Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Status Quo: Safety & Security in Störfall-relevanten Betriebsbereichen

Umwelt Bundesamt

Änderungshistorie

Version	*Datum*	*Beschreibung*
1.0	15.09.2021	Veröffentlichung

Tabelle 1 Änderungshistorie

Bundesamt für Sicherheit in der Informationstechnik Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: ics-sec@bsi.bund.de
Internet: https://www.bsi.bund.de

Vorwort

Die fortschreitende Digitalisierung und Vernetzung durchdringt das allgemeine Leben und Unternehmen immer stärker. IT-Sicherheitslücken, die in immer mehr Systemen publik werden, geben Anlass zu Besorgnis. Ehemals abgeschottete Produktionssystem werden vernetzt und damit auch anfälliger für Angriffe. Während Angriffe auf Büroinfrastrukturen häufig finanzielle Schäden oder den Abfluss sensitiver Daten zur Folge haben, können bei Angriffen auf Produktionsanlagen physische Folgen für Mensch und Umwelt hinzukommen.

Doch wie steht es um die Safety-Systeme, die dem Schutz von Mensch und Umwelt dienen? Diese Studie soll einen Überblick zu Herausforderungen geben, die sich im Zusammenspiel aus Safety und Security ergeben. Die Studie wurde gemeinsam vom Umweltbundesamt und Bundesamt für Sicherheit in der Informationstechnik (BSI) konzipiert und durchgeführt.

Vorwort des Umweltbundesamtes

Das Umweltbundesamt als zentrale Umweltbehörde des Bundes fördert die Anlagensicherheit und Störfallvorsorge, in dem es dazu Forschung betreibt und mit den erzielten Ergebnissen die Bundesregierung, wie etwa das Bundesumweltministerium, für ihre Politik berät.

Das Ziel von Anlagensicherheit und Störfallvorsorge ist es, Störungen in Anlagen, in denen mit Gefahrstoffen umgegangen wird, zu verhindern. Die Auswirkungen von Störungen, die dennoch eintreten, gilt es, für Mensch und Umwelt zu begrenzen.

Rechtsvorschriften und Normen bilden die entscheidende Grundlage für die Festlegung von Anforderungen an die Anlagensicherheit. Daher bringt das Umweltbundesamt seine Expertise sowohl bei der Erarbeitung und Fortentwicklung von Rechtsvorschriften und Normen als auch bei der Unterstützung und Verbesserung ihrer Anwendung in die Vollzugspraxis ein.

Das Bundesimmissionsschutzgesetz (BImSchG) und die Störfallverordnung (12. BImSchV) formulieren gegenüber dem Betreiber von Betriebsbereichen bestimmte Pflichten. Zu diesen Pflichten zählt auch, das Eingreifen Unbefugter zu verhindern, soweit es geeignet ist, Ursache für einen Störfall zu sein. Die Erfüllung dieser Pflichten nachzuweisen, ist gleichzeitig Genehmigungsvoraussetzung und Inhalt bei regelmäßig durchzuführenden Überwachungen der Anlagen.

Mit der vorliegenden Studie wird ein Beitrag geleistet, das hohe Niveau der Anlagensicherheit auch unter den Bedingungen einer fortschreitenden, durchgängigen Digitalisierung und auch im Hinblick auf eine Entwicklung in Richtung Industrie 4.0 zu sichern.

Das Umweltbundesamt wird die Erkenntnisse der Studie in die zukünftige Arbeit zur Weiterentwicklung des Standes der Sicherheitstechnik einfließen lassen. Die erzielten Ergebnisse zu diesem Thema sind ein wertvoller Beitrag, sowohl für die Regelsetzung als auch den Vollzug. Das Umweltbundesamt bedankt sich bei BSI für die sehr gute Zusammenarbeit und intensive Einbeziehung in die Projektbearbeitung.

Vorwort des Bundesamtes für Sicherheit in der Informationstechnik

Das Bundesamt für Sicherheit in der Informationstechnik als zentrale IT-Sicherheitsbehörde des Bundes fördert die Cyber-Sicherheit in Deutschland. Dies erfolgt durch Prävention, Reaktion und Detektion in Zusammenarbeit von Staat, Wirtschaft und Gesellschaft. In der Störfallvorsorge ist diese Zusammenarbeit, insbesondere von Behörden und Betreibern von Betriebsbereichen, bereits geübte Praxis. Durch die Digitalisierung wird die Cyber-Sicherheit zunehmend zu einem integralen Bestandteil der präventiven Maßnahmen um Störfalle zu verhindern.

Das BSI hat bereits eine Vielzahl von allgemeinen Empfehlungen zum Schutz industrielle Steuerungs-und Automatisierungssysteme veröffentlicht. Mit dieser Studie soll ein tieferer Blick in Unternehmen und Betriebsbereiche genommen werden. Dazu werden bestehende Herausforderungen erfasst und Lösungswege sowie Hinweise zum Umgang gegeben. Dabei wird auch ein Blick auf sich abzeichnende Entwicklungen und

Trends geworfen. Zudem wird auf die Zusammenarbeit zwischen Betreibern, Behörden und Sachverständigen eingegangen.

Die Erkenntnisse aus der Studie werden in zukünftige Arbeiten zum Schutz von industriellen Steuerungs- und Automatisierungssystemen Eingang finden. Zudem soll Sie dazu dienen, den Austausch mit Behörden und Betreibern zu intensivieren.

Danksagung

Das BSI dankt dem Projekt-Team aus TÜV Informationstechnik GmbH, der TÜV NORD Systems GmbH & Co KG und TÜV NORD InfraChem GmbH & Co. KG für die Erstellung dieser Studie.

Die Zusammenarbeit in dem interdisziplinären Team war geprägt durch Hilfsbereitschaft, Offenheit und Zuverlässigkeit. Eine vergleichbare produktive, kollegiale Arbeitsatmosphäre sei auch den Lesenden gewünscht und denen, die OT-Security in Ihrem Umfeld mitgestalten. Für das Interesse und die Zeit zur Studie des Berichtes gilt ein herzlicher Dank. In Vertretung für die Zielgruppen dieses Berichtes wurden insgesamt 19 Personen zu ihren Erfahrungen, empfundenen Herausforderungen und Praxisbeispielen befragt. Ohne die offene Bereitschaft

- der Gascade Gastransport GmbH,
- der DOW Deutschland Anlagengesellschaft mbH,
- der Clariant SE,
- der H&R Ölwerke Schindler GmbH,
- der Thyssen Krupp Steel Europe AG,
- der TÜV Rheinland AG,
- der TÜV NORD Systems GmbH & Co KG,
- der TÜV NORD InfraChem GmbH & Co. KG,
- der Behörde für Umwelt, Klima, Energie und Agrarwirtschaft der Freien und Hansestadt Hamburg,
- des staatlichen Gewerbeaufsichtsamts Cuxhaven und dem Regierungspräsidium Darmstadt,
- sowie einigen weiteren Unternehmen und Behörden,

ihre praktische Erfahrung zur Anwendung der OT-Security in diesen Bericht einfließen zu lassen, hätten die aktuellen Herausforderungen an Betreiber, Behörden und Sachverständige nicht mit der gleichen Praxisrelevanz behandelt werden können. Ein herzlicher Dank für die freundliche Unterstützung gilt allen Interviewten und Mitarbeitenden, ohne die dieser Bericht nicht derart umfassend und praxisnah gelungen wäre. Ein Dank geht dabei an alle Mitwirkenden und persönlich an Lara Berdelsmann, Jan Russmann, Hans-Peter Ziegenfuß, Ralf Schmitt, Jürgen Bode, Boris Göppert und Thorsten Lasrich für ihre wertvollen Beiträge.

Inhalt

1 Einleitung

Im Zeitalter von Industrie 4.0 führt der vermehrte Einsatz vernetzter elektronischer Komponenten zu komplexen Netzwerkstrukturen. Die klassische Trennung der Automatisierungsebenen nach dem Vorbild der Automatisierungspyramide (vgl. Abbildung 1) bildet in der Praxis längst nicht mehr die Realität ab. IT-Systeme wie ERP-, MES-, SCADA Systeme und OT-Steuerungen (PLS und SIS) sowie Feldgeräte verschmelzen zunehmend informationstechnisch mit Office Anwendungen und Internetdiensten.

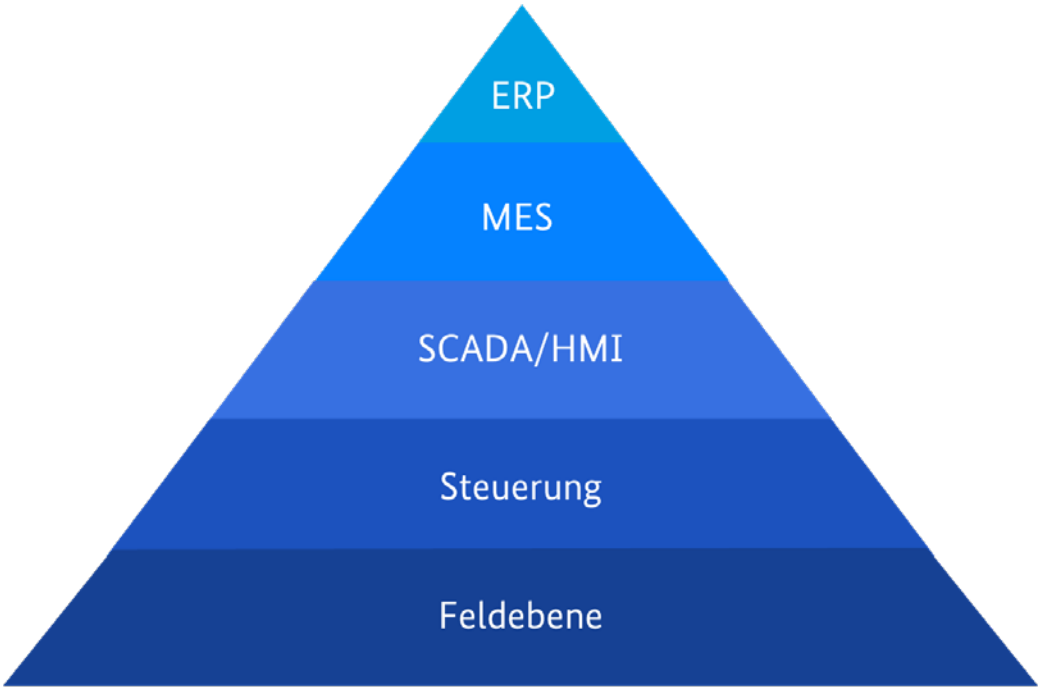

Abbildung 1 Automatisierungspyramide

Dieser Bericht wurde im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik (BSI) erstellt. Der Bericht soll eine Anregung, Inspiration und Anleitung geben, OT-Security in Betriebsbereichen nach 12. BImschV anforderungsgerecht umzusetzen. Hierzu werden Erfahrungen aus der Praxis zusammengestellt und Einschätzungen zu den neuen Technologien gegeben, die Sie dabei unterstützen sollen, die Digitalisierung und OT-Security in Ihrem Unternehmen zu meistern.

Der Bericht verwendet den Begriff **Betriebsbereiche**, um damit Betriebsbereiche der unteren und oberen Klasse gemäß 12. BImschV zu erfassen. Der Begriff wurde gewählt, um eine bessere Lesbarkeit zu erreichen. Grundsätzlich gelten viele Aussagen auch für andere prozesstechnische Anlagen, die nicht dem Störfallrecht unterliegen.

Bei der Einführung, Planung, Umsetzung und Inspektion von Cyber-Sicherheitsmaßnahmen sind Fachkräfte mit unterschiedlichen Erfahrungen und Wissensständen beteiligt. Die Studie soll dabei helfen die unterschiedlichen Mentalitäten besser zu verstehen und Missverständnisse abzubauen.

Hierzu werden die handelnden Personengruppen zunächst eingeführt und ihr möglicher Beitrag im Hinblick auf die Einführung und Instandhaltung von Cyber-Sicherheitsmaßnahmen unter den Gesichtspunkten der Wechselbeziehungen Mensch-Technik-Organisation untersucht. Hierbei werden

- häufig zu beobachtende Schwierigkeiten beschrieben und es wird ein Weg aufgezeigt, mit dem auch sehr inhomogene Interessengruppen eine Problemlösung entwickeln können,
- neue Technologien in den Blick genommen und
- die wesentlichen Regelwerke und Standards vorgestellt.

In den Bericht sind Einschätzungen von 19 interviewten Personen (Betreiber, Behörden und Sachverständige) eingeflossen. Diese wurden zu den Herausforderungen des Themas OT-Security und der Anwendung der KAS-51 befragt. Soweit möglich, gibt der Bericht durch Bezüge auf das Regelwerk oder durch Praxisbeispiele der Interviewten Hinweise zu möglichen Lösungsansätzen.

Eine von vielen Herausforderungen der Betreiber sind die noch fehlenden Konzepte, die die jeweils erforderlichen Security Maßnahmen beschreiben. Eine solche Herausforderung beschreibt z.B. die Frage, mit welchen Maßnahmen eine Anlage mit Remotesteuerung anforderungsgerecht gegen Cyberangriffe geschützt werden kann. Eine Frage, auf die es aufgrund von Unterschieden der Prozessführung, der individuellen Netzwerkstrukturen und verwendeten Bauteile keine pauschale Antwort geben wird.

Die Maßnahmen der Anlagensicherheit (z.B. 12. BImSchV; VDI/VDE 2180) und OT-Security (z.B. KAS-51, BSI-Standard 200-3) sollen auf einer Risikobeurteilung beruhen. Die Risikobeurteilungen basieren auf der Spezifikation der Betreiber, dem Anlagendesign des Integrators und dem Produktdesign der Hersteller. Das Ergebnis der Risikobeurteilung und die Wirksamkeit der Maßnahmen hängen also u.a. von den Schnittstellen zum Integrator und Hersteller ab. Die Kenntnisse und Erfahrung von Integratoren und Herstellern, Mitverantwortung zum Thema OT-Security zu übernehmen, dürfte aufgrund des relativ neuen Themas noch gering sein.

In den Bericht sind Erfahrungen und Erkenntnisse zur Methode, Vorbereitung, Durchführung und Ableitung von Maßnahmen aus einer IT-Risikoanalyse eingeflossen. Die IT-Risikoanalyse wurde am Beispiel eines aus der Ferne gesteuerten Gasspeichers durchgeführt. Gespräche mit einem Integrator und Hersteller komplettieren ein Bild über Herausforderungen und Empfehlungen bei der Gestaltung der Schnittstellen zum Betreiber.

Herausforderungen, zu denen der Autorenschaft derzeit noch keine Lösungen bekannt sind, sind als Defizite ausgewiesen. Die benannten Defizite sollen die adressierten Interessengruppen motivieren, Lösungen in Zukunft bereitzustellen.

Der Bericht gibt somit

- einen Überblick über das unterschiedliche Verständnis der handelnden Personengruppen,
- einen Einblick in den Stand des Wissens zur anforderungsgerechten Auslegung der Prozessautomatisierung von Störfallbetrieben,
- eine Anleitung für Cyber-Resilienz und ein sicheres Design sowie
- eine Unterstützung, um zukünftige Herausforderungen in den Blick nehmen zu können.

2 Problemanalyse zur OT-Security

Das Bewusstsein für Themen der Cyber-Security ist in Bezug auf produktionsnahe Automatisierungstechnik (engl.: Operational Technology, OT) bei den Verantwortlichen in deutschen Störfallbetrieben vorhanden. Die Chemie- und Pharmaindustrie gehören zu den am stärksten in Deutschland von Angriffen auf die IT-Systeme betroffenen Unternehmen (1). Dass die Angriffe nicht notwendigerweise auf IT-Systeme beschränkt sind, hat der im Dezember 2017 bekannt gewordene Cyber-Angriff mit der Schadsoftware "Triton/Trisis/HatMan“ (2) auf ein Sicherheitssystem belegt. Security ist daher kein Selbstzweck, sondern dient letztlich der eigentlichen Funktion der Anlage und deren Schutzeinrichtungen. OT-Security Maßnahmen sollen Schadpotentiale, die von außen wirken können, abwenden. Dabei dürfen durch die Security-Maßnahmen weder die Funktion der Produktion noch die Sicherheitsfunktionen beeinträchtigt werden. Letztlich ist OT-Security eine Entscheidung zwischen Nutzbarkeit und Risiko. In Bezug auf die Sicherheitsfunktion besteht jedoch ein hohes Risiko, sodass die Anforderungen an OT-Security zum Erhalt der Anlagensicherheit besonders hoch sind.

