verbindungen auch Datenverbindungen für die Produktionssteuerung notwendig, bei der Daten zwischen ICS-Netz und Office-Netz ausgetauscht werden müssen. In diesen Fällen können die Freigaben zu allgemein gefasst werden oder die Segmentierung des Netzes wird bereits bei der Planung unzureichend umgesetzt ([BSI GS] G 2.45). Dies öffnet ebenfalls nicht benötigte Kommunikationskanäle.

Der Zugriff auf das Internet aus dem ICS-Netz heraus stellt eine weitere Gefahrenquelle dar. Es können über diesen Kanal Daten abfließen oder Schadprogramme geladen werden.

Drüber hinaus können ICS-Komponenten beispielsweise über Verbindungen in unterschiedliche Level der Beispielarchitektur (vgl. Abbildung 3) verfügen (sog. Multi-homing). So kann es einem Angreifer ggf. möglich sein, mittels dieser Verbindung von einem der Netze ausgehend, unbefugt auf ein anderes Segment zuzugreifen (z. B. bei aktivierter Bridge- oder Routing-Funktionalität). Mögliche Schutzmaßnahmen auf Netzwerkebene werden so umgangen.

3.2.2 Mangelhafte Konfigurationen von Komponenten

In der Standard-Konfiguration von Software oder Komponenten sind Sicherheitsmaßnahmen nicht immer aktiviert, sodass dies unbefugte Zugriffe durch einen Angreifer erheblich erleichtert (vgl. [BSI GS] G 3.28, G 3.38, G 4.49, G 4.53, G 4.70). Werden diese in einer unsicheren Konfiguration betrieben, so stellen sie ein Sicherheitsrisiko auch für andere IT-Systeme mit einer Verbindung zu diesem System dar.

Die folgenden Beispiele veranschaulichen mögliche, Security-relevante Gefährdungen einer Standard -Konfiguration:

- unnötige Programme und aktivierte Dienste ggf. mit bekannten Schwachstellen,
- Standardbenutzer und -kennwörter,
- deaktivierte Sicherheitsfunktionen (z. B. Firewall),
- ungeschützte Administrationszugänge.

3.2.3 Fehlende Backups

Regelmäßige Datensicherungen bzw. Datensicherungen nach vorgenommenen Veränderungen ermöglichen einen zeitnahen Austausch fehlerhafter oder ausgefallener Komponenten durch das Einspielen der letzten Datensicherung auf die neue Komponente. Auf diese Weise kann der Betrieb umgehend wieder aufgenommen und die geforderte Verfügbarkeit garantiert werden.

Im alltäglichen Betrieb wird diese Datensicherung oft nicht durchgeführt, sodass im Bedarfsfall keine oder veraltete Daten zur Wiederherstellung vorliegen. Ein weiteres Problem kann die Aufbewahrung der Datensicherungen darstellen, die ggf. nicht an zentraler Stelle durchgeführt wird, sondern an unterschiedlichen und nicht dokumentierten Stellen. Hinzukommen zum Teil auch fehlende Möglichkeiten für die Erstellung von Backups bzw. deren Wiedereinspielen.

3.2.4 Mobile Datenträger und Laptops

Einige administrative Tätigkeiten können nicht über Fernwartungszugänge (siehe 3.1.3) durchgeführt werden, sodass ein Wartungstechniker vor Ort erscheinen muss. Hierzu nutzt ein Wartungstechniker mobile Datenträger (z. B. USB-Sticks) oder eigene Laptops, die mit dem ICS-Netz oder der betroffenen ICS-Komponente verbunden werden.

Hier besteht die Gefahr, dass sich auf diesen Geräten Schadprogramme befinden und diese sich im Netzwerk oder der Komponente ausbreiten (vgl. [BSI GS] G 5.23, G 5.142).

Dies gilt natürlich auch für die Verwendung von mobilen Datenträgern, die nur firmenintern genutzt werden. So nutzt der Wartungstechniker üblicherweise die Hardware auch in anderen ICS. Befindet sich ein Schadprogramm darauf und schließt der Wartungstechniker die Hardware an das ICS an, so kann ein Schadprogramm sich auf der Hardware einnisten und von einem ICS zum nächsten transportiert werden.

Unter Schadprogrammen (z. B. Würmer, Viren, Trojanische Pferde) wird jede Software verstanden, die zum Zweck entwickelt wurde, unbemerkt vom Benutzer schädliche ungewollte/unbeabsichtigte Funktionen auszuführen (u. a. Datendiebstahl, Löschung von Daten). Es sind bereits zahlreiche Infektionen durch Schadprogramme im ICS-Umfeld bekannt (siehe auch 3.1.4).

Wartungslaptops weisen darüber hinaus unterschiedliche Kommunikationsschnittstellen auf (z. B. Ethernet, WLAN, Bluetooth, Infrarot, Mobilfunknetze wie UMTS). Besteht beispielsweise bereits eine Internetverbindung über UMTS und wird der Laptop gleichzeitig mit dem ICS-Netz verbunden, so stellt dies eine Netzkopplung dar. Auf diesem Wege sind direkte Zugriffe aus dem Internet in das ICS-Netz denkbar.

3.2.5 Unzureichende Validierung von Eingaben und Ausgaben

Nehmen Anwendungen Eingaben zur Verarbeitung entgegen oder geben Daten zurück ohne diese ausreichend auf Validität zu prüfen, so ist es einem Angreifer beispielsweise möglich, Schadcode zur Ausführung auf dem System einzubringen (z. B. durch Pufferüberlaufe) oder Ausgaben auf eine Weise zu erzwingen, sodass Schadcode von der Anwendung an den Empfänger übermittelt wird (z. B. Cross-Site Scripting im Browser). Bei der Entwicklung von Anwendungen wird häufig auf Validierung der Ein- und Ausgabedaten verzichtet (vgl. [BSI GS] G 4.84). Dies gilt auch für selbstentwickelte Werkzeuge. Hierbei wird meist nur auf die Funktionalität geachtet und Routinen zur Fehlerkontrolle werden (meist aus Zeitgründen) nicht berücksichtigt.

Es handelt sich hierbei um eine Gefahr, die bereits bei der Entwicklung und Beschaffung berücksichtigt werden muss.

3.3 Vorsätzliche Handlungen

Allen folgenden Gefährdungen ist gemein, dass zum Teil immer weniger Know-How auf der Seite der Angreifer vorhanden sein muss. Es gibt diverse im Internet verfügbare Werkzeuge, die für solche Zwecke genutzt werden können.

3.3.1 Kommunikation von Mess- und Steuerwerten

Die Systeme in ICS kommunizieren untereinander über verschiedene Netzprotokolle und Technologien. Neben Protokollen und Technologien aus der Office-IT (z. B. Ethernet, TCP/ IP, WLAN, GSM) werden ICS-spezifische Protokolle eingesetzt. Diese sind nicht unter dem Gesichtspunkt der IT-Security entwickelt worden und bieten demgemäß keine oder nur eingeschränkte Security-Mechanismen.

Bei den übertragenen Informationen handelt es sich z. B. um Mess- oder Steuerwerte. Die Übertragung erfolgt häufig im Klartext und ist nur unzureichend vor einer Manipulation geschützt. Einem Angreifer mit physischem Zugang zum ICS-Netz ist es somit möglich, diese Werte zu lesen, zu verändern oder neue einzuspielen (z. B. zur Steuerung einer Maschine oder der Fälschung von Sensordaten; vgl. [BSI GS] G 0.14, G 0.15, G 0.43, G 5.7, G 5.8, G 5.24).

Werden beispielsweise falsche Sensordaten von einem Angreifer vorgetäuscht, können die Bediener des Systems keine verlässlichen, sensorischen Daten mehr ablesen und befinden sich u. U. in einem schweren Irrtum über den tatsächlichen Systemzustand. Die Manipulation von Sensordaten, auf denen vollautomatische Steuerungen (closed loop control) basieren, führt u. U. zu falschen Steuerungskommandos und kann daher direkt Auswirkungen auf den Prozess haben.

Insbesondere bei ungesicherten Funkverbindungen ist ein einfacher Zugriff auf die übertragenen Daten möglich. Durch gezielte Überlagerung ist das Einspielen oder Verändern von Daten möglich sowie die Störung der Kommunikation insgesamt.

Derartige Angriffe können zu drei Problemen (siehe auch 3.3.4) führen:

- Verlust der Anzeige (loss of view),
- Manipulation der Anzeige (manipulation of view) und
- Störung oder Verlust der Kontrolle (loss of control).

So können beispielsweise Sensordaten (z. B. Füllstand, Temperatur, Druck) verfälscht werden, um Abschaltungen oder Regelungen zu verhindern und damit den Produktionsprozess zu beeinflussen. Denkbar ist auch das Verfälschen von Produktionsparameter (z. B. Frequenzen, Umdrehungen, Dauer eines

Schweißvorgangs), um gezielt Fehlproduktionen zu verursachen. Unter Umständen werden die falschen Produktionsparameter erst bei der Qualitätskontrolle bemerkt, da in der Visualisierung die dargestellten Parameter nicht mit den tatsächlich eingestellten Parametern durch den Angreifer übereinstimmen.

Darüber hinaus lassen sich ggf. Safety-Mechanismen auslösen oder stören (z. B. Selbstabschaltung bei Überschreitung eines Drucks oder Unterschreitung eines Füllstandes oder Unterdrückung der automatischen Selbstabschaltung).

3.3.2 Ermitteln von Zugangsdaten mittels Wörterbuch- und Brute-Force-Angriffen

Erfordert der Zugang zu Systemen eine Authentisierung mittels Zugangsdaten, so kann ein Angreifer versuchen, diese zu erraten. In der Regel werden hierzu automatisierte Angriffswerkzeuge verwendet, die auf unterschiedlicher Datenbasis versuchen, Kennwörter zu ermitteln (vgl. [BSI GS] G 5.18).

Bei einem Brute-Force-Angriff (deutsch: *rohe Gewalt*) werden alle denkbaren Kombinationen an Zeichen für das Passwort durchgetestet (z. B. Alphabet mit Zahlen und Sonderzeichen). Hierbei steigt der Aufwand exponentiell mit der Passwort-Länge und dem möglichen Zeichensatz. Daher ist ein Brute-Force-Angriff oftmals sehr zeitintensiv und von zahlreichen, nicht erfolgreichen Anmeldeversuchen gekennzeichnet.

Aufgrund des ineffizienten Vorgehens bei einem Brute-Force-Angriff mit allen denkbaren Kombinationen für ein Passwort wird häufig die Datenbasis zur Ermittlung der Passwörter auf ein definiertes Wörterbuch eingeschränkt. In diesem Fall spricht man von einem Wörterbuch-Angriff (engl. *dictionary attack)*. Hierbei handelt es sich somit um eine Variante eines Brute-Force-Angriffs. Entgegen dem oben beschriebenen Brute-Force-Angriff ist der Erfolg bei einem Wörterbuch-Angriff jedoch stark abhängig von der Qualität des Wörterbuchs. Solche Wörterbücher mit häufig genutzten Passwörtern werden daher rege im Internet ausgetauscht.

Insbesondere Standardzugangsdaten (vgl. 3.2.2) und nicht ausreichend komplexe, triviale und zu kurze Passwörter können mittels dieser Angriffstechniken effizient und in kurzer Zeit ermittelt werden (vgl. [DUD 2009], [BSI 2008]).

3.3.3 Systematische Schwachstellensuche über das Netzwerk

Sind ICS für einen Angreifer über das Netzwerk erreichbar, so kann er verfügbare Dienste identifizieren und ggf. bekannte, vorhandene Schwachstellen mittels unterschiedlicher Techniken über das Netzwerk ermitteln. Hierfür können frei verfügbare Programme verwendet werden, die den Prozess automatisieren.

Mittels eines sogenannten Port-Scans lassen sich die erreichbaren Dienste über das Netz ermitteln (z. B. TCP- und UDP-Scan). Anschließend kann ein sogenannter Schwachstellenscanner die identifizierten Dienste auf Schwachstellen prüfen. Hierfür sind in Schwachstellenscanner Testvektoren hinterlegt, welche die Dienste auf spezifische, bekannte Schwachstellen überprüfen (z. B. Pufferüberläufe, SQL-Injection, Broken Authentication oder fehlerhaftes Sessionmanagement (vgl. [OWASP Top10])).

3.3.4 Denial-of-Service-Angriffe (DoS)

Denial-of-Service-Angriffe verfolgen das Ziel, die Verfügbarkeit von Systemen oder angebotenen Diensten einzuschränken. Werden beispielsweise von einem Angreifer gezielt Ressourcen durch eine Vielzahl von gleichzeitigen Anfragen gebunden, so ist die Komponente aufgrund der Last ggf. nicht mehr für andere Nutzer erreichbar. Dieser Angriff kann auf Netzebene erfolgen (z. B. Überlastung der Übertragungskapazität) oder auch auf Anwendungsebene durch das gehäufte Ausführen ressourcenintensiver Operationen. Darüber hinaus kann auch das Ausnutzen von softwarebasierten Schwachstellen (z. B. Pufferüberlauf zum Ausfall des Systems oder Dienstes führen und damit für einen DoS-Angriff genutzt werden (vgl. [IX 2013], S. 64-67).

Wenn die Kommunikation mittels Funk erfolgt, kann ein Angreifer diese durch gezielte Überlagerungen unterbrechen.

Der Angriff kann auch über eine verteilte Infrastruktur beispielsweise ein Bot-Netz erfolgen. In diesem Fall wird dies als Distributed-Denial-of-Service (DDoS) bezeichnet.

3.3.5 Man-in-the-Middle-Angriff

Bei einem Man-in-the-Middle-Angriff (MitM-Angriff) nimmt der Angreifer eine Position zwischen zwei Kommunikationspartnern ein, um beispielsweise die übertragenen Daten mitzulesen oder zu manipulieren (vgl. Kapitel 3.3.1 und [BSI GS] G 5.143). Dies kann physisch z. B. durch das Auftrennen einer Leitung und der direkten Verbindung zu den beiden Kommunikationspartnern geschehen oder logisch über das Vortäuschen der Identität des jeweils anderen Kommunikationspartners, sodass der Angreifer fälschlicherweise für den jeweils anderen Partner gehalten wird.

Im ICS-Umfeld spielt aufgrund des verbreiteten Ethernet-Einsatzes und der Kommunikation über das IP-Protokoll insbesondere ARP-Spoofing als MitM-Angriffstechnik eine wichtige Rolle.

3.3.6 Phishing

Bei einem Phishing-Angriff gibt sich der Angreifer dem Benutzer als vertrauenswürdige Person oder Stelle aus (z. B. Administrator, Kollege, ICS-Hersteller). Er versucht auf diese Weise an Informationen wie Zugangsdaten zu gelangen oder den Benutzer dazu zu veranlassen gewisse Aktionen durchzuführen (z. B. Änderung einer sicherheitsrelevanten Konfiguration, Installation eines Schadprogramms im E-Mail-Anhang). Der Angreifer versucht also, Vertrauensbeziehungen des Benutzers auszunutzen (vgl. [BSI GS] G 5.157, G 5.158)

Gewöhnlich werden solche Phishing-Angriffe über gefälschte Internetauftritte und den Versand von E-Mails oder Nachrichten in sozialen Medien durchgeführt. Über den Massenversand solcher E-Mails lassen sich Phishing-Angriffe auf eine Vielzahl von Benutzern ausdehnen.

Neben dem ungezielten Versand von Nachrichten, gibt es einen Trend zu zielgerichteten Attacken. Hierbei werden Informationen aus öffentlichen Quellen oder sozialen Netzwerken genutzt, um eine möglichst persönliche Ansprache zu erreichen. Auf diese Weise wird die Wahrscheinlichkeit erhöht, dass das Opfer einen Anhang öffnet oder einen Link anklickt, der auf eine mit einem Schadprogramm infizierten Seite verweist.

3.3.7 **Injection-Angriffe**

Bei einem Injection-Angriff übergibt ein Angreifer einer Anwendung präparierte Eingabedaten und versucht damit Befehle auszuführen. Dies betrifft im wesentlichen verarbeitende Dienste und beruht auf einer mangelhaften Validierung von Eingabedaten (vgl. 3.2.5). Ein Beispiel sind SQL-Injection-Angriffe, bei denen einer Web-Anwendung, Daten übermittelt werden, die einen Befehl auf der Datenbank ausführen sollen. Wenn die Daten nicht ausreichend auf Plausibilität geprüft werden, ist eine Manipulation der Inhalte in der Datenbank möglich (vgl. [BSI GS] G 5.174 und G 5.131), weil diese als Befehl interpretiert werden.

Weitere Beispiele sind LDAP-Injection, Mail-Command-Injection, OS-Command-Injection, SSI-Injection, Xpath-Injection oder Code-Injection.

3.3.8 Cross-Site-Scripting

Cross-Site-Scripting-Angriffe (XSS-Angriffe) richten sich gegen die Benutzer einer Web-Anwendung. Hierbei versucht ein Angreifer indirekt Schadcode (in der Regel Browser-seitig ausführbare Skripte, wie z. B. JavaScript) an den Client des Benutzers einer Web-Anwendung zu senden.

Werden die Ein- und Ausgaben von einer Web-Anwendung nicht ausreichend validiert (vgl. 3.2.5), so kann ein Angreifer schadhaften Code in die Web-Anwendung einschleusen (z. B. innerhalb eines Kommentars zu einem Artikel) und so verteilen. Wird eine infizierte Webseite von einem Benutzer aufgerufen, führt der Client (z. B. Browser) den eingefügten Schadcode aus. Aus Sicht des Benutzers stammt der schadhafte Code von der Web-Anwendung und wird somit als vertrauenswürdig eingestuft. Daher wird der Schadcode im Sicherheitskontext der Web-Anwendung interpretiert und es ist dem Angreifer möglich, Befehle im Kontext einer möglicherweise bestehenden Sitzung des betroffenen Benutzers auszuführen.

3.3.9 Drive-By-Downloads

Durch Schwachstellen in Browsern und deren Erweiterungen kann allein das Betrachten einer mit Schadcode präparierten Seite zu einer Infektion des Rechners mit einem Schadprogramm führen. Dies wird Drive-By-Download (auch Drive-By-Exploit) genannt. Es ist hierfür keine weitere Interaktion mit dem Benutzer erforderlich (vgl. [BSI 2012]).

3.3.10 Schadsoftware **auf EWS**

Zur Konfiguration und Programmierung von ICS-Komponenten werden Engineering-Workstations (EWS) genutzt. Wenn die EWS mit einem Schadprogramm infiziert ist, können hierüber:

- Die Programme auf der SPS verändert werden. Es kann somit etwas an dem Ablauf verändert werden. Dies kann sich in veränderten Darstellungen, zusätzlichen Steuerbefehlen oder Ähnlichem auswirken.
- Die Programme und Abläufe auf der SPS entwendet und an den Angreifer übertragen werden.

Für Angreifer ist dieser Angriffsvektor besonders wertvoll, da hierdurch nicht nur die SPS kompromittiert und die Produktion auf eine gewünschte Weise gestört wird. Es wird gleichzeitig die Visualisierung des Steuerungszustands im Sinne des Angreifers beeinflusst. In der Folge bemerkt das Bedienpersonal die Auswirkung des Angriffs nicht, schöpft keinen Verdacht und setzt die Produktion unvermindert fort. Beeinträchtigte Systeme können dann über einen langen Zeitraum sabotiert werden, ohne dass dies bemerkt wird.

3.3.11 Schadprogramme

Neben der gezielten Infektion mit Schadprogrammen können Varianten, die eigentlich auf die Unternehmens-IT abzielen, für Schäden im ICS verantwortlich sein (Kollateralschäden). Dies kann zu Abstürzen, veränderten Laufzeiten oder einer Zunahme des Netzwerkverkehrs führen, wodurch es zu Ausfällen kommt. Mögliche Wege der Infektion wurden bereits in 3.2.4, 3.3.6 oder 3.3.9 beschrieben.

3.3.12 Replay-Angriff

Kann ein Angreifer den Netzverkehr mitschneiden (z. B. das Ausführen eines Befehls mit privilegierten Rechten) ist es ihm u. U. möglich, durch das Wiedereinspielen dieser Daten in das Netz die mitgeschnittene Aktion unbefugt erneut auszuführen. Dies setzt voraus, dass das verwendete Protokoll zur Datenübertragung mehrfach versendete Daten nicht unterscheiden kann. Daher können erstmalig legitim übertragene Daten nicht von einer Kopie der zuvor übertragenen Daten abgegrenzt und ggf. verworfen werden. Diese Technik wird als Replay-Angriff bezeichnet.

Auf diese Weise kann der Angreifer korrekt formatierte und auch verschlüsselte oder signierte Daten in den Verkehr bringen, die der Empfänger als authentische Information weiterverarbeitet, ohne z. B. die Verschlüsselung brechen zu müssen oder zuvor ein Passwort in Erfahrung zu bringen.

Beispielsweise kann ein Schaltbefehl (z. B. Einschalten einer Pumpe) oder die Parameterübertragung (z. B. Festlegen einer Solltemperatur eines Ofens) an eine ICS-Komponente von einem Angreifer aufgezeichnet und zu einem späteren Zeitpunkt, zu dem mit einem Schaden zu rechnen ist, wiederholt werden.

3.3.13 Physischer Angriff zur Provokation administrativer Eingriffe

Je nach Einsatzfeld der ICS-Installation kann ein Angreifer eine der Komponenten (z. B. externer Sensor oder Aktor physisch manipulieren, um eine Reaktion der Bedienmannschaft zu provozieren. Auf diese Weise kann ein Angreifer gewisse Aktionen wie die Durchführung von administrativen Tätigkeiten beeinflussen und dann beispielsweise für weiterführende Angriffe nutzen.

So kann z. B. ein Temperatursensor erhitzt werden, um einen Alarm auszulösen und in der Folge eine gewisse Reaktion des Bedienpersonals hervorzurufen. Dies ist beispielsweise dann möglich, wenn der Angreifer annehmen kann, dass

- ein Wartungszugriff erfolgt, bei dem ein Passwort unsicher übertragen wird (Mitschneiden des Passwortes an einer Netzkomponente),
- ein Steuerbefehl (z. B. Neustart oder Schnellabschaltung) abgesetzt wird, den er für einen späteren Replay-Angriff benötigt oder
- ein ungesicherter Fernwartungszugang aktiviert wird, weil die provozierte Störung das Eingreifen eines Lieferanten-Mitarbeiters erfordert und er diesen Zugang dann für sich selbst nutzen kann.

Der Angriffsvektor kombiniert daher das Wissen über das produktive System selbst mit vorhandenen Schwachstellen von ICS-Komponenten.

Eine ähnliche Vorgehensweise stellt die ständige Alarmierung dar. Der Angreifer löst wiederholt eine Alarmierung aus (z. B. Unterbrechung einer Lichtschranke). Kommt es mehrfach zu einem administrativen Eingriff ohne eine Ursache identifizieren zu können, so wird ggf. vom Bedienpersonal von einer Fehlalarmierung ausgegangen, die durch eine Fehlfunktion ausgelöst wurde, und der Alarm bis auf Weiteres deaktiviert. Auf diese Weise kann der eigentliche Angriff vorbereitet werden, der denselben Alarm auslösen würde.

4 Organisationen, Verbände und deren Standards

Dieses Kapitel gibt einen Überblick über nationale und internationale Organisationen sowie deren Standards und Handreichungen im Bereich Security in ICS. Der Fokus liegt auf security-relevanten Standards; safety-spezifische Normen sind nicht aufgenommen.

Die Zielsetzung, Adressaten, Inhalte und Anwendungsbereiche der Standards und Quasi-Standards sind dargestellt.

4.1 Internationale Standards

4.1.1 ISO/ IEC

Die Internationale Organisation für Normung (ISO; http://www.iso.org) erarbeitet international gültige Normen in allen Bereichen. Zusammen mit der Internationalen Elektrotechnischen Kommission (IEC; http://www.iec.ch), die für den Bereich der Elektrik und der Elektronik zuständig ist und der Internationalen Fernmeldeunion (ITU), die für den Bereich der Telekommunikation zuständig ist, bilden diese drei Organisationen die World Standards Cooperation (WSC).

4.1.1.1 ISO/ IEC 27000 Reihe Informationssicherheitsmanagementsysteme ISMS)

Die Normenreihe ISO/ IEC 27000 [ISO/IEC 27000] ist reserviert für Themen zur Informationssicherheit. Die Normenreihe wird vom Technischen Komitee JTC 1 (joint technical committee), SC 27 (subcommittee) entwickelt (vgl. [ISO Standards 2013]).

Ziel der ISO/ IEC 27001 ist es, allgemeine Anforderungen an ein Informationssicherheitsmanagementsystem (ISMS) im Rahmen eines Prozessansatzes zu definieren. Ein ISMS ist gekennzeichnet durch ein Risikomanagement, welches darauf abzielt, angemessene technische und organisatorische Maßnahmen gegen identifizierte Risiken zu ergreifen. Die generischen Anforderungen sind auf alle Organisationen anwendbar. Sie sind überwiegend prozessorientiert und haben einen niedrigen, technischen Detaillierungsgrad [BITKOM/DIN 2007]. Zielgruppe der ISO/ IEC27001 und ISO/IEC 27002 sind im ICS-Umfeld Betreiber. Integratoren und Hersteller können die für eine Zertifizierung notwendige Informationen liefern.

Die ISO/ IEC 27002 gehört zu den allgemeinen Richtlinien und definiert den Rahmen und allgemeine Prinzipien für ein ISMS in einer Organisation. Sie dient als Leitfaden zur Umsetzung eines ISMS und deckt folgende Themen ab:

- Risikoeinschätzung und -behandlung,
- Sicherheitsleitlinie,
- Organisation der Informationssicherheit,
- Management von organisationseigenen Werten,
- Personalsicherheit,
- Physische und umgebungsbezogene Sicherheit,
- Betriebs- und Kommunikationsmanagement,
- Zugangskontrolle,

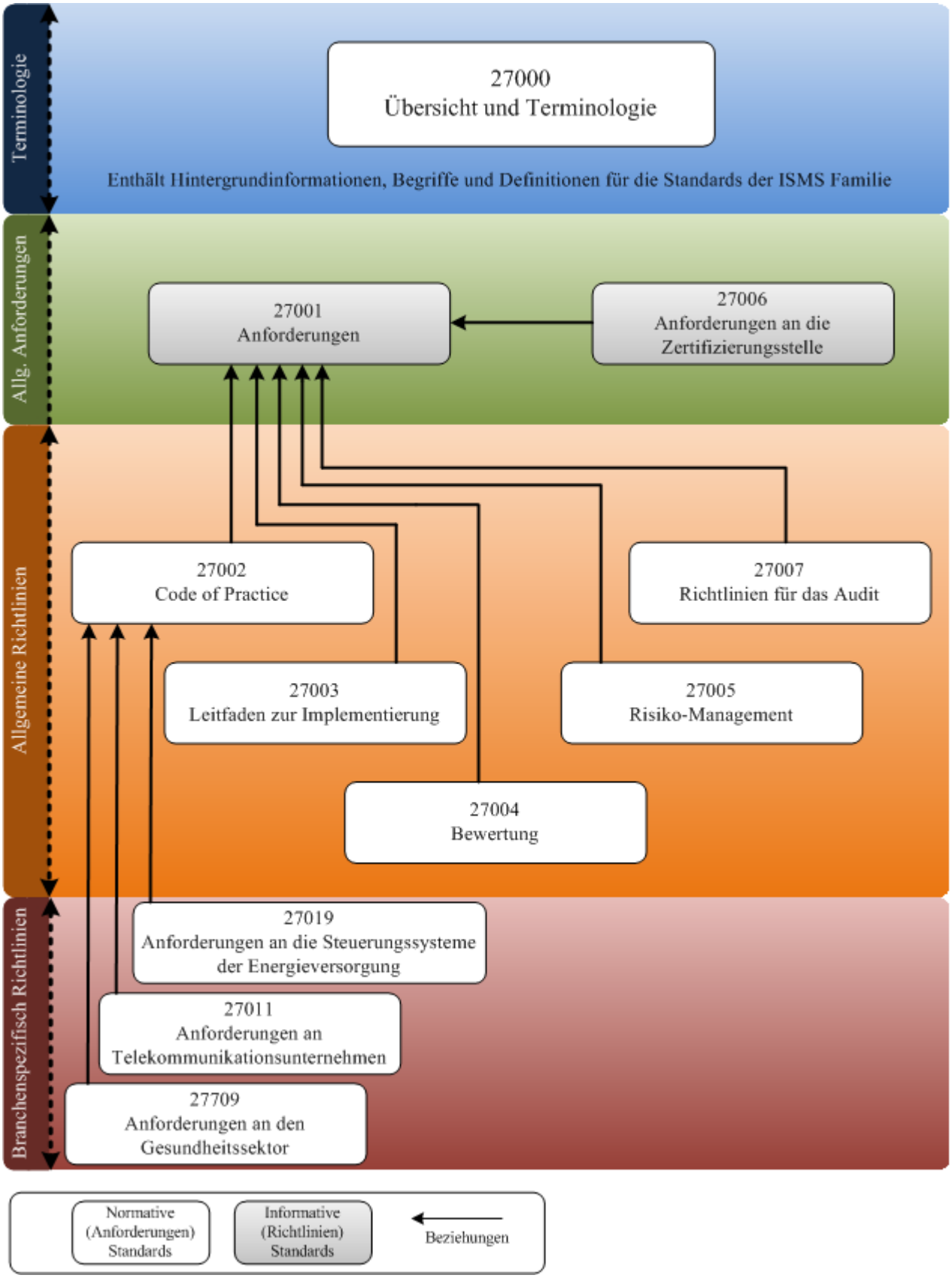


Abbildung 6 Aufbau der ISO 27000-Normenreihe in Anlehnung an ISO 27000:2009)

- Beschaffung, Entwicklung und Wartung von Informationssystemen,
- Umgang mit Informationssicherheitsvorfällen,
- Sicherstellung des Geschäftsbetriebs und
- Einhaltung von Vorgaben.

Weitere allgemeine Richtlinien behandeln beispielsweise die Themen

- ISO/ IEC 27003: Anleitung zur Umsetzung,
- ISO/ IEC 27004: Messungen,
- ISO/ IEC 27005: Risikomanagement und
- ISO/ IEC 27007: Audits.

Darüber hinaus existieren branchen- und themenspezifische Richtlinien, z. B. ISO/ IEC 27011 Information security management guidelines for telecommunications organizations based on ISO/ IEC 27002. Diese Zusammenhänge sind in der Abbildung 6 dargestellt.

Die nationale Norm DIN SPEC 27009 (siehe Kapitel 4.2.1) wurde im Juni 2012 mittels Fast Track bei JTC 1 als ISO/ IEC TR 27019 Information security management guidelines based on ISO/ IEC 27002 for process control systems specific to the energy market eingebracht. Die englische Übersetzung der DIN SPEC 27009 ist als ISO/ IEC DTR 27019 verabschiedet.

4.1.1.2 IEC 62443 – Industrial communication networks – Network and system security

Die Normenreihe IEC 62443 wird von der Arbeitsgruppe 10 des Technischen Komitees 65 IEC TC 65 WG 10) erstellt. Das nationale Spiegelgremium ist bei der Deutschen Kommission Elektrotechnik Elektronik Informationstechnik (DKE) im Gremium DKE UK 931.1.

Die Normenreihe IEC 62443 Industrial communication networks – Network and system security setzt auf ein prozessorientiertes Vorgehensmodell zur Herstellung von IT-Sicherheit für die industrielle Automatisierung und Kontrollsysteme (IACS: Industrial automation and control systems) [BMWi 2009]. Sie spezifiziert die Inhalte eines Cybersicherheitsmanagementsystems (CSMS) und gibt Hinweise für die Vorgehensweise zur Entwicklung eines CSMS. Die Norm richtet sich an Hersteller, Integratoren und Betreiber.

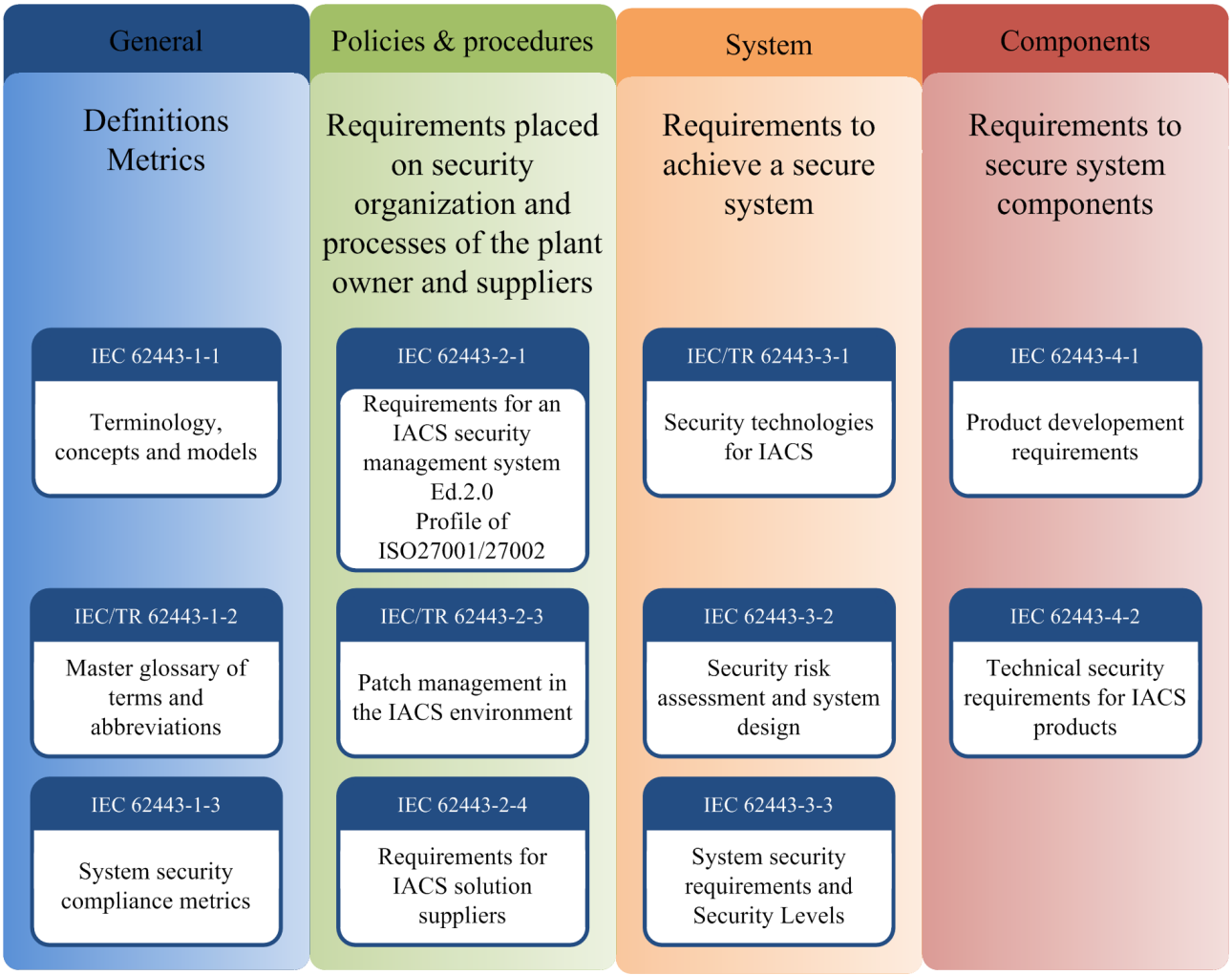


Abbildung 7: Übersicht IEC 62443

Die Entwicklung der IEC 62443-Normenreihe wird seit 2009 zusammen mit der ISA vorangetrieben. Die ISA ist das Industrial Automation and Control System Security Komitee der International Society of Automation (ISA; http://isa99.isa.org). Sie veröffentlicht Standards, Best Practices und technische Berichte, die Vorgehensweisen zur sicheren Implementierung von ICS sowie zur Bewertung von Sicherheitsmaßnahmen definieren.