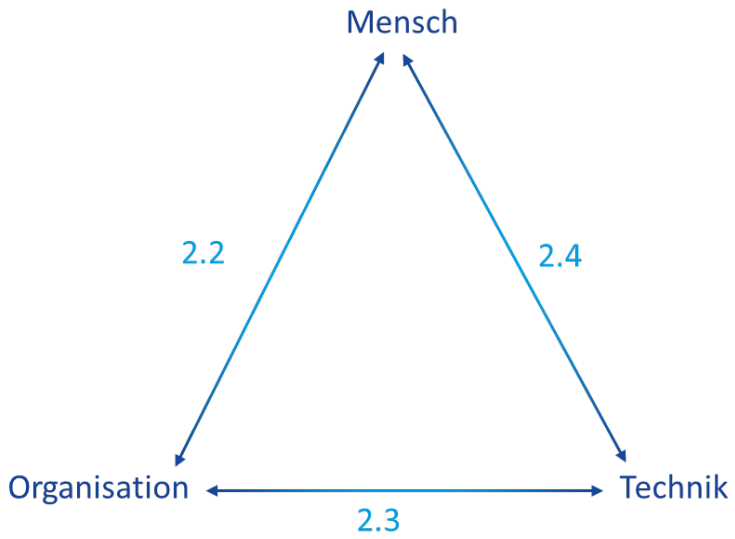

Abbildung 2 MTO-Betrachtung OT-Security

Den Einstieg in die Problemanalyse gibt eine fiktive „Short Story“. Daran anschließend werden anhand von Beispielen häufig auftretende Probleme, die allgemein bei der Einführung neuer Technologien beobachtet werden, thematisiert und mögliche Lösungswege aufgezeigt. Zum Teil werden in den Beispielen bereits spezifische Herausforderungen bei der Umsetzung von Safety & Security in Störfallbetrieben (im Folgenden als OT-Security bezeichnet) thematisiert.

In den Abschnitten 2.1, 2.2, 2.3 und 2.4 werden allgemeine Probleme und Herausforderungen, die das Thema OT-Security in Störfallbetrieben mit sich bringt, analysiert. Hierbei wird das Thema vor dem Kontext der Wechselbeziehungen zwischen den Bereichen Mensch, Technik und Organisation (vgl. Abbildung 2) untersucht. Diese Betrachtung gestattet es, Probleme bei der Einführung von OT-Security von allen Seiten zu beleuchten. Die Studie soll neben dem Problembewusstsein, auch Anregungen für mögliche Lösungen vermitteln. Hierzu werden Verknüpfungen zwischen den beschriebenen Problemen mit den einschlägigen Regelwerken, Normen (siehe Abschnitt 4) sowie Praxisbeispielen (siehe Abschnitt 6) hergestellt.

2.1 Allgemeine Betrachtungen

2.1.1 Short Story

Bitte stellen Sie sich vor, dass Sie eine zentrale Messwarte einer chemischen Anlage betreten. Ihr Blick fällt als erstes auf die zwölf Großbildschirme an der gewölbten Stellwand. Die Monitore übertragen Bilder von

Überwachungskameras im Feld, Messverläufe aus dem Anlagenprozess, Messwerte und Schaltzustände von Armaturen in das SCADA (Supervisory Control and Data Acquisition) System. Vor den Großbildschirmen sind Computerarbeitsplätze für fünf Anlagenfahrer vorhanden. Zurzeit sind zwei von diesen besetzt. Auf dem Boden ausgelegte Kabel verschwinden hinter der Stellwand. Zangen, Kabelbinder und ein Laptop sind auf einem Stuhl abgelegt. Scheinbar wird parallel noch hinter der Stellwand an der Verkabelung der Prozessleittechnik (PLT) gearbeitet. Einer der beiden Anlagenfahrer unterbricht seine Arbeit, um sich Ihnen zuzuwenden.

Der Anlagenfahrer informiert Sie: „Gegenüber dem früheren diskontinuierlichen Produktionsprozess, fahren wir heute mit der vollautomatisierten kontinuierlichen Anlage bis zu 50% mehr Produkt. Diese zentrale Messwarte gehört zu den modernsten und leistungsstärksten in unserem Unternehmen. Während der noch laufenden Modernisierungsarbeiten an unserer 20km entfernten Schwesteranlage fahren wir beide Anlagen von dieser Messwarte. Die Verbindung zwischen den beiden Anlagen erfolgt über eine gesicherte Internetverbindung…“ Der Bericht des Anlagenfahrers wird plötzlich durch ein kreischendes „Beep“ – „Beep“ – Alarmsignal unterbrochen.

Sie haben ein flaues Gefühl in der Magengegend. Was hat das Signal ausgelöst? Haben wir in der Risikoanalyse an alles gedacht? Es ist Mittwoch 10:52 Uhr, die Windrichtung liegt bei 69°. Eine Stofffreisetzung würde in Richtung Ihres Wohnhauses getragen und ca. 50.000 Einwohner Ihrer Heimatstadt müssten gewarnt werden.

Die beiden Anlagenfahrer haben den Alarm quittiert und verschaffen sich routiniert einen Überblick über die Situation. Auf den Großbildschirmen wechseln die angezeigten Darstellungen. Auf dem SCADA-System erscheint eine Zeichnung von Reaktor 2. „Es gibt ein Problem mit Reaktor 2. Druck und Temperatur sind zu hoch – das hat den Alarm ausgelöst.“, sagt der Reaktorfahrer. Konzentriert werden der Anlagendruck und die in gelben Symbolen dargestellten PLT-Sicherheitseinrichtungen (PLT-S) beobachtet. Erneut wird die Stille von einem Alarmsignal gestört. „Der Anlagendruck ist sehr hoch und das Sicherheitssystem hat NICHT ausgelöst.“, ruft der andere Anlagenfahrer. Die beiden Anlagenfahrer besprechen sich und ziehen aus einem Ordnerregal die betreffende Notfallprozedur des Betriebshandbuches hervor.

Während des aufmerksamen Lesens im Betriebshandbuch, wechselt die Beleuchtung im Raum. Alle Großbildschirme zeigen nun grüne Schrift auf schwarzem Grund an. Auf den Monitoren ist zu lesen „YOU GOT HACKED“.

Sicherlich sind auch Sie neugierig zu erfahren, was dort in der Anlage genau vor sich geht. Hat sich ein Scriptkiddie einen „Spaß“ erlaubt? Sind Cyber-Kriminelle auf Ruhm aus? Haben diese politische Motive oder sind sie auf Lösegeld aus? Steckt gar staatliches Handeln dahinter?

Technisch ist ein derartiger Angriff auf industrielle Kontrollsysteme (engl.: Industrial Control System, ICS oder auch Operation Technology, OT) grundsätzlich möglich. Allein im ersten Halbjahr 2020 wurden in der „Nationalen Datenbank für Sicherheitslücken“ (engl.: National Vulnerability Database, NVD) mehr als 270 kritische und zumeist aus der Ferne ausnutzbare ICS-Schwachstellen aufgedeckt. Unter Ausnutzung derartiger Schwachstellen und gängiger Werkzeuge, können Advanced Persistent Threat (APT) Hacker einen derartigen Angriff, wie z.B. 2010 Stuxnet oder 2017 Triton, ausführen. In der Praxis sind diese Angriffe heute noch die Ausnahme. Allerdings wird vom Bundesamt für Sicherheit in der Informationstechnik (BSI) im „Bericht zur Lage der IT-Security in Deutschland 2019“ (3) vor der steigenden Anzahl der verfügbaren Werkzeuge und APT-Dienstleistungsunternehmen gewarnt. Laut (3) sind Ransomware-Angriffe, wie 2019 auf einen norwegischen Aluminiumkonzern mittels LockerGoga, die stärkste Gefährdung für die Wirtschaft.

> *“Wir sind nicht nur verantwortlich für das, was wir tun, sondern auch für das, was wir nicht tun.“ - Molière*

Das Bild von boshaften externen Angreifenden – wie in einem James Bond Film – verstellt häufig den Blick auf die tatsächlichen Täter. In der Meldung der Bitkom vom 06. November 2019 (4), sind von den betroffenen Unternehmen folgende Tätergruppen als Urheber von Cyber-Angriffen benannt worden (Mehrfachnennungen waren möglich):

- 8% Einzeltäter,
- 33% ehemalige Mitarbeitende (ein absichtliches Fehlverhalten kann bei ca. 10% unterstellt werden),
- 21% organisierte Kriminalität
- 20% Mitbewerber
- 12% ausländische Geheimdienste.

Egal ob Sie sich als Führungskraft, Mitwirkende der Anlagensicherheit (Betreiber, Behörden und Sachverständige), Verantwortliche für Automatisierungstechnik, Planung, Integrator, Informationssicherheitsbeauftragte, IT-Verantwortliche oder Fachkräfte in die „Short Story“ hineingedacht haben, ist Ihnen sicherlich die Verantwortung für Ihr Handeln bewusst geworden. Das Zitat des Dramatikers und Philosophen Molière lässt sich insofern auf jeden der vorgenannten Verantwortlichen übertragen – Ihr Unternehmen braucht in Bezug auf den Schutz vor Cyber-Risiken Ihr Zutun.

In der „Short Story“ symbolisiert die zentrale Messwarte die Organisation der Tätigkeiten der Prozessautomation im Betriebsbereich. Von der Planung, Errichtung bis hin zum Anlagenbetrieb sind die notwendigen Tätigkeiten zu organisieren, um eine sichere und wettbewerbsfähige Produktion zu realisieren. Die via Internetverbindung gefahrene Schwesteranlage beschreibt die Leistungsfähigkeit moderner Automatisierungs- und Informationstechnik. Das Szenario des Angriffs durch Cyber-Kriminelle erinnert daran, dass hierbei neue Risiken zu managen sind.

> *“Die Arbeitsaufgabe verknüpft einerseits das soziale mit dem technischen Teilsystem, sie verbindet andererseits den Menschen mit den organisationalen Strukturen“ - Eberhard Ulich*

Menschen analysieren, planen, errichten, bedienen und beobachten die technischen Anlagenprozesse. Moderne Automatisierungs- oder Prozessleittechnik ist zunehmend vernetzt und softwarebasiert. Die Schnittstellen können ausgenutzt werden, um Software boshaft oder versehentlich zu verändern. Die Organisationsstrukturen produktionsnaher Prozesse und Betriebsabläufe unterscheiden sich heute deutlich von denen in IT-Abteilungen. Wie kann das Zusammenspiel im produktionsnahen Bereich zwischen den Menschen, der Technik und den Organisationsstrukturen im Unternehmen organisiert werden? Gemäß der von Eberhard Ulich und Oliver Strohm entwickelten Betriebsanalyse (5) kann die Einführung neuer Techniken in einem Unternehmen nur dann den angestrebten Erfolg bewirken, wenn sowohl menschliche als auch technische Ressourcen sowie Umweltgegebenheiten, Erwartungen und Erfahrungen beachtet werden.

2.2 Mensch und Organisation

Sofern Sie noch nicht vollständige Prozesse und Verantwortlichkeiten zum Thema OT-Security in Ihrem Unternehmen etabliert haben, gibt Ihnen dieses Kapitel einen Überblick über den Kreis der Akteure, deren Mitwirkung wesentlich für den Erfolg ist. Hierbei werden Anregungen gegeben, wie zusammen mit der Geschäftsführung die Grundlagen für ein Security-Management gelegt werden können.

> *„Ich glaube, es ist verlockend, wenn das einzige Werkzeug, das man hat, ein Hammer ist, alles zu behandeln, als ob es ein Nagel wäre.“ - Abraham Maslow*

Ziele, Strategien und die Organisation des Unternehmens bilden die Grundlage, auf die sich ein Security-Managementsystem aufbaut. Identifizieren Sie den Personenkreis, der an der Umsetzung eines Security-Managements in Ihrem Unternehmen im Wesentlichen beteiligt ist. Wer gestaltet inhaltlich Ziele und die

Unternehmensstrategie? Wer im Unternehmen ist in Bezug auf das Thema außerdem betroffen? Je besser Sie die Aufgaben, Motivationen und Denkmuster der Mitwirkenden kennen, desto besser wird die Zusammenarbeit funktionieren. Dann finden Sie – anders als im Zitat von Maslow – zusammen Lösungen zur Verbesserung der Security, auf die Sie alleine möglicherweise nicht gekommen wären. Das Zitat von Maslow soll Sie daran erinnern, dass Security ein Teamsport ist. Die Berücksichtigung der unterschiedlichen Blickrichtungen und Lösungsansätze helfen dabei, im Unternehmen akzeptierte, robuste und effiziente Security-Maßnahmen umzusetzen. Im Allgemeinen sind im OT-Security-Management beteiligt:

- Unternehmensführung und -strategie
- IT-Verantwortliche und Fachkräfte
- Mitwirkende der Anlagensicherheit und
- OT-Security-Verantwortliche

In den folgenden Kapiteln werden die Personengruppen und verbreiteten Aufgaben und Denkweisen vorgestellt.

2.2.1 Unternehmensführung und -strategie

> *... operative Exzellenz, das heißt bessere Verfügbarkeiten von Anlagen, die Reduktion von Energiekosten und anderen variablen Kosten, Maßnahmen zur Digitalisierung und Automatisierung sowie Effizienzsteigerungen in den operativen Unternehmensbereichen. - Martin Brudermüller / BASF / 18. August 2019 / Handelsblatt*

Die Unternehmensführung denkt bei Automatisierung meist an Kostenreduktion und Effizienzsteigerung in der Produktion. Die chemische Industrie investiert laut VCI (6) ca. 16% des Umsatzes in Forschung und Entwicklung sowie laut Statista (7) zwischen 1,6 % bis 2,9% in Informationstechnik. Aufwendungen für Informationstechnik sind jedoch nicht zwangsläufig Aufwendungen für IT- und OT-Security. Bei dem Thema IT-Security wird vom Management gerne hinterfragt, inwieweit der finanzielle Aufwand für die Abwehr einer Bedrohung gerechtfertigt ist. Eine Antwort ist nur schwer möglich, da der Wert für Menschenleben, Zeit, Image, Zufriedenheit der Kundschaft sowie Qualität kaum quantitativ bestimmt werden kann. Nichtsdestotrotz sind Maßnahmen zur OT-Security erforderlich, um

- die Betriebsgenehmigung durch Einhaltung der rechtlichen Rahmenbedingungen (vgl. Abbildung 3, äußerer Rahmen) und
- die wirtschaftliche Produktivität (vgl. Abbildung 3, innerer Kreislauf) des Unternehmens vor den technologischen Risiken (Schadsoftware, Fehlbedienung und Angriffe durch Cyber-Kriminelle)

zu schützen.

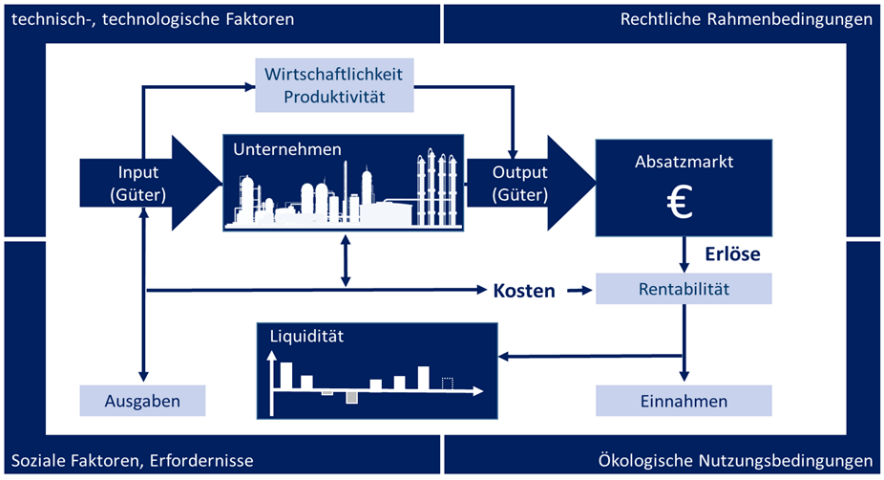

Abbildung 3 Betriebswirtschaftliche Aktivitäten

Für diese Maßnahmen sind laufend Personal- und Sachkosten aufzuwenden. Wenn sich der Nutzen von Maßnahmen der OT-Security auch nicht absolut quantifizieren lässt, so lässt dieser sich jedoch in Bezug zum Eintrittsrisiko und den möglichen Folgen beschreiben. Laut „Allianz Risk Barometer 2020“ (8) bewerten 39 % der Unternehmen Cyber-Vorfälle als das höchste Betriebsrisiko für Unternehmen. Damit steigen im Allianz Risk Barometer 2020 Cyber-Risiken weltweit zum Top-Risiko für Unternehmen auf. Aber wie wahrscheinlich ist ein derartiges Szenario für Betreiber der Prozessindustrie wirklich?

> *„Mehr als zwei Drittel der Chemie- und Pharmaunternehmen in Deutschland hatten in den letzten zwei Jahren ein Cyber-Security Problem. Besonders betroffen waren dabei die Bereiche Produktion sowie Forschung und Entwicklung.“ - CT-Report: Cyber-Security in der Chemieindustrie | 9. März 2017 | ChemieTechnik*

Die Eintrittswahrscheinlichkeit für Cyber-Vorfälle ist demnach recht hoch, aber mit welchem Schaden müssen Unternehmen rechnen? Laut einer Veröffentlichung von it-daily.net (9), benötigen Unternehmen durchschnittlich 16 Tage um z.B. nach einem Ransomware-Angriff (erpresserische Datenverschlüsselung) die infizierten Rechnersysteme zu identifizieren und mit hoffentlich nicht infizierten Backups neu aufzusetzen. Bei einer großen Raffinerie entstehen nur durch die Produktionsunterbrechung Kosten in zweistelliger Millionenhöhe. Zusätzlich entstehen ggf. auch Kosten durch Recovery-Maßnahmen, Imageschäden, Patentrechtsverletzungen, Umsatzeinbußen und anlagentechnische Instandsetzungen. In der Studie „Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie“, bezifferte Bitkom den Schaden durch Cyber-Angriffe für die deutsche Wirtschaft in den Jahren 2017/2018 auf 43,4 Milliarden EUR (4). Dies macht deutlich, wie groß die betriebswirtschaftlichen Schäden bereits sind.