4.1.1.3 IEC 62351 – Power systems management and associated information exchange – Data and communication security

Die Norm IEC 62351 [IEC 62351] wird von der Arbeitsgruppe 15 des technischen Komitees 57 (IEC TC 57 WG 15) erarbeitet und befasst sich auf technischer Ebene mit der Absicherung der in der Energietechnik eingesetzten Kommunikationsprotokolle. Ziel ist die Entwicklung von Sicherheitsmaßnahmen für die von IEC TC 57 entwickelten Kommunikationsprotokolle, insbesondere für die Normenreihe IEC 60870-5, IEC 60870-6, IEC 61850, IEC 61970 und IEC 61968. Die Norm richtet sich in erster Linie an die Mitglieder der Arbeitsgruppen, die die entsprechenden Kommunikationsprotokolle entwickeln. Zudem sind die Hersteller von Produkten, die diese Kommunikationsprotokolle implementiert haben, Zielgruppe der Norm. Abbildung 8 zeigt die Struktur der Norm und den Bezug zu verschiedenen Kommunikationsstandards.

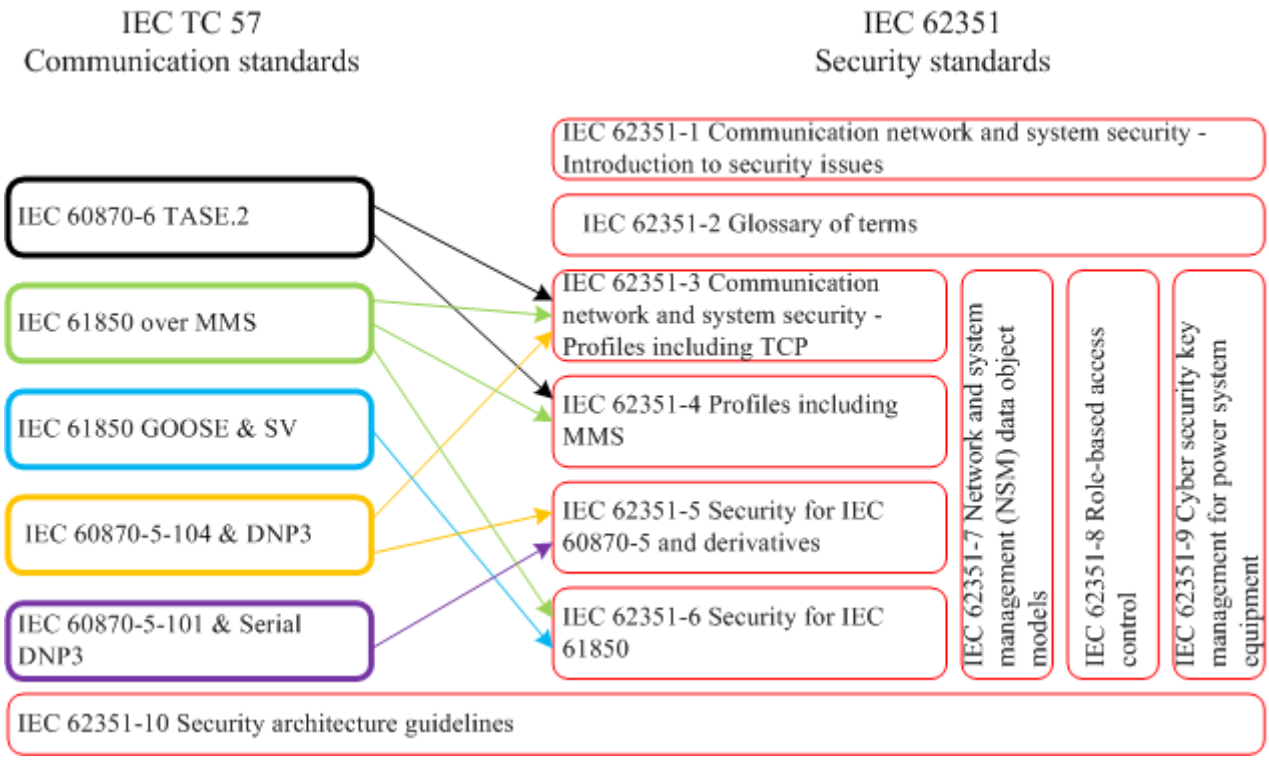


Abbildung 8 Zuordnung IEC 62351-Teile zu Protokollen und Standards (entnommen aus [Cleveland 2012]

4.2 Nationale Standards und Handreichungen

4.2.1 DIN

Das Deutsche Institut für Normung e. V. (DIN, http://www.din.de) ist die bekannteste nationale Normungsorganisation in Deutschland.

4.2.1.1 DIN SPEC 27009 - Leitfaden für das Informationssicherheits- Management von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/ IEC 27002

Die DIN SPEC 27009 beschreibt einen Umsetzungsleitfaden für ein sektorspezifisches Informationssicherheits-Managementsystem analog zur ISO/IEC 27001 zur Anwendung in der Netzleittechnik in der Energieversorgung. Die Maßnahmen aus der ISO/IEC 27002 wurden um sektorspezifische Anforderungen ergänzt.

Sie wird beim DIN vom Normenausschuss (NA) 043 „Informationstechnik und Anwendungen“ (NIA) im Arbeitsgremium NA 043-01-27-01 AK - „Anforderungen, Dienste und Richtlinien für IT Sicherheitssysteme“ betreut (vgl. [DIN SPEC 27009 2013]).

Die Norm richtet sich primär an die Betreiber von Prozesssteuerungssystemen der Energieversorgung sowie an die zuständigen Informationssicherheitsverantwortlichen. Darüber hinaus ist die Norm für Hersteller, Integratoren und Auditoren von Interesse. Im Fokus der Norm sind Systeme und Netze zur Steuerung und Überwachung von Erzeugung, Übertragung und Verteilung von Strom, Gas und Wärme in Kombination mit der Steuerung von unterstützenden Prozessen. Dies umfasst

- die Leit- und Automatisierungssysteme,
- die Schutz- und Safetysysteme sowie
- die Messtechnik inklusive der zugehörigen Kommunikations- und Fernwirktechnik.

Zusammenfassend werden diese Systeme Prozesssteuerungssysteme genannt [DIN SPEC 27009 2012]. Der Aufbau der DIN SPEC 27009 erfolgt analog zur ISO/ IEC 27002 [TeleTrusT 2012]:

1. Bei unveränderter Übernahme der Maßnahmen (Controls) erfolgt ein Verweis auf den ISO/IEC 27002-Abschnitt.
2. Bei Erweiterung der entsprechenden Maßnahmen gilt der ursprüngliche ISO/ IEC 27002-Inhalt mit zusätzlichen spezifischen Inhalten in den Kategorien
3. Umsetzungsanleitung für die Energieversorgung
4. weitere Informationen für die Energieversorgung
5. Ergänzende Maßnahmenziele und Controls wurden in den entsprechenden ISO/IEC 27002-Kapiteln eingefügt.
6. Im Anhang erfolgt ein Verweis auf das BDEW-Whitepaper (siehe 4.2.4.1) und ein Abgleich der Maßnahmen der DIN SPEC 27009 auf die entsprechenden Sicherheitsanforderungen des Whitepapers.

Folgende Inhalte deckt die DIN SPEC 27009 ab. Zusätzlich ist die Anzahl der branchenspezifischen Erweiterungen im Vergleich zur ISO/ IEC 27002 angegeben:

- Kapitel 5 – Sicherheitsleitlinie: keine Erweiterungen,
- Kapitel 6 – Organisation der Informationssicherheit: 5 Erweiterungen,
- Kapitel 7 – Management von organisationseigenen Werten: 3 Erweiterungen,
- Kapitel 8 – Personalsicherheit: 3 Erweiterungen,
- Kapitel 9 – Physische und umgebungsbezogenen Sicherheit: 11 Erweiterungen,
- Kapitel 10 – Betriebs- und Kommunikationsmanagement: 9 Erweiterungen,
- Kapitel 11 – Zugangskontrolle: 6 Erweiterungen,
- Kapitel 12 – Beschaffung, Entwicklung und Wartung von Informationssystemen: 2 Erweiterungen,
- Kapitel 13 – Umgang mit Informationssicherheitsvorfällen: keine Erweiterungen,
- Kapitel 14 – Sicherstellung des Geschäftsbetriebs: 2 Erweiterungen und
- Kapitel 15 – Einhaltung von Vorgaben – 1 Erweiterung.

4.2.2 VDI, VDE und DKE

Der Verein Deutscher Ingenieure e.V. (VDI; http://www.vdi.de) ist eine Vereinigung von Ingenieuren, Naturwissenschaftlern und Informatikern in Deutschland, die unter anderem bei Normierungen unterstützt. Der Verband der Elektrotechnik Elektronik Informationstechnik e.V. (VDE; http://www.vde.com) ist ein technisch-wissenschaftlicher Verband der Elektrotechnik und Elektronik.

Die Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN (siehe 4.2.1) und VDE erarbeitet Standards zu den Themen Elektrotechnik, Elektronik und Informationstechnik. Die DKE (http://www.dke.de) wird vom VDE getragen und ist ein Normenausschuss im DIN. Die DKE ist ebenfalls Mitglied im IEC und CENELEC. Ferner ist die DKE die für Deutschland zuständige Nationale Normungsorganisation (NSO) des Europäischen Institut für Telekommunikationsnormen (ETSI).

4.2.2.1 VDI/ VDE – Richtlinie 2182 Informationssicherheit in der industriellen Automatisierung

Der VDI und der VDE beschreiben in der Richtlinie 2182 ein Vorgehensmodell zur Umsetzung konkreter Schutzmaßnahmen mit praxisnahen Beispielen. Durch den prozessorientierten, zyklischen Ansatz wird der gesamte Lebenszyklus und die Zusammenarbeit von Herstellern, Integratoren und Betreibern berücksichtigt. Dies gilt im speziellen für den Informationsaustausch zwischen den drei Parteien.

Die Richtlinie wurde vom Fachausschuss FA 5.22 Security der VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA) erarbeitet und setzt sich aus sechs Blättern zusammen. In Blatt 1 Informationssicherheit in der industriellen Automatisierung - Allgemeines Vorgehensmodell wird die grundlegende Vorgehensweise erläutert. Es besitzt folgenden Inhalt:

- Anwendungsbereich,
- Begriffe,
- Methodik,
  - Abhängigkeiten,
  - Rollen,
  - Strukturanalyse,
  - Anlass,
  - Dokumentation und
- Vorgehensbeschreibung [VDI 2182 2011].

Ein wichtiger Aspekt beim Entwurf war neben der Verzahnung der drei Lebenszyklen, eine Verschlankung der Ansätze aus ISO 27000 und IT-Grundschutz.Abbildung 9 stellt die Vorgehensbeschreibung grafisch dar (vgl. [VDI 2182 2011]).

Beispiele zur Anwendung aus unterschiedlichen Blickwinkeln der Hersteller, Integratoren und Betreiber werden in den folgenden Blättern erläutert (vgl. [VDI/VDE Richtlinien 2013]):

- VDI/ VDE 2182 Blatt 2.1 Informationssicherheit in der industriellen Automatisierung - Anwendungsbeispiel des Vorgehensmodells in der Fabrikautomation für Hersteller - Speicherprogrammierbare Steuerung (SPS),
- VDI/ VDE 2182 Blatt 2.2 Informationssicherheit in der industriellen Automatisierung - Anwendungsbeispiel des Vorgehensmodells in der Fabrikautomation für Maschinen- und Anlagenbauer – Umformpresse,

- VDI/ VDE 2182 Blatt 3.1 Informationssicherheit in der industriellen Automatisierung - Anwendungsbeispiel des Vorgehensmodells in der Prozessautomation für Hersteller - Prozessleitsystem einer LDPE-Anlage,

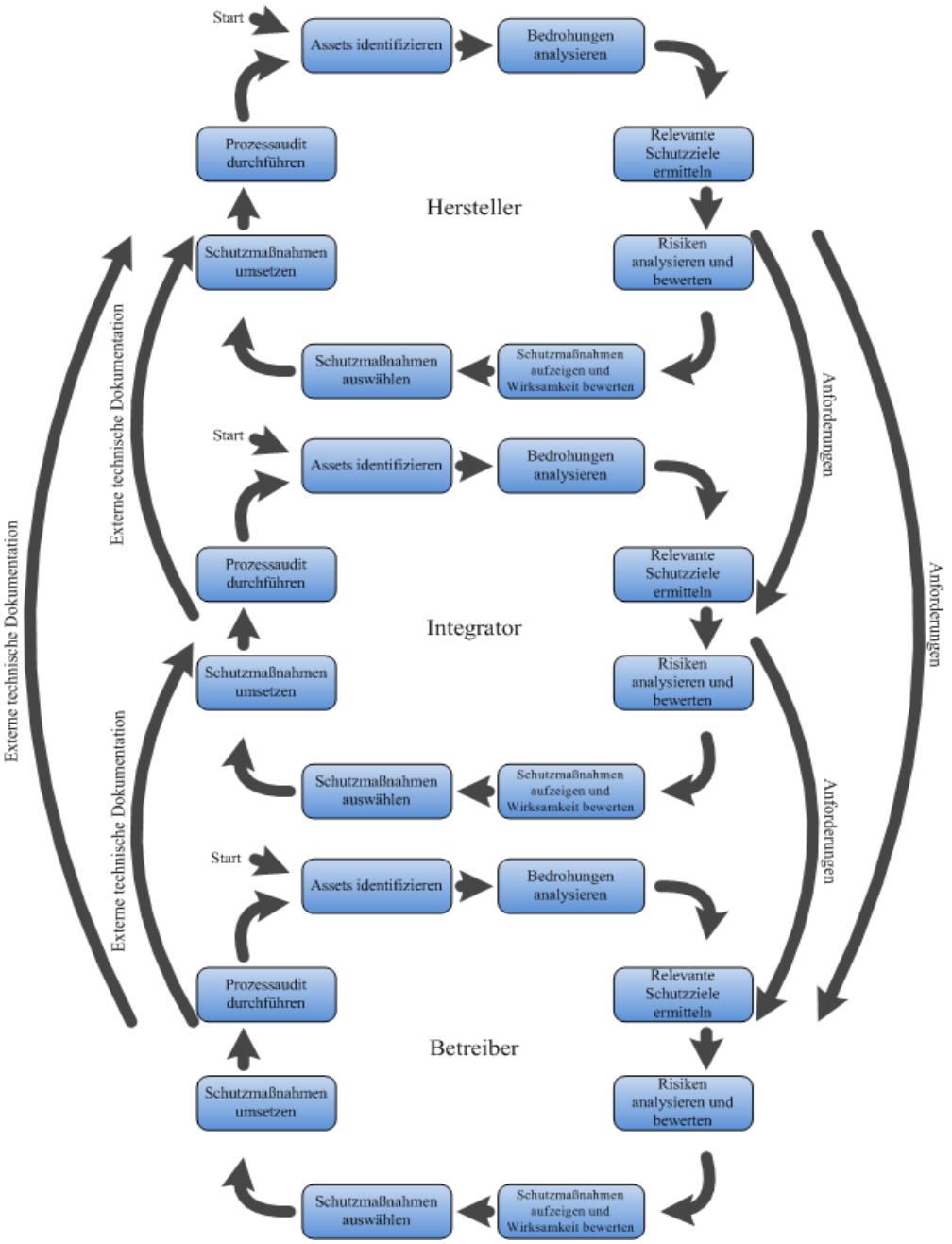


Abbildung 9 Vorgehen nach VDI/VDE 2182 in Anlehnung an [VDI 2182 2011]

- VDI/ VDE 2182 Blatt 3.2 Informationssicherheit in der industriellen Automatisierung - Anwendungsbeispiel des Vorgehensmodells in der Prozessautomation für Integratoren – LDPE[2] -Reaktor sowie
- VDI/ VDE 2182 Blatt 3.3 Informationssicherheit in der industriellen Automatisierung - Anwendungsbeispiel des Vorgehensmodells in der Prozessautomation für Betreiber – LDPE-Anlage.

2 Low-Density-Polyethylen; deutsch: Weich-Polyethylen

4.2.3 NAMUR

Die Normenarbeitsgemeinschaft für Meß- und Regeltechnik in der chemischen Industrie (NAMUR, http://www.namur.de) ist ein internationaler Verband der Anwender von Automatisierungstechnik in der Prozessindustrie. Zu den Tätigkeiten gehört unter anderem die Mitwirkung bei der nationalen und internationalen Normung.

4.2.3.1 NA 115 IT-Sicherheit für Systeme der Automatisierungstechnik

NAMUR veröffentlichte im Jahr 2006 das Arbeitsblatt 115 [NA 115 2006], welches die Randbedingungen der Automatisierungstechnik für IT-Sicherheitsprodukte aus Anwendersicht beschreibt. Das Arbeitsblatt richtet sich zum einen an Hersteller, die bei dem Entwurf neuer Systeme die spezifischen Randbedingungen in der Prozessindustrie berücksichtigen sollen. Zum anderen sollen Integratoren Sicherheitsmechanismen gemäß diesen Gegebenheiten umsetzen. Außerdem sollen Anwender die Kriterien aus dem Dokument für zukünftige Kaufentscheidungen heranziehen können. Nach einer Unterscheidung der Schutzziele zwischen klassischer IT und der Automatisierungstechnik werden grundlegende Maßnahmen zur Absicherung bestehender Systeme diskutiert. Im anschließenden Kapitel werden die wichtigsten Anforderungen für die Entwicklung zukünftiger Systeme erläutert. Dabei sind die einzelnen Kriterien kurz und allgemeingültig formuliert.

4.2.4 BDEW

Im Bundesverband der Energie- und Wasserwirtschaft e.V. (BDEW, http://www.bdew.de) sind ca. 1800 Unternehmen organisiert. Er vertritt die Anliegen seiner Mitglieder gegenüber Politik, Fachwelt, Medien und Öffentlichkeit.

4.2.4.1 BDEW-Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme

Für die Unternehmen der Energiewirtschaft wurde 2008 ein Whitepaper mit grundsätzlichen Sicherheitsmaßnahmen für Steuerungs- und Telekommunikationssysteme mit Bezug zur ISO/ IEC 27002 (siehe Kapitel 4.1.1) veröffentlicht. Ziel ist es dabei, die Systeme gegen Sicherheitsbedrohungen im täglichen Betrieb angemessen zu schützen. Die in dem Whitepaper festgelegten Sicherheitsmaßnahmen werden für alle neuen Steuerungs- oder Telekommunikationssysteme empfohlen. Hiermit verfolgt das Whitepaper das strategische Ziel, die Produktentwicklung hinsichtlich der Sicherheitsaspekte positiv zu beeinflussen und ein gemeinsames Verständnis in der Branche für den Schutz dieser Systeme zu vermitteln. Sicherheitsanforderungen werden sowohl für den Betreiber als auch für den Hersteller definiert.

In der Planungsphase eines neuen Steuerungs- oder Telekommunikationssystems ist möglichst frühzeitig eine Schutzbedarfsfeststellung durchzuführen. Der Prozess zur Durchführung einer Schutzbedarfsfeststellung ist beispielsweise in [BSI100-1] und [BSI 100-2] beschrieben. Ergibt sich ein normaler Schutzbedarf, so ist die Umsetzung der Anforderungen des Whitepapers ausreichend. Im Falle eines hohen oder sehr hohen Schutzbedarf es ist eine ergänzende Risikoanalyse erforderlich.

Im Fokus des Whitepapers sind Anforderungen an Systeme und Komponenten sowie an die entsprechenden Entwicklungs- und Wartungsprozesse. Das Whitepaper ist in erster Linie für Ausschreibung vorgesehen. Nach Ende der planerischen Phase werden die ermittelten endgültigen Sicherheitsanforderungen mit den folgenden Unterlagen in das Lastenheft integriert:

- eine Kopie des aktuellen Whitepapers
- ggf. konkretisierte Anforderungen und zusätzliche Maßnahmen sowie Umsetzungsvorgaben aus den Ergebnissen der Risikoanalyse

- den zulässige Ausnahmen oder Workarounds [BDEW 2008].

Für folgende Themen werden Sicherheitsanforderungen definiert:

- Allgemeines/Organisation,
- Basissystem,
- Netze/Kommunikation,
- Anwendung,
- Entwicklung, Test und Rollout sowie
- Datensicherung/-wiederherstellung und Notfallplanung.

4.2.4.2 Anforderungen an sichere Steuerungs- und Telekommunikationssysteme: Ausführungshinweise zur Anwendung des BDEW-Whitepaper

Oesterreichs Energie und der BDEW haben 2012 gemeinsam einen Praxisleitfaden zum Whitepaper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“ veröffentlicht. Ziel der Ausführungshinweise ist es, zu den einzelnen Anforderungen des BDEW-Whitepapers Umsetzungsbeispiele und Anwendungshinweise für die unterschiedlichen Technologiebereiche im Bereich der Prozesssteuerung in der Energieversorgung zu geben. Die Ausführungshinweise dienen dabei als Ergänzung zu den Anforderungen des BDEW-Whitepapers [OE BDEW 2012].

4.2.5 VGB

Der VGB PowerTech e.V. (Verband der Großkraftwerks- Betreiber, VGB; http://www.vgb.org) ist ein europäischer Fachverband für Strom- und Wärmeerzeugung und ein freiwilliger Zusammenschluss von Unternehmen, für die die Strom- und Wärmeerzeugung und somit der Kraftwerksbetrieb und die dazugehörige Technik eine wichtige Grundlage sind.

4.2.5.1 Richtlinie R175: IT-Sicherheit für Erzeugungsanlagen

Die 2006 erschienene Richtlinie [VGB R 175] des VGB soll Kraftwerksbetreibern Hinweise und Empfehlungen zur Verbesserung der IT-Sicherheit geben. Dazu werden in den einführenden Kapiteln grundlegende Begriffe aus der IT-Sicherheit erläutert und typische Bedrohungen aus dem Kraftwerksbetrieb beschrieben. Um diesen Bedrohungen zu begegnen, wird in nachfolgenden Kapiteln eine Sammlung an Best-Practices aus organisatorischen und technischen Maßnahmen zur Verfügung gestellt. Die einzelnen Maßnahmen sind in unterschiedlicher Detailtiefe beschrieben.

Momentan wird die Richtlinie von einer VGB-Arbeitsgruppe überarbeitet. Nach der Überarbeitung wird sie unter dem Titel VGB – Standard S175 IT-Sicherheit für Erzeugungsanlagen veröffentlicht.

4.3 Ausländische Handreichungen

Dieser Abschnitt enthält ICS-spezifische Empfehlungen aus verschiedenen Ländern. Diese können als Informationsquelle dienen. Bei der Umsetzung der dort beschriebenen Maßnahmen sind die unterschiedlichen regulatorischen Vorgaben in diesen Ländern zu beachten. Für die Umsetzung in Deutschland können daher Anpassungen notwendig sein, um gesetzeskonform zu sein. Sie sollten daher als ergänzende Informationsquelle angesehen werden, die keinen normativen Charakter für Deutschland haben.

4.3.1 NERC

Die North American Electric Reliability Corporation (NERC, http://www.nerc.com) ist zuständig für die Koordinierung der elektrischen Stromnetze und die Gewährleistung der elektrischen Energieversorgung im nordamerikanischen Raum.

4.3.1.1 NERC CIP: Cyber Security Standards Critial Infrastructure Protection

Die Cyber Security Standards werden von NERC zum Schutz kritischer Infrastrukturen und mit dem Ziel entwickelt, die elektrische Stromversorgung sicherzustellen. Im Jahr 2006 wurde diese Critical Infrastructure Protection (CIP)-Reihe durch die Bestätigung der Federal Energy Regulatory Commission (FERC) für Nutzer und Betreiber von Stromnetzen in den USA, Kanada und Teilen von Mexiko verpflichtend. Die CIP-Standards setzen sich aus mehreren Dokumenten mit Anforderungen und Schutzmaßnahmen zu verschiedenen Themen zusammen und werden regelmäßig überarbeitet. Somit existieren diverse Revisionen jedes Standards. Die Standards behandeln folgende Themen [NERC CIP]:

- CIP-001 Sabotage Reporting
- CIP-002 Cyber Security - Critical Cyber Asset Identification
- CIP-003 Cyber Security - Security Management Controls
- CIP-004 Cyber Security - Personnel & Training
- CIP-005 Cyber Security - Electronic Security Perimeter(s)
- CIP-006 Cyber Security - Physical Security of Critical Cyber Assets
- CIP-007 Cyber Security - Systems Security Management
- CIP-008 Cyber Security - Incident Reporting and Response Planning
- CIP-009 Cyber Security - Recovery Plans for Critical Cyber Assets.

Jeder der Standards gliedert sich im Wesentlichen in die fünf Abschnitte Einleitung, Anforderungen, Maßnahmen, Compliance und regionale Unterschiede. Die Dokumente weisen dabei eine feste Struktur geprägt durch Aufzählungen auf.

4.3.2 NIST

Das National Institute of Standards and Technology (NIST, http://www.nist.gov) ist eine Bundesbehörde der Vereinigten Staaten die zuständig für Standardisierung ist.

4.3.2.1 SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations

NIST beschreibt in dem Entwurf der Special Publication 800-53 Rev. 4 [SP 800-53] aus dem Jahr 2012 Sicherheitsmechanismen für den Schutz von Informationssystemen der US-Behörden. Die US-Behörden sollen bei der Auswahl und Umsetzung angemessener Sicherheitsmechanismen durch ein Risikomanagement unterstützt werden, welches die Organisations-, Prozess- und Informationsebene betrachtet. Die definierten und empfohlenen Schutzmaßnahmen aus dem Dokument sollen somit im Rahmen eines Risiko-Management-Prozesses umgesetzt werden. Im Anhang I werden hierzu spezifische ICS-Sicherheitsmechanismen erläutert.

4.3.2.2 SP 800-82 Guide to Industrial Control Systems Security

Mit der Special Publication 800-82 [SP 800-82] aus dem Jahr 2011 stellt NIST Begriffsdefinitionen sowie Best Practices zur Umsetzung von Schutzmaßnahmen für einen sicheren Betrieb von ICS zur Verfügung und richtet sich somit an Betreiber und Integratoren. Nach einer grundlegenden Begriffsklärung und Funktionsbeschreibung von ICS-Komponenten werden typische Bedrohungen und Schwachstellen von ICS erläutert. Um den daraus resultierenden Risiken zu begegnen, werden anhand eines Business Cases die notwendigen Schritte zur Entwicklung eines ICS Security-Programms beschrieben. In nachfolgenden Kapiteln werden mögliche Schutzmaßnahmen mit Verweisen auf vertiefende NIST-Dokumente angeführt. Die Schutzmaßnahmen beinhalten streckenweise technisch sehr konkrete Empfehlungen, wie z. B. zu protokollspezifischen Firewall-Einstellungen.

4.3.2.3 NISTIR 7628 Guidelines for Smart Grid Cyber Security

Durch die Umstellung des Stromübertragungsnetzes in ein elektronisches Smart Grid sind gravierende Änderungen an der Infrastruktur vorgesehen. Dabei soll das herkömmliche, elektrische Netz zu einer dezentralen, digitalen Infrastruktur umgebaut werden, die eine Zwei-Wege-Kommunikation zur Übertragung von Information und zur Steuerung der ICS-Komponenten sowie der Verteilung des Stroms ermöglicht. Die aus dem Jahr 2010 stammenden Guidelines for Smart Grid Cyber Security [NISTIR 7628] stellen für beteiligte Organisationen, von Netzbetreibern über Hersteller von elektrischen Fahrzeugen und Aufladestationen, in einem dreiteiligen Bericht ein analytisches Framework zur Verfügung. Mithilfe dieses Frameworks sollen effektive Sicherheitsstrategien entwickelt werden, die zugeschnitten auf Smart Grid-Charakteristiken, -Risiken und -Schwachstellen des spezifischen Einsatzfeldes sind.

4.3.3 DHS

Die Hauptaufgabe des United States Department of Homeland Security (DHS, deutsch: Heimatschutzministerium, http://www.dhs.gov) ist der Schutz der amerikanischen Bevölkerung und Staatsgebiete vor terroristischen und anderen Bedrohungen.

Im Folgenden werden die wichtigsten Veröffentlichungen des DHS im Rahmen des Control Systems Security Program (CSSP) erläutert. Best Practices und Empfehlungen zur Absicherung von ICS-Anlagen finden sich unter http://us-cert.gov/control_systems/practices/Recommended_Practices.html .

4.3.3.1 Cyber Security Procurement Language for Control Systems

Die Cyber Security Procurement Language [DHS CSPL 2009] des DHS aus dem Jahr 2009 dient Betreibern von Automatisierungs- und Steuerungstechnik als Grundlage für Ausschreibungen. Der Fokus liegt hierbei auf IT-Sicherheitsmerkmalen, welche die Systeme der Hersteller erfüllen müssen. Langfristiges Ziel ist, IT-Sicherheit in den Lebenszyklus der Automatisierungs- und Steuerungstechnik zu integrieren. Im Dokument sind für grundlegende IT-Sicherheitsmerkmale (z. B. Systemhärtung, Auditing und Protokollierung, Firewall) von ICS-Komponenten Beispiele für Ausschreibungstexte formuliert, aus denen Betreiber konkrete Anforderungen ableiten können. Diese sollen in Verträge zwischen den Vertragspartnern einfließen und hierdurch ein ausreichendes Sicherheitsniveau in der Automatisierungs- und Steuerungstechnik sicherstellen.

4.3.3.2 Cyber Security Assessments of Industrial Control Systems

Der Good Practice Guide „Cyber Security Assessments of Industrial Control Systems“ [DHS Assessment 2010] des DHS und CPNI (siehe Kapitel 4.3.4 aus dem Jahr 2010 macht auf die Besonderheiten eines Security Assessments in ICS-Umgebungen aufmerksam. Zudem werden für Betreiber die Methodik und ein

Vorgehensmodell für die Durchführung eines ICS Security-Assessments vorgestellt. Nach einer knappen Einführung in die Unterschiede zwischen klassischen Penetrationstests und einem ICS-Assessment wird eine Vorgehensweise und der Ablauf eines solchen ICS-Assessments mit den einzelnen, erforderlichen Phasen erläutert. Hierbei nimmt der Punkt Reporting mit konkreten Beispielen einen wesentlichen Bestandteil des Kapitels ein. Im Folgenden werden Abhängigkeiten und mögliche Einflussfaktoren, welche den Umfang und die Art eines Assessment bestimmen, knapp erläutert (z. B. vorhandener Quelltext, Budget). Abschließend werden unterschiedliche Assessment-Methoden (z. B. Interviews, Dokumentenprüfung, technische Tests in der Produktionsumgebung oder Testumgebung) vorgestellt und diskutiert.

4.3.3.3 Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies

Die „Recommended Practice Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies“ [DHS DiD 2009] des DHS aus dem Jahr 2009 gibt Betreibern und Integratoren Hilfestellung bei der Entwicklung einer ganzheitlichen Abwehrstrategie. Anhand von prominenten Schwachstellen werden die Lösungsmöglichkeiten dargestellt. Dabei wird das Paradigma der „Defens-In-Depth“ dargestellt, den Schutz der Systeme schichtweise aufzubauen und so das Eindringen eines Angreifers zu erschweren.

4.3.3.4 Recommended Practice for Patch Management of Control Systems

Die „Recommended Practice for Patch Management of Control Systems“ [DHS PM 2008] des DHS aus dem Jahr 2008 soll Betreibern eine Hilfestellung bei der Entwicklung eines Patch Management -Programms für die Automatisierungs- und Steuerungstechnik geben. Dazu empfiehlt das DHS bewährte Praktiken für das Patch Management und deren Umsetzung in der Automatisierungs- und Steuerungstechnik. Nach einem kurzen Überblick über die wesentlichen Elemente eines Patch Management -Programms (z. B. Patch Management-Plan, Patch Testing) werden Methoden vorgestellt, anhand derer Schwachstellen und das resultierende Risiko bewertet werden können. Ein möglicher Handlungsbedarf kann schließlich von dem ermittelten Risikograd abgeleitet werden.

4.3.3.5 Recommended Practice for Securing Control System Modems

Die „Recommended Practice for Securing Control System Modems“ [DHS Modem 2008] des DHS aus dem Jahr 2008 beschreibt zum einen Methoden und Werkzeuge, um Modem-Verbindungen zu identifizieren und zu analysieren. Zum anderen werden überwiegend technische Maßnahmen empfohlen, um Modem-Verbindungen abzusichern.

4.3.3.6 Configuring and Managing Remote Access for Industrial Control Systems

Das Dokument „Configuring and Managing Remote Access for Industrial Control Systems“ [DHS Remote 2010] von DHS und CPNI (siehe Kapitel 4.3.4) aus dem Jahr 2010 gibt Betreibern und Integratoren Empfehlungen, wie ICS-Fernzugänge abgesichert werden können. Dazu werden die involvierten Rollen definiert und die Risiken anhand von Beispielen erläutert. Zudem werden Maßnahmen für die Absicherung und den Betrieb von Fernzugängen beschrieben.

4.3.3.7 Recommended Practices Guide For Securing ZigBee Wireless Networks in Process Control System Environments

Der Draft „Recommended Practices Guide For Securing ZigBee Wireless Networks in Process Control System Environments“ [DHS ZigBee 2007] des DHS aus dem Jahr 2007 soll Betreiber und Integratoren bei der sicheren Installation und dem Betrieb von ZigBee-Funknetzen im ICS-Umfeld unterstützen. Hierzu werden grundlegende Design-Prinzipien und Best Practices zu diesem Funkstandard vorgestellt. Das Dokument ist aus einer technischen Sicht geschrieben und behandelt neben grundlegenden Informationen zu dem Funkstandard wesentliche Design-Prinzipien sowie die verfügbaren Sicherheitsmechanismen. Hierbei werden konkrete Empfehlungen aus Best Practices ausgesprochen, wobei in einem eigenen Kapitel auf die Besonderheiten im ICS-Umfeld mit möglichen Lösungsansätzen hingewiesen wird.

4.3.3.8 Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability

Betreiber von ICS-Anlagen werden in der „Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability“ [DHS IR 2009] des DHS aus dem Jahr 2009 bei der Entwicklung von Prozessen für die Behandlung von Sicherheitsvorfällen angeleitet. Darin spricht das DHS Empfehlungen aus, wie Betreiber von ICS-Anlagen sich auf Sicherheitsvorfälle vorbereiten und darauf reagieren können. Hierzu zählen beispielsweise die Analyse des Vorfalls und das Wiederherstellen der Betriebsumgebung nach Sicherheitsvorfällen. Die Inhalte sind allgemein gehalten, sodass an vielen Stellen auf weiterführende Literatur verwiesen wird, wobei Besonderheiten von ICS hervorgehoben werden.