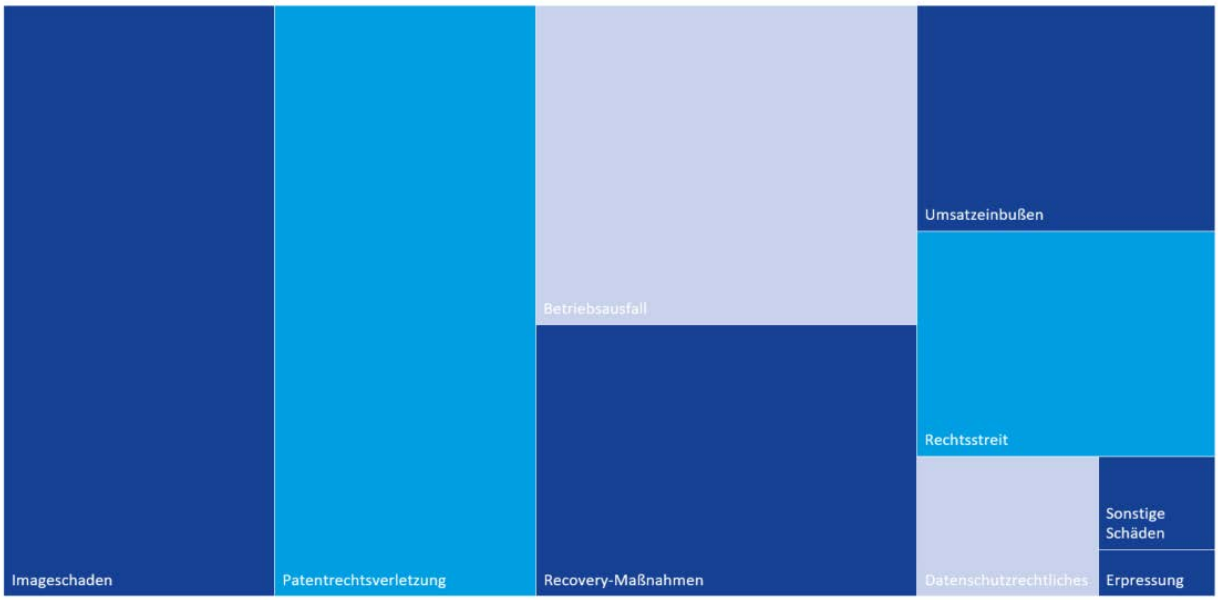

Abbildung 4 43,4 Milliarden Euro Schaden in 2017/2018 in Anlehnung an (10)

Schäden wie die Zerstörung von Anlagen, Tote und Verletzte sind zum Glück noch nicht Bestandteil der Statistik. Dies dürfte u.a. daran liegen, dass verheerende Cyber-Angriffe 2014 als ein „bewaffneter Angriff“ im Sinne von Artikel 5 des NATO Vertrags eingestuft wurde. Dass die Zerstörung von Anlagen und damit einhergehende Gefährdung für Menschen durch Cyber-Angriffe jedoch möglich sind, hat der im Jahr 2010 ausgeführte Angriff auf die Steuerungssysteme einer iranischen Urananreicherungsanlage mit dem Computerwurm Stuxnet gezeigt. Ende 2017 attackierten Hacker eine Anlage in Saudi-Arabien. Ziel der Cyber-Attacke war es vermutlich, die Anlage zu zerstören. Die Angreifer nahmen dabei Tote und Verletzte in Kauf. Der außergewöhnlich anspruchsvolle Angriff fiel nur auf, weil die Malware versehentlich eine Sicherheitsabschaltung der Anlage auslöste (11). Das Sicherheitssystem, über das der Angriff geführt wurde, ist auch in Hunderten deutschen Industrieanlagen im Einsatz. Auf Sicherheitssysteme ausgeführte Angriffe können besonders kritische Folgen haben.

Es dürfte deutlich geworden sein, dass ein Cyber-Angriff für Unternehmen tatsächlich zu einem Risiko werden kann. Das Thema OT-Security sollte daher aufgrund der möglichen katastrophalen Folgen für das Unternehmen nicht reaktiv, sondern proaktiv von der Geschäftsführung gesteuert werden. Nur auf diese Weise wird sichergestellt, dass Prozesse aufgebaut werden, die das Unternehmen widerstandsfähig gegen Cyber-Angriffe und somit zu einer resilienten Organisation machen. Die aktive Mitarbeit hilft im Schadensfall der Geschäftsführung auch, sich glaubhaft gegenüber Stakeholdern zu entlasten.

2.2.1.1 IT-Verantwortliche und -Fachkräfte

> *„Es ist die Hardware, die einen Computer schnell macht; und die Software, die ihn wieder verlangsamt." - Craig Bruce | Softwareentwickler*

Das Zitat von Craig Bruce beschreibt den Arbeitsbereich von IT-Verantwortlichen, den verfügbaren Speicherplatz, die hohe Rechnerleistung und flexible Softwareanwendungen. Hardware wie Telefonanlagen, Server, Drucker, Personal Computer und mobile Endgeräte zu administrieren und diverse Softwareanwendungen zur störungsfreien und sicheren Nutzung von Office-Anwendungen sowie des Enterprise Resource Planning Systems für Anwendende nutzbar zu machen, beschreibt die Tätigkeiten einer klassischen IT-Abteilung. Unternehmen aller Größen und Branchen sind auf eine reibungslos funktionierende IT-Infrastruktur angewiesen. Bei der Planung, Umsetzung und bei Problemen oder Ausfällen sind Fachleute gefragt. Am meisten verbreitet sind Systemfachkräfte für CISCO, Microsoft, Linux und SAP. Der hohe Grad der Standardisierung dieser Herstellersysteme gestattet große Mengen an IT-Systemen und Nutzenden zentral zu verwalten, Softwareupdates zu verteilen, Neuinstallationen durchzuführen und auf Vorfälle zu reagieren.

Industriesteuerungen, Feldgeräte, Bussysteme der Prozessautomation und Engineering Tools werden in der Regel dezentral von betriebsinternen EMSR-Ingenieurfachkräften (Elektrisches Messen, Steuern und Regeln) sowie externen Integratoren betreut. Da die Standardisierung der operativen Technik noch in den Anfängen steckt, ist eine zentralisierte Betreuung derzeit für die in der Regel über Jahrzehnte gewachsene OT-Netzwerkstruktur noch nicht sehr verbreitet.

Doch mit dem Aufkommen des industriellen Internets und der Integration von komplexen physikalischen Maschinen mit vernetzten Sensoren und Software, verwischen die Grenzen zwischen den beiden Teams IT und OT. Obwohl beide Teams vergleichbare Technik betreuen, haben sich hier unterschiedliche Herangehensweisen entwickelt. Die IT hat das Wissen, um zentral viele Nutzende und Geräte zu verwalten. Die OT-Ingenieursfachkräfte kennen die aus dem Produktionsprozess und den aus den Risikoanalysen stammenden Spezifikationsanforderungen und den Aufbau und die Funktionsweise industrieller Steuerungen. Für den Erfolg des OT-Security-Managements ist daher die erfolgreiche Zusammenarbeit der IT mit den EMSR-Ingenieursfachkräften (OT) von hoher Bedeutung.

2.2.1.2 Mitwirkende der Anlagensicherheit

> *„Das Restrisiko ist das Risiko, das einem den Rest gibt." - Pierre Chevalier | Höhlenforscher*

Das Zitat von Pierre Chevalier beschreibt recht treffend die Aufgabe der Anlagensicherheit. Aufgrund der immer wieder auftretenden Zwischenfälle und Unfälle (z.B. 1968 Chemieunfall in Bitterfeld, 1976 Sevesounglück, 1984 Katastrophe von Bhopal, 1986 Sandoz-Katastrophe, 2001 Explosion in Toulouse, 2003 Gasexplosion von Chuandongbei und 2015 Explosionskatastrophe von Tianjin) sowie der intensiven Industrialisierung in Ballungsräumen, hat die Anlagensicherheit in Deutschland einen hohen Stellenwert. Im Sicherheitsmanagementsystem sind die für den dauerhaft zuverlässigen Betrieb wesentlichen Organisationsstrukturen, Verantwortungsbereiche, Handlungsweisen, Verfahren, Prozesse und Mittel definiert.

Zentrales Instrument ist hierbei die in der 12. BImschV verankerte Gefahrenanalyse, mit der zu den anlagentechnischen und stofflichen Gefährdungen Schutz- und Sicherheitsmaßnahmen zur Verhinderung von

Störfällen abgeleitet werden. Auf diese Weise werden Risiken für Menschen und für die Umwelt auf ein vertretbares Restrisiko minimiert, welches aber aktuell in der deutschen Gesetzgebung nicht mit Zahlen hinterlegt ist. In der Gefahrenanalyse erfolgt eine Auseinandersetzung mit den größten anzunehmenden Schäden, deren Eintrittswahrscheinlichkeiten sowie der Wirksamkeit der Sicherheitsmaßnahmen. Zu den Sicherheitsmaßnahmen gehören eine inhärent sichere Auslegung der Behälter und Rohrleitungen, PLT-Sicherheitseinrichtungen und mitigierende Notfallschutzmaßnahmen.

Bei rechnerbasierten Systemen wird aus der Vergangenheit und den bisherigen Erfahrungen von einer hohen Zuverlässigkeit ausgegangen. Integrierte Fehlerdiagnosen und Fehlermeldungen sowie modulare redundante Auslegungen, gestatten eine ereignisorientierte Instandsetzung ohne Betriebsunterbrechung. Mitunter haben wirtschaftliche Erwägungen dazu geführt, dass Einrichtungen des Prozessleitsystems und der PLT-Sicherheitseinrichtungen gemeinsame Komponenten (wie Sensoren, Armaturen, Engineering-Stationen oder sogar die Controller der Steuerung) nutzen.

Dabei wurden (und mussten) Cyber-Angriffe aufgrund der abgeschotteten Betriebsweise bisher nicht berücksichtigt (werden). Durch das Vernetzen der Anlagen hat sich die Situation jedoch verändert. Bei Ausnutzung einer Schwachstelle in der gemeinsam genutzten Komponente ist es Cyber-Kriminellen möglich, die PLT-Sicherheitseinrichtung zu deaktivieren und dadurch eine kritische Situation oder gar einen Störfall auszulösen.

Aus der Perspektive der Anlagensicherheit und nach der Norm DIN EN 61511, sind PLT-Sicherheitseinrichtungen grundsätzlich unabhängig zu anderen Anlagenteilen zu bauen. Die beste Lösung dafür wäre eine komplette Trennung ohne eine Verbindung. Dies ist jedoch eher selten geworden. Oftmals wird nur noch davon ausgegangen, dass keine Verbindung besteht. Durch Änderungen an der Technik und die damit verbundene Vernetzung ist dies in der Realität teilweise nicht mehr der Fall.

Die Mitwirkenden der Anlagensicherheit besitzen das notwendige Wissen über die Produktionsprozesse, anlagentechnische Gefährdungen und deren Absicherung mittels rechnerbasierter Systeme. Cyber-Risiken stellen eine neue natürliche Erweiterung zu den etablierten Betrachtungen der Gefahrenanalyse im Sinne der 12. BImschV dar.

2.2.1.3 OT-Security Verantwortliche

Unter OT sind Hardware und Software zu verstehen, die Anlagenprozesse überwachen und steuern. In den meisten Betrieben unterstehen die OT-Systeme dem COO (Chief Operating Officer). Betriebsinterne EMSR-Ingenieurfachkräfte (Elektrisches Messen, Steuern und Regeln) pflegen die OT, die in der Regel von externen Integratoren geplant und errichtet wird. Bei getrennt arbeitenden IT- und OT-Teams kann es aufgrund von mangelnder Abstimmung in den Grenzbereichen zu Sicherheitslücken kommen. Daher ist eine Zusammenarbeit von OT-verantwortlichen EMSR-Ingenieure und IT-Fachkräften für ein Gelingen eine Grundvoraussetzung.

Eine Umfrage von ForeScout (12) ergab, dass 44% der befragten IT-Fachleute die Hauptverantwortung für die Absicherung und Überwachung der betriebenen OT-Systeme in einem Unternehmensnetz im Security Operations Center (SOC) sehen. Bei Befragten der Geschäftsbereichsleitung taten dies nur 36%. Dieses Spannungsfeld beschreibt recht treffend eine verbreitete Problematik im Bereich Mensch-Organisation für OT-Security. Die Übertragung von Verantwortlichkeiten sollte aufgrund der breiten Palette von Sicherheitstechnologien – von Next-Generation Firewalls über Cyber-Sicherheitsinformations- und Event-Managementsysteme, bis hin zum Identitäts- und Zugangsmanagement – fachlich und adminstrativ, je nach Kompetenz der betreffenden Ressourcen, auf IT und OT verteilt werden. Dabei sollten die Schnittstellen und Prozesse so gestaltet werden, dass eine optimale Zusammenarbeit gewährleistet wird.

Es gilt die entsprechenden Schnittstellen und Verantwortlichkeiten zwischen Planung und Betrieb zu schaffen.

Wer auch immer verantwortlich ist, wird mit den anderen Bereichen des Unternehmens zusammenarbeiten müssen, um das seinen Verantwortungsbereich und die Schnittstellen zu anderen vollständig zu erfassen, zu schützen und instand zu halten.

In der Regel ist der OT-Security Verantwortliche einer von vielen Verantwortlichen im Unternehmen. Die Geschäftsleitung bindet diese je nach Zuständigkeit zu tagesaktuellen Themen (z.B. behördliche Auflagen zum Nachweis der OT-Security) ein. Die Ernennung eines Verantwortlichen alleine entbindet die Geschäftsführung jedoch nicht von ihrer Verantwortung. Der allgemeine Strategieprozess ist ein geeignetes Steuerungsinstrument der Geschäftsführung, um die schrittweise Einführung von OT-Security anzugehen und aktiv mitzugestalten. Hierbei könnte die Geschäftsführung, oder von ihr benannte Verantwortliche, Meilensteine zur Durchführung der Bestandaufnahme, Gap-Analyse und zur Erstellung bzw. Verabschiedung einer Security Strategie mit dem OT-Verantwortlichen abstimmen sowie in dem geregelten Unternehmensprozess die notwendigen Ressourcen planen.

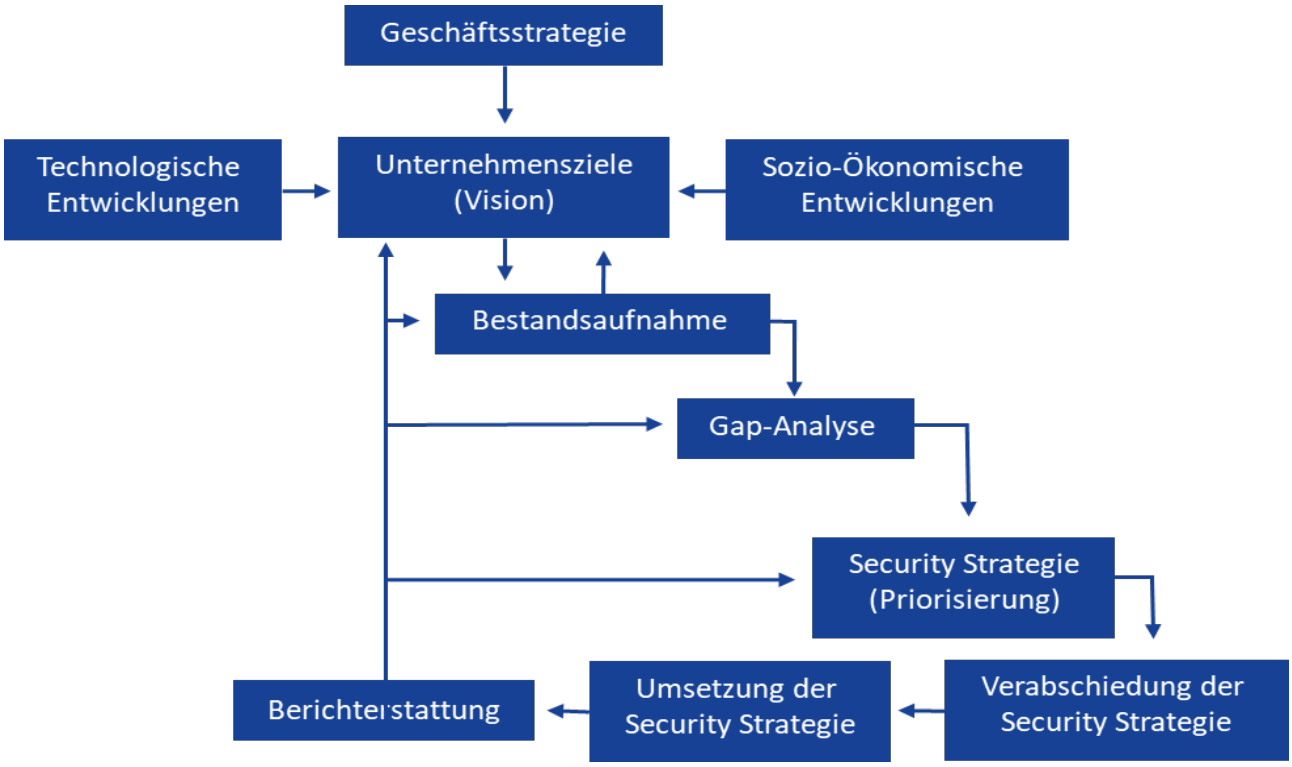

Abbildung 5 Steuerung der OT-Security durch die Geschäftsführung

Der an der Umsetzung eines OT-Security-Managements im Wesentlichen beteiligte Personenkreis setzt sich in der Regel (wie bereits am Anfang von Kapitel 2.2 beschrieben) zusammen aus

- der Unternehmensführung und -strategie
- den IT-Verantwortlichen und -Fachkräften
- den Mitwirkenden der Anlagensicherheit und
- dem OT-Security-Verantwortlichen.