Das Dokument gliedert sich in die folgenden vier Hauptkapitel:

- Cyber Incident Response Planning,
- Incident Prevention,
- Incident Management und
- Postincident Analysis and Forensics.

4.3.3.9 Catalog of Control Systems Security: Recommendations for Standards Developers

Da branchenspezifische Standards durch ihre Schwerpunkte nicht immer konsistent untereinander und vergleichbar z. B. hinsichtlich des Detaillierungsgrads sind, versucht dieser umfangreiche Katalog [DHS Standards 2009] des DHS aus dem Jahr 2009 eine Auswahl an bewährten, branchenunabhängigen Schutzmaßnahmen für ICS anzubieten, welche die Unterschiede der Standards deutlich werden lassen. Damit soll der Katalog Normungsgremien bei der Entwicklung von branchenspezifischen Standards unterstützen. Darüber hinaus soll der Katalog den Betreibern von ICS als Framework für die Entwicklung eines Cybersecurity-Programms dienen. So sollen die Maßnahmen aus dem Katalog bei der Umsetzung von Best-Practices, Richtlinien und Standards für ICS berücksichtigt werden.

4.3.3.10 Using Operational Security OPSEC to Support a Cyber Security Culture in Control Systems Environments

Der Draft in der Version 1.0 [DHS OPSEC 2007] des DHS aus dem Jahr 2007 richtet sich an Manager und IT-Sicherheitsspezialisten, welche bei der Entwicklung eines Operational Security (OPSEC) Programms für die Automatisierungs- und Steuerungstechnik unterstützt werden sollen. Durch Methoden aus der operationellen Sicherheit sollen Prozesse und Richtlinien erarbeitet werden, welche die Sicherheit im alltäglichen Betrieb erhöhen und eine Kultur für Cybersicherheit fördern. Hierzu werden wesentliche

Schlüsselelemente der Cybersicherheit von Automatisierungs- und Steuerungstechnik (z. B. Access Control, Risk Assessment, Compliance) knapp beschrieben und es wird erläutert, wie diese Elemente den Aufbau einer sicherheitssensibilisierten Kultur im Betrieb fördern können. Hierbei unterstützt das Empfehlungspapier bei der Entwicklung von operationellen Sicherheitsstrategien wie beispielsweise der Erstellung eines OPSEC-Plans und dem Einbringen von Sicherheitsaspekten in den betrieblichen Lebenszyklus. Das Dokument behandelt die Themen auf einer abstrakten Ebene und ersetzt somit keine branchenspezifischen Sicherheitsstandards.

4.3.3.11 Personnel Security Guidelines

Das Ziel der „Personnel Security Guidelines“ [DHS Personnel 2004] des DHS aus dem Jahr 2004 ist es, Hilfestellung bei Auswahl, Vorbereitung und Sensibilisierung von Personal zu geben. Hierzu werden konkrete Maßnahmen aufgeführt, welche das Personal angemessen auf ihre Arbeit in einem ICS-Betrieb vorbereiten und die notwendige Sensibilisierung (Awareness) für Sicherheit fördern sollen. Aus diesen Empfehlungen können betriebsspezifische Maßnahmen abgeleitet werden. Die Empfehlungen zu personalbezogener Sicherheit sind in folgende drei Themenbereiche untergliedert:

- Vertrauenswürdigkeit (Trustworthiness),
- Tauglichkeit (Capability) und
- Sicheres Umfeld (Secure Environment).

Die vorgeschlagenen Maßnahmen sind knapp als Anforderung formuliert und häufig um Listen mit Beispielen oder zu berücksichtigenden Punkten ergänzt. Es sind hierbei ggf. unterschiedliche rechtliche Rahmenbedingungen zwischen den USA und Deutschland zu beachten.

4.3.4 CPNI Großbritannien

Das Centre for the Protection of National Infrastructure (CPNI, http://www.cpni.gov.uk) ist eine Behörde von Großbritannien, deren Aufgabe es ist, die kritischen Infrastrukturen zu schützen. Dazu werden Empfehlungen zur physischen und personellen Sicherheit sowie Cyber-Sicherheit gegeben.

4.3.4.1 Good Practice Guide – Process Control and SCADA Security

Mit dem Good Practice Guide aus dem Jahr 2008 [CPNI 2008] beabsichtigt das CPNI für Betreiber von ICS bewährte, grundlegende Prinzipien der IT-Sicherheit für die Leittechnik zur Verfügung zu stellen. Hierzu wird ein Framework vorgestellt, welches die folgenden sieben Themengebiete umfasst:

- Understand the business risks,
- Implement secure architecture,
- Establish response capabilities,
- Improve awareness and skills,
- Manage third party risks,
- Engage projects,
- Establish ongoing governance.

Zu jedem Themengebiet existiert ein eigenes Dokument, in dem in abstrakter Form Empfehlungen gegeben und die jeweiligen Grundprinzipien zur Anwendung erläutert werden.

4.3.4.2 Good Practice Guide – Firewall Deployment for SCADA and Process Control Networks

Das CPNI spricht in dem 2005 erschienenen Good Practice Guide [CPNI 2005] Empfehlungen für Firewall-Architekturen, die Konfiguration und das Management von Firewalls zur Absicherung von ICS aus und richtet sich damit an Betreiber. Hierzu werden die unterschiedlichen Firewall-Komponenten und Technologien beschrieben und grundlegende Architekturen miteinander verglichen und bewertet. Des Weiteren werden bis auf Protokollebene Hinweise für ein sicheres Firewall-Regelwerk gegeben und Lösungen für mögliche Problemfälle vorgeschlagen sowie grundlegende Tätigkeiten zum Management der Komponenten beschrieben.

4.3.5 IEEE

Das Institute of Electrical and Electron ics Engineers IEEE; http://www.ieee.org ist der weltweit größte Berufsverband von Ingenieuren und Informatikern.

4.3.5.1 IEEE 1686-2007 - IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities

Der IEEE-Standard definiert Sicherheitsfunktionen, die von IED bereitgestellt werden sollen. Der Standard richtet sich an Hersteller von IED.

5 Best Practice Guide für Betreiber

Dieses Kapitel gibt einen Überblick über einige architektonische, technische und organisatorische Best Practices für die Betreiber von ICS. Diese Best Practices stellen eine Sammlung von sinnvollen Maßnahmen dar, welche sich zum einen in der Praxis bewährt haben und sich zum anderen aus den vorhandenen Standards ISO 27000/IT-Grundschutz, IEC 62443 und VDI 2182 ableiten lassen. Diese sind zu den Best Practices in Bezug gesetzt.

Die Ausführungen in diesem Kapitel adressieren die Aspekte möglichst breit. Daher wird auf detaillierte technische Darstellungen verzichtet.

An dieser Stelle soll betont werden, dass die hier beschriebenen Best Practices nur den Einstieg in einen geordneten IT-Sicherheitsprozess innerhalb eines ICS bzw. eines ganzen Unternehmens ermöglichen sollen. Ziel sollte es sein, ein funktionierendes Informationssicherheitsmanagement auf Basis von ISO27000, IT-Grundschutz oder IEC62443 aufzubauen.

Bei der Umsetzung der beschriebenen Maßnahmen ist zu beachten, dass insbesondere folgende Maßnahmen als erstes umgesetzt werden sollten:

- 1 Aufbau einer Security-Organisation
- 2 Erstellen und Pflegen der Dokumentation
- 3 Etablieren eines Security Managements
- 4 Netzplan
- 5 Liste der IT-Systeme und installierten Anwendungen
- 6 Administrations- und Benutzerhandbücher

Diese dienen dazu, einen Überblick über die eigenen Systeme und die Infrastruktur zu erhalten, Verantwortlichkeiten zu definieren und sich der bestehenden Risiken bewusst zu werden. Für die Erfassung der Bestandsdaten kann auch auf die in Kapitel 6 beschriebene Methodik für Audits zurückgegriffen werden, da dort viele der relevanten Fragestellungen aufgegriffen werden.

Die Risiken und die sich daraus ableitenden Schutzmaßnahmen sind für jede ICS-Installation individuell. Dennoch gibt es aufgrund der bisherigen Erfahrungen mit ICS Best Practices, deren Umsetzung geeignet ist, um das IT-Sicherheitsniveau des ICS zu erhöhen und der aktuellen Bedrohungslage gerecht zu werden. Für eine angemessene Auswahl und Umsetzung der Maßnahmen ist eine individuelle Risikoanalyse jedoch zwingend notwendig (vgl. Kapitel 1.2).

Eine Umsetzung aller Maßnahmen ohne Betrachtung der bestehenden Risiken, kann dazu führen, dass Maßnahmen umgesetzt werden, die nicht notwendig sind oder die Gefährdungen nicht betrachtet werden.

Bei der Umsetzung der Maßnahmen kann es aufgrund der Betriebsgröße und der Organisationsform ebenfalls zu gewissen Abweichungen kommen oder zu der Entscheidung, dass eine Maßnahme nicht umgesetzt wird. Hier muss auf Aufwand, Nutzen und das verbleibende Risiko in Relation gesetzt werden. Es sollte sich hierbei jedoch um eine bewusste Entscheidung handeln, bei der man die verbleibenden Risiken ausdrücklich eingeht.

Bei der Vorgehensweise sollte darauf geachtet werden, dass als erstes ein definierter Prozess für das Thema Security etabliert wird. Danach sollte ein geeigneter Perimeterschutz erfolgen, sowie mehrschichtige Sicherheitsmaßnahmen auf Netzwerkebene. Im Anschluss sollte der Schutz auf den Komponenten selbst verbessert werden. Bei neuen Anlagen sollte dies bereits in der Planung berücksichtigt werden.

Im den folgenden Abschnitten ab 5.2 werden die Best Practices inhaltlich gruppiert und nummeriert dargestellt.

5.1 Grundsätzliches Vorgehen im Engineering-Prozess

Da große Teile von ICS individuell nach den Anforderungen des jeweiligen materiellen Produktionsprozesses gestaltet werden, kommt den zugehörigen Engineering-Prozessen entscheidende Bedeutung zu. Grundsätzliche Vorgehensweisen sind in internationalen Standards wie z.B. IEC 62337 (Milestones) oder IEC 62382 (Loopcheck) fixiert.

Darüber hinaus existieren anwendungsspezifische Vorgaben wie EN 50156 (Feuerungsanlagen), EN 61511 (verfahrenstechnische Anlagen) oder EN ISO 13849 (Maschinen) zur Ausgestaltung der Engineering Prozesse für den Bereich der Sicherheitstechnik.

Im Bereich der IT Security gibt die IEC 62443 Hinweise zu Aspekten der IT Security im Hinblick auf ICS. Darüber hinaus existieren in Form des BDEW Whitebooks „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“ (Kapitel 4.2.4.1) und der VDI/VDE 2182 „Informationssicherheit in der industriellen Automatisierung“ (Kapitel 4.2.2.1) branchenspezifische Festlegungen.

Der Grundtenor dieser Dokumente gestaltet sich im Hinblick auf die IT Security wie folgt:

1. Festlegung, welche Betrachtungseinheiten untersucht werden sollen und welche Bedrohungen für die jeweilige Betrachtungseinheiten relevant sind.

   Beispiel:

   > Ist eine Anlage mit einem Kran zur Ausführung von Wartungsarbeiten ausgestattet, so ist zu prüfen ob und in welchem Umfang die Kransteuerung einer Betrachtung bzgl. IT-Security unterzogen werden muss.

   Es ist zu fixieren, welche Bedrohungen für eine Anwendung bedeutsam sind. Eine ICS Applikation ohne Fernwartungszugang braucht z. B. nicht hinsichtlich möglicher diesbezüglicher Konsequenzen bewertet zu werden. Allerdings muss sichergestellt sein, dass z. B. die temporäre Einrichtung eines solchen Zuganges spätestens unmittelbar vor deren Einrichtung betrachtet wird.

2. Festlegen, welche Risiken aus den Bedrohungen abzuleiten sind

   Die ungewollte Veröffentlichung von Prozessdaten ist z. B. in einer Pharmaanwendung anders zu bewerten, als in einer Kläranlage.

3. Festlegen, welche Maßnahmen zur Risikoabwehr getroffen werden (können)

   Bei der Festlegung dieser Maßnahmen sind der wirtschaftlich vertretbare Rahmen und – speziell bei Bestandsanlagen – die technisch möglichen Maßnahmen zu definieren. Ggf. ist hier ein spezifischer Iterationsprozess erforderlich um Wünsche, resultierende Anforderungen und notwendige Maßnahmen aufeinander abzustimmen.

   Beispiel:

   > Viele ICS benötigen aus funktionaler Sicht keinen permanenten Anschluss an das Internet oder Intranet. Ein diesbezüglicher Verzicht kann helfen, IT-Security Risiken zu minimieren.

4. Umsetzen dieser Maßnahmen auf allen Ebenen des ICS (Defence in Depth)

   Die getroffenen Maßnahmen müssen auf allen Ebenen des ICS umgesetzt werden. Dabei gilt, dass die Wirksamkeit des Gesamtpaketes sowohl von den Einzelmaßnahmen, als auch von der Staffelung dieser abhängt.

5. Regelmäßige Kontrolle der getroffenen Maßnahmen auf Einhaltung und Wirksamkeit

Ziel dieser Kontrollen (Audits) ist es sicher zu stellen, dass einerseits getroffene Maßnahmen während der gesamten Nutzungsdauer eines ICS eingehalten werden. Darüber hinaus ist zu verifizieren, dass die getroffenen Maßnahmen hinreichend wirksam sind. Diese Überprüfungen haben bezogen auf die IT Security von ICS besondere Bedeutung, da sich diesbezügliche Bedrohungs-Szenarien häufig ändern können.

VDI/VDE 2182 beschreibt einen diesbezüglichen umfassenden Prozess nebst Art und Umfang des Informationsaustauschs und den dabei zu beteiligenden Stellen (Gerätehersteller, Systemintegratoren und Betreiber).

5.2 Einstieg

1. Aufbau einer Security-Organisation

Der Betreiber sollte eine Security-Organisation aufbauen, welche die Rollen und Verantwortlichkeiten für die IT-Security von ICS-Komponenten regelt. Dabei sollte die Security-Organisation alle an dem Betrieb von ICS-Komponenten beteiligten Parteien berücksichtigen (z. B. Hersteller, Outsourcing-Partner, Drittanbieter, Spezialisten für die physische Sicherheit, Produktions- und Instandhaltungsleiter).

Das Management sollte sich zu dem Security-Programm bekennen.

Für Anlagen und Komponenten sollten Verantwortliche bestimmt werden. Es hat sich als sinnvoll erwiesen, Verantwortliche für bestimmte Systemgruppen oder Netzbereiche zu bestimmen, beispielsweise aufgeteilt nach den einzelnen Führungsebenen (siehe Abbildung 3).

Es sollte eine enge Kooperation zwischen den ICS- und den IT-Security-Experten stattfinden, um gegenseitig voneinander zu profitieren, ein gemeinsames Ziel zu verfolgen und Fehlplanungen zu vermeiden.

2. Erstellen und Pflegen der Dokumentation

Dokumente und Informationen zur IT-Security von ICS-Komponenten (z. B. Risiko- und Schwachstellenanalysen, Netzpläne, Netzmanagement, Konfiguration, Security-Programm und -Organisation) sollten in Lieferantenvorgaben enthalten sein, erstellt, gepflegt und ausreichend vor unbefugtem Zugriff geschützt (ggf. durch Verschlüsselung) werden.

In einer IT-Sicherheitsrichtlinie zum Dokumentenmanagement sollte ein Prozess den Lebenszyklus der Dokumente beschreiben. Dazu zählt die Klassifizierung, Pflege, das Archivieren und die Vernichtung der Dokumente. Demgemäß sollten in der IT-Sicherheitsrichtlinie beispielsweise auch Vertraulichkeitsstufen zur Klassifizierung dieser Dokumente definiert werden (z. B. öffentlich, vertraulich).

In regelmäßigen Abständen sollte die IT-Sicherheitsrichtlinie auf Aktualität geprüft und bei Bedarf überarbeitet werden.

3. Etablieren eines Security Managements

Es sollte ein Informationssicherheits-Managementsystem (ISMS) für den Betrieb des ICS etabliert werden. Ziel eines ISMS ist, die Informationssicherheit dauerhaft zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.

die wichtigste Aufgabe ist dabei das Risikomanagement. Dies hat die Betrachtung sämtlicher funktionaler als auch IT-Security-spezifischer Komponenten eines ICS zum Gegenstand. Im Rahmen eines Risikomanagements werden umfassende Überlegungen zu Sicherheitskonzeption, Priorisierung von Sicherheitsmaßnahmen und der Abschätzung von Restrisiken angestellt.

Bei der Integration in ein eventuell bereits vorhandenes ISMS sind die technischen Besonderheiten eines ICS zu beachten. Eine unreflektierte Übernahme der Vorgaben aus der Office-IT ist wegen der spezifischen Rahmenbedingung nicht zielführend und meist nicht umsetzbar.

Vorgaben und Hinweise zum Aufbau eines ISMS und zur Risikoanalyse finden sich beispielsweise in [VDI 2182 2011], [IEC 62443], [ISO/IEC 27000] und [BSI GS].

4. Netzplan

Die Struktur des Netzes sollte in einem physischen und einem logischen Netzplan dokumentiert werden. Der physische Plan zeigt die Orte und Infrastruktur des ICS, z. B. Kabel, Gebäude, Funkverbindungen. Der Plan soll mindestens enthalten:

- IP-Netzadressen und Netzmasken z. B. 192.168.1.0/24,
- IP-Adressen aller angeschlossenen Netzinterfaces z. B. 192.168.1.54
- MAC-Adressen,
- Computername und Funktionalität der Systeme,
- (falls vorhanden) DNS-Name,
- (falls vorhanden) FQDN (FullyQualifiedDomainName) und
- die technische Dokumentation sollte im gesamten Lebenszyklus aktualisiert und gepflegt werden (beginnend bei den Vorgaben an Lieferanten und Planer).

Der logische Netzplan stellt die physischen Gegebenheiten nicht dar und fokussiert auf die strukturelle Sicht und die Sicherheitszonen.

5. Liste der IT-Systeme und installierten Anwendungen

Um Inkompatibilitäten und Inkonsistenzen von Software in spezifischen Versionen sowie Konfigurationen (z. B. IP-Adressen-Konflikte) zu vermeiden, sollte in einer Liste die Konfiguration der einzelnen ICS-Komponenten dokumentiert sein. Darüber hinaus können auf diese Weise ICS-Komponenten schnell identifiziert werden, wenn neue Updates verfügbar oder Konfigurationsänderung nötig sind. Auch wenn Updates nicht möglich sind, so kann anhand einer solchen Liste die potentielle Betroffenheit zeitnah bewertet werden.

Die Liste kann beispielsweise folgende Eigenschaften dokumentieren:

- Funktionaler Name,
- Computername,
- Zuständiges Administrations-Personal mit hinterlegten Kontaktdaten (ggf. auch Servicezeiten),
- Physischer Aufstellungsort,
- MAC-Adresse(n),
- IP-Adresse(n),
- DNS-Bezeichnung,
- FQDN,
- Betriebssystem,
- installierte Anwendungen und Dienste unter Angabe von Ports und eingesetzten Protokollen,
- Patchstand jeder Software mit dem Datum der Einspielung des Patches,
- Datum des letzten Viren-Scans (z. B. täglich automatisierter Scan, manueller Scan am 23.01.2013) und
- Backup-Intervall (vollständig und inkrementell), Umfang der Datensicherung und die zuletzt durchgeführte Datensicherung.

6. Administrations- und Benutzerhandbücher

Für den sicheren und unterbrechungsfreien Betrieb ist es notwendig, dass das Service- und Wartungspersonal sowie Administratoren alle Funktionen des ICS kennen und diese bedienen können. Kommt es zu Ausfällen beim Personal (z. B. krankheitsbedingt oder aufgrund einer Kündigung), sollte sichergestellt sein, dass die benötigten Informationen weiterhin im Unternehmen verfügbar und für die Mitarbeiter zugänglich sind.

Daher sollte für alle ICS und Anwendungen ein Administrations- und Benutzerhandbuch verfügbar sein. Die Dokumente sollten dabei folgende Punkte zur IT-Sicherheit abdecken:

- notwendiges Firewall-Regelwerk (mit Dienst, Protokoll und Port),
- Anweisungen zur Härtung spezifischer Anwendungen,
- Anweisungen zur sicheren Konfiguration,
- spezifische Risiken (z. B. bei der Aktivierung einer bestimmten Konfiguration),
- Systemwiederherstellung (zur Notfallvorsorge vgl. 5.3.4).

5.3 Security-spezifische Prozesse / Richtlinien

5.3.1 Security Management

7. Entwicklung und Integration von Individualsoftware

ICS werden als Verbund von Hard- und Software ausgeliefert. Die Anpassung auf die individuellen Gegebenheiten und Bedürfnisse wird durch die Konfiguration realisiert. In vereinzelten Fällen kann es notwendig sein, eigene Software zu entwickeln (z. B. Skripte, Batch-Dateien zur Stapelverarbeitung), um gewisse Automatismen oder Funktionen nachträglich zu integrieren. Werden eigene Programme oder auch Skripte entwickelt, so sollte sowohl die sichere Erstellung (Secure-Coding-Guidelines) der Programme als auch die sichere Integration in die bestehende Umgebung durch eine interne Softwareentwicklungsrichtlinie geregelt werden.

8. Entsorgung von Hardware

Bevor ein defektes Gerät zur Reparatur oder Wartung an einen Drittanbieter herausgegeben wird, sollte sichergestellt werden, dass keine vertraulichen Informationen oder Konfigurationen auf dem Gerät gespeichert sind (z. B. Festplatte oder interner Speicher). So sollten beispielsweise Speichermedien mit vertraulichen Informationen vorher entfernt oder sicher gelöscht werden.

Mit der Entsorgung von Hardware sollten vertrauenswürdige Dienstleister beauftragt werden. Hierbei sollten die defekten Geräte bis zur Abholung so gelagert werden, dass sie vor unbefugten Zugriffen geschützt sind (z. B. durch abgeschlossene Schränke).

5.3.2 Technische Dokumentation

9. Auditberichte

Die Ergebnisse aus durchgeführten Audits sollten in Form von Audit-Berichten dokumentiert werden. Hinweise zum Aufbau und Inhalt von Auditberichten sind in Kapitel 6 erläutert. Die Inhalte der Dokumente sind hochgradig sensibel. Die Berichte sind bzgl. ihrer Geheimhaltungsstufe zu klassifizieren und entsprechend zu behandeln (siehe 2).

5.3.3 Durchgängiges Management aller ICS-Komponenten

10. Festlegung der betrieblichen Aufgaben von Betreiber, Integrator und Hersteller

Die jeweils betrieblichen Aufgaben des Betreibers, Integrators und Herstellers sollten definiert und schriftlich dokumentiert sein. Dies kann beispielsweise die Administration von Komponenten im Feld bis hin zur Anwendungsentwicklung oder auch das Patchmanagement betreffen.

11. Changemanagement

Für Änderungen am ICS sollte ein Changemanagement-System etabliert werden. Dabei sollte eine Rollentrennung umgesetzt werden, sodass nicht die Person, die eine Änderung freigibt, diese auch umsetzen kann. Alle geplanten Änderungen sollten von geeigneten Personen dahingehend geprüft werden, ob sie sicherheitsrelevante Auswirkungen auf das ICS haben.

12. Security-Monitoring

Durch das frühzeitige Erkennen von sicherheitsrelevanten Ereignissen kann rechtzeitig auf diese reagiert und somit ein möglicher Schaden abgewendet werden. Daher sollte im Vorfeld in einem Security Incident Response Plan eine Strategie entwickelt werden, wie sicherheitsrelevante Ereignisse erfasst und erkannt werden, welche Reaktionen erforderlich sind und wie ein sicherer Zustand wiederhergestellt werden kann. Der Security Incident Response Plan sollte die Phasen Planung, Reaktion und Wiederherstellung berücksichtigen und hierfür Prozesse z. B. zur Klassifizierung der Ereignisse, Benachrichtigung, Dokumentation, Untersuchung des Ereignisses und den daraus abgeleiteten Aktionen definieren.

Insbesondere sollten die Verantwortlichkeiten und Rollen (vgl. 1) sowie das weitere Vorgehen (z. B. Meldung an Behörden oder Veröffentlichung) festgelegt werden. Hier ist insbesondere der Datenschutzbeauftragte des Unternehmens einzubinden.

Der Plan sollte in regelmäßigen Abständen und mindestens jährlich erprobt, auf Aktualität geprüft und bei Bedarf überarbeitet werden.

5.3.4 Notfallmanagement

13. Wiederherstellungsplan (Business Continuity Plan) für die schützenswerten Assets

In einem Wiederherstellungsplan sollte festgelegt werden, wie grundlegende Funktionen im ICS nach einer signifikanten Störung wieder aufgenommen werden können. Es sollten im Vorfeld Aktionen abgeleitet werden, die nach Eintritt einer Produktionsstörung oder eines Security-Vorfall den Wiederanlauf der Produktion in einer angemessenen Zeit sicherstellen. Dazu zählen beispielsweise Prozesse zur Datensicherung, Wiederherstellung und dem regelmäßigen Testen von Backups, Prozeduren zur Systemwiederherstellung, Reparatur defekter Komponenten und Vorhalten von Ersatzteilen als auch alternative Kommunikations- und Steuerungsmöglichkeiten bei Ausfällen.

Der Plan sollte in regelmäßigen Abständen und mindestens jährlich auf Aktualität geprüft und bei Bedarf überarbeitet werden.

5.3.5 Personal

14. Training des Personals

Das Personal (z. B. Mitarbeiter, Vertragspartner und Dritte) sollten regelmäßig in sicherheitsspezifischen Qualifizierungs- und Fortbildungsprogrammen die fachliche Qualifikation zur Bewältigung ihrer zugeordneten Tätigkeit auffrischen und erweitern. Damit soll sichergestellt werden, dass das Personal keine Fehlentscheidung z. B. aus Unwissenheit oder mangelnder Qualifikation trifft.

Zusätzlich zu den Qualifizierungsprogrammen sollte das Personal in regelmäßigen Awareness-Schulungen über denkbare Bedrohungen und Schwachstellen informiert und hierfür sensibilisiert werden. Dabei sollen insbesondere Änderungen bereits bestehender Richtlinien vorgestellt werden (siehe auch 3, 12, 13).

Das Service- und Wartungspersonal sowie Administratoren sollten durch Schulungen in die Lage versetzt werden, mögliche Schwachstellen zu identifizieren und zu bewerten sowie diesen durch angemessene Gegenmaßnahmen zu begegnen.

15. Sicherheit des Personals

Um das Risiko durch menschliches Fehlverhalten zu reduzieren (z. B. fachliche Fehlentscheidungen, Diebstahl, Betrug), sollten die folgenden Punkte bei der Personalverwaltung berücksichtigt werden.

In einer Anstellungsrichtlinie sollten Voraussetzungen für eine Anstellung festgelegt werden. So sollten Bewerber beispielsweise hinsichtlich ihrer Tauglichkeit für eine Stelle anhand einer zuvor definierten und präzisen Stellenbeschreibung bewertet werden. Darüber hinaus können angegebene Qualifikationen und Referenzen überprüft werden.

Das Personal sollte auf seine Pflichten zur Befolgung der Richtlinien zur IT Security hingewiesen werden (siehe 1). Dies kann ebenfalls Teil des Angestelltenvertrages sein (z. B. auch bei Dienstleistern). So sollte beispielsweise eine Vertraulichkeitsvereinbarung Vertragsbestandteil sein (siehe 19).

Das Personal (z. B. Mitarbeiter, Vertragspartner und Dritte) mit Berechtigungen für den Zutritt oder Zugriff auf das ICS sollten in einer Liste erfasst werden. Die Liste sollte regelmäßig hinsichtlich der notwendigen Berechtigungen der einzelnen Angestellten überprüft, aktualisiert und bei Bedarf Berechtigungen neu vergeben oder entzogen werden.

Die Richtlinien für das Personal und Stellenbeschreibungen sollten in regelmäßigen Abständen auf Aktualität geprüft und bei Bedarf überarbeitet werden.

Hinweise zum Thema Innentäter finden sich in [BSI CS-061].

16. Prozesse für Einstellung, Wechsel und Ausscheiden von Personal

Es sollten Prozesse etabliert sein, die sicherstellen, dass bei Neueinstellungen, Wechsel der Rolle bzw. des Aufgabengebietes innerhalb des Unternehmens und bei Abgängen von Mitarbeitren die Zugangs-, Zutritts- und Zugriffsberechtigungen der betroffenen Personen der neuen Situation entsprechen.

5.3.6 Revision & Tests

17. Auditierung

Audits der IT-Sicherheit der Netze und weiteren Komponenten eines ICS sollten regelmäßig durchgeführt werden. In komplexen Systemen ist die Etablierung von spezialisierten Teams zur Identifikation und Bewertung möglicher Angriffsszenarien unabdingbar. Eine Methodik für die Durchführung von Audits in ICS-Installationen ist in Kapitel 6 beschrieben.

18. Komponentenprüfung

Bei der Auswahl von Komponenten sollte eine Überprüfung von definierten (funktionalen und IT-sicherheitsrelevanten) Anforderungen durchgeführt werden. Dabei können einzelne Komponenten bis hin zum gesamten ICS Prüfgegenstand sein.

5.4 Auswahl der verwendeten Systeme und Komponenten sowie der eingesetzten Dienstleister und Integratoren

5.4.1 Vertrauenswürdigkeit

19. Vertraulichkeitsvereinbarung mit den Herstellern, Lieferanten und externen Betreibern

Der Betreiber sollte mit Vertragspartnern (Hersteller, Lieferanten oder externe Betreiber) Vertraulichkeitsvereinbarungen treffen. Diese sollten insbesondere Mitarbeiter des Vertragspartners mit IT-Security-relevanten Informationen und Kenntnissen über das ICS des Betreibers berücksichtigen (z. B. für den Fall, dass Mitarbeiter des Vertragspartners die Position oder Firma wechseln).

Darüber hinaus sollte geregelt werden, wie der Betrieb der ICS erhalten werden kann, falls der Vertragspartner keine Wartungsdienste oder Dienstleistungen mehr anbietet (z. B. wegen Insolvenz des Vertragspartners). So sollte dem Betreiber beispielsweise der notwendige Zugriff auf diese Systeme auch weiterhin möglich sein und ausreichend Dokumentation zur Wartung und zum Betrieb der ICS verfügbar sein.

Im Fall der Geschäftsaufgabe eines Vertragspartners sollte vertraglich geregelt sein, dass ausgehändigte, vertrauliche Informationen an den Betreiber zurückzugeben sind.

5.4.2 IT-Security-Merkmale von ICS-Komponenten

20. Mitteilung der IT-Security-Anforderungen an den Systemintegrator

Die IT Security-Anforderungen des Betreibers für das ICS, die sich aus der Risikoanalyse ergeben, sollten dem Systemintegrator mitgeteilt werden. Dieses sollte als Bestandteil des Lastenhefts erfolgen.

Die Anforderungen sollten auf Basis der konkreten Anwendungen formuliert werden. So können sie sich auf geforderte Eigenschaften oder Informationen beziehen. Es sollten keine Lösungen, sondern Anforderungen beschrieben werden.

21. Berücksichtigung der IT-Security-Spezifikation des Systemintegrators

Der Betreiber muss die IT-Security-Spezifikation, die der Systemintegrator für ein ICS bereitstellt, im Zyklus der Risikoanalyse berücksichtigen. Aufbauend auf den Informationen des Systemintegrators können weitere Maßnahmen durch den Betreiber definiert werden.

22. Robustheit der Produkte

Neben der Hardware (z. B. Industrie-Rechner) sollte auch die Software (z. B. Protokollstack, ICS-Anwendungen) robust auf ungültige Eingaben reagieren. So sollten beispielsweise ungültige Netzpakete nicht zum Absturz oder zu Fehlern der Software führen, sondern von dem Protokollstack ignoriert und bei Bedarf protokolliert werden.

Die Robustheit der Komponenten sollte bereits durch die Hersteller sichergestellt werden. Diese Anforderung sollte bereits bei der Anschaffung neuer Komponenten durch den Betreiber gefordert werden.

5.4.3 Kompatibilität eingesetzter Technologien zu Standards

23. Kompatibilität

Das zu beschaffende ICS und deren Komponenten sollten gängige Standards der jeweiligen Technologie umsetzen und gemäß dieser Standards kompatibel zu anderen Systemen sein. Dazu zählt insbesondere die Unterstützung der IT-Sicherheitsmechanismen.

5.4.4 Inbetriebnahme in sicherer Konfiguration

24. Verzicht auf überflüssige Produktfunktionen

Falls ICS-Komponenten Dienste oder Schnittstellen besitzen, die nicht von dem Betreiber benötigt werden, sollten diese nach Möglichkeit entfernt oder zumindest deaktiviert werden. Die durchgeführten Änderungen an dem ICS sollten nachvollziehbar dokumentiert werden.

25. Individuelle Zugangsdaten

Die Zugangsdaten des ICS und der Anwendungen sollten bei der Inbetriebnahme individuell geändert werden, sodass diese nicht in der öffentlich verfügbaren Dokumentation eingesehen werden können (siehe auch 46). Eine andere Möglichkeit sind bei der Herstellung zufällige und individuell pro Geräte vergebene Zugangsdaten.

26. Aktivierte Sicherheitsmechanismen und aktueller Patchstand

Die Komponenten des ICS sollten bei der Inbetriebnahme über einen aktuellen Patchstand verfügen, sodass sie in dem ausgelieferten Zustand keine relevanten Schwachstellen aufweisen. Verfügbare IT-Sicherheitsfunktionen sollten aktiviert und restriktiv konfiguriert sein (z. B. Firewall). Entsprechend sollte das ICS weitestgehend gehärtet sein und explizite Freigaben von Benutzerzugriffen durch den Integrator vor der Inbetriebnahme erfordern.

5.4.5 Soft- und Hardware Support

27. Langfristige Gewährleistung der IT-Security

Betreiber, Systemintegratoren und Hersteller sollten bereits bei der Planung eine Strategie erarbeiten, wie langfristig die IT-Security der Anlage gewährleistet werden kann. Dies gilt für die gesamte Laufzeit der Anlage. Dies umfasst auch die weitere Nutzung von abgekündigter Software. Es sollten daher bereits frühzeitig alternative Schutzmaßnahmen berücksichtigt werden.

28. Unterstützung von Virenschutz-Lösungen

Falls notwendig sollten die zu beschaffenden ICS mit einem Virenschutzprogramm ausgestattet sein oder zumindest den Betrieb von Virenschutzprogrammen unterstützen. In der Regel unterstützt der Hersteller ausgewählte Produkte von Virenschutzanbietern (siehe auch Kapitel 5.6.7).

5.4.6 Fernwartung durch Hersteller und Integrator

29. Sichere Fernwartung

Die Systeme, mit denen die Fernwartung durchgeführt werden, sollten das gleiche Schutzniveau aufweisen wie das ICS-Netz. So sollten die IT-Sicherheitsleitlinien des ICS-Netzes mit denen der Fernwartungssysteme vereinbar sein.

Der Verbindungsaufbau sollte mindestens eine Zwei-Faktor-Authentisierung verlangen (z. B. Token und Passwort) und die Daten sollten ausschließlich in verschlüsselter Form übertragen werden (vgl. 72).

Soll der Verbindungsaufbau für die Fernwartung von extern erfolgen, so sollte keine direkte Verbindung in das ICS etabliert werden. Die Verbindung in das ICS-Netz sollte vielmehr über einen sog. Sprungserver/Proxyserver in einer DMZ (vgl. 32) erfolgen. Dieser besitzt die Möglichkeit, eine entsprechende Verbindung in das ICS aufbauen. Gleichzeitig kann er alle Aktivitäten aufzeichnen.

Als Alternative zum Sprungserver kann der Verbindungsaufbau anstatt von extern von intern aus dem ICS-Netz heraus erfolgen. Das ICS verbindet sich somit zum Hersteller. Auf diese Weise werden eingehende Verbindungen vermieden und nach extern keine zusätzlichen Dienste angeboten.

Die Fernwartungs-Zugangsmöglichkeit für den Hersteller sollte nur bei Bedarf aktiviert werden und sonst vom Betreiber deaktiviert sein. Dies reduziert die Gefahr für mögliche Angriffe. Darüber hinaus sollte ein Verbindungsaufbau durch die Bediener bestätigt werden, bevor ein Zugriff auf ICS möglich ist.

5.4.7 Absicherung von Feldgeräten

30. Anforderungen an Feldgeräte

Die Absicherung von Feldgeräten (z. B. Sensoren und Aktoren) ist u. a. wichtig, um Angreifern mit physischem Zugriff auf diese Geräte entgegenzuwirken. Sofern diese Geräte über IT-Sicherheitsmechanismen, z. B. Authentisierung, Verschlüsselung, Zugriffskontrolle oder Protokollierung verfügen, sollten Betreiber darauf drängen, dass diese verwendet werden. Insbesondere ältere Komponenten sind aber häufig rein funktional ausgelegt und verfügen nicht über integrierte IT-Sicherheitsmechanismen, falls diese über höhere Protokolle angesprochen werden können. In diesem Fall sollten flankierende physikalische, organisatorische oder zusätzliche technische Maßnahmen eingesetzt werden. Hierzu gehören beispielsweise speziell für den Einsatz im industriellen Umfeld konzipierte Security-Appliances, die den übertragenen Datenverkehr filtern.

5.5 Bauliche und physische Absicherung

31. Physische Absicherung

Es müssen Absicherungen des ICS gegen unberechtigten physischen Zutritt, Zugang und Zugriff getroffen werden. Dies gilt für Gebäude und Räume sowie Schränke.

Zutritte sollten kontrolliert, überwacht und protokolliert werden. Gehäuse und Schränke sollten verschließbar sein. Unbefugte Zutritte oder Zugriffe sollten zeitnah erkannt werden z. B. durch Auslösen von Alarmen.

5.6 Technische Maßnahmen

Bei der Umsetzung der technischen Maßnahmen sind die Vorgaben der Hersteller bzw. der Produktdokumentation zu beachten. Oftmals geben Hersteller Beschreibungen oder Einschränkungen für die Umsetzung der aufgeführten Maßnahmen.

5.6.1 Absicherung der Netze

32. Netzsegmentierung

Ein ICS-Netz sollte aus mehreren Netzsegmenten mit individuellen Schutzbedarfen bestehen. Der Datenverkehr zwischen den verschiedenen Leveln (vgl. Abbildung 3) sollte durch eine Datenflusskontrolle, z. B. Firewall, auf das betriebliche notwendige Maß reglementiert werden.

Bei entsprechend hohem Schutzbedarf sollte zwischen der Produktionsführung und der Betriebs-/Prozessführung eine Demilitarisierte Zone (DMZ) eingefügt werden. Eine DMZ ist ein Zwischennetz, das an Netzübergängen gebildet wird, aber weder zu dem einen noch zu dem anderen Netz gehört. Sie stellt ein eigenes Netz dar, das nicht so stark gesichert ist wie das eigentlich zu schützende Netz. Sie wird aus zwei physisch getrennten Firewalls aufgebaut, sowie einem Application Level Gateway. Proxy-Dienste mit Filtermöglichkeiten bis hin zum Layer 7 sollten den Datenverkehr steuern und kontrollieren.

Neben der Trennung von Netzen mit unterschiedlichen Funktionalitäten (vertikale Integration vgl. Abbildung 1) sollten auch standortübergreifende Netze oder allgemein organisatorisch unabhängige Maschinen/Anlagen untereinander segmentiert werden (horizontale Integration, vgl. Abbildung 2). So wird z. B. verhindert, dass sich Schadprogramme ungehindert auf alle Maschinen ausbreitet.

Der Verbindungsaufbau sollte immer aus dem Netzsegment mit dem höheren Schutzbedarf in das Netzsegment mit dem niedrigeren Schutzbedarf aufgebaut werden.

Eine Umgehung der Netztrennung durch undokumentierte Verbindungen darf nicht stattfinden. Insbesondere sollten keine unkontrollierten Verbindungen zu Netzsegmenten mit unterschiedlichem Schutzbedarf zugelassen werden.

33. Absichern der elektronischen, externen Schnittstellen

Alle externen Schnittstellen zum ICS-Netz sollten identifiziert und dokumentiert werden (z. B. in einem Netzplan; vgl. 4). Hierzu zählen neben offensichtlichen Schnittstellen wie die Verbindung zum Büro-Netz über eine DMZ auch weniger offensichtliche, externe Kommunikationskanäle wie Funknetze und serielle Verbindungen z. B. zwischen Gebäuden bei geographisch verteilten Systemen und Leitungen.

Es sollte ein Prozess definiert sein, der eine regelmäßige Prüfung der Dokumentation und im Fall von Änderungen eine zeitnahe Aktualisierung vorsieht (siehe 2).

Sind externe Schnittstellen notwendig, sollten hierbei direkte Zugriffe von extern in das ICS-Netz vermieden werden (z. B. direkte Modem-Verbindungen an ein ICS, Administration über eine direkte Verbindung aus dem Internet). Dagegen sollten nach Möglichkeit alle externen Verbindungen über einen Proxy-Dienst in der DMZ in das ICS-Netz erfolgen und somit über eine zusätzliche IT-Sicherheitsebene. Auf diese Weise sind Zugriffe auf das ICS-Netz ausschließlich über diesen Dienst und nicht direkt in das ICS-Netz möglich. Ein solcher, möglicherweise notwendiger externer Zugriff ist die Fernwartung (siehe 29).

Bei externen Schnittstellen sollten insbesondere folgende IT-Sicherheitsmaßnahmen berücksichtigt werden, um unbefugte Zugriffe von außen in das ICS-Netz zu verhindern:

- Zugriffe über externe Schnittstellen sollten eine starke Authentisierung erfordern (z. B. Rückruf des Modem auf eine vorkonfigurierte Telefonnummer, Exklusivverbindung zu einer konfigurierten IP-Adresse, Hardwareschlüssel im Modem).
- Verbindungsversuche und Zugriffe sollten protokolliert und überwacht werden (z. B. bei Modem-Verbindungen durch eine Telefonanlage; siehe auch 73).
- Für einen längeren Zeitraum nicht benötigte, externe Schnittstellen (z. B. Fernzugänge) müssen abgeschaltet werden. Nur bei Bedarf sollten die Geräte wieder (elektrisch) eingeschaltet werden.
- IT-Sicherheitsrelevante Daten sollten nicht übertragen werden (z. B. Zugangsdaten, kritische und privilegierte Befehle).
- Die Speicherung von Daten (Engineering Daten, Produktionsdaten) sollte nur in der ICS-Umgebung, nicht jedoch auf externen Systemen erfolgen.
- Soweit möglich sollten Fernwartungszugänge ausschließlich lesenden Zugriff ermöglichen.

34. Statische Netz-Konfiguration

Insbesondere bei einer überblickbaren Anzahl an ICS sollte die statische Zuweisung der Netz-Konfiguration einer dynamischen vorgezogen werden. Dazu zählt die statische Vergabe von IP-Adressen, Subnetzmasken und Routen innerhalb des ICS-Netzes. Auch die Konfiguration von WINS/DNS-Servern kann erforderlich sein, falls über diese Namen aufgelöst werden sollen.

Bei der Zuweisung von IP-Adressen sollten verbreitete Konventionen nach Möglichkeit eingehalten werden. So sollten Routern die ersten, verfügbaren IP-Adressen in dem Netzsegment zugewiesen werden (z. B. 192.168.0.1) und Switches und Gateways die nachfolgenden IP-Adressen (z. B. 192.168.0.2), gefolgt von ICS mit anderer Funktion.

Die Adressierung der Systeme muss dokumentiert werden (siehe auch 5). Darüber hinaus sollte darauf geachtet werden, dass eine IP-Adresse nicht mehrfach vergeben wird.

Wenn eine statische Netz-Konfiguration der ICS durchgeführt wird, sollten auf den ICS die DHCP-Client-Software deinstalliert oder zumindest deaktiviert werden. Auf diese Weise überschreibt ein unbeabsichtigtes DHCP-Paket eines Rechners nicht die statische Netz-Konfiguration.

35. Gleiche Sicherheitsmaßnahmen für ICS in einem Netzsegment

Alle Komponenten in einem Netzsegment (z. B. Prozessführung, siehe Abbildung 3) sollten das gleiche IT-Sicherheitsniveau erfüllen. Wird ein ICS beispielsweise mit einem geringeren IT-Sicherheitsniveau durch einen Angreifer kompromittiert, so stellt dieses System für alle anderen ICS im gleichen Netzsegment und damit in der gleichen Sicherheitszone eine Bedrohung dar. Ausgehend von diesem kompromittierten System kann ein Angreifer weiterführende Angriffe auf die anderen Systeme durchführen und ggf. Vertrauensbeziehungen zwischen den Systemen ausnutzen. Daher sollten alle ICS in der gleichen Sicherheitszone und damit mit der gleichen Vertrauensstellung untereinander auch vergleichbar geschützt sein.

36. Unabhängiger Betrieb der Netzsegmente

Falls die Verbindung zwischen zwei Netzsegmenten im ICS-Netz abbricht, sollte dies nicht oder nur in geringem Maße die Produktion beeinträchtigen. Daher sollten Abhängigkeiten zwischen Netzen vermieden werden. Somit werden mögliche Auswirkungen eines Netzsegmentausfalls weitestgehend reduziert.

37. Absichern der Funktechnologien

Der Einsatz von Funktechnologie erfordert sorgfältige Planung. Da es sich hierbei um ein sogenanntes Shared Medium handelt, ist der Zugriff auf das Übertragungsmedium für Angreifer in der Regel auch aus großen Distanzen und außerhalb des Betriebsgeländes möglich und nur schwierig einzuschränken.

Die Reichweite von Funknetzen sollte daher soweit wie möglich eingeschränkt werden. IT-Sicherheitsfunktionen (z. B. Passwörter, PIN-Eingabe) sollten aktiviert sein und in der Konfiguration von den vorgegebenen Einstellungen bei der Erstinstallation abweichen.

Funktechnologien sollten nicht für Einsatzzwecke verwendet werden, die hohe Anforderungen an die Verfügbarkeit voraussetzen (z. B. kann durch Störsignale eine Funkverbindung immer unterbrochen oder stark eingeschränkt werden). Darüber hinaus sollten die verwendeten Technologien über hinreichende IT-Sicherheitsmechanismen gemäß dem Stand der Technik verfügen, sodass kein unbefugter Zugriff auf die übertragenen Daten möglich ist (z. B. Verschlüsselung des Datenverkehrs).

Die IT-Sicherheit bei Funknetzen sollte nicht ausschließlich auf den IT-Sicherheitsmerkmalen der eingesetzten Technologie basieren, sondern es sollten zusätzliche IT-Sicherheitsmechanismen auf Netzebene umgesetzt werden. Dabei sollte darauf geachtet werden, dass nicht nur eine Schutzmauer errichtet wird, sondern mehrere Hürden errichtet werden. Dazu gehören z. B. Netzsegmentierung und der zusätzliche Einsatz von kryptographischen Algorithmen bei der Datenübertragung (siehe dazu auch 32, 43, 58). Dementsprechend sollten Funknetze vorzugsweise nicht direkt mit dem ICS-Netz verbunden werden, sondern aufgrund des unterschiedlichen IT-Sicherheitsniveaus über Proxy-Dienste in der DMZ mit den ICS kommunizieren (siehe 33).

Verfügbare Protokolldaten der Geräte sollten regelmäßig auf Auffälligkeiten geprüft werden (z. B. Kommunikation mit unbekannten Geräten).

38. Einsatz von Firewalls

Zur logischen Trennung von Netzsegmenten sollte eine Firewall eingesetzt werden, die als Filterkomponente den Datenfluss zwischen den Segmenten reglementiert (siehe auch 32)..

Hierbei kann nach den folgenden Kategorien von Firewalls auf Netzebene unterschieden werden (Host-based Firewalls werden in 39 adressiert):

- Paketfilter (Filterung nach IP-Adresse und Port),
- Stateful Inspection Firewall (Filterung nach IP-Adresse, Port und Verbindungsstatus),
- Application Level Gateway (Zusätzliche Filterung bis auf Anwendungsebene).

Es sollten vorzugsweise Firewalls als dedizierte Hardware eingesetzt werden. Hierbei sollte geschultes Personal für die Konfiguration und den Betrieb der Firewalls zuständig sein. Die folgenden Punkte sollten bei der Konfiguration einer Firewall beachtet werden:

- Die Firewall sollte restriktiv konfiguriert sein und daher gemäß dem White-List-Ansatz grundsätzlich alles verbieten, sodass explizit Verbindungen und Zugriffe freigeschaltet werden müssen.
- Nur Verbindungen, die zwingend notwendig für den Betrieb der ICS sind, sollten freigegeben werden.
- Verbindungen vom ICS-Netz zu externen Netzen (z. B. Office-Netz) sollten ausschließlich über Proxy-Dienste in der DMZ erfolgen. Direkte Verbindungen zwischen den Netzen müssen verhindert werden. Die Kommunikation mit anderen Netzen sollte komplett unterbunden werden.
- Vorzugsweise sollten eingehende Verbindungen von externen Netzen in das Netzwerk des ICS vollständig unterbunden werden. Wenn dies nicht möglich ist, sollten die Inhalte der Verbindungen gefiltert und auf Konformität geprüft werden.
- Die Filterung sollte so feingranular wie möglich erfolgen. Nach Möglichkeit sollten daher der Zugriff auf einzelne IP-Adressen oder kleine definierte Adressbereich beschränkt werden.
- Es sollten lediglich die zwingend notwendigen Ports für TCP oder UDP freigegeben werden.
- Es sollte eingehender als auch ausgehender Datenverkehr gefiltert werden.
- Der Platzhalter ANY sollte vermieden werden.
- Die letzte Filterregel sollte immer alles verbieten (DENY ALL, PERMIT NONE).

Darüber hinaus sollten die Protokolldaten der Firewall regelmäßig hinsichtlich Auffälligkeiten überprüft werden. Hierbei ist hervorzuheben, dass die reine Installation einer Firewall keinen zusätzlichen Schutz bietet, wenn keine sorgfältige und restriktive Konfiguration der Regeln und eine Überwachung vorgenommen wird.

Die Beschaffungskriterien unterscheiden sich dabei von Fall zu Fall. Je nach Einsatzart können Funktionen zur Filterung und Überwachung der Protokolle eingesetzt werden. Es ist zu empfehlen, dass nicht nur eine Filterung auf IP-Adressen und Ports stattfindet, sondern auch der Protokolle selbst.

39. Host-based Firewalls

Eine Host-basierte Firewall ist eine Software zur Filterung des Netzverkehrs von und zu einem Rechner. Entgegen einer Netz-Firewall ist eine Host-basierte Firewall auf dem zu schützenden Rechner installiert. Häufig sind diese Firewalls Bestandteil des Betriebssystems.

Soweit möglich sollte auf allen ICS eine Host-basierte Firewall installiert sein und genutzt werden.

40. Datendiode (One-Way-Gateway)

Eine Datendiode ermöglicht es, dass die Datenübertragung nur in eine Richtung erfolgt. Ein Rückkanal ist nicht vorhanden, was zu gewissen Einschränkungen führt. Falls ein Rückkanal für Quittungen notwendig ist, sollten die einzelnen Verbindungen in dem Gateway terminiert werden, eine Prüfung des Protokolls durchgeführt werden und erst danach die Weiterleitung erfolgen.

Je nach Ausrichtung der Datendiode können unterschiedliche Ziele verfolgt werden. So kann verhindert werden, dass beispielsweise Steuerbefehle von einem Netz mit niedrigem Schutzbedarf (z. B. Office-Netz) in ein Netzwerk mit hohem Schutzbedarf (z. B. ICS-Netz) übertragen werden. Auf der anderen Seite kann bei umgekehrter Positionierung der Abfluss von vertraulichen Informationen aus einem Netzwerk mit hohem Schutzbedarf verhindert werden.

Die Einschränkungen gelten in diesem Fall auch für den Bezug von Updates und die Konfiguration der Komponenten über das Netzwerk. Die Einrichtung von Verbindungen an der Datendiode vorbei für diesen Zweck hebelt die Funktion aus und muss vermieden werden.

Wenn Kommunikation in beide Richtungen stattfinden muss, gibt es Lösungen, die Filter und Kontrollmöglichkeiten bieten. Auf diese Weise kann eine Prüfung der Konformität und der möglicherweise übertragenen Werte und Befehle auf der Bereich oder Gültigkeit erfolgen.

41. Geeignete logische Trennung und VLAN

VLANs können zur logischen Trennung von Netzsegmenten eingesetzt werden. Zur Trennung von Netzsegmenten mit unterschiedlichem Schutzbedarf muss auf Geräteebene eine physikalische Trennung erfolgen.

Bei der Verwendung von VLANs sollte das Default-VLAN deaktiviert sein. Ungenutzte Ports an dem Switch sollten einem eigenen VLAN zugeordnet werden.

42. Implementierung von Intrusion-Detection- bzw. Intrusion-Prevention-Systemen

Mithilfe von Intrusion-Detection Systemen (IDS) und Intrusion-Prevention Systemen (IPS) lassen sich Angriffsversuche in einer frühen Phase erkennen, sodass der Administrator rechtzeitig alarmiert wird (z. B. durch ein IDS) oder bereits eine automatisierte Reaktion auf den Angriff eingeleitet wird (z. B. durch ein IPS).

Hierzu arbeiten IDS/IPS auf der Grundlage von Heuristiken, um Angriffsversuche von gewöhnlichen, gewünschten Verhalten und Daten zu unterscheiden. Demgemäß müssen diese Heuristiken regelmäßig aktualisiert werden. Darüber hinaus müssen die Heuristiken auf das ICS und seine individuelle Gegebenheiten angepasst werden. Typische Vorfälle und Ereignisse, die durch ein solches System erkannt werden können, sind z. B. unbefugte Zugriffe auf Systeme und die unbefugte Installation von Software oder Manipulationen von Daten. Zudem können hierdurch auch unbeabsichtigte und versehentliche Änderungen (z. B. in Konfigurationsdateien) bemerkt werden.

Ein IDS/IPS kann einzelne Server überwachen (Hostbasierte IDS/IPS; HIDS/HIPS) oder durch Sensoren im Netz den Datenverkehr prüfen (Netzbasiertes IDS/IPS; NIDS/NIPS).

Wird ein NIDS/NIPS verwendet, so sollten die Sensoren im Netz zur Überwachung des Datenverkehrs insbesondere bei externen Schnittstellen platziert werden (z. B. DMZ). Von externen Schnittstellen geht gewöhnlich eine höhere Bedrohung durch Angriffe aus (z. B. Internet). Ebenso sollte ein HIDS auf allen ICS installiert werden. Die Protokolldaten des HIDS sollten in ein zentrales Logging integriert werden (siehe 73).

IDS/IPS sollten als zusätzliche Schutzmaßnahme angesehen werden und ersetzen kein Monitoring der Systeme und des Netzes (z. B. mittels eines Security Information Event Management (SIEM) Systems).

Der Einsatz und der Betrieb eines IDS kann nur größeren Unternehmen empfohlen werden, da die Einrichtung, die Pflege und die Sichtung der Meldungen (insbesondere in der Anfangsphase) mit einem nicht unerheblichen Aufwand verbunden sind. In kleineren Anlagen ist der Aufwand und der Nutzen vorab zu prüfen und es sind ggf. alternative Härtungs- und Schutzmaßnahmen umzusetzen.

Bei der Umsetzung eines IPS ist zudem zu beachten, dass bei der Planung auch sehr spezielle Situationen berücksichtigt werden, damit diese legitimen Übertragungen nicht verhindert werden. Vor einer Aktivierung dieser Funktionen ist daher eine sehr sorgfältige Probephase zu absolvieren.

Die Effektivität eines IDS/IPS ist stark abhängig von einer angepassten und individuellen Konfiguration. So kann die Effektivität beispielsweise durch eine hohe Anzahl an immer wiederkehrenden False Positives beeinträchtigt werden. Insbesondere IPS sollten mit bedacht eingesetzt werden. Vorrangig ist hier der laufende Betrieb, der ggf. durch ein fehlerhaftes Eingreifen des IPS gestört werden könnte.

Daher erfordert nicht nur die initiale Konfiguration des IDS/IPS ein geschultes Fachpersonal, sondern auch im Betrieb muss eine Person im Notfall einen gemeldeten Angriffsversuch von einem False Positive unterscheiden können. Diese Person sollte ständig erreichbar sein, sodass nach der Klassifizierung der Meldung ggf. entsprechende Gegenmaßnahmen eingeleitet werden können.

Für zusätzliche Informationen zu IDS/IPS sollte entsprechend zugeschnittene Literatur konsultiert werden (z. B.[BSI IDS]).

43. Nutzung von sicheren Protokollen

Für administrative und security-kritische Aufgaben (z. B. Anmeldung an der Komponente oder Konfiguration) sollte die Vertraulichkeit und Integrität der Daten sichergestellt sein. Es sollter daher der Einsatz unsicherer Protokolle (z. B. Telnet, FTP, HTTP) vermieden werden. Schwache Protokolle sollten durch sichere Protokolle ersetzt (z. B. SSH, SFTP, HTTPS) oder durch zusätzliche, kryptographische Verfahren abgesichert werden (z. B. SSL/ TLS).

Bei Echtzeitdaten kann auf die Verschlüsselung verzichtet werden, wenn die Vertraulichkeit der Informationen als nachrangig einzustufen ist. Es sollten jedoch trotzdem Maßnahmen ergriffen werden, um die Authentizität und Integrität sicherstellen zu können, sowie das Einspielen von Nachrichten zu erkennen bzw. zu verhindern.

Bei neuen Anlagen sollte darauf geachtet werden, dass sichere Protokollvarianten zum Einsatz kommen.

Falls schwache Protokolle nicht abgesichert oder durch sichere Alternativen ersetzt werden können (z. B. im Fall von proprietären, ICS-spezifischen Protokollen), sollten zusätzliche Schutzmaßnahmen ergriffen werden, um die übertragenen Daten vor einem unbefugten Zugriff zu schützen (z. B. Platzierung des betroffenen ICS in ein separates Netz und restriktive Filterung des Datenverkehrs zwischen den Netzsegmenten).

5.6.2 Absicherung von Diensten und Protokollen

44. Namensauflösung (DNS)

Das Domain Name System (DNS) löst in IP-Netzen die Namen der Rechner in ihre IP-Adresse auf und ist somit für die Kommunikation der ICS untereinander erforderlich.

Für das ICS-Netz sollten dedizierte DNS-Server zuständig sein, die getrennt von DNS-Servern in anderen Netzen (z. B. Büro-Netz) betrieben werden. Besteht eine Verbindung in andere Netze, so sollte eine Filterkomponente (z. B. Firewall) Zugriffe von außerhalb des ICS-Netzes auf den DNS-Server unterbinden.

Der DNS-Dienst sollte ausschließlich für den Namens- und Addressraum der spezifischen ICS-Installation zuständig und konfiguriert sein und somit nur Zoneninformationen für Rechner aus dem ICS-Netz verwalten und speichern.

Vorzugsweise sollte das ICS-Netz vollständig abgeschottet sein, sodass Namen externer Rechner nicht aufgelöst werden müssen. Ist dies dennoch erforderlich, so sollte die Auflösung der Namen ausschließlich über den DNS-Server im ICS-Netz erfolgen, der wiederum stellvertretend einen DNS-Server beispielsweise hinter der Firewall im Büro-Netz kontaktiert. Anfragen zur Namensauflösung sollten in keinem Fall direkt auf externe DNS-Dienste erfolgen.

Die Verfügbarkeit von DNS-Servern sollte durch eine Redundanz z. B. in Form von Master-/Slave-Paaren sichergestellt werden. Hierbei verwaltet ein DNS-Dienst als Master die Zoneninformationen und sichert diese in regelmäßigen Abständen mittels sogenannter Zonentransfers auf einen Slave-Rechner.

Die Übertragung von Zonentransfers sollte soweit wie möglich eingeschränkt werden, da die Information einem potenziellen Angreifer unnötig Einblicke in die Struktur des ICS-Netzes gibt. Daher sollten im ICS-Netz bevorzugt statische IP-Adressen für die Rechner vergeben werden, sodass sich die DNS-Einträge nicht regelmäßig ändern und in der Folge keine übermäßigen Zonentransfers notwendig sind (siehe auch 34).

Zonentransfers sollten ausschließlich zwischen vertrauenswürdigen Systemen möglich sein und eine vorherige Authentisierung erfordern (z. B. mittels kryptographischer Signaturen; siehe auch [RFC 2845 2000]).

Die IP-Adressvergabe sollte statisch erfolgen (siehe 34). Falls die IP-Adressvergabe dynamisch erfolgen muss, sollten ausschließlich Änderungsmitteilungen der IP-Adresse von DNS-Servern bearbeitet werden, wenn diese von vertrauenswürdigen Rechnern stammen.

Des Weiteren sollten Schutzmaßnahmen gegen Cache Pollution und Cache Poisoning bei der Absicherung des DNS-Dienstes beachtet werden.

45. Zeitsynchronisierung

Eine Vielzahl an Prozessen, aber auch administrative Tätigkeiten, beruhen in ICS-Umgebungen auf einer genauen und abgestimmten Zeit (z. B. Nachvollziehbarkeit verteilter Protokolldaten, Beigabe von Zusatzstoffen in der Produktion zum richtigen Zeitpunkt). Es muss aufgrund der Applikationsanforderungen abgewogen werden, wie die Zeitsynchronisation erfolgt.

Für die Synchronisation kann Network Time Protocol (NTP) oder IEEE 1588 genutzt werden.

Das Zeitsignal für den Server sollte aus einer vertrauenswürdigen Quelle stammen. Die Clients auf den ICS sollten die Zeit in einem einheitlichen, standardisierten Format interpretieren (z. B. unter Berücksichtigung von Zeitzonen, Winter- und Sommerzeit).

5.6.3 Härtung der IT-Systeme

46. Standard-Benutzerkonten und -Passwörter

Standard-Benutzer und -Passwörter auf Systemen und in Anwendungen sind oft weltweit bekannt und dokumentiert, beispielsweise in Handbüchern. Daher sollten Standard-Benutzer mindestens deaktiviert, besser gelöscht werden. Voreingestellte Passwörter in Systemen und Anwendungen sollten bei der Installation in sichere Passwörter geändert werden.

Vor der Änderung von Standard-Benutzern und -Passwörtern muss geprüft werden, ob die Systeme und Anwendungen nach einer Änderung ihre vorgesehene Funktionalität weiter ausführen können. Wenn beispielsweise der SNMP-Community-String auf Routern geändert wird, muss diese Änderung auch dem Server bekannt sein.

Die Änderung von Passwörtern ist anderen Maßnahmen vorzuziehen. Nur in Ausnahmefällen (z. B. bei im Programmcode fest hinterlegten Passwörtern) sollte vom Betreiber akzeptiert werden, dass das Passwort nicht geändert wird. Je nach Risiko sollten flankierende Maßnahmen ergriffen werden, dazu gehört beispielsweise die Anbindung über eine Security-Appliance mit einem VPN.

47. Individuelle Benutzerkonten

Falls möglich sollte jeder Mitarbeiter über ein eigenes Benutzerkonto verfügen und sich ausschließlich mit seinem Konto an dem Betriebssystem und an Anwendungen anmelden.

In ICS-Umgebungen ist dies oftmals nicht möglich, sodass häufig mehrere Mitarbeiter ein Benutzerkonto gemeinsam benutzen. Somit lassen sich durchgeführte Aktionen nicht einer Person zuordnen und das Passwort ist einer größeren Gruppe an Personen bekannt.

In solchen Fällen sollte durch eine Risikoanalyse geprüft werden, inwieweit die vorhandenen Schutzmaßnahmen ausreichen, um einen unbefugten Zugriff auf die ICS zu verhindern (z. B. abgeschlossene Türen im Leitstand). Darüber hinaus sollten die Passwörter für solche Gruppenkonten mindestens in jedem Netzsegment unterschiedlich sein. Dies betrifft Benutzerkonten sowohl auf Betriebssystem- als auch auf Anwendungsebene.

48. Entfernen von unnötiger Software und Diensten

Sind Programme und Dienste auf ICS-Komponenten installiert oder aktiviert und werden nicht für den Betrieb der Produktion benötigt, so sollten diese entfernt oder mindestens deaktiviert werden. Häufig ist solche Software bei der Auslieferung von ICS vorinstalliert und wird ggf. unbemerkt bei dem Startvorgang des Rechners automatisch aktiviert.

Eine Auflistung der benötigten Software und Netzdienste sollte der Dokumentation des Herstellers entnommen werden oder vom Hersteller angefordert werden. Wird nur der lokale oder explizite Zugriff ausgewählter Systeme auf Dienste benötigt, sollte die Verfügbarkeit dieser Dienste z. B. durch eine lokale Firewall eingeschränkt werden (siehe auch 39).

49. Anpassen der Standard-Einstellungen

Die Standard-Einstellungen bei der Auslieferung von ICS Hard- und Software können Schwachstellen aufweisen, sodass beispielsweise IT-Sicherheitsmaßnahmen nur unzureichend aktiviert und eingestellt sind. Daher sollte die Konfiguration insbesondere nach der Auslieferung oder Änderungen des Systems (z. B. Software-Updates, neue Software) oder der Infrastruktur (z. B. neue Verbindungen zu Netzsegmenten) kontrolliert und ggf. angepasst werden.

Die folgenden Beispiele veranschaulichen mögliche, IT-Sicherheitsrelevante Einstellungen einer Standard -Konfiguration:

- deaktivierte IT-Sicherheitsfunktionen (z. B. Firewall),
- wenig restriktives, den Datenverkehr einschränkendes Regelwerk der Firewall,
- ungeschützte Administrationszugänge,
- Standardbenutzer und -kennwörter (siehe auch 46),
- unnötige Programme und aktivierte Dienste mit ggf. Schwachstellen (siehe auch 48).

50. Anpassen der Hardware-Konfiguration

Nicht für den produktiven Betrieb benötigte Hardware sollte entfernt oder mindestens deaktiviert werden. Dies beinhaltet lokale Schnittstellen wie USB-Ports, CD/ DVD-Laufwerke und andere Speichermedien-Geräte.

Eine Deaktivierung kann beispielsweise durch eine mechanische Sperrvorrichtung, softwaregesteuert oder durch Siegel z. B. an USB-Ports erfolgen. Werden diese Geräte trotz der Absicherung unbefugt genutzt, sollte dies für den Administrator des Systems nachvollziehbar sein (z. B. durch gebrochene Schlösser, Siegel oder Protokolleinträge im System).

Im Fall einer Software-Lösung sollte der Administrator zu Wartungszwecken den Sperrmechanismus kurzzeitig deaktivieren und aufheben können, sodass Zugriffe auf die Hardware möglich sind.

51. Zugriff auf das Internet innerhalb des ICS-Netzwerk

Insbesondere durch das Surfen im Internet besteht die Gefahr der Infektion mit Schadsoftware durch Drive-By-Downloads. Daher sollte der freie Zugriff auf das Internet aus dem ICS-Netzwerk unterbunden werden.

Wenn beispielsweise in Level 4 dennoch ein Zugriff auf das Internet möglich ist, so sollte der Datenverkehr durch einen Virenscanner geprüft werden und aktive Inhalte herausgefiltert werden.

5.6.4 Patchmanagement

52. Umgang mit Patches

Fehler in Software stellen ein großes Problem in ICS dar. Durch die hierdurch verursachten Schwachstellen kann ein Angreifer Zugriff auf das System erlangen oder den Ablauf der Software stören. Daher gilt grundsätzlich, dass diese Fehler behoben werden sollten.

Es sollte ein Patchprozess mit rollenspezifischen Verantwortlichkeiten definiert werden, welcher neben den vom Hersteller freigegebenen Patches und Updates ebenso zusätzliche Drittanbietersoftware berücksichtigt (z. B. Büroanwendungen, PDF-Reader). Der Prozess sollte mindestens folgende Elemente beinhalten:

- Regelmäßige Prüfung auf neue Schwachstellenmeldungen bei den Herstellern der ICS-Komponenten oder Drittanbietersoftware
- Bewertung der Kritikalität von Patches, beispielsweise mit Common Vulnerability Scoring System (CVSS)[3],
- Beziehen der Patches und Updates,
- Testen,
- Freigabeprozess,
- Umgang mit Hersteller-Freigaben von Patches und
- Umgang mit dem Patchen von zusätzlicher Software.

Bezugsquellen für die Meldung von Schwachstellen sind die Hersteller oder auch CERTs.

CVSS ist eine Methodik zur Bewertung und Klassifizierung von Schwachstellen in Abhängigkeit des individuellen Risikos des einzelnen Betriebs. In die Basis-Bewertung (Base-Score) fließt u. A. ein, wie die Schwachstelle ausgenutzt werden kann (z. B. lokal oder entfernt) und welche Konsequenzen drohen (z. B. Denial of Service oder Code-Ausführung). Ein zweiter Wert (temporal-score) bewertet über die Zeit veränderbare Rahmenbedingungen. Dazu zählt z. B. die Verfügbarkeit von Exploit-Code. Eine dritte Komponente stellt den Bezug zur lokalen Umgebung des Anwenders her. Dieser muss anhand seiner Umgebung einschätzen, was dies Schwachstelle für ihn bedeutet. Die ersten beiden Informationen werden auf verschiedenen Webseiten zu Schwachstellen zur Verfügung gestellt (z. B. CVE MITRE, Secunia, Qualys). Eine detaillierte Beschreibung der Vorgehensweise kann der Webseite des Forum of Incident Response and Security Teams (FIRST)[4] entnommen werden.

3 http://www.first.org/cvss
4 http://www.first.org

Das Einspielen von Patches und Updates erfordert gewöhnlich die Freigabe durch den Hersteller des ICS. Daher können in der Regel z. B. bereits im Internet verfügbare Patches und Updates durch den Betreiber nicht eingespielt werden, da ein Funktionsverlust möglich wäre und durch den Hersteller keine Garantie übernommen würde.

Aus diesem Grund sollte der Betreiber mit dem Hersteller vertraglich Zeiträume zur Freigabe und Bereitstellung von Patches und Updates oder alternativen Workarounds für Schwachstellen festlegen. Die Zeiträume sollten möglichst kurz gewählt werden, da in diesem Zeitfenster das betroffene System durch die Schwachstelle einem erhöhten Risiko ausgesetzt ist.