> *"Es hört doch jeder nur, was er versteht!" - Johan Wolfgang von Goethe*

Aufgrund der unterschiedlichen inhaltlichen Aufgaben und Perspektiven der vorgenannten Personengruppen ist es wichtig, dass Entscheidungen in Fragen der OT-Security für alle Beteiligte verständlich aufbereitet werden. Auf diese Weise werden alle Beteiligten - wie im Zitat von Goethe beschrieben - inhaltlich abgeholt und es kann Missverständnissen vorgebeugt werden.

2.2.1.4 Verständliche Aufbereitung der OT-Security Themen ist der Schlüssel

Die unterschiedlichen Blickwinkel und fachlichen Qualifikationen der am OT-Security-Management beteiligten Personen sind Fluch und Segen zugleich.

Die fachliche Diversität erschwert die Kommunikation zwischen den Beteiligten, da für diese mitunter Begriffe und Abkürzungen unbekannt sind oder aufgrund von mehrfachen Bedeutungen Sachverhalte fehlinterpretiert werden.

Ein Beispiel dafür ist der Begriff „Schutzziele“. Im Umfeld der Anlagensicherheit wird darunter die Integrität der Anlage, der Arbeitsschutz, der Drittschutz und der Umweltschutz verstanden. In der Informationstechnik wird unter Schutzzielen Vertraulichkeit, Integrität und Verfügbarkeit verstanden. Weitere Beispiele, die zu Missverständnissen führen können finden Sie auch im Abschnitt 2.4 „Mensch und Technik“.

Unverständnisse und Missverständnisse können zu Demotivation und Ablehnung führen. Als Folge daraus wird die Verantwortung für das Thema gerne auf einzelne Personen projiziert. Ein Einzelner ist aber nicht imstande alleine ein OT-Security-Managementsystem aufzubauen und zu pflegen. Die im OT-Security-Managementsystem zu definierenden Prozesse müssen schließlich von den betreffenden Anwendern verstanden und richtig angewendet werden.

Ist der Anwender an der Entwicklung der Prozesse beteiligt, so kann dies zu einem tieferen Verständnis für die Notwendigkeit und Akzeptanz bei der Anwendung des Prozesses führen. Ist der Anwender der Prozesseigner und implementiert mit Unterstützung von Fachleuten OT-Security Anforderungen in seine Arbeitsprozesse, dann könnte so eine hohe Akzeptanz für mitunter unpopuläre OT-Security Maßnahmen erreicht werden.

Wie können Fachleute aus diversen Unternehmensbereichen gemeinsam eine Lösung erarbeiten? Diese Fragestellung ist keine rein OT-Security-spezifische, daher wird eine mögliche Lösung im Folgenden und nicht im Kapitel 6 vorgestellt. Am Beispiel einer Moderation lässt sich skizzieren, wie eine produktive interdisziplinäre Zusammenarbeit aussehen kann. Voraussichtlich werden Sie, wenn Sie den Ansatz in Ihrem Unternehmen anwenden - wie im Beispiel 1 dargestellt - die Ausgangsfrage nicht gleich lösen können. Sie werden jedoch die Punkte identifizieren können, die zur Lösung der Aufgabe und zur verständlichen Aufbereitung von OT-Security Themen notwendig sind.

Thomas McCall von Gartner hat diesbezüglich einen pragmatischen Ansatz (13) vorgestellt, mit dem eine inhomogene Personengruppe mit unterschiedlichsten Kenntnisständen im Thema IT/OT-Security sich verhältnismäßig schnell ein Problem erschließen und relevante Entscheidungen treffen kann. Im Wesentlichen beschreibt der Ansatz die Auseinandersetzung mit den drei folgenden Leitfragen:

- Was ist wichtig?
- Was ist gefährlich?
- Was ist real?

Begonnen wird mit einem Brainstorming zu den drei Fragen. Die gesammelten Antworten werden anschließend durch eine Priorisierung von den Teilnehmenden nach ihrer Wichtigkeit geordnet. Auf diese Weise entsteht ein differenziertes „Bild“ des Problems und seiner inhaltlichen Ausprägungen. Dieses „Bild“ unterstützt die Teilnehmenden die Standpunkte anderer Teilnehmender im Gesamtkontext besser zu verstehen und anforderungsgerechte Handlungen abzuleiten. Die Handlungen werden in einem Aktionsplan zwischen den Beteiligten abgestimmt (Wer macht was und wie?).

Verfolgen Sie anhand eines Beispiels, wie die drei Leitfragen in der Praxis zur Anwendung kommen können:

Beispiel 1 Migration des Leitsystems

Das Leitsystem eines Betriebsbereichs ist veraltet und soll durch ein modernes Leitsystem ersetzt werden. Die Notwendigkeit sich mit OT-Security auseinandersetzen kommt aus den zurate gezogenen Regelwerken. Es ist zudem bekannt, dass seitens der Behörde ein unabhängiger Nachweis der Cyber-Sicherheit gefordert wird.

Ausgangssituation

Noch ist unklar, wie der Nachweis geführt werden soll. Die Betriebsleitung berät daher in einem Meeting, wie mit dieser Nebenbestimmung umgegangen werden soll. In dem Unternehmen gibt es bislang noch keine Verantwortlichen oder Prozesse, die sich im OT-Umfeld mit Cyber-Sicherheitsanforderungen befassen.

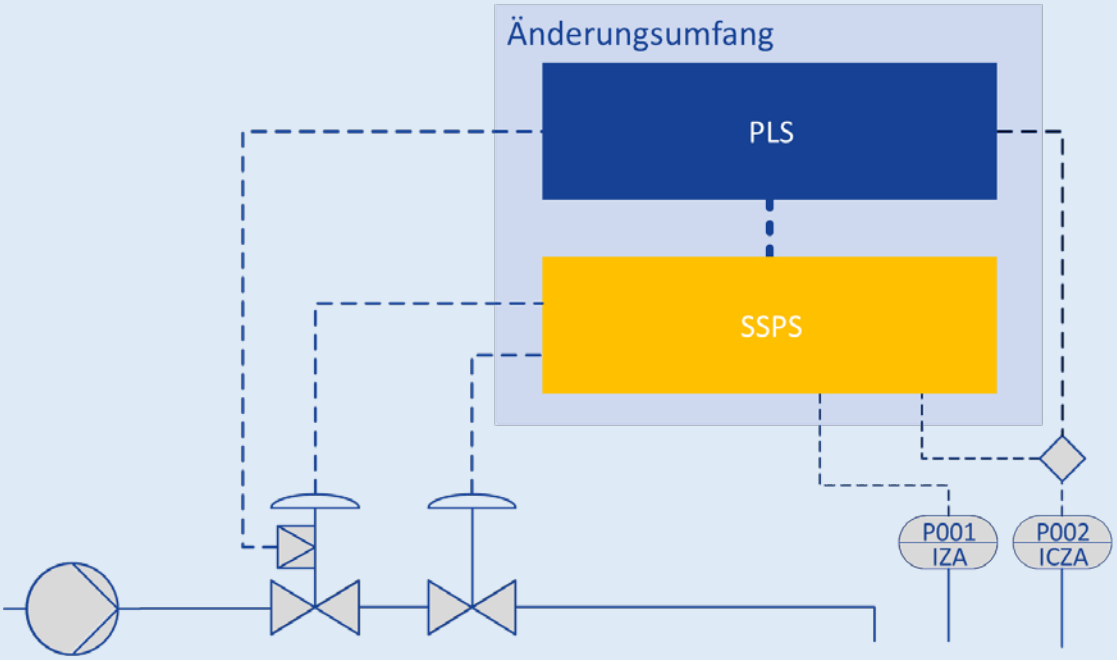

Abbildung 6 Migration des Leitsystems

Das Treffen wird von der Anlagensicherheit geleitet und die Beteiligten sollen zunächst zu drei Leitfragen ihre Gedanken auf Moderationskarten schreiben. Die Beteiligten stellen ihre Antworten vor und übereinstimmende Antworten werden zu einem Aspekt zusammengefasst. Daran anschließend gibt jeder Beteiligte ein Votum ab, welche Aspekte aus seiner Sicht eine hohe Priorität haben. Dies kann mit Klebepunkten durchgeführt werden. Jeder erhält halb so viele Punkte, wie es Aspekte gibt. Anschließend können die Aspekte nach ihrer Priorität sortiert werden. Nachfolgend finden Sie zur Veranschaulichung wie das Ergebnis aussehen könnte. Die Priorisierungen (niedrig: 1; hoch: 4) in diesem Beispiel sind fiktiv und dienen ausschließlich der Veranschaulichung der Methode.

Leitfragen und Antworten der Beteiligten:

- Was ist wichtig?
  - „Der Austausch des Leitsystems muss in 9 Monaten im Rahmen des zweiwöchigen Anlagenstillstands erfolgen.“, [4]
  - „Gesetzliche und behördliche Vorgaben sind einzuhalten.“ [4]
  - „Die Kosten müssen in Relation zum Nutzen stehen.“ [2]
  - „Die PLT-Sicherheitseinrichtungen (PLT-S) müssen vor Cyber-Angriffen geschützt sein.“ [2]
- Was ist gefährlich?
  - „Eine Manipulation der PLT-S kann zu einem Störfall führen.“ [4]

- „Wenn das Prozessleitsystem (PLS) und die SSPS gleichzeitig gehackt werden, kann ein Angreifer gezielt einen Störfall auslösen. Er könnte die Anlage gezielt in einen kritischen Bereich fahren.“ [4]
- „Wenn Wartungen komplexer IT-Systeme durch ungeschulte Arbeitskräfte erfolgen.“ [3]
- „Wenn gegen Gesetze und behördliche Auflagen verstoßen wird.“ [2]

– Was ist real?

- „Berücksichtigung von vorhandenen Regelwerken, aus denen sich bereits wichtige Punkte ergeben (z.B. VDI 2180 mit dem Nachweis der Rückwirkungsfreiheit von SSPS und PLS; IT Risikoanalyse für Z Komponenten)“ [4]
- „Im Anwendungsbereich der 12. BImschV gibt es bereits konkrete Anforderungen an die Cyber-Sicherheit von Störfallbetrieben (KAS-51).“ [4]
- „Wir zusätzliche Kosten für die Cyber-Sicherheit abschätzen und von der Geschäftsleitung genehmigen lassen.“ [4]
- „Zu den ausgewählten Leitsystemkomponenten sind Cyber-Sicherheitsschwachstellen öffentlich bekannt.“ [3]
- „Wir haben derzeit nicht die Ressourcen, um auch noch die Cyber-Sicherheit von OT-Systemen zu übernehmen, außerdem kennen wir das KAS-Regelwerk nicht.“ [2]
- „In Deutschland wurde ein Stahlwerk gehackt und der Hochofen hat schweren Schaden genommen, so dass die Produktion nicht wiederaufgenommen werden konnte.“ [1]

Ergebnis

– Priorisierung der Statements
Die Diskussion und anschließende Priorisierung der vorgenannten Standpunkte in Bezug auf die Ausgangsfrage hat ergeben, dass eine schnelle Lösung auf die Frage „Wie soll der Nachweis der Cyber-Sicherheit erbracht werden?“ nicht möglich ist. Die Antworten verdeutlichen, dass hierzu den Teilnehmenden die Anforderungen an die Cyber-Sicherheit von Leitsystemen zum jetzigen Zeitpunkt im Detail noch nicht bekannt sind. Gleichwohl helfen die Leitfragen den Beteiligten, die wesentlichen Herausforderungen zu identifizieren und geeignete Handlungen abzuleiten. Auf diese Weise wird das Thema verständlich aufbereitet.

– Aktionsplan
Unter Berücksichtigung der Statements mit der höchsten Priorität entwickeln die Teilnehmenden dann einen Aktionsplan für die nächsten Schritte. Hier könnte der Aktionsplan wie folgt formuliert sein:

- Der Nachweis soll durch Umsetzung der Anforderungen aus KAS-51 geführt werden und deutlich vor dem Stillstand (in 7 Monaten) der Behörde vorgelegt werden.
- Im Nachweis gem. KAS-51 sind Maßnahmen zum Schutz der Prozesssteuerung/Sicherheitssteuerung vor Cyber-Risiken aufzuzeigen.
- Für die Planung, Organisation und Durchführung der Tätigkeiten wird von der Geschäftsleitung zunächst ein Personenjahr Personalkosten geplant. Zur Durchführung des Projektes soll eine hauptverantwortliche Person benannt und freigestellt werden.
- Zugehörige der IT-Abteilung, der Instandhaltung, der Anlagensicherheit und einer externen Beratung unterstützen die hauptverantwortliche Person. Diese wird in einem Monat ein Konzept erarbeiten und dieses dann mit der Anlagenleitung und der Behörde abstimmen.
- Nach der Konzeptfreigabe erfolgt die Umsetzung.
- Die Geschäftsführung ist monatlich über den Projektfortschritt zu unterrichten. Probleme bei der Umsetzung bzw. Investitionsbedarfe werden mit der Geschäftsführung beraten.

Der Einstieg in das Thema OT-Security kann, wie in diesem Beispiel, reaktiv (d.h. auf Anforderungen von Behörden) beginnen. Damit Unternehmen durch OT-Security geschützt sind, sollte das Thema jedoch proaktiv z.B. in einem OT-Security-Management gestaltet werden. Anknüpfungspunkte hierzu ergeben sich auch aus den in der KAS-51 genannten Basisanforderungen.

- Festlegung von Verantwortlichkeiten
- Regelungen für Fremdpersonal
- Sensibilisierung/Schulung von Mitarbeitenden

- Zugangs- und Zutrittsmanagement
- Zugriffsmanagement auf Prozesssteuerung
- Manipulationserkennung und -schutz
- Reaktion auf neue Schwachstellen und IT-Bedrohungen

2.2.2 OT-Security-Management

Zum Thema Mensch und Organisation gehören reproduzierbare Prozesse und Verfahren. Damit ein systematischer Aufbau einer Organisation mit den benötigten Mitteln entstehen kann, muss der Prozess von der Leitungsebene gesteuert werden. Eine abgestimmte Vorgehensweise erhöht die Erfolgschancen, ein effizient funktionierendes OT-Security-Management aufzubauen.

Für den Gestaltungsrahmen bedarf es neben dem OT-Verantwortlichen demnach noch unterstützende Personen und realistische Ziele. Um Cyber-Risiken Rechnung zu tragen und die OT-Security durch Einführung von Basismaßnahmen (z.B. der KAS-51) zu verbessern, könnte die Geschäftsführung z.B. folgende Ziele im Strategieprozess (vgl. Abbildung 5 auf Seite 15) definieren:

- Die Geschäftsleitung und Führungskräfte nehmen ihre Vorbildfunktion wahr und tragen gemeinsam die Verantwortung für die Umsetzung und Einhaltung der rechtlichen Rahmenbedingungen auf dem Gebiet der Anlagensicherheit und OT-Security.
- Bis zum 03. Januar 2022 sind Recovery-Maßnahmen definiert und ein regelmäßiger Überprüfungsprozess dieser initiiert, sodass ein Cyber-Angriff auf OT-Systeme zu einer kalkulierbaren betriebswirtschaftlichen Bedrohung wird (Resilienz gegen Cyber-Angriffe auf OT-Systeme).

Ziele unterstützen dabei, ein Thema fokussiert anzugehen. Insbesondere wenn die Ressourcen knapp sind, helfen Ziele dabei die Ressourcen effektiv einzusetzen. Die Einsicht, dass ein Cyber-Angriff nicht ausgeschlossen werden kann, macht es erforderlich, diese als Ursache für Störfälle zu minimieren oder Schäden durch Produktionsausfälle zu vermeiden und dadurch das Überleben der Organisation zu sichern. Im OT-Security-Management sind die Verantwortlichkeiten, Ziele, Prozesse und wesentliche Maßnahmen der OT-Security beschrieben. In Kapitel 6.2 sind die wesentlichen Arbeitsweisen des OT-Security-Managements beschrieben.

2.3 Technik und Organisation

Nachdem die Verantwortlichen und Unterstützenden für die Einführung und Umsetzung einer OT-Security Strategie identifiziert sind, wird in diesem Kapitel das Augenmerk auf Herausforderungen, die sich bei der Organisation von Prozessen auf technologischer Ebene ergeben können, gerichtet.

Viele Betreiber von Betriebsbereichen sind internationale Konzerne. Für die Verantwortlichen im Unternehmen haben standardisierte Prozesse eine hohe Bedeutung. Standardisierte Prozesse erlauben standortunabhängig Tätigkeiten effektiv und mit vergleichbarer Qualität zu organisieren, zu überwachen und zu optimieren. Zudem können Vorgehensweisen z.B. aus internationalen Normen durch die Aufnahme in einem Unternehmensprozess verbindlich zur Anwendung gebracht und durch unternehmenseigene Formulare anwendungsbezogen ausgestaltet werden.

Das Top-down Prinzip ist erfolgreich bei global tätigen Konzernen zur strategischen Einführung von OT-Security, der innerbetrieblichen Standardisierung, dem Leistungsvergleich und der Berichterstattung. Globale Zusammenhänge lassen sich auf diese Weise gut erkennen und organisieren. Denken Sie in diesem Zusammenhang z.B. an Sicherheitsupdates, die in regelmäßigen Abständen verteilt und auf die Systeme gespielt werden müssen.

Wichtige Impulse für Verbesserungen kommen in der Regel von der Basis (Bottom-up) oder von außen (Gesetzte, Regelwerke, Markentwicklungen, ...). Angenommen, Sie sind die ersten in Ihrem Unternehmen, die wie im Beispiel 1 mit der Migration des Leitsystems beginnen. Im Idealfall würden Sie das Projekt gemeinsam mit der Zentrale durchführen und Ansätze, die sich im Projekt bewährt haben, würden zu Unternehmensstandards weiterentwickelt.

> *„Globale Zusammenhänge zu erkennen, ist das eine, daraus zu lernen, spaltet die Interessen." - Raymond Walden*

In der Praxis hat aber die Zentrale nicht immer die Ressourcen, um im Projekt mitzuarbeiten. Oder aus Sorge, dass durch die Einbindung der Zentrale sich das Projekt in die Länge zieht und die Umsetzung im nächsten geplanten Anlagenstillstand gefährdet ist, wird diese erst gar nicht eingebunden. Im schlimmsten Fall weichen später die OT-Security Konzepte stark voneinander ab. Wie in dem Zitat von Raymond Walden benannt, spaltet die Annahme von Verbesserungsvorschlägen dann die Interessen. Aus Sorge vor zusätzlichen Aufwänden werden der Betrieb und die Zentrale vermutlich an ihren Lösungen festhalten wollen. Mindestens sollte bei derartigen Projekten die Cyber-Risikoanalyse, die OT-Security Spezifikation und die Entwurfsplanung mit der Zentrale abgestimmt werden.

Auch für kleinere und mittelständische Unternehmen hat der Rückgriff auf standardisierte Vorgehensweisen Vorteile. Das Unternehmen muss nicht von Grund auf neue Prozesse entwickeln, sondern kann auf den bereits beschriebenen aufbauen. So legt z.B. das u.a. von der Berufsgenossenschaft Rohstoffe und Chemische Industrie in (14) beschriebene Freigabescheinverfahren für alle Beteiligten zeitlich, räumlich und bezogen auf die Arbeiten verbindliche Regeln fest. Da das Freigabescheinverfahren bei vielen Betreibern und Dienstleistern bekannt und akzeptiert ist, ließen sich auch OT-Security relevante Tätigkeiten (z.B. Hardwareaustausch, Softwareänderungen, Datensicherung, Behandlung von Sicherheitsvorfällen) in einem Freigabescheinverfahren kleinerer und mittelständischer Unternehmen abbilden. Es könnte dabei Beteiligte bei der sicheren und anforderungsgerechten Durchführung von Arbeiten unterstützen. Problematisch ist bei der Übertragung der Standardprozesse z.B. der TRBS 1112 (15) häufig nur, dass diese für kleinere Unternehmen überdimensioniert sind. Hierbei ist jedoch meist eine Vereinfachung möglich. Es gibt zudem deutlich weniger Schnittstellen und die Aufwände für die Abstimmung zwischen unterschiedlichen verantwortlichen Abteilungen sind deutlich geringer. Dies begünstigt eine effiziente Umsetzung.

2.3.1 Dokumentation

Bevor Sie Cyber-Risiken analysieren und technische Maßnahmen der OT-Security definieren können, benötigen Sie eine Dokumentation.

Die Dokumentation sollte die errichtete Anlage korrekt und aktuell beschreiben. Bei der Durchsicht und Strukturierung der Anlagendokumentation werden Sie schnell weitere Herausforderungen zu meistern haben. Ihr Betriebsbereich ist in der Regel das Ergebnis von mehreren Bauphasen. Betrachten Sie exemplarisch den Lebenszyklus einer Anlage. Die Anlage wurde z.B. als Pilotanlage begonnen, in Teilerrichtungen um weitere Produktionsanlagen und die Notstromversorgung erweitert, Lagertanks und Leitungen wurden instandgesetzt und aktuell wird die Prozessleittechnik modernisiert. Im Ergebnis hat die Anlage eine gewachsene Dokumentation, die von dicken Ordnern mit großformatigen ausgedruckten R&I-Fließschemas, mehreren Gigabyte Datenspeichern mit Spezifikations-, Planungs-, Verifikations- und Validierungsdokumenten bis hin zu DVDs mit Softwarebackups reicht. Das Engineering, die Errichtung und die Inbetriebnahme der einzelnen Gewerke erfolgen durch unterschiedliche Firmen. Jede dieser Firmen hat ihre eigenen Prozesse und Security Konzepte.

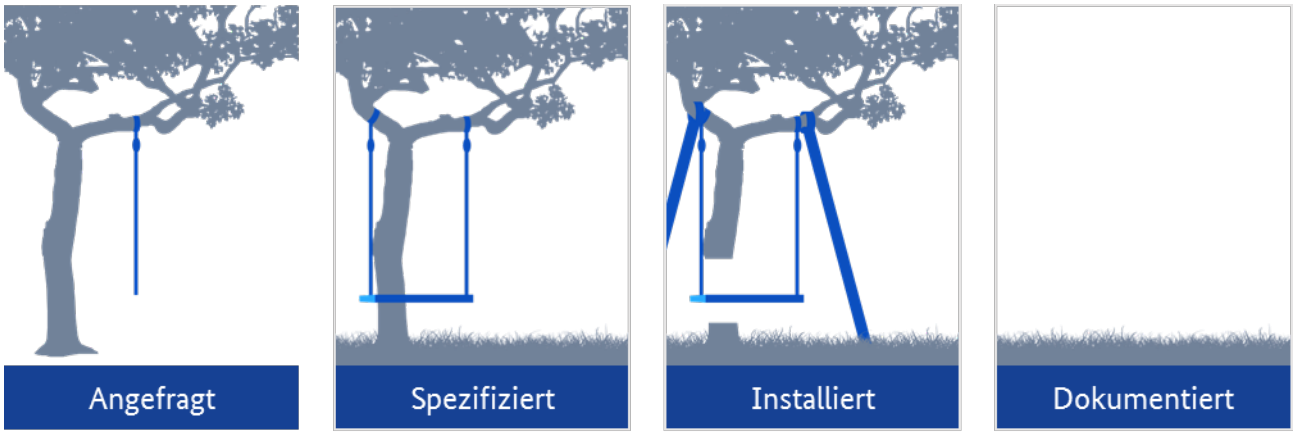

Abbildung 7 Probleme der Security in der Anlagenplanung

Abbildung 7 soll das Zusammenspiel in der Anlagenplanung verdeutlichen. Die Entwicklung von Security-Konzepten und -Lösungen wird bisher noch selten von Betreibern angefragt oder die Anfoderung sind wenig konkret. Viele Planenden und Integratoren sehen Security auch nicht als ihre Aufgabe an oder es werden Lösungen nach eigenen Vorstellungen umgesetzt (auch aufgrund fehlender Vorgaben). Dies kann dazu führen, dass bei Installation und Inbetriebnahme der Anlage weitere Anpassungen an den Security-Maßnahmen notwendig sin, um die vom Integrator spezifizierten Maßnahmen in die Infrastruktur des Betreibers zu integrieren. Am Ende steht das allgemein bekannte Problem, dass diese Änderungen, Anpassungen und Konzepte wenig dokumentiert werden.

Viele klein- und mittelständische Unternehmen haben noch kein Konfigurationsmanagement in ihrem Unternehmen eingeführt, sodass die Dokumentation der Anlage lückenhaft oder nicht aktuell ist. Dies erschwert wesentliche Aspekte der OT-Security, da zur Systemanalyse, zum Aufbau von Security Maßnahmen und zur Fehlersuche nur lückenhafte Informationen zur Verfügung stehen.

Eine weitere wesentliche Herausforderung der OT-Security ist die Organisation der technischen Fehlersuche und -behebung. Angenommen Sie stellen fest, dass eines der technischen OT-Systeme durch verdächtige Reaktionen auffällt. Wie würden Sie und ihre Organisation auf den Cyber-Sicherheitsvorfall dann reagieren? In der Regel gibt es zumindest einen IT-Verantwortlichen (z.B. den Chief Information Security Officer, CISO), der dergleichen Tätigkeiten organisiert. In dem folgenden hypothetischen Beispiel ist der Ablauf eines möglichen Falls durchgespielt.

Beispiel 2 - Anlassbezogene Reaktion auf einen Cyber-Sicherheitsvorfall

Beim Hochfahren der Engineering Workstation (Laptop, der zur Programmierung von PLT-Systemen genutzt wird) bemerkt ein MSR-Ingenieur Unregelmäßigkeiten und informiert die IT-Hotline (siehe Abbildung 8). Diese nimmt den Vorfall auf und stuft den Fehler zunächst als Softwareproblem ein. Der MSR-Ingenieur wird an das Team „Applikationssicherheit“ der IT-Abteilung weitergeleitet. Bei der genaueren Untersuchung der Engineering-Workstation wird eine gefährliche Schadsoftware gefunden. Die IT-Abteilung möchte nun von dem MSR-Ingenieur (vgl. in Abbildung 8, die Entwicklungsabteilung) wissen, auf welche anderen Systeme sich die Schadsoftware ausgebreitet haben kann. Ziel ist es die möglicherweise betroffenen Systeme zu isolieren, auf die Schadsoftware zu scannen und diese bei Bedarf zu entfernen.

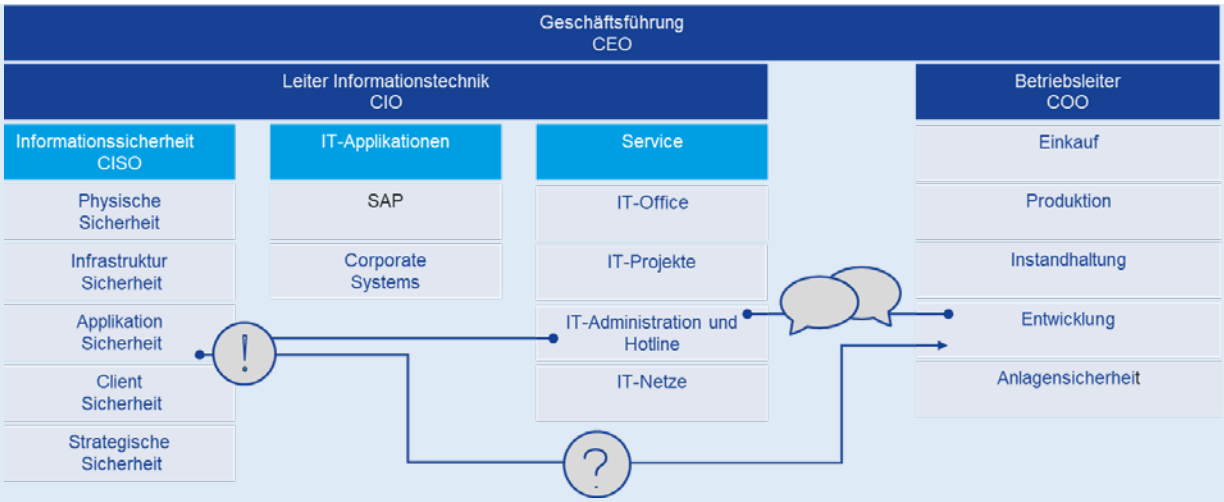

Abbildung 8 Reaktion auf einen Cyber-Sicherheitsvorfall

Ausgangssituation

Es existiert noch keine zentrale Archivierung und Pflege der Anlagendokumentation, aus denen die erfolgten Verbindungen recherchiert werden könnten. Der CISO lädt daher die Betriebsleitung und die Anlagensicherheit zu einem Ad-hoc-Treffen ein, um die Bedeutung des Vorfalls und das weitere Vorgehen abzustimmen. Es gilt die Frage zu klären, ob sich die Schadsoftware in der Anlage ausgebreitet hat und ob eine Gefährdung der Anlagensicherheit besteht und Maßnahmen erforderlich sind.

Die Diskussion und anschließende beispielhafte Priorisierung (Priorität niedrig: 1; hoch: 4; berücksichtigt das Erfordernis und ggf. auch die Reihenfolge bestimmter Handlungen) der vorgenannten Standpunkte in Bezug auf den Cyber-Vorfall hat ergeben, dass mehrere Maßnahmen zur Feststellung der möglichen Ausbreitung der Schadsoftware im Netzwerk notwendig sind.

Leitfragen und Antworten der Beteiligten

- Was ist wichtig?
  - „Zum Einspielen müssen nicht kompromittierte Backups der Anwendungssoftware verfügbar sein.“ [4]
  - „Zum Wiederherstellen eines nicht kompromittierten Zustands ist es wichtig, den Zeitpunkt der Systeminfektion zu bestimmen.“ [4]
  - „Zur Erfassung des Umfangs der kompromittierten Systeme ist es wichtig, Datenträger und Datenverbindungen, die im Austausch mit der Workstation stehen, zu identifizieren und ggf. deren Schadsoftwarestände zu bereinigen.“ [4]
  - „Es ist wichtig festzustellen, welche Änderungen nach der Infektion durch reguläre Nutzende vorgenommen worden sind.“ [3]
  - „Lagerbestände gefährlicher Stoffe, die aktuell nicht im Prozess genutzt werden, können vorsorglich zu den Verriegelungen der Prozessleittechnik durch Handarmaturen gesichert werden.“ [2]
- Was ist gefährlich?
  - „Wenn die Schadsoftware nicht entfernt wird, könnte diese die Parameter oder Funktionen in den Anlagensteuerungen boshaft verändern.“ [3]
  - „Wenn Angreifende durch Veränderungen im PLS die Prozessführung gefährlich ändern und gleichzeitig das PLT-Sicherheitssystem unwirksam gemacht wird.“ [4]
  - „Wenn die Backups der Anwendungssoftware (z.B. des PLS oder SIS) ebenfalls infiziert worden sind.“ [2]
- Was ist real?
  - „Für Betriebsbereiche, von denen eine besondere Gefährdung bei Eingriffen Unbefugter ausgeht, müssen Sicherungsanalysen durchgeführt werden. In einer IT-Risikobeurteilung sind Schwachstellen, IT-Bedrohungen und Gefährdungen zu identifizieren und die Effektivität der Schutzmaßnahmen zu bewerten. Ohne genaue Kenntnis, ob das PLS und/oder die SIS betroffen sind, ist der Zustand der Anlagensicherheit unklar.“ [4]

- „Eine vorsorgliche Trennung des OT-Netzwerkes von den anderen Bereichen des Unternehmens in einen Inselbetrieb ist technisch möglich.“ [4]
- „Änderungsstände an der Anwendungssoftware auf dem PLS oder SIS lassen sich unter Umständen durch Überprüfung der dokumentierten Checksummen feststellen.“ [4]
- „Die Engineering-Workstation nutzen gleichermaßen Arbeitskräfte der Entwicklungsabteilung, der Instandhaltung und externe Servicearbeitskräfte des Herstellers. Die zurückliegenden Änderungen an den Anwendungssoftwareständen sind im Detail nicht dokumentiert und müssen bei den Nutzenden erfragt werden.“ [3]
- „Sollten zur Durchführung von Untersuchungen und Systeminstandsetzungen Anlagenteile abgeschaltet werden müssen, dann sind unter Berücksichtigung aktueller Produktvorräte und der Auftragslage ungeplante Stillstände von maximal einer Woche realisierbar.“ [2]

Ergebnis

– Aktionsplan
  Unter Berücksichtigung der Statements mit der höchsten Priorität, entwickeln die Teilnehmenden einen Aktionsplan für die nächsten Schritte. Hier könnte der Aktionsplan wie folgt formuliert sein: Der voraussichtliche Zeitpunkt der Infektion sowie die registrierten Zugriffe durch Anwendende sind umgehend durch die OT- und IT-Abteilung zu ermitteln.

- Die aktuellen Anwendungssoftwarestände sind bis Ende der Woche auf Infektionen bzw. Manipulationen zu überprüfen und zu sichern. Während dieser Untersuchung ist das OT-Netzwerk in einen Inselbetrieb zu nehmen und derzeit ungenutzte Gefahrstofftanks durch Handarmaturen zu sichern.
- Aktuelle notwendige Arbeiten an der Anwendungssoftware sind mit einer nicht infizierten Workstation auszuführen.
- Die Programmierteams sollen befragt werden, welche der an der Workstation vorhandenen Schnittstellen für welche Tätigkeiten genutzt werden. Die hierbei verwendeten Datenträger und Geräte sind bis Ende nächster Woche auf Infektionen zu überprüfen.
- Ein Mitglied der Entwicklungsabteilung wird als verantwortlich für OT-Security benannt und analysiert bis Ende nächster Woche den Vorfall.