Sofern die Möglichkeit besteht, kann der Betreiber selber vor der Installation Tests durchführen. Alternativ sollten die Updates sequenziell installiert und getestet werden. Hierbei sollten zuerst redundante Systeme bespielt werden. Vor dem Einspielen von Patches und Updates wird empfohlen, für jedes ICS eine Datensicherung durchzuführen. Dies betrifft insbesondere ICS, die notwendig für die Produktion sind. ICS mit keiner oder sehr geringer Bedeutung für die Produktion können ggf. nach der Bestätigung durch eine Risikoanalyse auch ohne vorherige Datensicherung und umfangreiche Tests gepatcht werden.

Zudem sollte geprüft werden, ob ein Neustart nach dem Patch durchgeführt wird oder erforderlich ist. Dies muss bei der Planung berücksichtigt werden.

Insgesamt sollte das Einspielen von Patches in die Betriebszyklen der Anlage integriert werden. So können Wartungsfenster an der Anlage genutzt werden, um Patches zu installieren. Bei redundant ausgelegten Komponenten kann ggf. ein schrittweises Vorgehen gewählt werden, um den Zeitpunkt der Installation nicht zu lange aufzuschieben.

Steht kein Patch zur Verfügung, sollten in einer Risikoanalyse alternative Maßnahmen betrachtet und ergriffen werden, um die Ausnutzung der Schwachstelle zu verhindern. Als alternative Maßnahme ist es beispielsweise möglich, die betroffenen ICS in ein separates Netzsegment zu platzieren und den Datenverkehr zu diesem Netzsegment mittels einer Firewall zu filtern (siehe 32 und 38).

53. Umgang mit End Of Support (EOS)

Falls für ICS-Komponenten oder darin verwendeter Software der End of Support erreicht wird, stellen diese Komponenten aus Securitysicht ein erhöhtes Risiko dar. Dies gilt im speziellen für Software aus dem IT-Umfeld (z. B. Betriebsysteme). In diesem Fällen ist es durchaus möglich, dass weiterhin Schwachstellen entdeckt werden, diese jedoch nicht mehr geschlossen werden. In diesem Fall sind ggf. zusätzliche Schutzmaßnahmen notwendig, z. B. die Migration auf eine neue Softwareversion.

Hierfür sollte eine Risikoanalyse durchgeführt werden und darauf aufbauend sollten in Abhängigkeit der Funktion der ICS und Bedeutung für die Produktion angemessene IT-Sicherheitsmaßnahmen identifiziert werden. So kann beispielsweise eine Separierung von ICS mit ungepatchten Schwachstellen in ein eigenes Netzsegment und einer restriktiven Firewall zur Filterung des Datenverkehrs die Systeme schützen.

Langfristiges Ziel sollte der Austausch der betroffenen ICS durch vom Hersteller unterstützte Komponenten sein. Ohne Support durch den Hersteller können zukünftig auftretende Fehler und Ausfälle die Produktion stark beeinträchtigen, da die Erarbeitung von Lösungen ohne Hilfe durch den Hersteller aufwendiger sind.

Es sollte insbesondere bei der Anschaffung darauf geachtet werden, dass keine Komponenten zum Einsatz kommen, die bereits durch den Hersteller abgekündigt wurden.

5.6.5 Authentisierung

54. Technische Authentisierungsmaßnahmen

Soweit möglich sollte die Nutzung aller ICS eine Authentisierung der Benutzer und Dienste erfordern, sodass eine Bedienung der Systeme nur im authentisierten Zustand möglich ist (vgl. 46, 47). Dazu zählen neben gewöhnlichen Rechnern auch Router, Switches und SPS.

Zur Authentisierung können unterschiedliche Verfahren und Merkmale eingesetzt werden. Es wird zwischen den Authentisierungsmerkmalen Wissen (z. B. Passwort, PIN), Besitz (z. B. Token, Smartcard, Zertifikat) und körperliche Merkmale (z. B. Fingerabdruck, Iriserkennung) unterschieden.

Zusätzlich zu einem Merkmal können auch mehrere Merkmale zur Authentisierung herangezogen werden und so ein höheres IT-Sicherheitsniveau etablieren (z. B. Zwei-Faktor-Authentisierung mittels Token und Passwort). Hierbei sollten Merkmale aus unterschiedlichen Klassen (Wissen, Besitz, Biometrie) kombiniert werden.

Bei der Auswahl der Authentisierungsmethoden ist eine Risikoanalyse durchzuführen. Diese müssen mit weiteren Anforderungen (z. B. Störfallverordnung) und organisatorischen Rahmenbedingungen (z. B. Zugangrestriktionen) abgeglichen werden, um zu einer geeigneten Auswahl zu kommen.

55. Passwortverteilung und -management, Passwort-Richtlinie

Es sollte eine Passwort-Richtlinie erstellt und umgesetzt werden, welche die folgenden Punkte berücksichtigt. Dabei können technische Lösungen als auch organisatorische Maßnahmen festgelegt werden.

- Der Benutzer sollte durch Komplexitätsanforderungen daran gehindert werden, schwache Passwörter zu wählen (z. B. Länge, Alphabet mit Zahlen und Sonderzeichen).
- Das Passwort sollte nur für einen vordefinierten Zeitraum gültig sein. Der Benutzer sollte daraufhin aufgefordert werden, ein neues, vom alten abweichendes Passwort zu wählen.
- Die Anzahl fehlgeschlagener Anmeldeversuche sollte begrenzt werden (z. B. temporäre Sperrung des Benutzerkontos).

Die Verwaltung der genannten Anforderungen sollte vorzugsweise über eine zentrale Management-Lösung realisiert werden (z. B. in einem Verzeichnisdienst innerhalb des ICS).

Nicht alle Maßnahmen sind vollumfassend auf alle ICS anwendbar. So kann beispielsweise ein Angreifer durch provozierte, fehlgeschlagene Anmeldeversuche das Benutzerkonto sperren. Somit wäre ein Zugriff auf das betroffene System durch den legitimen Benutzer nicht mehr möglich. Daher muss der Sicherheitszugewinn durch die jeweilige Maßnahme und mögliche Einschränkungen sonstiger Anforderungen an das ICS (z. B. erforderlicher, unmittelbarer Zugriff) gegeneinander abgewogen werden.

56. Vermeidung von Missbrauch

Ein unbefugter Zugriff auf Systeme sollte verhindert werden. Es sollte erkennbar und dokumentierbar sein, welcher Benutzer aktiv war.

Es gibt bestimmte Betriebssituationen, die einen unmittelbaren Bedienzugriff in das ICS benötigen. Dabei ist eine Abmeldung oder Bildschirmsperre nicht akzeptabel. In diesen Fällen sollten die Systeme durch kompensierende Schutzmaßnahmen vor dem unbefugten Zugriff geschützt werden (z. B. besetzter Leitstand).

In weniger kritischen Bereichen sollte die Bedienung gesperrt werden und lediglich eine Anzeige der aktuellen Informationen erfolgen. Auf diese Weise ist eine Beobachtung weiterhin möglich, der ungehinderte Zugriff jedoch verhindert.

Zur Authentisierung können Lösungen unter Nutzung von Chip- oder RFID-Karten genutzt werden, um die Eingabe von Passworten zu vermeiden.

5.6.6 Zugriffskontrolle

57. Autorisierung

Soweit möglich sollten auf allen ICS in Abhängigkeit von dem angemeldeten Benutzer nur die jeweils erforderlichen Zugriffsrechte vergeben sein. Dementsprechend sollte die Berechtigungsvergabe z. B. auf das Dateisystem dem Prinzip der geringsten Privilegien folgen (engl. *principle of least privilege)*. Einem Benutzer oder Dienst sollten somit nur solche Rechte zugewiesen werden, die zur Durchführung seiner Tätigkeiten erforderlich sind.

Gewöhnlich werden Zugriffsrechte auf Dateisystem-Ebene (Lesen, Schreiben, Ausführen und Löschen von Dateien) und auf Netzebene (Zugriff auf Netze und Netzdienste) vergeben.

Bei der Verwaltung von Benutzern, Gruppen und Berechtigungen (z. B. in Windows-Netzen) ist es zu empfehlen, Benutzerkonten Gruppen zuzuordnen und auf diese Gruppen Berechtigungen zu vergeben. Somit wird ein sogenanntes rollenbasiertes Berechtigungskonzept umgesetzt (engl. Role Based Access Controll; *RBAC)*.

58. Einsatz geeigneter kryptographischer Algorithmen

Wenn kryptographische Algorithmen (z. B. Hashfunktion, symmetrische und asymmetrische Verschlüsselung) zum Einsatz kommen, sollten diese dem Stand der Technik (z. B. BSI TR-02102) entsprechen.

5.6.7 Schutz vor Schadprogrammen

59. Installation und Betrieb von Virenschutzprogrammen

Ist die Installation und der uneingeschränkte Betrieb von Virenschutzprogrammen auf einem ICS möglich und durch den Hersteller freigegeben, sollten diese Systeme automatisiert mit aktuellen Viren-Signaturen versorgt werden (z. B. über einen lokalen Viren-Signaturen-Verteildienst in der DMZ; siehe 62).

Gewöhnlich werden vom Hersteller die folgenden ICS-Komponenten für die uneingeschränkte Installation und den Betrieb von Anti-Virensoftware freigegeben:

- EWS,
- Systeme für die Prozessdatenverarbeitung und -darstellung,
- Bedien- und Beobachtungssysteme,
- Engineeringsysteme,
- Asset Management Systeme und
- Systeme für Konfiguration der Feldgeräte.

60. Geeignete Alternativen für den Fall, dass keine Virenschutzprogramme möglich sind

Es gibt Fälle, bei denen keine oder nur eine eingeschränkte Installation eines Virenschutzprogramms auf einem ICS möglich ist (z. B. es steht kein Virenscanner zur Verfügung). Davon betroffen sind üblicherweise Steuerungssysteme, SPS und Feldgeräte. In diesem Fall müssen zusätzliche, kompensierende Sicherheitsmaßnahmen umgesetzt werden, um die Systeme ausreichend vor Schadprogrammen zu schützen. Die folgende Auflistung führt einige beispielhafte Kriterien zur Identifikation solcher Systeme auf:

- Der Hersteller hat keine Virenschutzprogramme freigegeben.
- Es ist nur ein eingeschränkter Betrieb des Virenschutzes möglich, sodass kein hinreichender Sicherheitsgewinn besteht.
- Die Viren-Signaturen können nicht zeitnah aktualisiert werden (z. B. tägliche Updates).
- Es besteht ein zu hohes Risiko, dass die Verfügbarkeit beeinträchtigt wird.

Ausgehend von individuellen Risikoanalysen für jedes ICS sollte eine angemessene Kombination an kompensierenden Schutzmaßnahmen identifiziert werden. Dazu zählen unter anderem folgende Sicherheitsmaßnahmen:

- Einsatz einer Wechseldatenträgerschleuse, wenn Wechseldatenträger an das Gerät angeschlossen werden (siehe 67),
- falls möglich, regelmäßiges Scannen des ICS von einem Boot-Medium oder USB-Device mit aktuellem Virenschutzprogramm und aktuellen Signaturen, beispielsweise während eines geplanten Wartungsfensters (auf diese Weise kann, wenn auch verspätet, eine Infektion erkannt und dann beseitigt werden),
- Ausgliederung der betroffenen ICS in ein eigenes Netzsegment mit einer Filterkomponente (siehe 64)
- Application Whitelisting (siehe 65)
- Deaktivierung von Dateifreigaben im Netzwerk.

61. Sichere Konfiguration von Virenschutzprogrammen

Aufgrund der hohen Verfügbarkeitsanforderungen in ICS-Umgebungen sollte bei kritischen Systemen u. U. eine angepasste Konfiguration für Virenschutzprogramme verwendet werden. Dabei sollten Einstellungen deaktiviert werden, die zu einer unbeabsichtigten Beeinträchtigung der Produktion führen können (z. B. aufgrund einer hohen System-Last durch einen Scan-Vorgang). Oftmals geben Hersteller nur solche eingeschränkten Konfigurationen zum Betrieb von Virenschutzprogrammen auf den ICS frei.

Virenschutzprogramme können gewöhnlich in zwei unterschiedlichen Modi operieren. Zum einen kann vor dem Zugriff auf Anwendungen oder Dateien allgemein eine Überprüfung stattfinden oder der Scanvorgang wird manuell oder zeitgesteuert ausgelöst. Gewöhnlich sollte das Virenschutzprogramm automatisiert bei allen Zugriffen scannen.

Die Auswahl sollte dabei durch in Abhängigkeit von Empfehlung des Herstellers des Virenschutzprogramms und der ICS-Komponente erfolgen. Sollte eine kontinuierliche Prüfung (z. B. aus Performancegründen) nicht möglich sein, sollten zusätzlich alternative Schutzmaßnahmen ergriffen werden.

Darüber hinaus sollte in regelmäßigen Abständen ein vollständiger Scan aller Daten durchgeführt werden. Ein zusätzlicher, vollständiger Scan mit aktuellen Signaturen sollte nach der Erstinstallation und nach Änderungen am System durchgeführt werden.

Grundsätzlich sollten folgende Einstellungen bei der Konfiguration der Virenschutzprogramme berücksichtigt werden:

- Manuelle Scans sollten ausschließlich bei Stillstand der Produktion durchgeführt und dokumentiert werden..
- Ausschließlich lokale Medien sollten geprüft werden. Netzlaufwerke sollten nicht gescannt werden, um parallele Scans durch mehrere Rechner zu vermeiden.
- Nur der Administrator sollte die Befugnisse haben, das Virenschutzprogramm zu konfigurieren oder zu deaktivieren.

Der Installationsprozess sowie die Konfiguration sollten für jedes ICS dokumentiert werden.

62. Zentraler Viren-Signaturen-Verteildienst

Das ICS-Netz sollte soweit möglich autark betrieben werden und nur zwingend notwendige Verbindungen in andere Netze erlauben. Sind Verbindungen in andere Netze notwendig, so sollte diese nicht direkt erfolgen, sondern immer über einen Proxy-Server .

Daher sollten die Signaturen für das Virenschutzprogramm nicht direkt aus dem Internet, sondern über einen zentralen Viren-Signaturen-Verteildienst in der DMZ bezogen werden. Dieser lädt die aktuellen Signaturen stellvertretend aus dem Internet und stellt sie den ICS zur Verfügung. Somit sind keine direkten Verbindungen der ICS in das Internet erforderlich.

63. Zeitnahe Aktualisierung der Viren-Signaturen

Oftmals sind zeitnahe Updates der Viren-Signaturen und der Virenschutzprogramme in ICS-Umgebungen nicht möglich. Daher sind hierbei folgende Aspekte zu berücksichtigen.

Die ICS sollten gemäß ihres möglichen Update-Intervalls in Gruppen unterteilt werden. Zusätzlich sollten redundant ausgelegte ICS-Komponenten unterschiedlichen Gruppen zugeordnet werden, um beispielsweise auf die Verteilung von fehlerhaften Viren-Signaturen in der Produktionsumgebung (z. B. False Positives) umgehend reagieren zu können.

Die Verteilung der Viren-Signaturen in die Gruppen mit redundanten ICS sollte mit einer Zeitverzögerung durchgeführt werden (z. B. 12 Stunden), um bei Problemen weiterhin den Betrieb mit dem zweiten System aufrecht erhalten zu können.

Aufgrund der hohen Verfügbarkeitsanforderungen sollten nur vom ICS-Hersteller freigegebene und als unkritisch klassifizierte Signaturen verteilt werden.

64. Virenschutzprogramm auf der Firewall (Virus Wall)

Eine Virus-Wall untersucht den Datenverkehr zwischen zwei Netzen auf Schadprogramme. Auf diese Weise kann sie stellvertretend für ICS mit keinem oder eingeschränktem Virenschutzprogramm übermittelte Daten prüfen. Dazu werden diese ICS in ein separates Netzsegment platziert und der Datenverkehr zu und von diesem Netz durch ein Application Level Gateway (ALG) mit installiertem Virenschutzprogramm gefiltert und auf Schadprogramme untersucht.

Es sollte beachtet werden, dass verbreitete ALG-Produkte gewöhnlich ICS-spezifische Protokolle nicht unterstützen. In dem Fall ist eine Prüfung der über dieses Protokoll übermittelten Daten nicht möglich. Dennoch können insbesondere Kollateralschäden durch nicht-zielgerichtete Malware hierdurch weitgehend vermieden werden.

65. Application Whitelisting

Es besteht die Möglichkeit, mittels spezieller IT-Sicherheits-Software zur Applikationskontrolle das Ausführen von Programmen zu überwachen und einzuschränken. Entgegen gängiger Virenschutzprogramme wird nicht versucht unerwünschte Software zu blockieren, sondern es wird der Ansatz verfolgt, ausschließlich erwünschten Programmen die Ausführung zu erlauben.

Demzufolge können zwei unterschiedliche Ansätze unterschieden werden, um Anwendungen und unerwünschtes Verhalten eines Systems zu erkennen und zu verhindern (z. B. im Fall von Schadprogrammen). Bei dem Blacklisting-Ansatz gewöhnlicher Virenschutzprogramme geschieht dies auf der Grundlage bekannter Signaturen und Heuristiken unerwünschter Anwendungen. Diese Herangehensweise weist einige Schwachstellen auf wie z. B., dass sich neuartige Schadprogramme selbstständig bei jeder neuen Kopie verändern können und somit eine neue, noch unbekannte Signatur aufweisen. So ist der erfolgreiche Schutz von der Aktualität und Verfügbarkeit der Signaturen abhängig.

Beim Application Whitelisting werden nur solche Anwendungen und solches Verhalten erlaubt, welches explizit freigegeben wurde. Alles andere ist verboten. Auf diese Weise besteht keine Abhängigkeit zu aktuellen Signaturen. Insbesondere bei Systemen wie im ICS-Umfeld, die nur geringfügigen Änderungen durch Softwareinstallationen unterliegen, eignet sich dieses Verfahren. Daher sollte, soweit möglich, eine Applikationskontrolle immer gemäß dem Whitelisting-Ansatz erfolgen.

Um das Ausführen von unerlaubter Software zu verhindern, kann eine solche Schutzsoftware beispielsweise auf folgende unterschiedliche Attribute zurückgreifen:

- Zertifikate (Signieren von vertrauenswürdiger Software z. B. durch eine zentrale Stelle),
- Dateisystempfad (Bestimmte Bereiche werden als vertrauenswürdig deklariert),
- Hashes (Die Anwendungen und möglicherweise unbefugte Änderungen werden anhand eines Hashes der Dateien identifiziert),
- System- und Benutzerverhalten (z. B. Nutzung gewisser TCP-Ports, Bedienung nur zu bestimmten Zeiten).

Application Whitelisting stellt derzeit keinen äquivalenten Ersatz für ein Virenschutzprogramm dar.

5.6.8 Mobile Datenträger

66. Umgang mit Wechseldatenträgern

Für die Nutzung von Wechseldatenträgern sollten Regelungen für den Umgang aufgestellt und bekannt gemacht werden.

Auf den Komponenten sollte die Nutzung auf bestimmte Geräte eingeschränkt werden (Device Control). Dies ist meist mit Funktionen des Betriebssystems oder über zusätzliche Software möglich.

67. Wechseldatenträgerschleuse (Quarantäne-PC)

Ein Quarantäne-PC kann stellvertretend für ICS Speichermedien auf Schadprogramme prüfen. Hierzu müssen die Mitarbeiter angewiesen werden, Speichermedien aus einer nicht vertrauenswürdigen Quelle (z. B. USB-Sticks) mittels des Quarantäne- PCs auf Schadprogramme zu überprüfen, bevor solche Datenträger in das ICS-Netz eingebracht oder an ICS mit keinem oder eingeschränktem Virenschutzprogramm angeschlossen werden.

Der Quarantäne-PC sollte einen aktuellen Patchstand der Virenschutzprogramme aufweisen und mit aktuellen Schadprogramm-Signaturen bespielt sein. Daher sollten die Signaturen von Quarantäne-PCs mindestens täglich aktualisiert werden.

Zusätzlich zu einer ggf. automatisierten Überprüfung der Speichermedien durch den Quarantäne-PC sollte immer auch ein manueller Scan für den Datenträger durchgeführt werden.

68. Einsatz von Notebooks zu Wartungszwecken

In Anwendungen kommen häufig Notebooks als mobile Wartungsgeräte zum Einsatz. Hinsichtlich des Schutzniveaus sind diese aus Sicht des ICS als Level 4 (sofern sie unter Kontrolle des Betreibers stehen) oder als Level 5 Geräte (sofern sie unter Kontrolle eines externen Serviceanbieters stehen) zu bewerten.

In beiden Fällen bedarf der Einsatz solcher Geräte besonderer Maßnahmen. Grundsätzlich ist vor jedem Einsatz zu definieren, welche Arbeiten auszuführen sind und der Mitarbeiter muss aufgrund seiner Ausbildung und Kenntnisse dazu in der Lage sein. Bei Arbeiten an Anlagen mit besonderem Schutzbedarf (SIL, GMP etc.) ist ggf. durch Zusatzmaßnahmen sicherzustellen, dass keine unbeabsichtigten Änderungen vorgenommen werden.

Es sind technische Sicherungsmaßnahmen (z. B. Schutz der Konfigurationsdaten des Feldgerätes mittels entsprechender Brücke) oder alternativ organisatorische Maßnahmen (Vieraugen Prinzip) anzuwenden.

Interne Geräte:

Über organisatorische Maßnahmen ist sicherzustellen, dass auf diesen Wartungsgeräten ausschließlich Software enthalten ist, die für Wartungszwecke erforderlich ist. Es sollte eine Systemhärtung wie für die Level 3 Geräte durchgeführt werden. Darüber hinaus sollten diese Geräte regelmäßig gepatcht und auf Malware untersucht werden.

Externe Geräte:

Für den Einsatz externer Wartungsgeräte empfiehlt sich zunächst der Abschluss eines entsprechenden Vertrages mit dem externen Anbieter, in welchem die Security Themen (speziell Verhaltensregeln für die externen Mitarbeiter) vertraglich geregelt werden.

Vor dem Einsatz eines externen Wartungsgerätes ist eine Bestandsaufnahme erforderlich. Zu klären ist in diesem Zusammenhang:

- Welche Software ist installiert (inkl. Betriebssystem und Patches)
- Welche Schnittstellen sind vorhanden und aktiv (GPRS!)
- Welcher Schutz für Schadprogramme ist installiert (sind aktuelle Signaturen vorhanden?)

Ist diese Inventarisierung abgeschlossen und hat keine negativen Erkenntnisse geliefert, ist im nächsten Schritt eine Untersuchung auf Malware unter Nutzung eines den betreiberseitigen Festlegungen genügenden Anti-Viren-Schutz durchzuführen.

Ist dieser Test erfolgreich abgeschlossen, so kann Zugang zum Produktivsystem gewährt werden.

In diesem Zusammenhang hat sich bei verschiedenen Anwendern die Nutzung individueller Firewalls (USB betriebene Kompaktgeräte) bewährt. Diese werden zwischen die jeweilige PNK und das Wartungsgerät geschaltet und sollen ungewollte Aktivitäten unterbinden.

69. Aktiviertes BIOS-Passwort und eingeschränkte Boot-Optionen

Durch Änderungen an der BIOS-Konfiguration der ICS kann die Schnittstelle für mobile Datenspeichermedien aktiviert und die Einstellung für das Boot-Medium geändert werden (z. B. USB-Port, CD/ DVD-Laufwerk). Auf diese Weise kann das ICS von externen Medien gestartet werden und ein Angreifer kann Vollzugriff auf das System erlangen.

Daher sollte der Passwort-Schutz des BIOS auf allen ICS aktiviert werden und darüber hinaus das ICS in der Standard-Konfiguration des BIOS nur von dem notwendigen Medium booten (z. B. interne Festplatte). Andere Boot-Optionen sollten deaktiviert sein (z. B. USB-Port, CD/ DVD-Laufwerk).

70. Deaktivierung der Autorun-Funktion

Die Autorun-Funktion sollte auf allen ICS deaktiviert sein. Falls diese Funktion aktiviert ist, können Programme z. B. auf mobilen Datenträgern unbemerkt nach deren Erkennung durch das Betriebssystem gestartet werden. Häufig nutzen Schadprogramme diese Funktion zur Verbreitung über mobile Datenträger.

5.6.9 Datensicherung

71. Datensicherungen der Systeme

Um das Risiko und die Folgen eines Datenverlusts zu reduzieren (z. B. durch unbeabsichtigte Änderungen der Daten, Hardwaredefekte), sollte erwogen werden auf allen IT-Systemen in regelmäßigen Abständen Datensicherungen durchzuführen.

Die zugrunde liegende Backup-Strategie sollte verschiedene Ebenen der Datensicherung umsetzen. Daher sollte für den schnellen Zugriff eine Datensicherung lokal auf den IT-Systemen vorgehalten werden und zusätzlich eine Datensicherung auf einem zentralen System erfolgen.

Abhängig von Aspekten wie der Verfügbarkeitsanforderungen oder Änderungen der Daten bei IT-Systemen kann das Intervall und der Umfang der Datensicherung variieren. So ändert sich beispielsweise die Konfiguration von Switches nur selten. Daher kann in solchen Fällen die Backup-Strategie auf das entsprechende Anwendungsszenario abgestimmt werden, sodass Datensicherungen z. B. ereignisbasiert durchgeführt werden können.

Die folgenden Punkte sollten beim Entwurf eines Datensicherungskonzepts beachtet werden:

- Die Datensicherung sollte inkrementelle als auch vollständige Backups umfassen. Falls möglich sollte die lokale Datensicherung täglich erfolgen. Für diesen Zweck kann beispielsweise eine zweite Festplatte verbaut werden.
- Es sollten Daten zur Sicherstellung der Integrität in der Datensicherung enthalten sein, sodass unbefugte Änderungen oder Defekte erkannt werden.
- Der Umfang der Datensicherung (z. B. inkrementell, vollständig) sollte für jedes IT-System mit dem Datum der zuletzt durchgeführten Datensicherung dokumentiert werden.

Die Datensicherung sollte generell alle Daten auf den Medien des IT-Systems miteinschließen. Dazu zählen beispielsweise:

- Betriebssystem und Firmware,
- Konfigurationen (z. B. Router, Switches, Anwendungen, Firewall Regelwerk),

- Anwendungen,
- Datenbanken,
- Produktionsdaten,
- sonstige Daten (z. B. Protokolldaten).

Datensicherungen sollten sequenziell bei den IT-Systemen durchgeführt werden. Darüber hinaus sollten Datensicherungen bevorzugt im Produktionsstillstand durchgeführt werden, sodass der Sicherungs-Prozess die Produktion nicht beeinträchtigt.

72. Aufbewahrung der Datensicherungen

Zur Sicherstellung der Integrität, Vertraulichkeit und Verfügbarkeit der Daten sollte die Datensicherung gemäß der folgenden Anforderungen gelagert werden:

- Die Speichermedien sollten in einem feuerfesten Tresor mit ausreichender Schutzklasse und in einem separaten Brandabschnitt zu den gesicherten IT-Systemen aufbewahrt werden.
- Der physische Zugriff auf die Speichermedien sollte durch organisatorische und technische Zutritts-, Zugangs- und Zugriffskontrollen verhindert werden (z. B. Vier-Augen-Prinzip, abgeschlossener Tresor).
- Im Notfall sollte der unmittelbare Zugriff auf die Datensicherungen gewährleistet sein.
- Die Aufbewahrungsstätte sollte die klimatischen Anforderungen zur Langzeitspeicherung erfüllen, da eine Lagerung unter falschen Bedingungen die Lebenszeit der Medien verkürzen kann.

5.6.10 Protokollierung und Auswertung

73. Logging / Monitoring

Logging dient dem frühen Erkennen von Fehlern und sicherheitsrelevanten Vorfällen wie beispielsweise unbefugte Zugriffsversuche auf Daten oder Identifikation von Übertragungsengpässen.

Die Protokollierungsdaten sollten auf einem zentralen Server gespeichert werden. So können die Protokollierungsdaten von verteilten Systemen und Komponenten zentral gesammelt, analysiert und in Zusammenhang gebracht werden.

In einem ICS sollten mindestens die folgenden Ereignisse protokolliert und zentral gesammelt werden, soweit diese verfügbar sind:

- lokale Ereignisse, z. B. der Betriebssysteme,
- Ereignisse von Domänen-Controllern,
- Firewall-/Router-/Switch-/Server-Ereignisse,
- Ereignisse der Virenschutzprogramme,
- Ereignisse des IDS/IPS.

Zusätzlich sollten zu den vorher genannten Ereignissen folgende Daten aufgezeichnet werden:

- Datum und Zeit,
- Beschreibung des Ereignisses,
- Kritikalität,
- Quelle des Ereignisses, z. B. Anwendung, Betriebssystem.

Weitere Informationen finden sich in [BSI LogDaten]. Außerdem ist auf die geltenden Datenschutzbestimmungen zu achten. Die Daten sollten durch ein zentrales System überwacht werden. Auf Grundlage von auftretenden Ereignissen und Grenzüberschreitungen bei überwachten Werten sollte ein Alarm ausgelöst werden, der den Administrator darüber informiert.

Die folgende Liste veranschaulicht mögliche Beispiele für solche Ereignisse und Muster:

- Auffälliges Verhalten, welches typisch für Schadprogramme ist (z. B. erhöhter Netzverkehr, Abnahme der Performance, zunehmende Fehler in Anwendungen und Integritätsverletzungen),
- Hardware-Defekte wie fehlerhafte Sektoren bei Datenspeichern (z. B. Festplatte) oder ausfallende Komponenten aufgrund von Hardware-Fehlern,
- Verlust der Netzverbindung,
- ungewöhnlicher Anstieg der CPU-Last und des Speicherverbrauchs.

5.7 Gegenüberstellung mit vorhandenen Standards

Tabelle 6 gibt an, in wie weit die Aspekte der Best Practices von den Normen und Standards

- IEC 62443 (siehe Kapitel 4.1.1.2),
- VDI/ VDE 2182 (siehe Kapitel 4.2.2.1),
- NERC CIP (siehe Kapitel 4.3.1.1) und
- DHS Best Practices (siehe Kapitel 4.3.3)

abgedeckt werden.

	IEC 62443	VDI/ VDE 2182	NERC CIP	DHS Best Practices
1 Aufbau einer Security-Organisation	2-1 Kap. A.3.2.3 2-1 Kap. 4.3.2.3 2-1 Kap. 4.3.2.3	Blatt 1 Kap. 3.2 Blatt 2.1 Kap. 4.2		
2 Erstellen und Pflegen der Dokumentation	2-1 Kap. A.3.4.4 2-1 Kap. 4.2.3.13	Blatt 1 Kap. 3.1 Blatt 1 Kap. 3.5 Blatt 2.1 Kap. 7 Blatt 2.1 Kap. 8 Blatt 3.3 Kap. 4.1.3 Blatt 3.3 Kap. 4.1.4		
3 Etablieren eines Security Managements	2-1 gesamt	Blatt 1 Kap. 3 Blatt 1 Kap. 4	CIP-002-1 CIP-002-2 CIP-002-3 CIP-002-3a CIP-002-3b CIP-002-4 CIP-002-4a CIP-002-5 CIP-003-1 CIP-003-2 CIP-003-3 CIP-003-4 CIP-003-5	
4 Netzplan	2-1 Kap. A.3.4.2.3.3 2-1 Kap. 4.2.3.5	Blatt 1 Kap. 3.3 Blatt 1 Kap. 4.1 Blatt 2.1 Kap. 4.3		PL Kap. 12.2
5 Liste der IT-Systeme und installierten Anwendungen	2-1 Kap. 4.2.3.4 3-1 Kap. 8.7	Blatt 1 Kap. 3.5.1 Blatt 1 Kap. 4.1 Blatt 2.1 Kap. 4.3.1 Blatt 3.3 Kap. 4.1.4		

	IEC 62443	VDI/ VDE 2182	NERC CIP	DHS Best Practices
6 Administrations- und Benutzerhandbücher	2-1 Kap. A.3.3.5	Blatt 1 Kap. 3.5 Blatt 2.1 Kap. 7 Blatt 2.1 Kap. 8		
7 Entwicklung und Integration von Individualsoftware	2-1 Kap. 4.3.4.3.1 2-1 Kap. 4.3.4.3.3 2-1 Kap. 4.3.4.3.4 2-1 Kap. 4.3.4.3.5	Blatt 1 Kap. 4 Blatt 2.1 Kap. 5.5 Blatt 2.1 Kap. 5.7		PL Kap. 5
8 Entsorgung von Hardware	2-1 Kap. 4.3.3.3.9		CIP-007-1 CIP-007-2 CIP-007-2a CIP-007-3a CIP-007-4a CIP-007-5	
9 Auditberichte		Blatt 1 Kap. 4.8		
10 Festlegung der betrieblichen Aufgaben von Betreiber, Integrator und Hersteller				
11 Changemanagement	2-1 Kap. A.3.4.3.6 2-1 Kap. 4.3.4.3.2			
12 Security-Monitoring	2-1 Kap. A.3.4.5 2-1 Kap. 4.3.4.5 2-1 Kap. 4.3.3.3.8	Blatt 2.1 Kap. 4.4	CIP-001-0 CIP-001-1 CIP-001-1a CIP-001-2a CIP-008-1 CIP-008-2 CIP-008-3 CIP-008-4 CIP-008-5	PL Kap. 6.2
13 Wiederherstellungsplan (Business Continuity Plan) für die schützenswerten Assets	2-1 Kap. A.3.2.5 2-1 Kap. A.3.4.3.8		CIP-009-1 CIP-009-2	

	IEC 62443	VDI/ VDE 2182	NERC CIP	DHS Best Practices
	2-1 Kap. 4.3.2.5 2-1 Kap. 4.3.4.3.9		CIP-009-3 CIP-009-4 CIP-009-5	
14 Training des Personals	2-1 Kap. A.3.2.4 2-1 Kap. 4.3.2.4		CIP-004-1 CIP-004-2 CIP-004-3 CIP-004-3a CIP-004-4 CIP-004-4a CIP-004-5	
15 Sicherheit des Personals	3-1 Kap. 10.3, 2-1 Kap. A.3.3.2 2-1 Kap. 4.3.3.2		CIP-004-3 CIP-004-3a CIP-004-4 CIP-004-4a	
16 Prozesse für Einstellung, Wechsel und Ausscheiden von Personal	2-1 Kap. 4.3.3.2			
17 Auditierung	2-1 Kap. A.3.4.2.5.4 2-1 Kap. 4.2.3.10 2-1 Kap. 4.4.2.2	Blatt 1 Kap. 4.8 Blatt 2.1 Kap. 5.8		
18 Komponentenprüfung	2-1 Kap. A.3.4.3.5 2-1 Kap. A.3.4.2.4.2 2-1 Kap. A.3.4.2.4.3 2-1 Kap. 4.3.4.3.1		CIP-007-1 CIP-007-2 CIP-007-2a CIP-007-3a CIP-007-4a CIP-007-5	
19 Vertraulichkeitsvereinbarung mit den Herstellern, Lieferanten und externen Betreibern				PL Kap. 4.7
20 Mitteilung der IT-Security-Anforderungen an den Systemintegrator	2-1 Kap. A.3.4.2.4 2-1 Kap. A.3.4.3	Blatt 1 Kap. 3.1 Blatt 1 Kap. 3.5		