In Bezug auf das Thema Technik und Organisation fällt auf, dass in dem konstruierten Beispiel 2 wesentliche Informationen wie Systemzugriffe, legitimierte Schnittstellen und autorisierte Softwareänderungen fehlen und somit die Schadensermittlung sowie Systembereinigung verzögert werden. Ein Unternehmen mit Konfigurationsmanagement hätte in diesem Fall wesentliche Informationen, die für die Analyse des Schadensausmaßes benötigt werden, auswertbar vorliegen. Der Fokus läge dann auf der Analyse und Feststellung ggf. erforderlicher Schutzmaßnahmen. Folglich können temporäre Maßnahmen wie der oben dargestellte Inselbetrieb (d.h. netzwerkseitige Trennung des SIS von anderen Systemen des Unternehmensnetzwerkes), Handabsperrungen (d.h. manuell betätigte Absperrarmaturen in Rohrleitungen) von Lagertanks und vorsorgliche Stillstände deutlich kürzer ausfallen oder gar vermieden werden. Warum hat jedoch noch nicht jedes Unternehmen ein Konfigurationsmanagement?

Das Konfigurationsmanagement muss zunächst vom Betreiber aufgesetzt werden, aus verschiedenen Datenquellen mit Stammdaten gefüttert werden und durch geeignete Prozesse, die auch externe Dienstleistungsunternehmen (z.B. Integratoren) einschließen, auf dem aktuellen Stand gehalten werden. Wenn ein Konfigurationsmanagement eingeführt wird, ist eine Schnittstelle auf die Systeme zur Anlagenverwaltung (Asset Management) sinnvoll. Im Asset Management sollten zu allen digitalen OT-Anlagenteilen (Server, Hardware mit eigener IP-Adresse, Software, Datensätze etc.), wesentliche Informationen (Softwareversion, Standort, Inbetriebsetzung, IP-Adresse, Ansprechpartner, Bedeutung für den Betrieb, Patch-Stand, ...) erfasst sein. Im Konfigurationsmanagement werden dann die Konfigurationen und Beziehungen zwischen den verschiedenen Komponenten verwaltet und administriert.

Der Aufwand zum Aufbau eines Asset- und Konfigurationsmanagements ist im Hinblick auf OT-Security nicht unerheblich, aber notwendig. Maßnahmen, wie die OT-Security-Risikoanalyse, Konfiguration der Firewall Regeln und das Notfallmanagement, erfordern

korrekte und aktuelle Informationen, die durch ein Asset- und Konfigurationsmanagement bereitgestellt werden. Neben der OT-Security werden aber auch vorbeugende Instandhaltungen, optimierte Planung von Arbeiten und das Lagermanagement durch ein Plant Asset Management (PAM) deutlich erleichtert. Allgemeine Anforderungen an Asset Managements beschreibt die VDI 2651 Blatt 1. In Kapitel 6.3 wird ein Praxisbeispiel für ein PAM vorgestellt.

Viele Betreiber haben Anlagenplanungen und -änderungen fremdvergeben. Die Änderungen sind dann projektbezogen - mehr oder weniger - detailliert in der Dokumentation der Anlagenplanung und der Integratoren beschrieben. Für die Produktion der Anlage ergibt sich nicht notwendigerweise das Erfordernis, diese Daten in einem System zu pflegen. Zudem sind vielfach die diesbezüglich notwendigen Ressourcen häufig zu gering. Dabei lassen sich durch den Aufbau und die Pflege eines Konfigurationsmanagementsystems, Eintrittshäufigkeiten systematischer Fehler (wie z.B. Bedienfehler) und aufwändige as-built-Analysen reduzieren. In Bezug auf OT-Systeme sind Anforderungen an ein Konfigurationsmanagement in der KAS-51 kurz unter der Überschrift „Veränderungsmanagement“ beschrieben. In Kapitel 6.9 finden Sie nähere Erläuterungen zu den Anforderungen an ein Konfigurationsmanagement.

Ein aktuell gehaltenes Konfigurationsmanagement unterstützt technische Abläufe, um diese zu optimieren und fehlerfreier zu gestalten. Gleichwohl „wird immer wieder versucht, neueste Technik in dafür ungeeignete Organisationsstrukturen zu implementieren“ (5). Dementsprechend sind bei der Auswahl einer geeigneten Software zur Einführung eines Konfigurationsmanagements, die Fähigkeiten aller potentiell anderen Nutzenden, und nicht nur die des Datenbankmanagements, in den Blick zu nehmen.

2.4 Mensch und Technik

> *„Die subjektive Wahrnehmung einer Arbeitssituation durch die Beschäftigten kann sich von den objektiven Merkmalen der Arbeitssituation erheblich unterscheiden.“ - Oliver Strohm | ETH Zürich | 1997 | Unternehmen arbeitspsychologisch bewerten (5)*

Mensch-Maschine-Interaktionen können zu Herausforderungen führen, wenn Technologien von den Menschen nicht angenommen oder verstanden werden. In diesem Kapitel werden exemplarisch für die Beziehung Mensch und Technik, Herausforderungen mit Remotezugriffen auf Teilanlagen und Tätigkeiten der Wartung und Pflege der OT-Security betrachtet.

Es stellen sich Frage wie:

- Welche Ursachen können Abweichungen zwischen der objektiven und subjektiven Wahrnehmung haben?
- Inwiefern kann dies bei der Umsetzung der OT-Security problematisch werden?

Häufig prägen individuelle Wahrnehmungen und Gefühle das Handeln. Dies führt auch dazu, dass Begrifflichkeiten aufgrund von Erfahrungen unterschiedlich interpretiert werden und bereits vorgefasste Meinungen existieren. Dies soll an den nachfolgenden Begriffen verdeutlicht werden:

2.4.1 Schutzziele

Häufig wird unterstellt, dass in der IT eine feste Priorisierung nach Vertraulichkeit, Integrität und Verfügbarkeit vorherrscht. Bei genauerer Betrachtung kann festgestellt werden, dass diese Priorisierung stark vom Anwendungsfall abhängig ist und nicht so starr dem Schema folgt wie häufig behauptet. Ein Beispiel wäre ein Informationsportal, dass wichtige Daten öffentlich bereitstellt. Dort ist die Verfügbarkeit und Integrität der Daten wichtiger als die Vertraulichkeit.

In der OT hängt die Gewichtung ebenfalls von der einzelnen Anlage ab. In der einen Anlage sind sensible Rezepturen gespeichert, die nicht öffentlich werden dürfen. Die andere Anlage muss dauerhaft verfügbar sein, weil eine Unterbrechung mit hohen Kosten verbunden wäre. Es müssen also auch die einzelnen Umstände betrachtet werden.

Eine Sonderrolle nimmt die Anlagensicherheit ein. Hier gilt eine klare Priorisierung der Integrität und Verfügbarkeit. Eine Veränderung der Systeme bzw. Daten oder ein Ausfall kann zu unerkannten und gefährlichen Zuständen führen. Dies ist immer zu vermeiden.

2.4.2 Redundanz & Diversität

In IT und OT ist Redundanz ein probates Mittel um Systeme zu schützen. Dahinter steht die Idee, dass Systeme, die das Gleiche leisten, aber mehrfach realisiert sind, auch gegen eine gegebene Störung unempfindlich sind und daher wahrscheinlich nicht alle gleichzeitig ausfallen.

In der IT ist dies vielfach einfacher zu realisieren (z.B. durch einen zusätzlichen Server). In der OT ist es schwer möglich, eine komplette zweite Produktionsanlage bereitzuhalten. Man beschränkt sich hier auf die einzelnen Komponenten.

Um aber auch systematische Fehler zu vermeiden, wird darüber hinaus bei besonders hohen Anforderungen auch noch Diversität eingesetzt. Hiermit soll ein Versagen durch gleichzeitige oder gleichartige Fehler ausgeschlossen werden. Dies wird ebenfalls in beiden Bereichen gemacht. In der IT ist dies z. B. bei Firewalls der Fall. In der OT hilft es bei für die Anlagensicherheit relevanten Systemen Ausfallzeiten zu vermeiden.

In der IT ist in vielen Anwendungen eine kurzzeitige Unterbrechung der Funktion durch ein Update tolerierbar. Arbeitsplatzrechner werden zudem regelmäßig zum Feierabend beendet und am nächsten neu gestartet. Wo dies nicht der Fall ist, kann durch redundante System und ein schrittweises Vorgehen eine Unterbrechung vermieden werden. In der OT ist Situation ebenfalls unterschiedlich. Manche Anlagen werden nur in einzelnen Schichten betrieben, andere laufen in einem kontinuierlichen Betrieb über Monate ohne Unterbrechung. Im ersteren Fall können Updates und damit verbundene Unterbrechungen ggf. nach einer Schicht oder während des Schichtwechsels erfolgen. Im zweiten Fall muss dies in die geplanten Wartungsfenster untergebracht werden. Dies muss insbesondere im Rahmen der Risikobetrachtung berücksichtigt werden.

2.4.3 Mensch-Technik Interaktion am Beispiel der Einführung einer Remoteverbindung

Nachfolgend wird zunächst ein verbreitetes industrielles Automatisierungs- und Steuerungssystem betrachtet. Einfallsmöglichkeiten für Cyber-Angriffe könnten u.a. die Vernetzung der Steuerungssysteme mit anderen Systemen, wie

- einem Logistiksystem oder
- einem Asset-Managementsystem des Firmenstandorts,
- Wartungslaptops oder Programmiergeräte,
- die Anbindung an das Firmennetzwerk,
- Fernzugriffsmöglichkeiten und
- das Internet

sein.

Diese Vernetzung wird durch wachsende Anforderungen an die Effektivität, Flexibilität und Wirtschaftlichkeit der Produktion weiter ausgebaut. Dabei stehen die Wünsche der Betriebs- oder Unternehmensleitung

oft den Anforderungen der Security entgegen. Aber auch in der täglichen operativen Arbeit gibt es Anforderungen, die mit neuen Technologien effektiver gelöst werden können. Hierbei ist aber oftmals eine weitere Vernetzung mit anderen Bereichen oder eine Verbindung zu Systemen im Internet erforderlich, um diese Aufgaben zu lösen (z.B. Onlineübersetzer im Internet).

Der Wunsch nach einem höheren Automatisierungsgrad und Flexibilität zur Kostenersparnis führt zu immer komplexeren Systemen, die zusätzliche Konnektivität bieten. Es besteht der Wunsch nach Schnittstellen zu den unterschiedlichsten Parteien, wie z.B. zu Servicedienstleistungsunternehmen. Diese Zusatzfunktionen bieten aber gleichzeitig neue Angriffspunkte und Fehlerquellen, denen mit Konzepten zur Security begegnet werden muss.

Hersteller setzen auf Internet of Things (IoT-) Technologien und bauen immer mehr Konnektivität in ihre Produkte ein bzw. setzen auf Commercial-of-the-Shelf-Komponenten. Auf der Seite der Anwendenden sind dann neue Konzepte zur sicheren Verwendung der neuen Geräte nötig.

Betrachten Sie nachfolgend diese Gemengelage anhand eines konkreteren technischen Anwendungsfalls genauer. Dienstleistungsunternehmen benötigen den Remotezugriff auf Komponenten einer Package Unit in der Anlage. Hier steht der Gedanke eines umfassenden Dienstleistungsangebots dem Designgrundsatz voneinander getrennter OT-Systeme gegenüber.

Die subjektive Wahrnehmung einer Remoteverbindung ist für eine IT-Arbeitskraft aus dem Office-Umfeld nichts Besonderes. Für sie gehören Videokonferenz- und Remote-Desktoptools sowie die Einbindung von Bluetooth und Wireless-LAN Geräten zum Alltag. Regelmäßige Updates und Patches zur Behandlung von Schwachstellen und Fehlern gehören zum Tagesgeschäft und stellen die sichere Nutzung der Remotetechnologien sicher.

Im produktionsnahen Umfeld (OT) sind die Systeme traditionell weniger vernetzt, modular, wartungsfrei und arbeiten weitestgehend noch mit Analogsignalen. Die für den Betrieb und die Instandhaltung der Systeme verantwortlichen MSR-Fachkräfte schätzen den modularen Aufbau und die Instandhaltung mit einfachen mechanischen Werkzeugen. Bei den wenigen digitalen Steuerelementen erfolgt die Programmierung der Anwendungssoftware ebenfalls modular, mittels vorgefertigter und getesteter Softwarebausteine. Remoteverbindungen sind in der subjektiven Wahrnehmung von OT-Verantwortlichen folglich unbekannte neue Konzepte, mit denen sie noch nicht vertraut sind.

Eine Remoteverbindung hebt die klassische Trennung der Automatisierungsebenen (vgl. Abbildung 1) auf und zu derem sicheren Betrieb muss zeitnah auf Schwachstellen und Bedrohungen reagiert werden. Der OT-verantwortlichen MSR-Fachkraft mangelt es an Zeit und dem notwendigen Fachwissen, da diese Technologie nicht zum ursprünglichen Betätigungsfeld gehört. Hinzu kommt, dass an heutige Anlagen eine sehr hohe Verfügbarkeitserwartung gestellt wird.

Nicht selten werden diese rund um die Uhr an 365 Tagen im Jahr betrieben und nur sehr selten für Wartungstätigkeiten außer Betrieb genommen. Für regelmäßige Updates und Patches müssen womöglich völlig neue Konzepte oder Alternativen entwickelt werden.

Im Hinblick auf die Mensch-Maschine-Interaktion muss sichergestellt werden, dass IT-Verantwortliche die Randbedingungen aus dem Anlagenbetrieb kennen. Die OT-verantwortliche MSR-Fachkraft benötigt sicherlich Schulungen, um die Remoteverbindung durch geeignete Security Maßnahmen anforderungsgerecht zu schützen.

Die klassische Trennung der Automatisierungsebenen (vgl. Abbildung 1) aufzugeben bringt zudem noch weitere Probleme mit sich. In der bisherigen Anlagenplanung und dem Betrieb industrieller Automatisierungstechnik wurde davon ausgegangen, dass die Anlagen für Zeiträume von 10-30 Jahren betrieben werden. Wenn in der IT von Zyklen zwischen zwei Jahren (Mobiltelefon oder Mobile-Devices) und bis zu vier Jahren (PC, Notebook) gedacht wird, stehen für den Zeitraum der industriellen Zyklen von 10 bis zu 30 Jahren kaum Servicedienste für Patches und Updates zur Verfügung. In der Vergangenheit hat sich daher trotz des Einzugs digitaler Technik die Trennung der Automatisierungsebenen bewährt. Daher rührt auch die Problematik, dass hier noch Rechner mit veralteten Betriebssystemen im Einsatz sind, da manche, dediziert

für einen Anwendungsfall konstruierte, Hardware nur mit Windows XP oder im Extremfall mit MS-DOS funktioniert. Der Austausch des Steuerungsrechners durch einen mit aktuellem Betriebssystem ausgestattetem System, würde dann gleich eine Investition von mehreren zehntausend Euro nach sich ziehen, da ggf. das gesamte Automatisierungs- oder Messsystem neu beschafft werden müsste.

Trotz der bestehenden Unterschiede bzgl. der Konzepte und Technologien ist auch in der industriellen Automatisierung der Einzug digitaler IT-Konzepte nicht mehr aufzuhalten. Zum einen gibt es zur Aufrechterhaltung der veralteten Technologien dauerhaft keine Ersatzteile und keine Unterstützung durch die Hersteller mehr. Zum anderen bringen moderne Systeme Vorteile, wie z.B. Remoteverbindungen, mit denen u.a. dem Fachkräftemangel begegnet werden kann. Weitere Vorteile können auch eine bessere Performance der Automatisierungsaufgaben oder mehr Werkzeuge zur Analyse sein. Da besonders in diesem Fall die verschiedenen Abteilungen miteinander kommunizieren müssen, ist ein gemeinsames Verständnis extrem wichtig. Und genau hier ergeben sich immer wieder Probleme, da unterschiedliche Auffassungen von Sachverhalten oder auch Begriffen bestehen. Das heißt, dass zwar die gleichen Worte benutzt werden, aber Unterschiedliches gemeint ist. Diesem Umstand kann mit organisatorischen Maßnahmen begegnet werden (siehe 2.2), allerdings ist ein gegenseitiges Verständnis der jeweils verwendeten Technologien und Begriffe unabdingbar.

Nichtsdestotrotz müssen Nutzen und Risiken gegeneinander abgewogen werden und eine Entscheidung zur technischen Lösung getroffen werden. Es ist jedoch notwendig, dass den Entscheidungen fällenden Personen auch alle relevanten Informationen zur Verfügung stehen. Zu diesem Zweck haben die Mitarbeitenden der beteiligten Abteilungen in einem Brainstorming die Fakten zusammengetragen:

Beispiel 3 – Remotezugriff auf eine Füllanlage für Fässer und Gebinde (Package Unit)

Ein Betreiber eines Betriebsbereichs verkauft seine Produkte in Stahlfässern und 1m³-Gebinden. Dazu soll eine neue Füllanlage errichtet werden, die vom Hersteller als „Package Unit“, als komplettes System inkl. aller Komponenten (auch der Steuerung), geliefert wird.

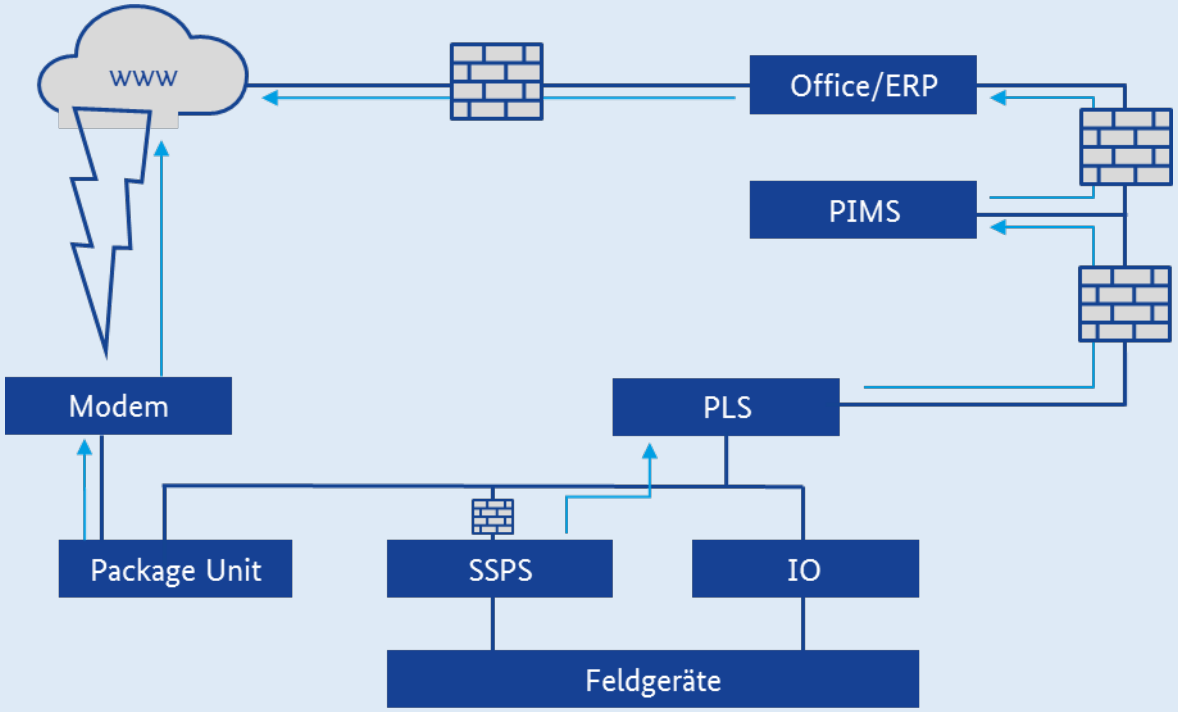

Abbildung 9 Kommunikationswege in einer Prozessanlage

Ausgangssituation

Da die verwendete Software eine Eigenentwicklung des Herstellers ist, kann der Service für die Anlage auch nur von diesem bezogen werden. Um aber umfassenden Support zu erhalten und Ausfallzeiten der Anlage möglichst gering zu halten, ist ein Zugriff aus der zentralen Serviceabteilung des Herstellers erforderlich.

Gleichzeitig ist die Steuerung der Füllanlage auch mit dem Netzwerk des zentralen Leitsystems der Prozessanlage verbunden (vgl. Abbildung 9), da die Bereitstellung der richtigen Produkte aus den Lagertanks und die Übermittlung der Stoffdaten für die Etikettierung erforderlich sind. Dazu kommt, dass in der Steuerung der Package Unit auch sicherheitsrelevante Funktionen ausgeführt werden, die zum Schutz von Leib und Leben und der Umwelt wichtig sind. Diese Einrichtungen werden inklusive der PLS-Sicherheitseinrichtungen vom Hersteller mitgeliefert und nur über eine Datenschnittstelle an das betriebliche Leitsystem angekoppelt.

Wie in Abbildung 9 zu sehen bietet sich die Möglichkeit eine Remote-Lösung des Herstellers zu nutzen (Blitz) oder über die eigene Infrastruktur eine Verbindung aufzubauen, die sich an das Konzept der Schutzebenen hält. Wenn Sie sich dabei noch an den Grundsatz halten, dass eine Verbindung immer nur von innen nach außen (cyan) hergestellt wird, erhalten Sie einen sehr wirksamen Schutz. Allerdings bedeutet die zweite Variante eine höhere Komplexität und verursacht einen deutlichen Mehraufwand.

Grundsätzlich soll alles möglichst einfach und unkompliziert gehalten werden. Jedoch ist ein höheres Maß an Cyber-Sicherheit auch mit höheren Anforderungen (quantitativ und qualitativ) an das Handeln des Personals verbunden.

Leitfragen und Antworten der Beteiligten

- Was ist wichtig?
  - „Es müssen regelmäßige Updates und Patches eingespielt werden, da die Anlage mit Verbindung zum Internet für Angriffe prädestiniert ist."
  - „Es dürfen keine Updates an der eigentlichen Anlagensteuerung im laufenden Betrieb durchgeführt werden, da die Anlage unterbrechungsfrei betrieben werden soll."
  - „Gesetzliche und behördliche Vorgaben sind einzuhalten, in diesem Fall will die Aufsichtsbehörde eine unabhängige Stellungnahme zur Security vor der Inbetriebnahme von uns."
  - „Die Kosten müssen in Relation zum Nutzen stehen."
  - „Die PLT-Sicherheitseinrichtungen müssen vor Cyber-Angriffen geschützt sein."
- Was ist gefährlich?
  - „Eine Remoteverbindung auf das SIS kann die Anlagensicherheit beeinträchtigen.".
  - „Eine Remoteverbindung auf das PLS kann die Anlagenverfügbarkeit beeinträchtigen.".
  - „Gemeinsam genutzte Komponenten (Controller, Netzwerk, Feldgeräte) können die Anlagensicherheit und Verfügbarkeit gefährden."
  - „Wartungen an komplexen IT-Systemen werden durch ungeschulte Arbeitskräfte vorgenommen."
  - „Ein Kompromittieren des Fernwartungszugangs ermöglicht unmittelbar einen unerlaubten Zugriff auf die Steuerung der Füllanlage, als auch mittelbar einen Zugriff auf das zentrale Leitsystem der Anlagen."
  - „Wenn durch einen Cyber-Angriff ein Personenschaden erfolgen sollte, steht der Staatsanwalt vor der Tür."
- Was ist real?
  - „Die angebotene Variante mit einem integrierten System für die betriebliche Steuerung und die PLT-Sicherheitseinrichtungen macht die Bewertung der IT-Security immens schwierig."
  - „Zusätzliche Kosten für die Cyber-Sicherheit können erst nach einer Risikoanalyse abgeschätzt werden und müssen ggf. von der Geschäftsleitung genehmigt werden."
  - „Wir haben derzeit nicht die Ressourcen, um auch noch die Cyber-Sicherheit von OT-Systemen zu übernehmen, außerdem kennen wir das KAS-Regelwerk nicht und haben auch niemanden, der sich damit beschäftigen kann..."
  - „Es gibt verschiedene Konzepte für den Fernwartungszugriff bei der IT-Abteilung und unserem Dienstleistungsunternehmen, die sich teilweise widersprechen."
  - „In Saudi-Arabien wurde eine Remoteverbindung aus Unachtsamkeit permanent betrieben und über diese ein Gaskraftwerk gehackt. Dadurch haben die Angreifenden einen Zugriff auf die PLT-Sicherheitseinrichtungen der Anlage bekommen."

In dem gegebenen Beispiel hat die Diskussion den Beteiligten die Komplexität der Sachverhalte vor Augen geführt und ein gemeinsames Verständnis geschaffen, mit dem sich ein Konzept als Entscheidungshilfe entwickeln lässt.

Die Zusammenfassung der größten Herausforderungen im Aktionsplan aus dem Beispiel erfolgt mit Hinweisen auf die allgemeinen Regelwerke (z.B. Grundschutz). Um zu einer objektiven Entscheidung zu kommen, ist eine High-Level-Risikoanalyse das Mittel der Wahl. Hier sind verschiedene Methoden verfügbar, die in diesem Kapitel vorgestellt werden.

2.4.4 Risikoanalyse auf Basis der Schutzebenen

Die Herausforderung bei der Risikoanalyse der o.g. Sachverhalte liegt primär darauf, die Risiken zu erkennen. Aber im Gegensatz zur Analyse der verfahrenstechnischen Risiken von Betriebsbereichen ist der Erfahrungsschatz auf diesem Gebiet für die Mitarbeitenden, welche sich mit dem Thema OT beschäftigen, noch nicht so ausgeprägt. Dazu kommt noch die Festlegung, welche Schutzziele (vgl. Abbildung 10) mit welcher Priorität in die Betrachtung mit eingehen sollen.

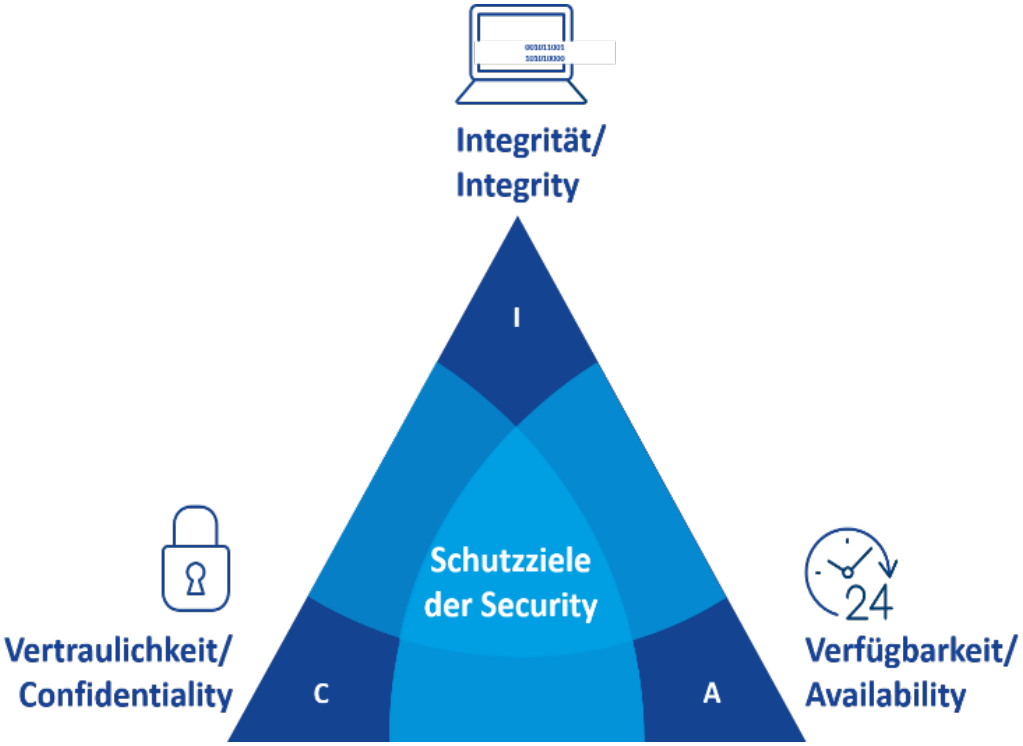

Abbildung 10 Schutzziele

Hier unterscheiden sich die Kategorien zwischen IT und OT nicht, wenn man das Schutzziel der Safety mit der Integrität gleichsetzt. Aus Sicht der Anlagensicherheit sind die Schutzziele der Integrität und Verfügbarkeit oberste Prämisse. Nur bei vollkommen integren Daten ist die Funktion von PLT-Sicherheitseinrichtungen gewährleistet, darüber hinaus ist auch die Verfügbarkeit der PLT-Sicherheitseinrichtungen zu gewährleisten. Zusätzlich wird dem Betreiber aber auch die Verfügbarkeit von Daten und damit auch die Verfügbarkeit der Anlage sehr am Herzen liegen. Falls es sich dann noch um verfahrenstechnische Sachverhalte handelt, die für Dritte interessant sind, ist auch die Vertraulichkeit zu schützen.

Ob nun von IT oder OT gesprochen wird, bedeutet dies in Summe, dass unterschiedliche Anforderungen und Ziele die Definition von Maßnahmen beeinflussen werden. Das kann und wird aber auch bedeuten, dass sich die unterschiedlichen Ziele widersprechen und die Maßnahmen für ein Schutzziel dem anderen Schutzziel entgegensprechen. Ein klassisches Beispiel für die OT wäre hier die Abwägung zwischen Integrität und Verfügbarkeit. Aus Sicherheitsaspekten würde man die Anlage bei dem kleinsten Hinweis auf eine Integritätsverletzung abschalten (z.B. nicht plausibler Messwert), aber aus Verfügbarkeitsgründen möchte man die Anlage weiter betreiben und nutzt zum Beispiel den letzten plausiblen Messwert.

Daher wird es erforderlich sein, bei der Definition der Maßnahmen in Abhängigkeit von Schutzzielen und Betreiberinteressen Abwägungen zu treffen und Prioritäten zu definieren. Um aber die Risikoanalyse strukturiert durchzuführen, stehen verschiedene Methoden zur Verfügung. Die Risiko-Analyse-Methoden werden in Kapitel 8.1 dargestellt.

2.5 Das Dilemma der unterschiedlichen Denk- und Betrachtungsweisen

Zu den in den vorherigen Kapiteln beschriebenen Herausforderungen gibt es darüber hinaus noch weitere, die sich aus den unterschiedlichen Denkweisen der Safety und Security bzw. der Handelnden aus IT und OT ergeben.

2.5.1 Zufällige vs. systematische Fehler

Die Definition von Fehlern mag sich auf den ersten Blick nicht als relevant für die Bewertung der Security angesehen werden. Um aber über die Wirksamkeit und Definition von Maßnahmen nachzudenken, ist ein Verständnis der Unterschiede erforderlich. Dabei erscheint es auch wichtig, dass sich die Beteiligten aus unterschiedlichen Bereichen (IT, OT) verstehen, wenn sie von Fehlern sprechen.

Wenn ein Anlagenbetreiber im Rahmen der Anlagensicherheit über Maßnahmen gegen Fehler nachdenkt, werden diese in zwei Kategorien eingeteilt. Es gibt den zufälligen Fehler, der beispielsweise im Bereich der Elektronik oder Elektrotechnik quantifizierbar ist und auf den ein wesentlicher Teil der Betrachtung der Safety entfällt. Hingegen spielen Fehler dieser Art bei der Security keine Rolle. Eine angreifende Person wird in der Regel nicht darauf warten, dass in einer Firewall ein Bauteil zufällig seine Funktion einstellt und dadurch ein Einfallstor geöffnet wird.

Als zweiten zu betrachtenden Fehler gibt es an dieser Stelle den systematischen Fehler. Davon wird gesprochen, wenn Fehler durch falsche Montage, Planung oder Auslegung entstehen. Das könnte in der Elektronik ein zu klein dimensioniertes oder fälschlicherweise verbautes Halbleiterbauelement sein oder in der Mechanik eine falsche Feder.

In der Safety werden viele systematische Analysen angestellt, um diese Fehler auszuschließen. Das kann eine systematische Überdimensionierung von Bauteilen sein oder die Verwendung von Standardgeräten, die ihre Eignung in unkritischen Anwendungen nachgewiesen haben. Weiterhin existieren bei den Unternehmen umfangreiche Checklisten, um bekannte systematische Fehler zu hinterfragen und im Planungs- bzw. Designvorgang sowie während des Betriebs zu betrachten.

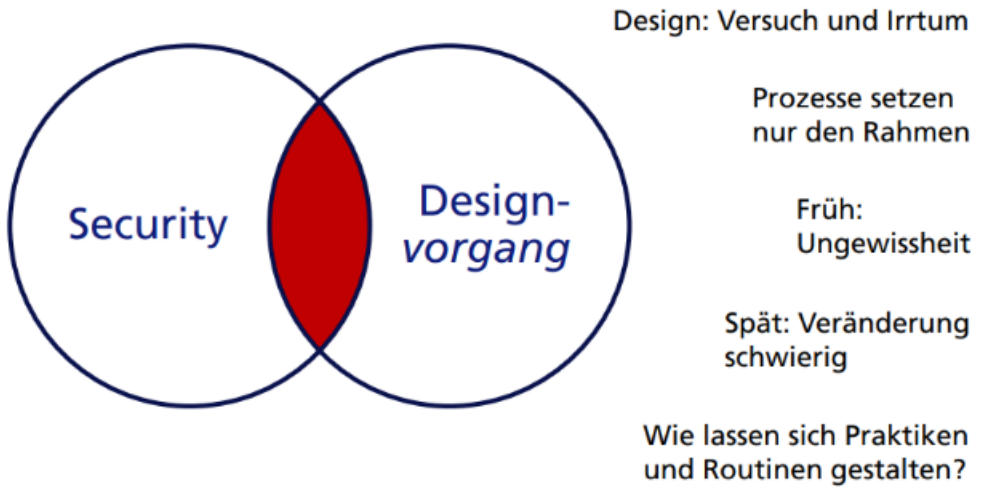

Abbildung 11 Security im Designprozess

Wie in Abbildung 11 dargestellt gehört zur Planung auch die Betrachtung der Security, was auch zu Anpassungen auf beiden Seiten führen kann. Im Rahmen des Designvorgangs wird versucht alle relevanten Folgen und Fehler zu betrachten. Am Ende können Fehler im besten Fall nicht mehr auftreten. Dies gilt insbesondere für Schäden an Mensch und Umwelt. Ansonsten sind die Folgen beherrschbar bzw. tolerierbar. Die Folgen sind also günstiger als die Absicherung gegen den Fehler sind. Um das zu verifizieren werden erstmalige und wiederkehrende Prüfungen durchgeführt.