	IEC 62443	VDI/ VDE 2182	NERC CIP	DHS Best Practices
		Blatt 2.1 Kap. 6 Blatt 2.1 Kap. 4.1.1 Blatt 3.3 Kap. 4.1.1 Blatt 3.3 Kap. 4.1.2		
21 Berücksichtigung der IT-Security-Spezifikation des Systemintegrators	2-1 Kap. A.3.4.2.4 2-1 Kap. A.3.4.3	Blatt 1 Kap. 3.1		
22 Robustheit der Produkte	2-1 Kap. A.3.4.2.4.2			
23 Kompatibilität				
24 Verzicht auf überflüssige Produktfunktionen			CIP-007-1 CIP-007-2 CIP-007-2a CIP-007-3a CIP-007-4a CIP-007-5	PL Kap. 2.1
25 Individuelle Zugangsdaten	2-1 Kap. A.3.3.5.3.13			
26 Aktivierte Sicherheitsmechanismen und aktueller Patchstand		Blatt 3.3 Kap. 4.1.4		
27 Langfristige Gewährleistung der IT-Security			CIP-009-1 CIP-009-2 CIP-009-3 CIP-009-4 CIP-009-5	
28 Unterstützung von Virenschutz-Lösungen				
29 Sichere Fernwartung	2-1 Kap. A.3.3.6.5.3 3-1 Kap. 7.4			PL Kap. 10 PL Kap. 12.2
30 Anforderungen an Feldgeräte				PL Kap. 9
31 Physische Absicherung	3-1 Kap. 10.2		CIP-006-1	PL Kap. 11

	IEC 62443	VDI/ VDE 2182	NERC CIP	DHS Best Practices
	2-1 Kap. A.3.3.3 2-1 Kap. 4.3.3.3		CIP-006-1a CIP-006-1b CIP-006-1c CIP-006-2 CIP-006-2a CIP-006-2b CIP-006-2c CIP-006-3a CIP-006-3c CIP-006-3d CIP-006-4c CIP-006-4d CIP-006-5	
32 Netzsegmentierung	2-1 Kap. A.3.3.4 2-1 Kap. A.3.4.2.3.3 2-4 Kap. 4.3.3.4		CIP-005-1 CIP-005-1a CIP-005-2 CIP-005-2a CIP-005-3 CIP-005-3a CIP-005-4a CIP-005-5	PL Kap. 12
33 Absichern der elektronischen, externen Schnittstellen	2-1 Kap. A.3.3.6.5.3		CIP-005-1 CIP-005-1a CIP-005-2 CIP-005-2a CIP-005-3 CIP-005-3a CIP-005-4a CIP-005-5	PL Kap. 10 PL Kap. 12.2
34 Statische Netz-Konfiguration				
35 Gleiche Sicherheitsmaßnahmen für ICS in einem Netzsegment	2-1 Kap. A.3.4.2.3.3			

	IEC 62443	VDI/ VDE 2182	NERC CIP	DHS Best Practices
36 Unabhängiger Betrieb der Netzsegmente				
37 Absichern der Funktechnologien				PL Kap. 13
38 Einsatz von Firewalls	3-1 Kap. 6.2			PL Kap. 3.1
39 Host-based Firewalls	3-1 Kap. 6.3			
40 Datendiode (One-Way-Gateway)				
41 Geeignete logische Trennung und VLAN	3-1 Kap. 6.4			
42 Implementierung von Intrusion-Detection- bzw. Intrusion-Prevention-Systemen	3-1 Kap. 8.4			PL Kap. 2.2 PL Kap. 3.2
43 Nutzung von sicheren Protokollen				PL Kap. 4.2 PL Kap. 10.3
44 Namensauflösung (DNS)				PL Kap. 8.1
45 Zeitsynchronisierung				
46 Standard-Benutzerkonten und -Passwörter	2-1 Kap. 3.3.5.3.9 2-1 Kap. 4.3.3.5.5 2-1 Kap. 4.3.3.5.7 2-1 Kap. A.3.3.5.3.13		CIP-007-1 CIP-007-2 CIP-007-2a CIP-007-3a CIP-007-4a CIP-007-5	PL Kap. 4.1
47 Individuelle Benutzerkonten	2-1 Kap. A.3.3.5.3.7 2-1 Kap. 4.3.3.5.2			PL
48 Entfernen von unnötiger Software und Diensten			CIP-007-1 CIP-007-2 CIP-007-2a CIP-007-3a CIP-007-4a CIP-007-5	PL Kap. 2.1

	IEC 62443	VDI/ VDE 2182	NERC CIP	DHS Best Practices
49 Anpassen der Standard-Einstellungen	2-1 Kap. A.3.3.5.3.13			PL
50 Anpassen der Hardware-Konfiguration				PL Kap. 2.4
51 Zugriff auf das Internet innerhalb des ICS-Netzwerk				
52 Umgang mit Patches	2-1 Kap. A.3.4.2.5.2 2-1 Kap. 4.3.4.3.7 2-1 Kap. 4.3.4.5.3 2-1 Kap. A.3.4.2.3.5	Blatt 2.1 Kap. 4.4	CIP-007-1 CIP-007-2 CIP-007-2a CIP-007-3a CIP-007-4a CIP-007-5	PL Kap. 2.6 PL Kap. 6.1 PL Kap. 6.2
53 Umgang mit End Of Support (EOS)	2-1 Kap. A.3.4.2.3.5			
54 Technische Authentisierungsmaßnahmen	2-1 Kap. A.3.3.6 2-1 Kap. 4.3.3.6 3-1 Kap. 5.3 3-1 Kap. 5.4 3-1 Kap. 5.5 3-1 Kap. 5.6 3-1 Kap. 5.7 3-1 Kap. 5.10		CIP-007-1 CIP-007-2 CIP-007-2a CIP-007-3a CIP-007-4a CIP-007-5	
55 Passwortverteilung und -management, Passwort-Richtlinie	3-1 Kap. 5.9		CIP-007-1 CIP-007-2 CIP-007-2a CIP-007-3a CIP-007-4a CIP-007-5	PL Kap. 4.3
56 Vermeidung von Missbrauch				
57 Autorisierung	2-1 Kap. A.3.3.5 2-1 Kap. A.3.3.7 2-1 Kap. 4.3.3.5		CIP-007-1 CIP-007-2 CIP-007-2a	PL Kap. 2.3 PL Kap. 4.5

	IEC 62443	VDI/ VDE 2182	NERC CIP	DHS Best Practices
			CIP-007-3a CIP-007-4a CIP-007-5	
58 Einsatz geeigneter kryptographischer Algorithmen	3-1 Kap. 7.2 3-1 Kap. 7.3 3-1 Kap. 7.4 3-1 Kap. 5.2			PL Kap. 4.2
59 Installation und Betrieb von Virenschutzprogrammen	3-1 Kap. 8.3 2-1 Kap. 4.3.4.3.8		CIP-007-1 CIP-007-2 CIP-007-2a CIP-007-3a CIP-007-4a CIP-007-5	PL Kap. 7
60 Geeignete Alternativen für den Fall, dass keine Virenschutzprogramme möglich sind				PL Kap. 7
61 Sichere Konfiguration von Virenschutzprogrammen				PL Kap. 7
62 Zentraler Viren-Signaturen-Verteildienst				
63 Zeitnahe Aktualisierung der Viren-Signaturen	2-1 Kap. A.3.4.2.4.2		CIP-007-1 CIP-007-2 CIP-007-2a CIP-007-3a CIP-007-4a CIP-007-5	PL Kap. 7
64 Virenschutzprogramm auf der Firewall (Virus Wall)				
65 Application Whitelisting				
66 Umgang mit Wechseldatenträgern				
67 Wechseldatenträgerschleuse (Quarantäne-PC)				

	IEC 62443	VDI/ VDE 2182	NERC CIP	DHS Best Practices
68 Einsatz von Notebooks zu Wartungszwecken				
69 Aktiviertes BIOS-Passwort und eingeschränkte Boot-Optionen				
70 Deaktivierung der Autorun-Funktion				
71 Datensicherungen der Systeme	2-1 Kap. 4.3.4.3.9			
72 Aufbewahrung der Datensicherungen	2-1 Kap. A.3.4.3.8			
73 Logging / Monitoring	3-1 Kap. 8.2 3-1 Kap. 8.6 3-1 Kap. 8.7 3-1 Kap. 8.8 2-1 Kap. 4.3.3.5.8 2-1 Kap. 4.3.3.6.4		CIP-007-1 CIP-007-2 CIP-007-2a CIP-007-3a CIP-007-4a CIP-007-5	PL Kap. 4.4

Tabelle 6 Gegenüberstellung der Best Practices mit IEC 62443, VDI/ VDE 2182, NERC CIP und DHS Best Practices

Tabelle 7 zeigt die Abdeckung der Best Practices durch bestehende Maßnahmen der IT-Grundschutz-Kataloge (12. Ergänzungslieferung). Sie wird in der nachfolgenden Tabelle in der Spalte Abd eckung (Abd) wie folgt indiziert:

- „E“ Best Practices wird eins zu eins von der IT-Grundschutz-Maßnahme abgedeckt.
- „M“ Best Practices wird von mehreren IT-Grundschutz-Maßnahmen zusammen abgedeckt.
- „T“ Best Practices wird in Teilen von Grundschutz-Maßnahme abgedeckt. (Zusatz hier: in welchen Teilen, siehe Spalte Bemerkung)
- „-/-“ Best Practices wird von keiner Grundschutz-Maßnahme abgedeckt.

Entsprechend ist in Tabelle 7 der Abdeckungsgrad durch die Anforderungen des Standards ISO/IEC 27001 (siehe Kapitel 4.1.1.1 unter Berücksichtigung der jeweils zugeordneten Controls der ISO/IEC 27002. Dabei wird die oben genannte Indizierung mit „E“, „M“, „T“ und „-/-“ entsprechend für Controls nach ISO/IEC 27001 und ISO/IEC 27002 sowie Kapitel aus dem Managementrahmen der ISO 27001 angewandt.

Hinweis: Wenn in den Bemerkungen der nachfolgenden Tabelle das Wort „hier“ verwendet wird, meint es die jeweilige Best Practice (erste Spalte) wie sie im vorliegenden Dokument enthalten ist.

	IT-Grund-schutz	Abd	Bemerkung	ISO 27001	Abd	Bemerkung
1 Aufbau einer Security-Organisation	M 2.193 M 2.336	M	Das Security-Programm sollte entsprechend durch ein Sicherheitskonzept nach IT-Grundschutz abgedeckt sein.	A.6.1.1 A.6.1.2 A.6.1.3	M	
2 Erstellen und Pflegen der Dokumentation	M2.201	E		4.3.2	E	
3 Etablieren eines Security Managements	BSI 100 B 1.0 B 1.16	M		4.1 4.2	M	
4 Netzplan	M 2.139	E	Anm.: Ebenfalls gemäß BSI 100-2, Kap. 4.2.3	A.7.1.1 A.10.6.1	T	Die Forderung nach einem Netzplan ergibt sich implizit aus den Controls. Konkrete Anforderungen nach einem physischen und einem logischen Netzplan und deren Inhalte existieren nicht.
5 Liste der IT-Systeme und installierten Anwendungen	B 4.2 M 2.168 M 2.171 M 2.25 M 2.10	M	Anm.: Ebenfalls gemäß BSI 100-2, Kap. 4.2.2 und 4.2.4	A.7.1.1		
6 Administrations- und Benutzerhandbücher	M 2.25 M 2.111 M 2.219	M		A.10.1.1	E	Anm.: Das Control fordert generell dokumentierte Betriebsprozesse.
7 Entwicklung und Integration von Individualsoftware	M 2.378	E	Wird zusätzlich auch durch M 2.379 unterstützt	A.12.5 A.12.5.2	T	ISO 27001 fordert keine explizite Richtlinie zur Software-Entwicklung.

	IT-Grund-schutz	Abd	Bemerkung	ISO 27001	Abd	Bemerkung
8 Entsorgung von Hardware	B 1.15	M	Innerhalb dieses Bausteins insbesondere M 2.13, M 2.431, M 2.436	A.9.2.6	E	
9 Auditberichte	M 2.119	E		6	E	
10 Festlegung der betrieblichen Aufgaben von Betreiber, Integrator und Hersteller	M 2.1 M 2.225	T	Die Maßnahmen behandeln Verantwortlichkeiten und Befugnisse nur generell, nicht aber speziell für die hier genannten Beteiligten.	A.6.1.3 A.6.2.3	T	Auch diese Controls behandeln die Zuweisung von Verantwortung für Informationssicherheit auf verschiedene Rollen bzw. Parteien (nur) allgemein.
11 Changemanagement	B 1.14	M		A.10.1.2 A.12.5.1	M	
12 Security-Monitoring	B 1.8 M 6.60 M 6.65	M	Teil: Melden der Sicherheitsvorfälle allgemein. Hier wird jedoch zusätzlich die explizite Meldung an die zuständige Behörde verlangt.	A.6.1.6 A.13 A.13.1.1 A.13.2.1	M	Teil: Melden der Sicherheitsvorfälle allgemein. Hier wird jedoch zusätzlich die explizite Meldung an die zuständige Behörde verlangt.
13 Wiederherstellungsplan (Business Continuity Plan) für die schützenswerten Assets	B 1.3 B 1.4	M		A.10.5.1 A.14 A.14.1.3 A.14.1.4 A.14.1.5	M	
14 Training des Personals	B 1.13 M 3.45 M 3.51	M		5.2.2 A.8.2.2	M	

	IT-Grund-schutz	Abd	Bemerkung	ISO 27001	Abd	Bemerkung
15 Sicherheit des Personals	B 1.2 M 2.30 M 2.220	T	Schutz von Personen vor Gefahr für Leib und Leben Safety ist nicht abgedeckt	A.8.1.1 A.8.1.2 A.8.1.3 A.8.2.1 A.6.1.5 A.11.2.4	T	Schutz von Personen Safety ist nicht abgedeckt
16 Prozesse für Einstellung, Wechsel und Ausscheiden von Personal	M 3.6	E		A.8.3.1 A.8.3.2 A.8.3.3	M	
17 Auditierung	M 2.199	E	Anm.: Das Thema Auditierung wird außerdem generell in BSI 100 behandelt und technik-bezogen in zahlreichen Bausteinen mit einzelnen Maßnahme, z.B. M 4.81, M 4.298, M 4.368, M 2.360...	6 A.6.1.8	M	
18 Komponentenprüfung	M2.199	E	Anm.: Testen vor Freigabe wird darüber hinaus z.B. in M 4.65 behandelt	A.15.2.2 A.10.3.2	M	
19 Vertraulichkeitsvereinbarung mit den Herstellern, Lieferanten und externen Betreibern	M 3.55 M 2.307	M		A.6.1.5 A.6.2.3	T	

	IT-Grund-schutz	Abd	Bemerkung	ISO 27001	Abd	Bemerkung
20 Mitteilung der IT-Security-Anforderungen an den Systemintegrator	M 2.80	T	Teil: In M 2.80 wird grundsätzlich ein Anforderungskatalog verlangt. Die vorliegende Best Practice hingegen bezieht sich konkret auf Anforderungen vom ICS- Betreiber an den Systemintegrator. Anm.: Generell werden Dienstleistungen durch Dritte in B 1.11 behandelt.	A.12.1.1	T	Teil: Nach A.12.1.1 sind generell Anforderungen an an Informationssysteme zu spezifizieren. Die vorliegende Best Practice hingegen bezieht sich konkret auf Anforderungen vom ICS-Betreiber an den Systemintegrator. Anm.: Generell werden Dienstleistungen durch Dritte in A.10.2.1 behandelt.
21 Berücksichtigung der IT-Security-Spezifikation des Systemintegrators	-/-	-/-		-/-	-/-	
22 Robustheit der Produkte	-/-	-/-	Anm.: Wie in der vorhergehenden Best Practice geht es hier um Produkteigenschaften. Dies wird so nicht von ISMS-Anforderungen abgedeckt.	-/-	-/-	
23 Kompatibilität	-/-	-/-		-/-	-/-	
24 Verzicht auf überflüssige Produktfunktionen	-/-	-/-	Anm.: Hier geht es um Produkteigenschaften, die Maßnahme M 4.95 bezieht sich lediglich auf ein minimales Betriebssystem.	-/-	-/-	

	IT-Grund-schutz	Abd	Bemerkung	ISO 27001	Abd	Bemerkung
25 Individuelle Zugangsdaten	M 4.7	E	Anm.: Auch in M 4.201 (für Router und Switches)	A.11.5.2	T	Teil: Personenbezogene (individuelle) Zugangsdaten. Der Austausch von Standardpasswörtern bei Auslieferung wird in A.11.5.2 nicht explizit gefordert.
26 Aktivierte Sicherheitsmechanismen und aktueller Patchstand	M 2.318 M 4.237 M 4.95	M		-/-	-/-	Anm.: A.10.3.2 fordert die Abnahme eines Systems vor produktiver Nutzung, nicht aber wie hier die explizite Aktualität und Aktivierung von Sicherheitsfunktionen.
27 Langfristige Gewährleistung der IT-Security	-/-	-/-	Anm.: Es existieren zahlreiche Baustein-) spezifische Maßnahmen zur Wartung oder zu Verträgen. M 2.4, M 2.27, M 2.213, M 2.369, M 2.253 ... Das Thema „End of Support“ wird aber nicht explizit behandelt.	-/-	-/-	
28 Unterstützung von Virenschutz-Lösungen	B 1.6	T	Teil: Schutz vor Schadprogrammen allgemein in B 1.6. Hier liegt der Fokus allerdings auf der Fähigkeit der ICS Virenschutz-Lösungen zu unterstützen.	A.10.4.1	T	Teil: Schutz vor Schadprogrammen allgemein in A.10.4.1. Hier liegt der Fokus allerdings auf der Fähigkeit der ICS Virenschutz -Lösungen zu unterstützen.

	IT-Grund-schutz	Abd	Bemerkung	ISO 27001	Abd	Bemerkung
29 Sichere Fernwartung	M 5.33 B 4.4	T	Teil: Hier wird die Zwei-Faktor- Authentisierung und ein Vier-Augen-Prinzip gefordert. M 5.33 verlangt dies nicht explizit	A.11.4.2	T	Teil: Hier wird die Zwei-Faktor- Authentisierung und ein Vier-Augen-Prinzip gefordert. A.11.4.2 verlangt dies nicht explizit
30 Anforderungen an Feldgeräte	-/-	-/-	Anm.: Im Prinzip wird hier ein Sicherheitskonzept für End Devices gefordert.	-/-	-/-	
31 Physische Absicherung	B 2.1 B 2.9 M 1.55 M 1.13 M 2.17 M 1.73 M 1.49 M 2.6 M 1.29	M		A.9.1.1 A.9.1.2 A.9.2.1	M	
32 Netzsegmentierung	B 4.1 M 5.61 M 5.62 M 5.77 M 2.141	M	Anm.: Die Forderungen zur Netzwerksegmentierung werden grundsätzlich abgedeckt. Hier wird jedoch konkret das ICS-Netz betrachtet.	A.11.4.5 A.10.6.1	M	Anm.: Die Forderungen zur Netzwerksegmentierung werden grundsätzlich abgedeckt. Hier wird jedoch konkret das ICS-Netz betrachtet.

	IT-Grund-schutz	Abd	Bemerkung	ISO 27001	Abd	Bemerkung
33 Absichern der elektronischen, externen Schnittstellen	B 4.1 B 4.3 B 4.4 B 4.5 B 4.6 B 3.301 M 2.139 M 2.204 M 5.150 M 5.141 M 4.81 M 5.39	M		A.10.6.1 A.10.6.2 A.11.4.2 A.11.4.3 A.10.10.1 A.10.10.2	T	Anm.: Die Forderungen zur Absicherung und Überwachung externer Schnittstellen werden grundsätzlich abgedeckt. Hier werden jedoch auch spezielle Schnittstellen (z.B. Modem) in das ICS-Netz betrachtet.
34 Statische Netz-Konfiguration	-/-	-/-	Anm.: Einzelne Maßnahmen wie *M 4.294 Sichere Konfiguration der Access Points* fordern statische IP, aber nur in speziellem Kontext	-/-	-/-	
35 Gleiche Sicherheitsmaßnahmen für ICS in einem Netzsegment	M 5.77 M 2.141	T	Teil: Die Grundschutz-Maßnahmen fordern Anwendungen und Systeme mit gleichem Schutzbedarf in einer Zone zu platzieren. Hier werden aber (umgekehrt) gleiche Sicherheitsmaßnahmen für alle ICS einer Zone verlangt.	A.11.4.5	T	Teil: Dieses Control fordert die Trennung der Netze (vgl. Grundschutz). Hier werden aber gleiche Sicherheitsmaßnahmen für alle ICS einer Zone verlangt.
36 Unabhängiger Betrieb der Netzsegmente	-/-	-/-		-/-	-/-	

	IT-Grund-schutz	Abd	Bemerkung	ISO 27001	Abd	Bemerkung
37 Absichern der Funktechnologien	B 4.6 B 4.8 M 2.381 M 4.133 M 4.293 M 4.294 M 4.298 M 5.77	M		A.11.4.2	T	Teil: Das Absichern der Funknetze wird nur in ISO 27002 und nur generell behandelt.
38 Einsatz von Firewalls	B 3.301	M		A.11.4.5 A.11.4.6 A.11.4.7	M	
39 Host-based Firewalls	M 4.238	E		-/-	-/-	Anm.: Keine Controls explizit zu Host-basierten Firewalls
40 Datendiode (One-Way-Gateway)	-/-	-/-		-/-	-/-	
41 Geeignete logische Trennung und VLAN	M 4.202 M 4.203 M 5.6.2	E	Anm.: M 4.203 stellt lediglich die Checkliste passend zu M 4.202 dar.	-/-	-/-	Anm.: Keine Controls explizit zu VLAN
42 Implementierung von Intrusion-Detection- bzw. Intrusion-Prevention-Systemen	M 5.71	E		-/-	-/-	Anm.: IDS wird nur als weitere Information oder indirekt in den Controls erwähnt.
43 Nutzung von sicheren Protokollen	M 5.39	E	Anm.: Die Vermeidung unsicherer Protokolle wird zusätzlich auch in einigen anderen Maßnahmen behandelt.	-/-	-/-	Anm.: Keine Controls explizit zur Vermeidung unsicherer Protokolle
44 Namensauflösung (DNS)	B 5.18 M 2.451	M		-/-	-/-	Anm.: Keine Controls explizit zu DNS

	IT-Grund-schutz	Abd	Bemerkung	ISO 27001	Abd	Bemerkung
45 Zeitsynchronisierung	M 4.227	E		A.10.10.6	E	Anm.: Dieses Control verlangt nicht explizit einen NTP-Dienst im eigenen ICS-)Netz.
46 Standard-Benutzerkonten und -Passwörter	M 4.7	E	Anm.: Auch in M 4.201 (für Router und Switches)	A.11.5.2	T	Teil: Personenbezogene (individuelle) Zugangsdaten. Der Austausch von Standardpasswörtern bei Auslieferung wird in A.11.5.2 nicht explizit gefordert.
47 Individuelle Benutzerkonten	M 2.220 M 2.30	M	Anm.: Wird darüber hinaus auch z.B. in M 4.244 und M 2.322 behandelt	A.11.5.2	E	
48 Entfernen von unnötiger Software und Diensten	M 4.95 B 3.301	M		A.11.4.6	T	Teil: Nur die Kontrolle des Netzes, nicht aber die Entfernung unnötiger Software und Dienste wird behandelt.
49 Anpassen der Standard-Einstellungen	M 4.237 M 4.82	M	Anm.: Wird darüber hinaus auch in anderen, Objekt-spezifischen Maßnahmen behandelt, u.a. M 4.201,.M 4.244,	A.12.5.3	T	Teil: Control behandelt nur die Kontrolle der Änderungen, nicht aber das eigentliche Anpassen der Standard -Einstellungen selbst.
50 Anpassen der Hardware-Konfiguration	M 4.4 M 4.200	M		-/-	-/-	Anm.: Keine Controls explizit zur Entfernung nicht benötigter Hardware (-Schnittstellen).

	IT-Grund-schutz	Abd	Bemerkung	ISO 27001	Abd	Bemerkung
51 Zugriff auf das Internet innerhalb des ICS-Netzwerk	M 5.69	E		A.10.4.2	T	Teil: Dieses Control lässt auch den kontrollierten Umgang mit aktiven Inhalten zu. Hier wird allerdings generell eine Verhinderung der Ausführung verlangt.
52 Umgang mit Patches	B 1.14 M 2.35 M 2.273	M E T	Teil: Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates wird in M 2.273 behandelt, Patchmanagement generell in B 1.14. Die Freigabe durch Dritte (Vermeidung von Garantie-verlust, etc) wird nicht behandelt.	A.10.1.2 A.12.6.1	M E	
53 Umgang mit End Of Support (EOS)	-/-	-/-		-/-	-/-	
54 Technische Authentisierungsmaßnahmen	M 4.15 M 2.7	T	Teil: Authentisierung wird im Control gefordert, nicht jedoch eine Zwei-Faktor-Authentisierung.	A.11.5.2	T	Teil: Authentisierung wird im Control gefordert, nicht jedoch eine Zwei-Faktor-Authentisierung.
55 Passwortverteilung und -management, Passwort-Richtlinie	M 2.11	E		A.11.3.1	E	
56 Vermeidung von Missbrauch	M 4.2	E		A.11.3.2	E	

	IT-Grund-schutz	Abd	Bemerkung	ISO 27001	Abd	Bemerkung
57 Autorisierung	M 2.8 M 2.30	M		A.11.2.2 A.11.6.1	M	Anm.: Die Best-Practice mit Gruppenberechtigungen zu arbeiten, wird in den Controls nicht behandelt.
58 Einsatz geeigneter kryptographischer Algorithmen	M 2.164	E	Anm.: Die Maßnahme enthält keine Referenz auf BSI TR 02102 (wenngleich doch beides vom BSI kommt)	A.12.3.1	T	Teil: Das Control fordert Risikobetrachtungen bzgl. Stärke und der Qualität der verwendeten Algorithmen. Ergebnis muss nicht der Stand der Technik sein.
59 Installation und Betrieb von Virenschutzprogrammen	B 1.6	M		A.10.4.1	E	
60 Geeignete Alternativen für den Fall, dass keine Virenschutzprogramme möglich sind	M 2.224	T	Teil: Nur Vorbeugung gegen Schadprogramme, die aber nicht als Alternativen gedacht sind.	-/-	-/-	
61 Sichere Konfiguration von Virenschutzprogrammen	M 4.3	T	Teil: Die Konfiguration der Virenschutzprogramme wird in der Maßnahme grundsätzlich behandelt. Hier werden jedoch weitere spezifische Anforderungen für Produktionsumgebungen gestellt.	-/-	-/-	

	IT-Grund-schutz	Abd	Bemerkung	ISO 27001	Abd	Bemerkung
62 Zentraler Viren-Signaturen-Verteildienst	-/-	-/-	Anm.: M 2.159 fordert die Aktualisierung der eingesetzten Viren-Schutzprogramme und Signaturen, aber keinen zentralen Viren-Signaturen-Verteildienst.	-/-	-/-	
63 Zeitnahe Aktualisierung der Viren-Signaturen	B 1.6 M 2.159	T	Teil: M 2.159 fordert die zeitnahe Aktualisierung der Viren-Schutzprogramme und Signaturen. Hier wird aber eine gruppenweise und verzögerte Verteilung der Signaturen nach ausgiebigen Test verlangt.	-/-	-/-	
64 Virenschutzprogramm auf der Firewall (Virus Wall)	-/-	-/-	Anm.: M 4.3 fordert die Prüfung auf Schadprogramme bei Datenübertragung im Allgemeinen, jedoch keine „ Virus Wall “	-/-	-/-	
65 Application Whitelisting	-/-	-/-		-/-	-/-	
66 Umgang mit Wechseldatenträgern	M 4.4	E	Anm.: Generell auch in B 5.14	A.10.7.1	T	Teil: Das Control erfasst Wechselmedien generell, erfordert jedoch nicht zwingend technische Kontrollen.
67 Wechseldatenträgerschleuse (Quarantäne-PC)	M 2.235	E		-/-	-/-	

	IT-Grund-schutz	Abd	Bemerkung	ISO 27001	Abd	Bemerkung
68 Einsatz von Notebooks zu Wartungszwecken	-/-	-/-		-/-	-/-	
69 Aktiviertes BIOS-Passwort und eingeschränkte Boot-Optionen	M 4.84	E		-/-	-/-	
70 Deaktivierung der Autorun-Funktion	M 4.57	E	Anm.: Auch in weiteren Maßnahmen wie M 4.280 und M 4.339	-/-	-/-	
71 Datensicherungen der Systeme	B 1.4	E		A.10.5	E	
72 Aufbewahrung der Datensicherungen	B 1.4	E		A.10.5	E	
73 Logging / Monitoring	B 1.8 B 4.2 M 4.225 M 5.9 M 4.312 M 2.157 M 4.205 M 2.133 M 2.140	M	Anm.: Weitere Maßnahmen behandeln das Monitoring unter spezifischen Aspekten (z.B. M 4.276, M 2.365 bei Windows Server 2003; M 4.321 für VPNs; M 6.130 zur Erkennung von Sicherheitsvorfällen	A.10.3.1 A.10.6.1 A.10.10.1 A.10.10.2 A.10.10.3 A.10.10.4	M	Anm.: Die Forderung nach einem Loghost ergibt sich implizit aus A.10.10.3. Teil: Die Controls konzentrieren sich auf die Überwachung der Zugangs- und Zugriffsversuche sowie Systemalarme. Monitoring der regulären Zustände steht weniger im Fokus.

Tabelle 7 Gegenüberstellung der Best Practices mit IT-Grundschutz und ISO 27001

6 Methodik für Audits von ICS-Installationen

Dieses Kapitel beschreibt eine Methodik für die Durchführung von Audits in ICS-Installationen. Dabei werden methodische Eckpunkte einer Auditierung dargestellt und die Phasen eines ICS-Audits im zeitlichen Verlauf beschrieben. Diese Eckpunkte beschreiben eine umfassende und ganzheitliche Auditierung (Maximalforderung), die je nach geltenden Rahmenbedingungen angepasst und verschlankt werden sollte.

6.1 ICS-Spezifika und IS-Revision

Die im Kapitel 4.2.2.1 vorgestellte VDE-Richtlinie 2182 beschreibt ein konkretes Vorgehensmodell zur Umsetzung von Schutzmaßnahmen und betrachtet den gesamten Lebenszyklus von ICS. Audits werden dabei als zeitlich oder ereignisgesteuerte Maßnahme beschrieben, die regelmäßig durchzuführen ist. Audit-Ergebnisse sind zu dokumentieren, um Mängel und Abweichungen festzustellen.

Die Informationssicherheitsrevision (IS-Revision) auf Basis von IT-Grundschutz legt den Schwerpunkt auf die ganzheitliche Prüfung der Informationssicherheit in einem Unternehmen oder einer Verwaltung. Dabei werden vom Aufbau einer Informationssicherheitsorganisation über Personalaspekte bis zur Konfiguration von Systemen alle Ebenen geprüft[5]. ICS-Spezifika werden von der IS-Revision jedoch nicht berücksichtigt, da sie sich allein auf die IT-Infrastruktur einer Organisation konzentriert.

Aufbauend auf der VDE-Richtlinie 2182 und dem Konzept der IS-Revision, erweitert um ICS-spezifische Systemeigenschaften, wird im Folgenden eine Audit-Methodik für ICS beschrieben. Diese stellt eine Methode der Erfolgskontrolle dar und dient zur Überprüfung von Sicherheitskonzept, -organisation und der Maßnahmenumsetzung.

Bei der Planung und Durchführung von Audits im Bereich ICS ist besonders darauf zu achten, dass die Durchführenden (insbesondere externe Dienstleister) nicht nur über die erforderlichen Fachkenntnisse hinsichtlich IT-Sicherheit verfügen, sondern auch die jeweils geltenden industriespezifischen Qualifikationen haben, die zum Umgang mit den jeweiligen Anlagen befähigen.

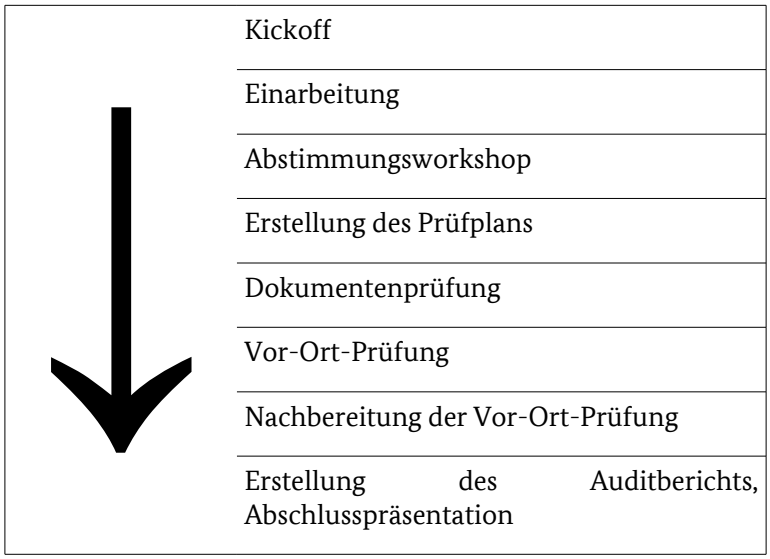
Audits sind ein wichtiger Baustein sicherer ICS und sollten daher umgesetzt werden. Der konkrete Umfang eines Audits ist dabei für das jeweilige Unternehmen passend zu wählen – insbesondere mit Blick auf die Unternehmensgröße und die zur Verfügung stehenden finanziellen Mittel. Hierbei sind sowohl Testbreite (welche Systeme) und Testtiefe (Art und Umfang der Prüfmethoden) zu bewerten.

Ein ogligatorischer Bestandteil eines Audits ist eine Risikoanalyse, in der insbesondere mögliche Folgen der durchgeführten Tests (Wechselwirkungen, funktionale Konsequenzen, etc.) betrachtet werden. Hieraus ergeben sich mitunter strenge Limitierungen bzgl. der möglichen Tests.

6.2 Ablauf

Der Ablauf der Auditierung kann in die folgenden acht Phasen unterteilt werden.

5 Informationssicherheitsrevision, vgl. [IS 10]



6.2.1 Kickoff

Die Vorbereitung des Audits beginnt mit einem Auftaktgespräch (Kickoff), in dem die Beteiligten über die weitere Vorgehensweise informiert werden und ihre jeweilige Aufgabe festgelegt wird. Notwendige Zustimmungen von Beteiligten werden beim Kickoff gegeben oder in der Folge des Gesprächs nach Rücksprache in Entscheidungsgremien eingeholt (z. B. seitens Geschäftsführung oder Betriebsrat). Zwingend von Beginn an zu beteiligen sind neben den IT-Verantwortlichen insbesondere diejenigen Personen, welche die Betriebsverantwortung für die jeweiligen Anlagen tragen.

Das Auditteam wird den anderen Beteiligten vorgestellt. Der Projektverantwortliche erläutert die geplante Vorgehensweise in technischer sowie organisatorischer Hinsicht und beantwortet die sich unmittelbar ergebenden Fragen. Mögliche Bedenken seitens der Systemverantwortlichen (Betriebsverantwortung) sollten während des Gesprächs vorgebracht werden, damit diese als später zu berücksichtigende Rahmenbedingung erkannt und in das Protokoll aufgenommen werden können. Fachexperten des Teams und korrespondierende Fachverantwortliche auf Betreiberseite (z. B. SPS-Spezialisten, Netzspezialisten) sollten sich persönlich kennenlernen können und direkte Kommunikationskanäle aufbauen. Eine grobe Terminplanung der nächsten Schritte sollte erfolgen. Im Vorfeld des Kickoffs wurden dazu bereits Meilensteinplanungen vorab mitgeteilt, damit sich die Beteiligten vorbereiten und Kollisionen mit anderen terminkritischen Projekten erkennen können.

Die für die weiteren Phasen benötigte Dokumentation wird beschrieben und bei den Fachverantwortlichen angefordert. Gegenseitige Informationspflichten sind zu fixieren und allen mitzuteilen, die nicht persönlich beim Auftaktgespräch anwesend sind.

Ziele des Kickoffs sind die Klärung der groben Rahmenbedingungen für die Auditierung und die Festlegung der Verantwortlichkeiten.

6.2.2 Einarbeitung

Liegen Dokumentation und ausstehende Zustimmungen vor, kann das Auditteam mit der Einarbeitung beginnen. Es gewinnt einen Überblick über die zu auditierenden Komponenten und ihr technisch-organisatorisches Zusammenspiel im Unternehmen. Rückfragen zu technischen Aspekten können direkt mit den Fachverantwortlichen geklärt werden.

Die Vollständigkeit, Qualität und Aktualität der vorgelegten Dokumentation ist zu bewerten. Zur erfolgreichen Auditplanung ist mindestens die folgende Dokumentation erforderlich:

- ICS-Sicherheitskonzept und Sicherheitskonzepte von Teilsystemen, die sämtliche personellen, organisatorischen und technischen Maßnahmen im Hinblick auf die ICS-Sicherheit umfassen,
- Organigramm,
- Beschreibung des Produktionsbereichs und der Testsysteme (soweit auditiert),
- Netzpläne, Kommunikationsbeziehungen, Systemkonfigurationen,
- Auflistung kritischer Produktionsprozesse,
- Leitlinie zur Informationssicherheit und
- Auditberichte der letzten fünf Jahre.

Fehlende oder unvollständige Dokumente sind nachzufordern. Stellt sich heraus, dass Dokumente nicht existieren, sollten diese nun erstellt werden, gegebenenfalls sind Interviewprotokolle mit Fachverantwortlichen als Ersatzdokument in die Sammlung aufzunehmen. Für die weitere Planung ist mindestens ein fortgeschrittener Entwurf jedes Dokumentes vorzulegen, damit spätere Auditergebnisse einen sinnvollen Bezug auf die Dokumentation nehmen können.

Das Auditteam unterzieht die Dokumentation einer Prüfung und klärt dabei die folgenden Fragestellungen:

- Ist die Dokumentation vollständig (alle Teilsysteme, Netze, physikalische Standorte erfasst)?
- Ergibt der Abgleich der Gefährdungen mit den Maßnahmen Abdeckungslücken oder überflüssige Maßnahmen?
- Welche Restrisiken verbleiben? Sind diese nach Aktenlage für die Geschäftsführung tragbar?
- Sind vorgeschriebene Maßnahmen nachvollziehbar, praktisch umsetzbar, verständlich beschrieben und angemessen?

Das Team erstellt anhand der vorliegenden Dokumente und bei den Beteiligten gesammelten Informationen einen detaillierten Auditplan. Dieser bezieht sich auf die Maßnahmen, die nicht allein aufgrund einer Prüfung der Dokumentation abschließend bewertet werden können. Bei einer Vielzahl von Einzelmaßnahmen ist eine sinnvolle Maßnahmen-Stichprobe auszuwählen, die mit vorangegangen Auditberichten abzugleichen ist. Von besonderer Bedeutung ist eine Risikoanalyse hinsichtlich der durchzuführenden Tests, die in enger Abstimmung mit den Betriebsverantwortlichen zu erfolgen hat. Nur so kann das Risiko von – ggf. kritischen – Auswirkungen von Tests auf die Anlagen minimiert werden.

Der Auditplan umfasst nach dieser Phase:

- Auflistung aller zu prüfenden Komponenten gemäß einer Priorisierung und der sie betreffenden und zu prüfenden Maßnahmen,
- Festlegung einer Prüfmethode für jede Maßnahme,
- Auflistung der Komponenten, für die eine Suche nach Schwachstellen erfolgen wird,
- Auflistung der organisatorischen Rollen und möglichst der sich daraus ergebenden Interviewpartner und Testbeteiligten sowie
- vorgeschlagene detaillierte Terminplanung.

Das Auditteam ist bei seiner Tätigkeit entsprechend zu unterstützen. Externen Teams soll daher ein eigener verschließbarer Raum in örtlicher Nähe der Systeme oder Systemverantwortlichen zur Verfügung zu stehen und Zugang zur Büro-Infrastruktur (Drucker, Kopierer, Büromaterial) gewährleistet werden.

6.2.3 Abstimmungs-Workshop

Der Workshop dient dazu, den erstellten Auditplan gemeinsam mit den Systemverantwortlichen zu analysieren und die Durchführbarkeit festzustellen. Damit die sich anschließende Testphase erfolgreich durchgeführt werden kann, müssen notwendige Zugangs- und Zutrittsrechte für die Auditoren eingeräumt und von den Systemverantwortlichen genehmigt werden.

Für die produktiven Bereiche sind Safety-Bestimmungen heranzuziehen und mit den geplanten Prüfmethoden abzugleichen. Einzelne Prüfmethoden, die Safety-kritische Systeme potenziell beeinträchtigen oder das Systemverhalten gefährlicher Komponenten beeinflussen können, sind auf ihre Durchführbarkeit hin zu überprüfen. Gegebenenfalls sind zusätzliche sichernde Maßnahmen während der Auditierung festzulegen (z. B. Evakuierung von Produktionsbereichen während eines Tests). Eine Einweisung der externen Auditoren in die Safety-Regularien hat spätestens mit Beginn der Testphase zu erfolgen.

Kern des Abstimmungs-Workshops ist die Festlegung von verbindlichen Einsatzregeln (sogenannten „Rules of Engagement“). Diese Regeln geben vor, welche Teilsysteme oder Schnittstellen von invasiven Untersuchungen ausgenommen werden müssen, wer vor und nach durch zu bestimmende Prüfmethoden zu informieren ist, wer eine Rufbereitschaft während der Testphase bereitstellt und welche Mitarbeiter bei welchen Tests anwesend sein müssen. Verbindliche Grenzen für die Auditoren sind Teil dieser Einsatzregeln:

- Welche Prüfmethoden sind tabu?
- Welche Systeme oder örtlichen Produktionsbereiche sollen keinesfalls in der Testphase tangiert werden?
- Wer hat Entscheidungsvollmacht bei unklarer Regelinterpretation während der Testphase?

Eine klare und detaillierte Regelung erleichtert die weitere Vorgehensweise sowohl für die Auditoren als auch für den Auftraggeber und verhindert bei ungeplanten Produktionsausfällen eine Auseinandersetzung um Haftungsfragen.

Die Ergebnisse des Workshops sind zu dokumentieren und haben ein abgestimmtes Testkonzept zu enthalten. Dieses Konzept listet alle Komponenten und zugehörige Prüfmethoden auf und benennt die jeweils verbindlichen Einsatzregeln. Ein gemäß der Workshop-Ergebnisse verfeinerter Terminplan ist dem Testkonzept beizufügen.

6.2.4 Prüfmethoden der Testphase

In der Testphase werden Prüfmethoden angewandt, die sich in drei Kategorien einteilen lassen: Penetrationstests, Vor-Ort-Prüfung und Interviews. Es werden zunächst diese Kategorien beschrieben. Für die Anwendung der Prüfmethoden auf verschiedenen Sachebenen werden mögliche Fragestellungen in 6.3 dar gestell t.

6.2.4.1 Penetrationstests

Externe und interne Penetrationstests können in den Auditplan aufgenommen werden. Diese Test sind optional und sollten mit Bedacht angewendet werden. Sinnvoll sind diese insbesondere im Rahmen von Factory Acceptance Tests oder Site Acceptance Tests. Das Problem bei Penetrationstests ist, dass Komponenten beim Auffinden von Schwachstellen in einen undefinierten Zustand gelangen können. Dies kann zu Problemen bei der Steuerung führen. Daher sollten diese Tests nur in Wartungsfenster durchgeführt werden. Zudem können Penetrationstests auf ausgewählte Komponenten (z.B. Engineering Workstations) beschränkt werden. Allgemein empfiehlt sich die Beschränkung von Penetrationstests auf

solche Systeme, die nicht unmittelbar mit dem Produktivbetrieb in Verbindung stehen. In einigen Anwendungsbereichen wird es unerlässlich sein, auf Penetrationstests weitgehend zu verzichten und sich stattdessen auf die Durchführung passiver Untersuchungsmethoden zu beschränken.

Die Penetrationstests decken insbesondere die im Kapitel 3 benannten Schwachstellenbereiche

- Einsatz von Standard-IT-Komponenten mit bereits identifizierten Schwachstellen,
- unzureichende Validierung von Eingaben,
- fehlende Absicherung von Standard -Konfigurationen,
- unvollständige Absicherung der Fernwartungszugänge,
- fahrlässiges Einrichten von Netzzugängen,
- lokaler Zugang über Steuernachrichten und
- unerwünschte, weitreichende Vernetzung

ab, beschränken sich aber nicht nur auf diese typischen Schwachstellen.

Für die im vereinbarten Rahmen des Audits zu prüfenden Systeme wird eine Liste von potenziellen Schwachstellen ermittelt und dokumentiert, die im weiteren Verlauf zu bewerten ist. Die Dokumentation sollte dabei einer festen Struktur unterliegen, um Penetrationstest-Ergebnisse aus verschiedenen Audits vergleichbar zu halten. So können Schwachstellen, die über IP-Netzzugänge ermittelt wurden, beispielsweise in einer Tabelle festgehalten werden, die folgender Spaltenstruktur entspricht:

ID	IP-Adresse	ICS-Komponente	Dienst	Beschreibung
1	10.1.1.3	MTU m13	http/ TCP 80	Webserverdienst apached mit bekannten Software-Schwachstellen (veraltete Version).
(...)				

Tabelle 8 Tabelle zur Dokumentation von IP-netzbasierten Schwachstellen

Relevante Industriestandards (z. B. [VDI 2182 2011], Blatt 2) geben beispielhafte Vorgaben für die tabellarische Dokumentation von Schwachstellen und ihrer Analysen.

Bei der Bewertung der Schwachstellen ist eine Zuordnung zu den im ICS-Sicherheitskonzept formulierten Schutzzielen vorzunehmen (z. B. Verfügbarkeit einer MTU oder Vertraulichkeit von Produktionsparametern) und das Ausmaß der Beeinträchtigung festzustellen. Eine Bewertung und Aufwandsabschätzung zur Beseitigung der Schwachstelle erfolgt auf der jeweiligen Sachebene.

6.2.4.2 Vor-Ort-Prüfung

Die Vor-Ort-Prüfung beginnt mit einem Eröffnungsgespräch mit den Hauptbeteiligten. Dann folgen Interviews (siehe Kapitel 6.2.4.3) und eine Begehung des Produktionsbereichs mit Inaugenscheinnahmen der Systeme sowie eine vorläufige Auswertung (vgl. [BSI IS-Revision 2010], Abschnitt 4, Durchführung einer IS-Revision).

Bei der Vor-Ort-Prüfung kommen regelmäßig die folgenden Prüfmethoden zum Einsatz.

- Inaugenscheinnahme von ICS-Komponenten und Räumlichkeiten
  - Entsprechen die Komponenten der Inventarliste und der dokumentierten Funktion?
  - Gibt es nicht vorgesehene Interfaces (z. B. Netzverkabelung)?

  - Sind Räume gemäß Dokumentation zutrittsbeschränkt? Gibt es undokumentierte Umbauten oder Abweichungen vom Raumplan?
  - Sind Systeme eindeutig bezeichnet und Produktionsbereichen zugeordnet?
  - In unzugänglichen Bereichen kann die Inaugenscheinnahme ersetzt werden durch Kamerafahrt, Aufzeichnungen oder indirekte Beobachtung.
- Beobachtung
  - zufällige Wahrnehmung von relevanten Ereignissen durch das Auditteam
  - Besonderheiten des Produktionsprozesses verstehen
  - Clear-Desk- und Clear-Screen-Status
- technische Prüfung
  - Alarmanlage, Zutrittskontrollfunktion, Schließzustände
  - Bedienung von Anlagen und HMI durch sachkundiges Personal
  - Überprüfung von automatisierten Abschaltvorgängen
  - Testweises Auslösen von Sensoren (z. B. Lichtschranke, Vibration, Hitze, Wasser, Rauch)
- Einsichtnahme in Daten (z. B. Logdateien, HMI-Zugang, gedruckte Protokolle)
  - Sicherheitsrelevante Ereignisse in den Aufzeichnungen identifizieren
  - getroffene Maßnahmen überprüfen (Angemessenheit, Vollständigkeit)
  - Überprüfen der Dokumentationspflichten
- Abarbeiten von Checklisten

Beendet wird die Vor-Ort-Prüfung mit einem Abschlussgespräch, bei dem wesentliche Beobachtungen den Beteiligten zurückgespiegelt und Anregungen zur Beseitigung von identifizierten Schwachstellen oder von Abweichungen zur Dokumentation aufgenommen werden.

6.2.4.3 Interviews

Auf das Eröffnungsgespräch mit den Hauptbeteiligten im Rahmen der Vor-Ort-Prüfung können Interviews mit dem Personal im Produktionsbereich folgen. Die in den Interviews getroffenen Aussagen sind zu dokumentieren:

- Festhalten von sicherheitsrelevanten Beobachtungen der Beteiligten
- Überprüfen des Wissensstandes in Bezug auf Richtlinien und Anweisungen
- Feststellung des Trainings- und Schulungsstandes des Personals
- Festhalten bisher nicht dokumentierter oder von der Dokumentation abweichender Verfahrensweisen
- Abgleich von Stellenbeschreibungen und tatsächlichen Tätigkeitsmerkmalen

Der Auditplan kann vorsehen im Vorfeld schriftliche Interviews anzufordern (z. B. Ausfüllen von Fragebögen), um die Interviews vorzubereiten.

6.2.5 Bewertung

Das Auditteam bewertet die festgestellten Sachverhalte im Hinblick auf die formulierten Vorgaben aus dem ICS-Sicherheitskonzept und den Abgleich mit der vorgelegten Dokumentation.

Die Vollständigkeit, Qualität und Aktualität der vorgelegten Dokumentation ist bereits während der Einarbeitungsphase zu bewerten. In dieser Phase soll es möglich sein, die Dokumentation nachzubessern, um etwa fehlende Schriftstücke zu ergänzen. Der Status jedes Teildokumentes (fortgeschrittener Entwurf, finale Version, veraltete Version) und die Qualität (z. B. vollständig, nur teilweise vollständig, fehlerhaft; Klarheit, angemessene Beschreibungstiefe) ist bei der Bewertung festzustellen und im Auditbericht zu dokumentieren.

Im Hinblick auf zu überprüfende Sicherheitsmaßnahmen kann in Anlehnung an die IS-Revision[6] des BSI das folgende Schema zur Feststellung des Umsetzungsstatus angewandt werden:

- Maßnahme umgesetzt
- Maßnahme teilweise umgesetzt
- Maßnahme nicht umgesetzt
- Maßnahme entbehrlich (z. B. weil andere Maßnahmen adäquat wirken)

Bei nicht oder nur teilweise umgesetzten Maßnahmen ist eine Bewertung des Sicherheitsmangels vorzunehmen. Ein geeignetes einfaches Schema ist zweistufig: „Sicherheitsmangel“ oder „schwerwiegender Sicherheitsmangel“.

Abweichungen des Ist-Zustandes zur Dokumentation sind detailliert aufzuführen. Dabei ist für jede Abweichung eine Bewertung durchzuführen:

- Liegt eine Abweichung vor, die allein durch die Aktualisierung der Dokumentation beseitigt werden kann?
- Zeigt die Abweichung, dass eine oder mehrere Maßnahmen nicht umgesetzt wurden? (Dann kann diese nach dem Schema für teilweise oder nicht umgesetzte Maßnahmen bewertet werden)
- Zeigt die Abweichung, dass Vorgaben aus dem ICS-Sicherheitskonzept nicht eingehalten werden? (Dann ist die Vorgabe zu benennen und die Nichteinhaltung im Hinblick auf das Sicherheitskonzept zu bewerten.)

Die im Verlauf der Auditierung identifizierten Schwachstellen sind, sofern sie nicht bereits im Sicherheitskonzept berücksichtigt und bewertet sind, von den Auditoren zu bewerten:

- Welche ICS-Komponenten sind von der Gefährdung betroffen? Welche Produktionsbereiche sind betroffen?
- Welche (Komponenten-übergreifende) Funktion ist von der Schwachstelle betroffen?
- Ist die Schwachstelle ausnutzbar? Welcher Aufwand wird dazu angenommen?
- Welche dem Sicherheitskonzept zuwiderlaufenden Ziele kann ein Angreifer unter Ausnutzung der Schwachstelle erreichen?
- Welche physikalische Wirkung, welcher Schaden kann durch Ausnutzen der Schwachstelle erzielt werden?
- Welcher Aufwand zur Beseitigung oder Entschärfung der Schwachstelle wird gemäß vorliegender Information angenommen?
- Gibt es Hinweise, dass die Schwachstelle bereits ausgenutzt wurde oder potenziellen Angreifern bekannt ist?

Die Bewertung anhand aller genannten Punkte ist zum Zeitpunkt des Auditabschlusses oft noch nicht möglich, da weitere Informationen eingeholt werden müssen (z. B. Auskünfte seitens der Hersteller) oder die Testabdeckung gemäß Auditplan nicht vollständig war. Inwieweit eine weitere Analyse einer Schwachstelle geboten ist, wird im Rahmen der auszusprechenden Empfehlungen behandelt.

6 https://www.bsi.bund.de/DE/Themen/weitereThemen/ISRevision/isrevision.html

Nach der Bewertung der Schwachstellen erfolgt die Formulierung von durchzuführenden Maßnahmen und Empfehlungen an den Auftraggeber.

- Die nicht oder nur teilweise umgesetzten Maßnahmen werden aufgelistet, sofern sie sich nicht als entbehrlich herausgestellt haben.
- Neue Maßnahmen, die aufgrund festgestellter Schwachstellen im Hinblick auf die im Sicherheitskonzept formulierten Ziele erforderlich erscheinen, werden aufgeführt.
- Es werden Empfehlungen in Bezug auf die Anpassung des Sicherheitskonzeptes im Lichte der festgestellten Sachverhalte formuliert (z. B. Identifikation unwirksamer Maßnahmen, Neubewertung von Risiken aufgrund technischen Fortschrittes, Klassifikation von Assets).
- Es werden Empfehlungen formuliert, auf welche Weise die festgestellten Schwachstellen beseitigt werden können und welche Vorgehensweise dabei angeraten ist.

6.2.6 Berichterstattung

Der Auditbericht einschließlich Referenzdokumenten ist dem Auftraggeber schriftlich bekannt zu geben. Den Verantwortlichen sollte im Rahmen einer Präsentation der Bericht und seine zentralen Ergebnisse näher erläutert werden. Die Präsentation sollte in zeitlicher Nähe mit der Auslieferung des Berichtes erfolgen. Art und Umfang des Auditberichtes sind bereits beim Abstimmungsworkshop festzulegen.

Der Bericht sollte auf die Spezifika der ICS-Installation eingehen und die Sachverhalte im Kontext der Produktivumgebung darstellen. Der Bericht soll die folgenden Punkte umfassen:

- Mitglieder und Leitung des Auditteams
- Ansprechpartner auf Auftraggeberseite, die beim Audit mitgewirkt haben
- zugrundeliegende Dokumentation
- Auditplan und Einsatzregeln
- Erläuterung der Prüfmethoden
- Prüfergebnisse und Protokolle
- Auflistung identifizierter und bewerteter Schwachstellen
- Berichtenswerte Ereignisse während der Auditdurchführung
- Maßnahmen und Empfehlungen
- Kurzzusammenfassung des Auditergebnisses

Auf die Präsentation können Feedbackgespräche der Gesamtgruppe oder von Beteiligten in kleineren Gruppen folgen. Dabei können Lob und Kritik in Bezug auf die Vorgehensweise des Auditteams und der Unterstützung seitens des Auftraggebers thematisiert werden. Zudem können Prüfmethoden und Ergebnisse mit den technischen Experten im Hinblick auf die festgestellten Ergebnisse diskutiert werden.

6.2.7 Umsetzung der Maßnahmen und Empfehlungen

Nach Abschluss des Audits und Diskussion des Auditberichtes erfolgt die Umsetzung der formulierten Maßnahmen und Empfehlungen nach Maßgabe der Leitungsverantwortlichen.

Maßnahmen können dabei die bloße Re-Konfiguration einer Komponente betreffen (z. B. Anpassung einer Konfigurationsdatei, Ändern der Netztopologie zur Netz- Segmentierung), die Aktualisierung der Software auf den Komponenten (z. B. Einspielen eines Sicherheitsupdates, Installation einer neueren Version) oder die Installation und Inbetriebnahme einer neuen Sicherheitskomponente (z. B. Einbringen einer Firewall als zusätzliche Netzkomponente).

Die Aufwände zur Umsetzung sind daher höchst unterschiedlich. Während eine Re-Konfiguration innerhalb eines Arbeitstages abgeschlossen sein kann, führt eine Inbetriebnahme einer zusätzlichen Komponente unter Umständen zur Planung eines langfristigen Rollout-Projektes. Die Priorisierung der Maßnahmen und Empfehlungen hat daher auf die Planung und Durchführung aufwendiger Maßnahmen erheblichen Einfluss und muss vorab von den Leitungsverantwortlichen durchgeführt werden.

6.2.8 ICS-Revisited

Zu einem definierten Zeitpunkt nach Abschluss des Audits kann ein Re-Audit erfolgen, um einen iterativen Umsetzungsprozess im Hinblick auf die Maßnahmen und Empfehlungen zu fördern. Dabei wird in einem verkürzten Verfahren der Status der auditierten Bereiche überprüft und sowohl die Abweichung zum auditierten Zustand als auch zum anvisierten Zustand ermittelt. Das Auditteam kann die Umsetzung einzelner Maßnahmen und Empfehlungen verifizieren und bei der Neubewertung des Ist-Zustandes behilflich sein. Es können bei Umsetzungsschwierigkeiten oder neuen technischen Entwicklungen alternative Maßnahmen und Empfehlungen formuliert werden, die es dem Auftraggeber erleichtern, seine Sicherheitsziele zu erreichen.

6.3 Testphase nach Sachebenen

6.3.1 Physische Sicherheit

Die Auditierung der physischen Sicherheit umfasst eine Überprüfung des in Kapitel 5.5 benannten Absicherungsplans für den physischen Schutz.

Das Auditteam überprüft hierbei sowohl das dokumentierte Konzept und nach Möglichkeit die baulichen Pläne auf Vollständigkeit und Eignung in Bezug auf die benannten Sicherheitsziele als auch dessen Umsetzung vor Ort. Der Auditplan kann vorsehen, dass nur ein Teilbereich (z. B. Umsetzungsprüfung) im Rahmen der Vor-Ort-Prüfung auditiert wird.

Im Rahmen der Vor-Ort-Prüfung können insbesondere passive Schutzmaßnahmen überprüft werden. Typische Fragestellungen sind:

- Entsprechen die vorhandenen Mauern, Zäune, Gräben, Fenster und Schächte den definierten Sicherheitsperimetern?
- Sind vorhandene Zugangsleitungen und Kommunikationsverbindungen physisch geschützt?
- Sind Türen mit der dokumentierten Zutrittskontrollfunktion ausgestattet und funktioniert diese ordnungsgemäß?
- Entspricht das Vorhandensein der Assets innerhalb der durch Perimeter getrennten Sicherheitszonen dem Sicherheitskonzept?
- Wurden ICS-Komponenten mit vergleichbarem Sicherheitsbedarf in Zonen zusammengefasst?
- Gibt es unbemannte Produktionsbereiche mit entsprechend festgelegter Schutzzone?
- Sind Komponenten, Materialien und Datenträger in verschlossenen Gehäusen oder Sicherheitsschränken untergebracht?
- Sind ICS-Steuermechanismen gemäß Rollenzuweisung zutrittsbeschränkt?
- Findet eine regelmäßige Wartung der Zutrittskontrollsysteme statt?

Die Auditierung aktiver Schutzmaßnahmen erfolgt abhängig von den Gegebenheiten sowohl vor Ort im Produktionsbereich als auch an zentraler Stelle (z. B. Pförtnerbereich):

- Findet die Öffnung von Türen und Toren (erst) nach Überprüfung der Berechtigung statt?
- Werden steuerbare Schranken oder andere Fahrzeughindernisse im Sicherheitskonzept erfasst? Wie werden die Mechanismen eingesetzt?
- Wie ist der Notfallzutritt geregelt?

Unterstützende Schutzmaßnahmen werden ebenfalls sowohl vor Ort als auch an zentraler Stelle auditiert:

- Sind vorhandene Videokameras und Bewegungssensoren im Sicherheitskonzept erfasst? Decken diese den zu schützenden Bereich ab?
- Wie werden aufgezeichnete Bildinformationen verwaltet? Ist ein kurzfristiger Zugriff auf eine für den Testfall vorgegebene Aufzeichnung möglich?
- Welche Meldekette existiert für verschiedene Vorfälle bzw. Alarmsituationen im Produktionsbereich? Wurde diese in der Vergangenheit eingehalten?

6.3.2 Richtlinien und Prozesse

Die Sachebene Richtlinien und Prozeduren bezieht sich auf die in Kapitel 5.3 definierten Best Practices und geht darüber hinaus. Es handelt sich um Prüfungen der organisatorischen Rahmenbedingungen. Eine solche Liste umfasst typischerweise die folgenden Punkte:

- Ist eine Sicherheitsleitlinie formuliert und ein Sicherheitsmanagement etabliert?
- Wurde eine Security-Organisation aufgebaut? Existieren Verantwortlichkeiten und Rollen für alle ICS-Komponenten? Sind den Rollen geeignete Spezialisten zugeordnet?
- Ist das Sicherheitskonzept für den Produktionsbereich dokumentiert und den Verantwortlichen bekannt?
- Werden die Sicherheit der ICS-Komponenten betreffende Informationen (z. B. Pläne, Organigramme) gepflegt und vor unbefugtem Zugriff geschützt?
- Wurden die betrieblichen Aufgaben von Betreiber, Integrator und Hersteller festgelegt und eingehalten?
- Existieren Vertraulichkeitsvereinbarungen mit Integratoren und Herstellern? Sind diese noch gültig?
- Gibt es eine Richtlinie zur sicheren Fernwartung von Komponenten? Ist eine Fernwartungs-Zugangsmöglichkeit für Hersteller oder Integratoren zum Auditzeitpunkt gegeben und aktiviert? Wer ist für die (De-)Aktivierung verantwortlich?
- Unterliegen Administration und Wartung der ICS-Komponenten einem Rollenkonzept? Ist dieses auch unter Produktionsbedingungen umsetzbar? (Abweichungen sind zu dokumentieren.)
- Existiert eine Softwareentwicklungsrichtlinie oder Konfigurationsrichtlinie? Wie werden diese durchgesetzt?
- Ist die Entsorgung von Hardware geregelt? Wurde eine diesbezügliche Richtlinie angewandt?
- Wie ist das Patch- und Changemanagement geregelt? Sind die dem Audit vorangegangenen Änderungen am ICS in vorgesehener Form erfolgt?
- Gibt es einen Prozess, der neue bekanntwerdende Schwachstellen in Bezug auf die ICS-Komponenten bewertet? Wurde in der Vergangenheit angemessen auf bekanntgewordene Schwachstellen reagiert?
- Existiert ein Wiederherstellungsplan für eine definierte Liste von Assets? Werden die flankierenden Maßnahmen (z. B. Datensicherung) tatsächlich umgesetzt?
- Gibt es eine Anstellungsrichtlinie? Entspricht das im ICS-Umfeld operative Personal dieser Richtlinie?
- Gibt es Prozesse für Stellenwechsel und das Ausscheiden von Personal? Wurde dies bei den dem Audit vorangegangenen Vorgängen angewandt?

- Existiert ein Qualifizierungsprogramm für das Personal in Bezug auf sicherheitsrelevante Kenntnisse? Wie ist der Qualifizierungsstand?

Zur Feststellung der in dieser Checkliste abgebildeten Sachverhalte ist sowohl eine Vor-Ort-Prüfung als auch die Durchführung von Interviews sowie eine Kombination von Prüfmethoden aus beiden Kategorien geeignet.

6.3.3 Netzebene

Die Auditierung auf Netzebene kann mit einer Überprüfung der Konfiguration von Routern, Switches und Firewalls beginnen. Dazu können die aktuellen Konfigurationen ausgelesen und gesammelt oder direkt aus den einzelnen Geräten abgelesen werden.

Zur Sicherheitsanalyse auf Netzebene finden Netzsniffer Verwendung. Diese Werkzeuge zeichnen den Netzverkehr in den einzelnen Subnetzen auf und stellen als Ergebnis eine Datei mit dem mitgeschnittenen Netzverkehr bereit, die für die weitere Analyse benutzt wird. Da noch selten Hubs genutzt werden, die ein direktes Mitschneiden des gesamten Datenverkehrs an einem freien physikalischen Port erlauben, müssen andere Maßnahmen ergriffen werden. Der Switch-Administrator kann dazu auf dem Switch einen Spiegelport (auch „Mirror Port“ genannt) einrichten, auf dem sämtlicher Datenverkehr eines oder mehrerer anderer Ports als Kopie bereitgestellt wird. Zudem kann mithilfe eines „Network Tap“ (ein „T-Stück“ auf unterer Netzebene) an den jeweiligen Netzanschlüssen der Datenverkehr mitgeschnitten werden. Beide Methoden führen zu nicht unerheblichen Eingriffen in das Netzwerk und sind daher nur mit Vorsicht einzusetzen.

Anhand der aufgezeichneten Daten können dann im Rahmen des Audits die folgenden Punkte überprüft werden:

- Sind die Endpunkte der festgestellten Datenverbindungen korrekt im Netzplan verzeichnet?
- Sind die Datenverbindungen in der Kommunikationsinfrastruktur vorgesehen? (Abweichungen können Fehlkonfigurationen, mangelnde Qualität der Dokumentation oder ein konkreter Hinweis auf ein Schadprogramm sein.)
- Existieren Verbindungen zu Büro-Arbeitsplatzrechnern oder ERP-Systemen?
- Sind Datenübertragungen unverschlüsselt?
- Entspricht das Datenvolumen den Erwartungen gemäß Komponentenbeschreibung?
- Können VPN- und Fernwartungszugriffe festgestellt werden?
- Werden physikalische Trennungen von Netzen oder Systemen („Air Gaps“) eingehalten?
- Erlauben die beobachteten übertragenen Nachrichten einen Replay- oder Man-in-the-Middle Angriff?

Neben den kabelgebundenen Netzen sind im Rahmen des Audits auch Funknetze zu überprüfen. Mittels entsprechender Scanner kann das Vorhandensein der jeweiligen Funknetztechnologien festgestellt und mit dem Netzplan abgeglichen werden. Zudem können unter günstigen Umständen entsprechende Zugangsdaten nicht dokumentierter Netze ermittelt werden, um in weiteren Auditschritten aktive Prüfmethoden in diesen Netzen anzuwenden.

Während die Sicherheitsanalyse mithilfe der Netzsniffer ohne begleitende Man-the-Middle-Angriffe eine passive Prüfmethode darstellt, die – abgesehen von der zusätzlichen Last auf dem Switch aufgrund eines Spiegelports – keine Beeinträchtigung der ICS-Komponenten bewirkt, können aktive Prüfmethoden weitere Schwachstellen während des Audits aufdecken und zu nicht kalkulierbaren Problemen führen. Es sollte daher möglichst darauf verzichtet werden.

Aktive Methoden im Produktivbereichen sind im Auditplan explizit festzuhalten und müssen von den vereinbarten Einsatzregeln gedeckt sein. Die möglichen Konsequenzen sollten vor der Durchführung bedacht werden, da es zu Ausfällen von Komponenten kommen kann!

Über einen Ping-Sweep und einen Port-Scan können aktiv die über das Netz erreichbaren Komponenten und ihre Netzdienste abgefragt werden, um einen Abgleich mit dem Netzplan zu ermöglichen (vgl. Kapitel 3.3.3). Mithilfe eines ARP-Scanners ist es möglich, über die Antworten auf ARP-Broadcast-Nachrichten Komponenten zu finden, die ICMP-Pakete blockieren und bei Ping-Sweeps verborgen bleiben. Die Verwendung dieser Werkzeuge erlaubt daher die zusätzliche Überprüfung der Punkte:

- Sind die im Netzplan verzeichneten Netzkomponenten vorhanden und sind die verzeichneten Dienste verfügbar?
- Gibt es Netzkomponenten oder Dienste, die nicht dokumentiert sind?
- Werden Dienste von der Firewall (wie dokumentiert) blockiert?
- Entspricht die Router- und Switch-Konfiguration dem Netzplan?

Hierbei ist vom Auditteam zu berücksichtigen, dass ein vom üblichen Verhalten abweichender Kommunikationsversuch bereits zu undefinierten Systemzuständen im Produktivsystem führen kann. Zwei Beispiele aus dem Audit-Umfeld werden von NIST (vgl. [SP 800-53]) benannt: Ein Ping-Sweep auf ein ICS-Netz, das protokollgemäß eine Ping-Reply jedes verbundenen Gerätes zur Folge gehabt hätte, führte überraschend zu einer 180°-Drehung eines 3m-langen Roboterarms. Ein anderer Sweep in einem ICS-Netz führte zum Stillstand eines Kontrollgerätes innerhalb der Produktionsstraße einer Chip-Produktion, wodurch Wafer im Wert von 50.000$ vernichtet wurden. Der bei diesen Sweeps verwendete ICMP-Echo-Request ist Bestandteil des (standardisierten) IP-Protokolls und sollte von einem konformen Zielsystem korrekt beantwortet oder ignoriert werden. Bei im industriellen Umfeld eingesetzten (zum Teil proprietären) Netzprotokollen müssen jedoch Abweichungen zu Kommunikationsprotokoll-Standards berücksichtigt werden.

6.3.4 Geräteebene

Mit der Geräteebene sind alle Arten von ICS-Komponenten gemeint, insbesondere im Fokus stehen HMI, Sensoren und SPS. Die Untersuchung auf Clientebene beginnt mit den Host-spezifischen Untersuchungen, die auf der Netzebene vorgenommen werden. Erste Prüfdaten sind daher: IP-Adresse(n), offene Ports, Betriebssystemparameter sowie angebotene Dienste des Hosts in den verschiedenen Subnetzen. Diese Daten sind mit der Dokumentation abzugleichen. Abweichungen sind zu dokumentieren.

Mithilfe von Schwachstellenscannern können die über das Netz potenziell ausnutzbaren Schwachstellen automatisiert ermittelt werden. Diese betreffen bekannte Sicherheitslücken in der Software, die einen Dienst bereitstellt, alte Versionen/fehlende Updates bei Serverdiensten, Standard-Passwörter oder schwache Passwörter und fehlerhafte Konfigurationen auf Betriebssystem- oder Dienstebene (z. B. Freigaben). Einige Schwachstellen können nur identifiziert werden, wenn sich der Scanner als ein Benutzer authentisieren kann oder wenn der Zugriff über ein bestimmtes Subnetz erfolgt. Diese Parameter sind im Auditplan zu berücksichtigen (z. B. Herausgabe eines User-Accounts an die Auditoren, Erlaubnis der Verwendung von undokumentierten Netzzugängen, die bei der Untersuchung auf Netzebene identifiziert wurden).

Die Prüfergebnisse der Schwachstellenanalyse dienen der Überprüfung der folgenden Punkte:

- Gibt es veraltete Softwareversionen (Betriebssystemkomponenten, Serverdienste, Applikationen) auf dem System, für die Schwachstellen bekannt sind?
- Gibt es nicht installierte (aber herstellerseitig empfohlene) Software-Sicherheitsupdates für das System?
- Entspricht die installierte Software der Dokumentation?
- Verfügt das System über ungesicherte Benutzerzugänge (z. B. anonymer Zugang, schwaches Passwort, leeres Passwort, Standard-Passwort, nicht benötigter Terminal-Zugang, etc.)?
- Werden Nutzerrollen auf dem System unterschieden (z. B. Benutzer versus Administrator) und sind die Privilegien den Rollen korrekt zugeordnet?

- Gibt es Fernadministrationswerkzeuge oder Mechanismen zentraler Softwareverteilung, die einer dokumentierten Sicherheitsleitlinie entsprechen?
- Werden sicherheitsrelevante Systemereignisse aufgezeichnet? Sind Aufzeichnungen aus der Vergangenheit vollständig verfügbar?

Auf den sicherheitsspezifischen Netzkomponenten (Firewalls, Router, Modemzugänge) ist im Falle der Host-basierten Auditierung speziell zu überprüfen:

- Sind Zugänge über Funknetze so abgesichert, dass nur im Netzplan dokumentierte Verbindungen möglich sind?
- Entsprechen die Firewallregeln und Routing-Tabellen den dokumentierten logischen Netzverbindungen?
- Sind die VPN- und Modemzugänge auf eine Whitelist von zugelassenen Zugängen beschränkt?
- Werden VPN- und Modemzugriffe protokolliert? Ergibt die Protokollauswertung eine Auffälligkeit?

Für eine identifizierte potenzielle Schwachstelle kann zur weiteren Beurteilung der Ausnutzbarkeit durch das Auditteam ein Exploit (vgl. Kapitel 3.3.3) entwickelt werden, der sich die Schwachstelle zunutze macht, um eine mögliche Systempenetration aufzuzeigen. Ein Grund für die Entwicklung kann darin bestehen, dass der ICS-Betreiber einen Nachweis haben möchte, dass die Ausnutzbarkeit tatsächlich gegeben ist, um aufwendige Maßnahmen und Produktionsausfälle in der Produktivumgebung rechtfertigen zu können. Zudem kann mithilfe des Exploitcodes das Systemverhalten im Angriffsfall getestet und damit das Risiko, das durch die Schwachstelle gegeben ist, präziser bewertet werden.

6.3.5 Anwendungsebene

Im ICS-Umfeld ist eine Untersuchung auf Anwendungsebene insbesondere für die Komponenten HMI-System, Data Historian, Historian Database, Engineering Workstation und Master Terminal Unit angezeigt. Diese verfügen über eine im Vergleich zu anderen Komponenten hohe Systemkomplexität, die eine Auftrennung der Analyse in verschiedene logische Ebenen rechtfertigt. Zudem weisen sie als Teil der Prozessführung Real Time und der Prozessführung innerhalb der DMZ des ICS eine direkte Netzverbindung zu den Devices in der Prozessführung auf.

Die Analyse kann sich dabei sowohl auf Standardanwendungen (z. B. telnet, ftp, Webserver) beziehen, aber auch speziell auf die auf den ICS-Einsatz zugeschnittenen Applikationen wie z. B. Web- und Datenbank-Applikationen zur Datenaufbereitung, der im ICS gemessenen Umweltdaten und Produktionsparameter durchgeführt werden.

Die Untersuchung auf Anwendungsebene bedient sich dabei sowohl der bereits in den vorherigen Abschnitten benannten Schwachstellenscanner (diese können auch zur Aufdeckung von Schwachstellen wie SQL-Injection oder Cross-Site-Scripting verwendet werden). Es werden aber auch teilautomatisierte und manuelle Analysen (z. B. Test der einzelnen Funktionen, Codereview) benötigt, um Applikationen, die nicht oder nur unzureichend von den Schwachstellenscannern abgedeckt werden, in die Analyse mit einzubeziehen.

Im Rahmen des Audits auf Anwendungsebene können die folgenden Punkte überprüft werden:

- Gibt es Remote-Zugriffsmöglichkeiten auf die Komponente? Entsprechen diese dem dokumentierten Zustand?
- Werden Zugriffe über schwachstellenbehaftete Protokolle wie ftp, telnet oder eine veraltete SSH-Implementierung ermöglicht? Sind diese auf die benötigten Kommunikationsverbindungen beschränkt?
- Gibt es eine Backup-Software auf dem System? Besitzt diese ausnutzbare Schwachstellen ?
- Existieren webbasierte Schwachstellen wie z.B. Cross-Site-Scripting?

- Gibt es Schwachstellen bei der SSL-Implementierung wie z.B. selbstsignierte Zertifikate?
- Existieren Schwachstellen im Rahmen mangelnder Input-Validierung wie z.B. SQL-Injection oder Pufferüberläufe?
- Ist die Authentisierung auf Anwendungsebene sichergestellt? Gibt es eine Zuordnung zu den dokumentierten Nutzerrollen und -privilegien?

6.3.6 Prozessführung Feld

Für ICS-Komponenten in der Prozessführung Feld sollte geprüft werden:

- Sind die Kommunikationsbeziehungen im Netzplan dokumentiert?
- Werden Sicherungsmechanismen (wie z. B. Signierung von Nachrichten und Verschlüsselung der übertragenen Nutzdaten nach OPC UA) gemäß Dokumentation angewandt?

6.3.7 ICS-Security-Test

Eine Auditierung der Security-Funktionen selbst wird über funktionale Tests durchgeführt. Der Auditplan kann eine Teilmenge von Sicherheitsfunktionen aufführen, die während des Audits zu überprüfen sind.

Je nach Vorhandensein unterschiedlicher Security-Mechanismen können sich funktionale Sicherheitstests auf die Klärung folgender Punkte beziehen.

- Wird eine Authentisierung des Benutzers bei kabelgebundenen und drahtlosen Netzzugriffen, Modemzugängen oder VPN-Zugängen erzwungen?
- Werden dem Benutzer die dokumentierten Rechte zugewiesen?
- Werden nicht autorisierte Zugriffsversuche unterbunden und in einer Logdatei aufgezeichnet? Werden sicherheitsrelevante Ereignisse zuverlässig aufgezeichnet?
- Werden die aufgezeichneten Logdateien automatisiert ausgewertet und wird bei entsprechenden Auffälligkeiten geeignet alarmiert?
- Ist der Zutrittsschutz aktiv?
- Wird die Alarmierung bei alarmrelevanten Ereignissen tatsächlich ausgelöst?
- Sind Viren-Definitionsdateien aktuell? Wird das Virenschutzprogramm gemäß Sicherheitskonzept verwendet?
- Ist Port Security bei Switches aktiviert?
- Ist ein IDS aktiv? Werden Alarme bei relevanten Ereignissen erzeugt?
- Werden nur dedizierte DNS- und Active-Directory-Server für die ICS-Komponenten eingesetzt und befragt?
- Wird die Zeitsynchronisierung über einen dedizierten NTP-Dienst vorgenommen?
- Werden Backupprozeduren eingehalten? Funktioniert der Wiederherstellungsvorgang?
- Werden Bildschirmsperren nach einer Timeout-Periode aktiviert (sofern notwendig)?

Die Prüfmethode in Bezug auf diese funktionalen Tests ist dabei eine regelmäßige, manuelle Überprüfung der Funktionalität anhand einer Checkliste.

7 Trends und daraus resultierender F&E-Bedarf

7.1 Aktuelle Trends

7.1.1 Industrie 4.0

Der Begriff Industrie 4.0 ist geprägt durch das gleichnamige Zukunftsprojekt der Bundesregierung (vgl. [BUND_2012]). Dieses Projekt beschäftigt sich mit dem Trend der zunehmenden Vernetzung und Leistungsfähigkeit der eingesetzten Industriekomponenten in der Produktion. Die Zahl vier soll auf eine neue, zukünftige Stufe der Industrialisierung hinweisen, die 4. industrielle Revolution. Dabei reiht sich diese Entwicklung ein in die Entwicklungsstufen Mechanisierung, Industrialisierung und Automatisierung. In der Entwicklungsstufe Industrie 4.0 hält das sogenannte Internet der Dinge Einzug in die Fabrik, in Form von Smart Factory. Diese ist gekennzeichnet durch vernetzte, intelligente Produktionskomponenten, welche eigenständig Informationen austauschen, Aktionen auslösen und sich selbstständig und gegenseitig steuern.

Durch diese neuartigen Kommunikationsbeziehungen und die zunehmende Verlagerung von Intelligenz in die Produktionskomponenten ergeben sich u. a. folgende Potenziale:

- Kleinserien aus individuellen Kundenwünschen lassen sich wirtschaftlich bis zur Losgröße eins herstellen.
- Der Ressourceneinsatz lässt sich optimieren und Prozesse können effizienter gestalte t werden.
- Zu jedem Zeitpunkt sind aktuelle Kennzahlen über den gesamten Produktionsprozess abrufbar.
- Es sind kurzfristige und flexible Reaktionen auf Störfälle sowie Änderungen der Konfiguration möglich.
- Neuartige Geschäftsmodelle können entstehen.

Dabei birgt dieser Trend mit steigender Komplexität von Produktionskomponenten und Kommunikationsinfrastruktur auch Risiken durch beispielsweise eine erhöhte Angriffsfläche und eine Vernetzung über Vertrauensgrenzen hinweg (z. B. zur Integration von Kunden und Geschäftspartnern in den Produktionsprozess).

Folgende Themen werden u. a. in Bezug auf diesen Trend zukünftig eine wesentliche Rolle bei dem Entwurf, Aufbau und Betrieb der notwendigen Infrastruktur spielen:

- Entwurf von Standards für die Smart Factory (z. B. eine Referenzarchitektur), welche Aspekte der IT-Sicherheit berücksichtigen.
- Entwicklung von sicheren Werkzeugen für die Steuerung und Kontrolle der zunehmend komplexer und intelligenter werdenden Systeme, welche auch IT-Sicherheitsfunktionen umsetzen.
- Absicherung von Produktionsanlagen vor Missbrauch und unbefugtem Zugriff durch den Menschen (neben dem Schutz des Menschen vor den Produktionsanlagen). Daher sollten Aspekte der IT-Sicherheit bereits in der Konzeptionsphase der neuartigen Infrastrukturkomponenten einfließen (z. B. durch eine integrierte IT-Sicherheitsarchitektur).

7.1.2 Cloud-Architekturen in der Industrie

Cloud Computing ist ein technologischer Paradigmenwechsel, der IT-Infrastrukturen wie Software, Serversysteme oder Dienste in einer über ein Netz erreichbaren zentralisierten Struktur (Cloud) beliebig skalierbar zusammenfasst. Anders als in öffentlich zugänglichen Cloud-Infrastrukturen zur Ablage und gemeinsamen Nutzung von Dateien oder zur Nutzung von Ressourcen über Smartphones können

Cloud-Service-Provider und Nutzer derselben Organisation angehören (sogenannte Private Clouds). Aber auch in einer solchen Private Cloud kann die Infrastruktur im Rechenzentrum der eigenen Organisation oder einer fremden Institution betrieben werden.

Ein sich abzeichnender Trend in Richtung Cloud Computing in der Industrie betrifft das Enterprise Resource Planning (ERP) im Hinblick auf Materialwirtschaft, Logistik und Business Intelligence. Dabei spielt der Cloud-Teilbereich „Software as a Service“ (SaaS) eine wesentliche Rolle: Der Zugriff auf die über die Cloud bereitgestellte Software geschieht dann im Unternehmen allein über internetfähige PC und beschränkt sich im Hinblick auf die Anforderungen an die Clients auf einen Browser. Es werden nur die ERP-Ressourcen vergütet, die auch tatsächlich vom Industrieunternehmen in Anspruch genommen wurden (Pay per Use). In einem Service Level Agreement werden die Leistungen, die der Service Provider zusichert, dem Industrieunternehmen vertraglich geregelt. Die Administration der ERP-Software sowie Service-Dienstleistungen (wie Updates, Wartung, Backups) wird zentralisiert ausgeführt. Erwartet wird vom nutzenden Unternehmen der Cloud-Infrastruktur eine bedeutende Kostenersparnis im Bereich der ansonsten lokal vorzuhaltenden und zu wartenden IT-Komponenten.

Eine weitere Cloud-basierte Innovation betrifft die Durchführung von Fernwartung. So können zwischen Komponentenlieferant und -betreiber individuelle Kommunikationslösungen geschaffen werden. *„Zukünftig verbinden sich Spezialisten nicht mehr manuell mit den Maschinen. Die Produktionssysteme verbinden sich als sogenannte Social Machines automatisch zu ihrer Cloud-basierten Telepräsenz-Plattform und suchen sich situationsabhängig die benötigten Experten* “ (siehe [DAT 2013]). Die ICS-Komponenten erweitern dann selbstständig ihre Funktionalität, indem sie benötigte Konfigurationen und Daten automatisch nachladen. Ob sich diese Zukunftsvision tatsächlich zum Trend entwickelt, kann derzeit noch nicht abgesehen werden. Diese Zukunftsbild er veranschaulichen aber das enorme Potenzial, das sich mit der Verbreitung von Cloud-Infrastrukturen auch für industrielle und bisher IT-ferne Produktionsbereiche entfaltet.

Das BSI hat in einem Eckpunktepapier Empfehlungen für sicheres Cloud Computing erstellt, die sich zunächst an Cloud Service Provider richten und eine Grundlage für die Diskussion zwischen CSP und Cloud-Kunden bieten (vgl. [BSI 2012]). Die Empfehlungen betreffen u. a. Aspekte wie Rechenzentrumssicherheit, Server-Sicherheit, Netzsicherheit, Anwendungs- und Plattformsicherheit, Datensicherheit und Krypto-Mechanismen.

Mit zunehmender Verbreitung werden Cloud-Services für Angreifer interessant, insbesondere wenn kritische, die industrielle Produktion betreffende Ressourcen in zentralen Rechenzentren vorgehalten und attackiert werden können. Es werden daher mittelfristig internationale Standards für die Cloud-Sicherheit benötigt, auf deren Grundlage Service Provider evaluiert und zertifiziert werden können.

7.2 Mehr Sicherheit

7.2.1 Best Practices für Hersteller, Betreiber und Integratoren

In verschiedenen Phasen des Produktlebenszyklus nehmen unterschiedliche Parteien Einfluss auf ein ICS (z. B. Hersteller, Integrator, Betreiber. Für die sichere Herstellung, Integration und den Betrieb von ICS sind daher Leitfäden zur IT-Sicherheit für alle beteiligten Parteien erforderlich. Dies gilt insbesondere vor dem Hintergrund der bisher historisch bedingt untergeordneten Rolle der IT-Sicherheit für ICS.

Dabei wurden in der Vergangenheit Empfehlungen und Maßnahmen zur IT-Sicherheit von ICS in Normen und Standards vorrangig für Betreiber und somit nahezu ausschließlich für den sicheren Betrieb behandelt. In den letzten Jahren wurden darüber hinaus verstärkt Anforderungen von Betreibern an Hersteller von ICS formuliert (z. B. [DHS CSPL 2009], [WIB 2010], [BDEW 2008]), die als Beschaffungskriterium für ICS herangezogen werden sollen.

Vor dem Hintergrund der gehäuften IT-Sicherheitsvorfälle in den vergangenen Jahren sollten neben Anforderungen von Betreiberseite auch zusätzlich Best Practices für Hersteller gesammelt werden. Auf diese Weise können beispielsweise in der Herstellung verursachte Schwachstellen frühzeitig erkannt und behoben werden, die ansonsten nur schwierig im späteren Betrieb durch zusätzliche Schutzmaßnahmen kompensiert werden können.

Daher ist eine zukünftige, enge Zusammenarbeit zwischen den am Produktlebenszyklus beteiligten Parteien Hersteller, Integrator, Betreiber für die sichere Herstellung, Integration und den Betrieb von ICS zwingend erforderlich. Hierfür könnten vergleichbar zu Kapitel 5 Best Practices für Hersteller hilfreich sein. Des Weiteren stellt das BSI bereits jetzt unter http://www.allianz-für-cybersicherheit.de Informationen zu verschiedenen der genannten Themen für Hersteller zur Verfügung.

7.2.2 Integration von Safety und Security

Historisch bedingt behandeln die verbreiteten Industrie-Standards vornehmlich Gefahren, die von der Produktionsanlage ausgehen (Safety). Dagegen werden Aspekte der IT-Sicherheit zum Schutz der Produktionsanlage vor dem Menschen und damit des Missbrauchs oder unbefugten Zugriffs wenig oder nicht berücksichtigt (Security). Eine Verbindung von Safety- und Security-Anforderungen ist in der Normenwelt bisher maximal rudimentär gegeben.

Wie in Kapitel 4 beschrieben, existieren bereits einige Standards mit teils weitreichenden Anforderungen an die IT-Sicherheit von ICS. In Zukunft gilt es, diese Security-Anforderungen mit Safety-Anforderungen in Einklang zu bringen und in der Normenwelt Safety- und Security-Anforderungen zu integrieren. Dazu gibt es erste Bestrebungen bei der Normierung und der Überarbeitung von Standards.

7.2.3 Tool für ICS-Audits

Audits bezüglich der IT-Sicherheit von ICS-Anlagen sind in der Vergangenheit aufgrund der mangelnden oder fehlenden Information in den Industrie-Sektoren nicht oder sehr unterschiedlich durchgeführt worden. Mit der steigenden Sensibilisierung für das Thema IT-Sicherheit gewinnt die Prüfung auf Konformität gemäß anerkannter Industrie-Standards an Bedeutung. Kapitel 6 beschreibt dafür eine Herangehensweise, bis ein umfassendes ISMS etabliert ist.

Zur Durchführung einheitlicher ICS-Audits sollten sowohl die Vorgehensweise als auch die geprüften Inhalte und die Prüftiefe vergleichbar sein. Ein Tool für ICS-Audits kann die Auditoren hierin unterstützen und die Vergleichbarkeit gewährleisten.

In den USA existiert beispielsweise ein vom DHS entwickeltes, frei erhältliches Tool, welches die Auditoren bei der Durchführung der Audits unterstützt. Das sogenannte Cyber Security Evaluation Tool (CSET®, siehe [ICSCERT CSET 2013]) hilft die zu schützenden IT-Assets in einer systematischen Vorgehensweise zu ermitteln und zu bewerten. Dies geschieht auf der Grundlage von vordefinierten Fragen und dem Abgleich zu anerkannten Industriestandards (z. B. vom NIST, NERC, DoD und ISO). Als Resultat erhält der Auditor eine Auflistung von Empfehlungen aus den Standards und Best Practices sortiert nach Priorität. Dieses Tool ist allerdings aufgrund der unterstützten Standards nicht für Anlagenbetreiber in Deutschland anwendbar.

Für Betreiber von ICS-Anlagen fehlt bisher ein Tool, welches insbesondere für klein- und mittelständige Unternehmen (KMU) anwendbar ist, welchen die finanziellen und personellen Mittel fehlen, um ein Informationssicherheits-Managementsystem nach ISO/IEC 27001 (siehe Kapitel 4.1.1.1) oder den BSI IT-Grundschutz umzusetzen. Daher bedarf es einer leichtgewichtigen Möglichkeit, welche einen kostengünstigen und schnellen Einstieg in ICS-Security vor allem für KMU ermöglicht. Dabei könnte der Betreiber beispielsweise mit Hilfe eines definierten Satzes an Fragen zur IT-Sicherheit geleitet werden, um Erkenntnisse hinsichtlich der Bedrohungslage und des Schutzbedarfs zu erhalten. Auf Basis dieser Erkenntnisse erhält der Betreiber Hinweise für mögliche Schutzmaßnahmen und konkrete Umsetzungsmaßnahmen.

7.2.4 Weitere Entwicklung von Defense-in-Depth-Strategien

Unter dem Defense-in-Depth-Ansatz wird ein Konzept verstanden, das eine Absicherung auf den verschiedenen Schichten einer Architektur vorsieht, sodass eine Redundanz im Falle des Versagens der Sicherheitsarchitektur auf nur einer Ebene oder nur wenigen Ebenen wirksam wird. Der Angreifer ist dabei gezwungen, Sicherheitsbarrieren über mehrere Ebenen hinweg zu durchbrechen, sodass er in seinem Fortkommen behindert ist oder zumindest verlangsamt wird.

Bezogen auf die IT-Sicherheit von ICS ergibt sich daraus die Anforderung, Schutzmaßnahmen auf der Prozessführung Feld weiter zu entwickeln, sodass ihre Sicherheit nicht mehr von ihrer physischen Unzugänglichkeit und dem Schutz der Steuerungsebene abhängig ist. Eine wirkungsvolle Defense-in-Depth-Strategie würde auch einen Angreifer abwehren, der unmittelbar Zugriff auf die Prozessführung Feld hat. So ist beispielsweise der unbefugte Zugriff über einen ungeschützten Wartungszugang denkbar. Zusätzliche Barrieren können auch dann verhindern, dass ein Angreifer sich innerhalb der Prozessführung Feld weitere Angriffswege erschließt und die Prozessführung Realtime über RTU und SPS attackieren kann.

Elemente zur Umsetzung der Defense-in-Depth-Strategie sind Feldbus-Firewalls, sichere Feldbus-Protokolle und automatisierte Anomalie-Erkennung in der Feldbuskommunikation. In den folgenden Unterkapiteln werden diese Abwehrmaßnahmen behandelt.

8 Resümee und Ausblick

ICS sind schon seit langer Zeit essenziell notwendig für das Messen, Steuern und Regeln von Abläufen, beispielsweise zur Automation von Prozessen und zur Überwachung von großen Netzen und Systemen. Der seit einigen Jahren anhaltende Trend, diese Systeme mehr und mehr zu vernetzen und Standard-IT-Produkte zu verwenden, führt dazu, dass IT-Sicherheitsaspekte aus der klassischen IT nun auch bei ICS beachtet werden müssen. Dass zukünftig die IT-Sicherheit eine zunehmend wichtige Rolle in Steuerungs- und Automatisierungsanlagen spielen wird, zeigen bereits jetzt diverse Vorfälle, die insbesondere die Schutzziele Verfügbarkeit und Integrität aber auch Vertraulichkeit negativ beeinflussen.

Das hier vorliegende Kompendium bildet den Ausgangs- und Verknüpfungspunkt für alle weiteren technisch-orientierten Projekte und Entwicklungen des BSI im Kontext der IT-Sicherheit von Steuerungs- und Automatisierungsanlagen. Zusammen mit zukünftigen Projekten wird so ein Standardwerk zur ICS-Security erstellt.

Das Kompendium soll sukzessive um weitere Informationen angereichert und auch an neue Gegebenheiten angepasst werden. Als nächstes Ziel sind Best Practices für Hersteller, Maschinenbauer und Integratoren geplant, die diesen Hinweise und Unterstüzung bei der Entwicklung sicherer Produkte geben sollen.

Insbesondere eine allgemein stärkere Umsetzung von IT- Sicherheitsmaßnahmen in ICS ist notwendig, um den Bedrohungen für ICS entgegen zu wirken. Dazu bedarf es zum einen einer verstärkten Zusammenarbeit von herkömmlicher IT und ICS und zum anderen einer Integration von Securityaspekten in Safety-Anforderungen (Security for Safety). Neben den Betreibern, die über die Best Practices in diesem Kompendium primär adressiert sind, müssen Integratoren und Hersteller einen notwendigen Beitrag zur Erhöhung des ICS-Sicherheitsniveaus leisten, beispielsweise durch verstärkte Tests der ICS-Produkte.

Literaturverzeichnis

BSI GS	Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kataloge. 12. Ergänzungslieferung. Bonn: Bundesamt für Sicherheit in der Informationstechnik 2011
DUD 2009	Fox, Dirk: Mindestlängen von Passwörtern und kryptographischen Schlüsseln. Datenschutz und Datensicherheit Nr. 10 (Oktober 2009): 620-623. Wiesbaden: Springer Gabler Verlag 2009
BSI 2008	Bundesamt für Sicherheit in der Informationstechnik: M 2.11 Regelung des Passwortgebrauchs. IT-Grundschutz-Kataloge. 12. Ergänzungslieferung. Bonn: Bundesamt für Sicherheit in der Informationstechnik 2011
OWASP Top10	Open Web Application Security Project: OWASP Top Ten Project. Version 2010. https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project (11.06.2013)
IX 2013	Waibel, Stefan: Gezielte Abwehr: Wie man sich vor Denial-of-Service-Angriffen schützt. iX Nr. 5 (Mai 2013): 64-67 Hannover: Heise Zeitschriften Verlag GmbH & Co. KG 2013
BSI 2012	Bundesamt für Sicherheit in der Informationstechnik: Sicherheitsempfehlungen für Cloud Computing Anbieter. Bonn: Bundesamt für Sicherheit in der Informationstechnik 2012
ISO/IEC 27000	Internationale Organisation für Normung; Internationale Elektrotechnische Komission: ISO/IEC 27000-Reihe Information technology – Security techniques
ISO Standards 2013	Internationale Organisation für Normung: Standards catalogue. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=45306 (11.06.2013)
BITKOM/DIN 2007	BITKOM; DIN: Kompass der IT-Sicherheitsstandards. Version 3.0. Berlin: BITKOM, DIN 2007
BMWi 2009	OFFIS - Institut für Informatik, SCC Schwarz Communication Consulting, mpc management project ciaching: Untersuchung des Normungsumfeldes zum BMWI-Förderschwerpunkt "e-Energy - IKT-basiertes Energiesystem der Zukunft". http://www.e-energy.de/documents/Zusammenfassung-2009-02-23_Untersuchung_des_Normungs-_und_Standardisierungsumfeldes__E-Energy%281%29.pdf (11.06.2013)
IEC 62351	Internationale Elektrotechnische Kommission: IEC 62351 Power systems management and associated information exchange – Data and communication security
Cleveland 2012	Cleveland, Frances: IEC 62351 Security Standards for the PowerSystem Information Infrastructure. http://xanthus-consulting.com/Publications/documents/IEC%20_TC57_WG15_White_Paper.pdf (11.06.2013)
DIN SPEC 27009 2013	Deutsches Institut für Normung e. V.: DIN SPEC 27009. http://www.nia.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738935&subcommitteeid=54742877&artid=151100155&bcrumblevel=2&languageid=de (12.06.2013)
DIN SPEC 27009 2012	Deutsches Institut der Normung e.V.: DIN SPEC 27009:2012-04 Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung auf der Grundlage der ISO/IEC 27002. Berlin: Deutsches Institut der Normung e.V. 2012
TeleTrusT 2012	Kasper, Rolf-Dieter: DIN SPEC 27009 Informationssicherheit in Energienetzen. http://www.teletrust.de/uploads/media/TeleTrusT-Infotag_SmartGrid_Kasper.pdf (11.06.2013)

VDI 2182 2011	Verein Deutscher Ingenieure; Verband der Elektrotechnik, Elektronik, Informationstechnik: VDI/VDE 2182 Informationssicherheit in der industriellen Automatisierung. Berlin: Beuth Verlag GmbH 2011
VDI/VDE Richtlinien 2013	VDI e. V.: VDI-Richtlinie: VDI/VDE-Handbuch Automatisierungstechnik. http://www.vdi.de/7776.0.html?&tx_vdirili_pi2[showUID]=89690 (12.06.2013)
NA 115 2006	Normenarbeitsgemeinschaft für Meß- und Regeltechnik in der chemischen Industrie: IT-Sicherheit für Systeme der Automatisierungstechnik: Randbedingungen für Maßnahmen beim Einsatz in der Prozessindustrie. NAMUR-Arbeitsblatt 115. 1. Auflage. Leverkusen: NAMUR (c/o Bayer Technology Services GmbH) 2006
BSI100-1	Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-1: Managementsysteme für Informationssicherheit
BSI 100-2	Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise
BDEW 2008	BDEW Bundesverband der Energie- und Wasserwirtschaft e.V.: Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme. Version 1.0. Berlin: BDEW 2008
OE BDEW 2012	Oesterreichs Energie; BDEW: Anforderungen an sichere Steuerungs- und Telekommunkationssysteme: Ausführungshinweise zur Anwendung des BDEW Whitepaper. Version 1.0. Wien: Oesterreichs E-Wirtschaft, Berlin: BDEW 2012
VGB R 175	VGB PowerTech e.V.: VGB-R 175 Richtlinie: IT-Sicherheit für Erzeugungsanlagen. 1. Auflage. Essen: VGB PowerTech e.V. 2006
NERC CIP	North American Electric Reliability Corporation: Critical Infrastructure Protection-Standards. http://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx (11.06.2013)
SP 800-53	National Institute of Standards and Technology: Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations. Version 4. Gaithersburg (Maryland, USA): NIST 2013
SP 800-82	National Institute of Standards and Technology: Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security. Gaithersburg (Maryland, USA): NIST 2011
NISTIR 7628	National Institute of Standards and Technology: NISTIR 7628 Guidelines for Smart Grid Cyber Security. Gaithersburg (Maryland, USA): NIST 2010
DHS CSPL 2009	Department of Homeland Security: Cyber Security Procurement Language for Control Systems. Washington (District of Columbia, USA): Department of Homeland Security 2009
DHS Assessment 2010	Department of Homeland Security; Centre for the Protection of National Infrastructure: Cyber Security Assessments of Industrial Control Systems. Washington (District of Columbia, USA): Department of Homeland Security 2010
DHS DiD 2009	Department of Homeland Security: Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies. Washington (District of Columbia, USA): Department of Homeland Security 2009
DHS PM 2008	Department of Homeland Security: Recommended Practice for Patch Management of Control Systems. Washington (District of Columbia, USA): Department of Homeland Security 2008
DHS Modem 2008	Department of Homeland Security: Recommended Practice for Securing Control System Modems. Washington (District of Columbia, USA): Department of Homeland Security 2008
DHS Remote 2010	Department of Homeland Security; Centre for the Protection of National Infrastructure: Configuring and Managing Remote Access for Industrial

	Control Systems. Washington (District of Columbia, USA): Department of Homeland Security 2010
DHS ZigBee 2007	Department of Homeland Security: Recommended Practices Guide For Securing ZigBee Wireless Networks in Process Control System Environments. Entwurf. Washington (District of Columbia, USA): Department of Homeland Security 2007
DHS IR 2009	Department of Homeland Security: Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability. Washington (District of Columbia, USA): Department of Homeland Security 2009
DHS Standards 2009	Department of Homeland Security: Catalog of Control Systems Security: Recommendations for Standards Developers. Washington (District of Columbia, USA): Department of Homeland Security 2009
DHS OPSEC 2007	Department of Homeland Security: Recommended Practice: Using Operational Security (OPSEC) to Support a Cyber Security Culture in Control Systems Environments. Version 1.0 (Entwurf). Washington (District of Columbia, USA): Department of Homeland Security 2007
DHS Personnel 2004	Department of Homeland Security: Personnel Security Guidelines. Washington (District of Columbia, USA): Department of Homeland Security 2004
CPNI 2008	Centre for the Protection of National Infrastructure: Good Practice Guide - Process Control and SCADA Security. CPNI 2008
CPNI 2005	Centre for the Protection of National Infrastructure: Good Practice Guide - Firewall Deployment for SCADA and Process Control Networks. CPNI 2005
IEC 62443	Internationale Elektrotechnische Kommission: IEC 62443 Normenreihe Industrial communication networks - Network and system security
BSI CS-061	Bundesamt für Sicherheit in der Informationstechnik: Cybersicherheitsempfehlung: Industrial Control System Security: Innentäter
BSI IDS	Bundesamt für Sicherheit in der Informationstechnik: BSI-Leitfaden zur Einführung von Intrusion-Detection-Systemen. https://www.bsi.bund.de/DE/Publikationen/Studien/ids02/index_htm.html (11.06.2013)
RFC 2845 2000	Network Working Group: Request for Comments 2845: Secret Key Transaction Authentication for DNS. Fremont (CA, USA): Internet Engineering Task Force 2000
BSI LogDaten	Bundesamt für Sicherheit in der Informationstechnik: Studie über die Nutzung von Log- und Monitoringdaten im Rahmen der IT-Frühwarnung und für einen sicheren IT-Betrieb. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Logdaten/logdatenstudie_pdf.pdf?__blob=publicationFile (11.06.2013)
IS 10	Bundesamt für Sicherheit in der Informationstechnik: Informationssicherheitsrevision - Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz. Version 2.0. Bonn: Bundesamt für Sicherheit in der Informationstechnik 2010
BSI IS-Revision 2010	Bundesamt für Sicherheit in der Informationstechnik: Informationssicherheitsrevision - Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz. Version 2.0. Bonn: Bundesamt für Sicherheit in der Informationstechnik 2010
BUND_2012	Bundesministerium für Bildung und Forschung: Industrie 4.0. http://www.hightech-strategie.de/de/59.php (10.05.2013)
DAT 2013	Deutsche Akademie der Technikwissenschaften: Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0. http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/

	Acatech/root/de/Projekte/Laufende_Projekte/Industrie_4.0/Bericht_Industrie_4.0_barrierefrei.pdf (13.05.2013)
WIB 2010	Werkgroup voor Instrument Beoordeling: M 2784-X-10 Process Control Domain - Security Requirements for Vendors. Version 2.0. Den Haag (NL): WIB 2010
ICSCERT CSET 2013	Industrial Control Systems Cyber Emergency Response Team: Cyber Security Evaluation Tool (CSET), http://ics-cert.us-cert.gov/Assessments, abgerufen am 10.05.2013
Yang 2006	Yang, Dayu; Usynin, Er; Hines, J. Wesley: Anomaly-Based Intrusion Detection for SCADA Systems. 5th International Topical Meeting on Nuclear Plant Instrumentation. 2006
Tsan 2005	Tsang, Chi-Ho; Kwong, Sam: Multi-agent intrusion detection system in industrial network using ant colony clustering approach and unsupervised feature extraction. IEEE International Conference on Industrial Technology (2005): 51–56 IEEE 2005
ISCdiary 2012	Pelaez, Manuel; Santander, Humberto: Snort 2.9.2 now supporting SCADA protocol checks. http://isc.sans.edu/diary/Snort+2.9.2+now+supporting+SCADA+protocol+checks/12346 (13.05.2013)
Gao 2010	Gao, Wei; Morris, T.; Reaves, B.; Richey, D.: On SCADA control system command and response injection and intrusion detection. eCrime Researchers Summit (2010): 1–9. eCrime 2010
Vald 2009	Valdes, A.; Cheung, S: Intrusion Monitoring in Process Control Systems. 42nd Hawaii International Conference on System Sciences (2009): 1–7. HICSS 2009
Gold 2013	Goldenberg, Wool: Accurate Modeling of Modbus/TCP for Intrusion Detection in SCADA Systems. 7th Annual IFIP Working Group. ICCIP 2013