In der Security, also in Bezug auf den Schutz vor Angreifern, wird sich nicht mit zufälligen, sondern ausschließlich mit systematischen Fehlern beschäftigt. Ein Ausschluss ist aber in diesem Thema nicht möglich, da die Systeme (und die Software) zu komplex sind. Es ist daran erkennbar, dass immer wieder Sicherheitslücken bei Anwendungen oder Betriebssystemen bekannt werden. Dies kann z. B. ein Fehler in einem Verschlüsselungsalgorithmus sein oder ein Fehler in der Programmierung eines Dienstes des Betriebssystems, der einen Zugriff auf die Maschine erlaubt. In den vorgenannten Fällen handelt es sich um systematische Fehler. Diese Problematik wird noch dadurch verstärkt, dass heute oft mit Software gearbeitet wird, die schnell entwickelt wurde und unzureichend geprüft ist oder aus Kostengründen von Drittanbietern bezogen wurde. Das modulare Arbeiten kann darüber hinaus dazu führen, dass einzelne Fehler auch eine große Verbreitung finden. Systematische Tests und Konzepte wie „Security by Design“ können hier zu maßgeblichen Verbesserungen führen.

2.5.2 Gemeinsam genutzte Komponenten

Dieses Thema musste in der Anlagensicherheit schon immer betrachtet werden und wird gerade in letzter Zeit wieder verstärkt diskutiert. Dabei geht es aber bisher ausschließlich um die Betrachtung der Feldgeräte, um Sensoren und Aktoren und ob diese sowohl für betriebliche Zwecke als auch für die Anlagensicherheit verwendet werden. Wird diese Frage aus Sicht der Security gestellt, stellt sich heraus, dass die PLT-Sicherheitseinrichtung auch in Bezug auf diesen Sachverhalt überprüft werden müssen. In Betriebsbereichen sind mit modernen Steuerungen einige Konstellationen üblich, die auf den zweiten Blick zu Problemen führen können. Es gibt heute Systeme, die betriebliche und Sicherheitssteuerungen in einem Gerät vereinen. Eine Kompromittierung eines solchen Systems würde dazu führen, dass gleichzeitig die betriebliche Einrichtung als auch die Sicherheitseinrichtung versagt. Ein Vorgang, der sowohl aus Sicht der Safety als auch aus Sicht der Cyber-Sicherheit (Defense in Depth) auf jeden Fall zu vermeiden ist. Aber auch bei separaten Systemen findet sich oft die Konstellation, dass Signale ausschließlich aus dem Feld in die Sicherheitssteuerung eingelesen oder ausgegeben werden und dabei das gleiche Signal gemeinsam in PLS und SSPS verwendet wird. In Abbildung 12 wird ein Anwendungsfall dargestellt, bei dem die Messsignale in der betrieblichen Steuerung (Regelfunktion) über eine Busverbindung zwischen PLS und SSPS ausgetauscht werden.

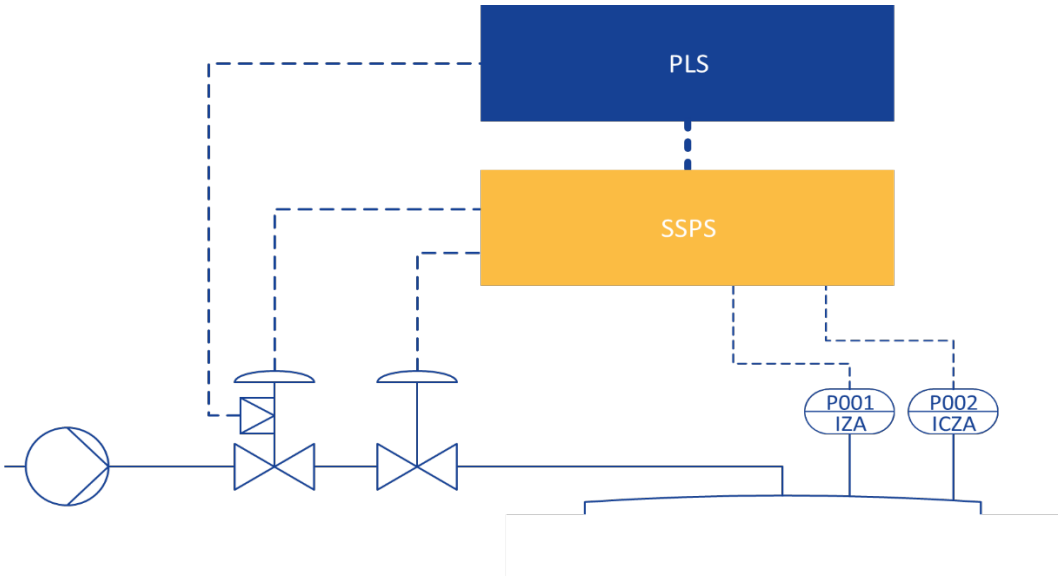

Abbildung 12 Mitbenutzung von Signalen

Bei einem Zugriff auf oder Manipulation der Sicherheitssteuerung wäre es möglich, den Messwert beider Sensoren zu manipulieren und damit auch die Anzeige und Verarbeitung im Prozessleitsystem (PLS) zu beeinflussen. So würde auch hier eine Manipulation ausschließlich der Sicherheitssteuerung oder des Sensors zu einem Doppelfehler führen, der darüber hinaus noch den Anforderungsfall der Störung herbeiführen und gleichzeitig das Ansprechen der PLT-Sicherheitseinrichtung verhindern würde.

2.5.3 Anlagenautomatisierung

Die in der Anlagenautomatisierung vorherrschenden proprietären Systeme gewährleisten durch die eingeschränkten Rechte und Möglichkeiten einen gewissen Schutz gegen unzulässige Änderungen. Und dadurch, dass für die Programmierung an vielen Stellen Programmiersprachen mit eingeschränktem Sprachumfang (LVL) zur Verfügung stehen, können auch Mitarbeitende, die das Programmieren nicht gelernt haben, Industriesteuerungen mit einer hohen Qualität verwenden. So mancher Betreiber wird sich fragen, wie diese bewährte Automatisierungslandschaft erhalten werden kann und dennoch moderne IoT-Technologien genutzt werden können.

Dagegen wird manch eine IT-Fachkraft im Umgang mit den proprietären Systemen fremdeln, was auch beim Thema Geräte-Diversität zutreffen wird.

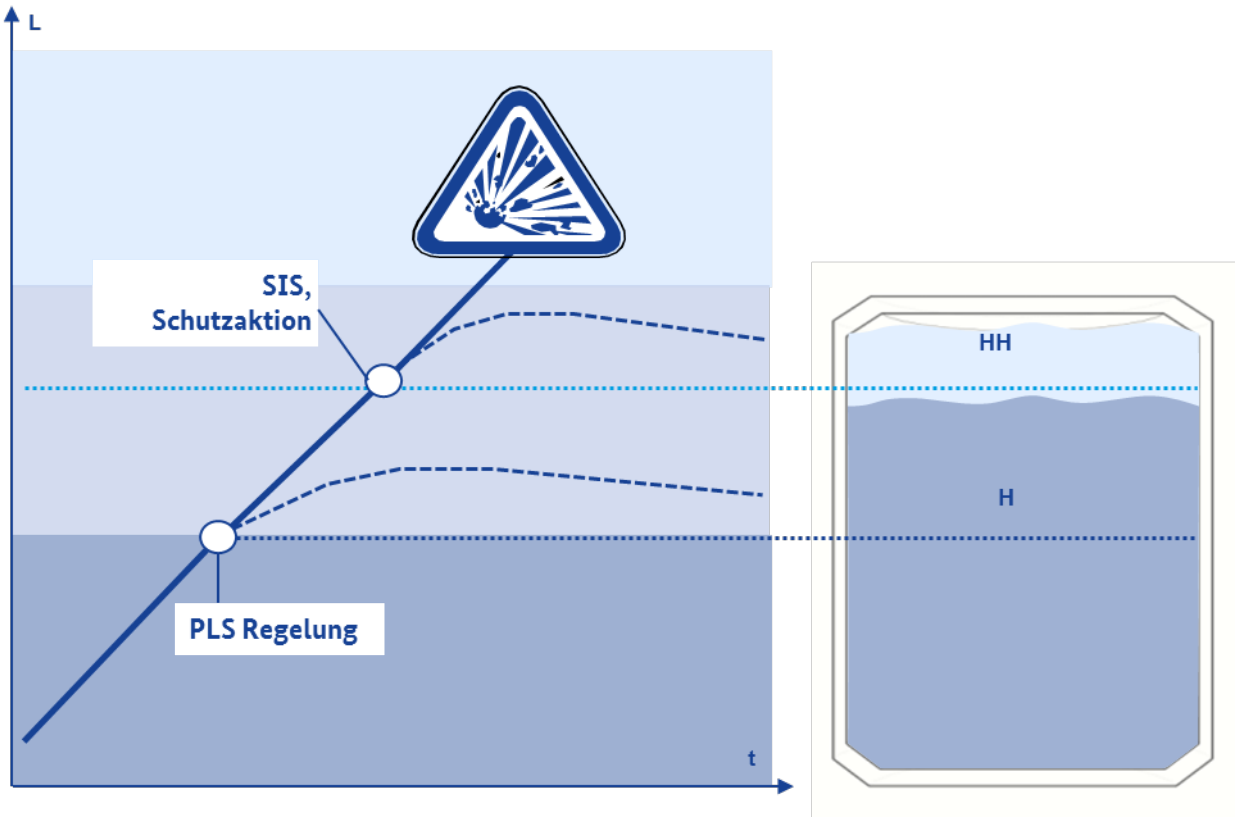

Abbildung 13 Schutzebenenkonzept in der Verfahrenstechnik in Anlehnung an (16)

Die in den Anlagen teilweise eingesetzte Geräte-Diversität ist das Ergebnis sorgfältiger Überlegungen, z.B. der Anlagensicherheit. So wird durch die technologische Trennung der Schutzebenen des PLS vom SIS verhindert, dass systematische Fehler gleichartiger Komponenten (z.B. der Steuerungen des PLS und SIS) nicht direkt zu einem Störfall (vgl. Abbildung 13) führen. In diesem Diagramm wird auf der Y-Achse der Füllstand in einem Behälter (L) dargestellt, der symbolisch auch rechts dargestellt wird. Bei einem ersten Grenzwert (H), wird durch das betriebliche Leitsystem die weitere Befüllung gestoppt. Bei einem Versagen dieser Einrichtung würde bei einem zweiten Grenzwert (HH) das SIS durch eine unabhängige Funktion die weitere Befüllung stoppen, was auch eine grundsätzliche Forderung in den Normen und Regelwerken der Funktionalen Sicherheit ist. Die vorherrschenden Systeme und Konzepte folgen dabei dem Grundsatz: je einfacher, desto besser.

Wird an dieser Stelle nun durch neue Technologien wie integrierte Systeme, Datenschnittstellen oder Busverbindungen die Unabhängigkeit aufgehoben, kann ein Angreifer den Zugriff auf beide Schutzebenen erhalten. Diese Vermischung der Schutzebenen ist aber an vielen Stellen nicht immer auf den ersten Blick erkennbar. Um solch eine Vermischung sicher zu vermeiden, kann es sinnvoll sein, zum einen unabhängige Systeme aber auch diversitäre Systeme zu verwenden, um die Erfolgsaussichten eines Angriffs zu verringern, da dies eine höhere Kompetenz des Angreifers voraussetzt.

Sollten zukünftig frei programmierbare Systeme mit standardisierten Baugruppen oder Kommunikationsprotokollen Einzug in die Prozessautomatisierung halten, dann sind auch bewährte Instandhaltungs- und Anlagensicherheitskonzepte neu zu bewerten.

2.5.4 Ein-Fehler-Prinzip

Ein Grundsatz der Gefahrenanalyse von prozesstechnischen Anlagen ist, dass nur ein Fehler gleichzeitig unterstellt wird (siehe HAZOP). Ein zeitgleiches Auftreten von mehreren, unabhängigen Fehlern ist vernünftigerweise in der Anlagentechnik (mechanische und elektrische Komponenten) auszuschließen, da die Wahrscheinlichkeit gleichzeitiger Fehler ausreichend gering erscheint, was durch langjährige Erfahrung auch zu belegen ist. Das führt allerdings am Ende dazu, dass ein Szenario mit mehreren gleichzeitigen Fehlern unter Umständen nicht durch die PLT-Sicherheitseinrichtungen der Anlage abgefangen werden kann.

Die Betrachtung einer geringen Eintrittswahrscheinlichkeit zeitgleicher Fehler funktioniert aber nur solange, bis eine gezielte Manipulation (z. B. Sabotage) stattfindet oder von einer solchen ausgegangen werden muss. Ein Vorgang, der in aktuellen Gefahrenanalyse nicht berücksichtigt wird, da dies bisher durch andere Maßnahmen (z.B. Zugangsschutz) als hinreichend ausgeschlossen betrachtet wurde. Mit Blick auf die Security ist unter Umständen auch hier Anpassungsbedarf notwendig. Zum einen kann es erforderlich sein, komplexere Fehler durch das betriebliche Leitsystem zu identifizieren, um die notwendigen Maßnahmen ergreifen zu können. Zum anderen wird die Sicherung und Unabhängigkeit der PLT-Sicherheitseinrichtungen und damit der Sicherheitssteuerung umso wichtiger, um auszuschließen, dass sowohl der Anforderungsfall als auch das Versagen der PLT-Sicherheitseinrichtung gleichzeitig auftritt.

2.5.5 Innentäter/unbeabsichtigte Fehler/vorhersehbarer Missbrauch

Durch sehr mächtige und komplexe Systeme muss gleichermaßen auch die Fragestellung zum Innentäter, z. B. einer unzufriedenen Arbeitskraft oder jemandem, der von anderen Leuten bedroht oder ausgenutzt wird, gestellt werden. Die Möglichkeiten der Manipulation sind größer, da viele Arbeitskräfte sich auch einen physischen Zugang zu den Systemen verschaffen können und die Möglichkeit der Nachverfolgbarkeit ist kleiner, da eine Arbeitskraft ggf. schon Zugang zu den Bereichen hat. Dazu kommt noch, dass Innentäter durchaus über vertieftes Wissen der Systeme und Verfahren verfügen, was die Auswirkung verstärkt und ggf. das Verwischen von Spuren vereinfacht. Daher ist die Annahme, dass ein Zutrittsschutz durch einen Werkszaun und eine ständig besetzter Kontrollraumausreichend ist, nicht unbedingt plausibel.

Es muss sich aber nicht unbedingt um Vorsatz handeln. Auch versehentliche Fehler können bei komplexen Verfahren und Systemen weitreichende Folgen haben. Beispielsweise könnte eine Verwechslung von Sensoren dazu führen, dass irrtümlich ein Grenzwert oder Schaltpunkt verändert wird und unbemerkt dazu führt, dass eine Sicherheitsfunktion gar nicht mehr ausgelöst werden kann.

3 Neue Herausforderungen und Risiken

Begriffe wie „Industrie 4.0“, „digitale Produktion“ oder „Internet der Dinge“ sind in aller Munde. Dabei ist der Grad der Automatisierung in der Chemiebranche schon seit Jahren sehr hoch. Die Branche fokussiert sich seit Langem auf Prozessoptimierung und Intensivierung sowie ressourceneffiziente Produktion. Hierbei fallen bereits heute große Datenmengen an, deren Potential noch nicht vollständig ausgeschöpft wird. „Ein vollständig digital gesteuerter und integrierter Chemiestandort basiert auf einer digitalen Anlage“, so beschreibt die DECHEMA 2016 die Vision zur Digitalisierung in der Chemieindustrie in einem Whitepaper (17). Hierbei spielt die Vernetzung von Prozessen, Integration von Anlagen und die Vernetzung über Standorte eine große Rolle. Im nachfolgenden Absatz werden die Technologien zur Umsetzung der Vision beschrieben. Wesentliche Wegbereiter für Industrie 4.0 sind die Datenanalyse, Feldgeräteintegration, Interoperabilität, Vernetzung und OT-Security.

Aus dieser Entwicklung resultieren Herausforderungen für die Anlagensicherheit, die ebenfalls zu den jeweiligen Trends beschrieben werden. In der derzeit stattfindenden Entwicklung Richtung Industrie 4.0 erfolgt durch die zunehmende Digitalisierung gleichzeitig die Auflösung der physischen Trennung zwischen IT (Office-Netzwerk) und OT (Anlagen-Netzwerk) und sogar darüber hinaus in die Cloud. Somit entstehen eventuell Zugriffsmöglichkeiten auf technische Anlagen aus dem klassischen Büro oder über Cloud-Anwendungen, die auch die Angriffsflächen für Cyber-Angriffe vergrößern. Es entstehen Anforderungen an die Datensicherung und den Datenschutz, um das Niveau der Anlagensicherheit zu halten.

In den folgenden Abschnitten werden bzw. wird daher die

- 3.1 Datenanalyse,
- 3.2 Feldgeräteintegration,
- 3.3 Interoperabilität,
- 3.4 Vernetzung und
- 3.5 OT-Security

als Wegbereiter für Industrie 4.0 behandelt.

3.1 Datenanalyse

> *Personal data is the new oil of the internet and the new currency of the digital world. (oft zitiert als „Daten sind das neue Öl.“) - Meglena Kuneva | EU Politikerin | 31. März 2009 | Roundtable on Online Data Collection, Targeting and Profiling*

Der eigentliche Schatz der Digitalisierung liegt in den Daten, die gesammelt, gespeichert und quasi in Echtzeit verarbeitet werden. Während die üblichen Applikationen des Leitsystems die Prozessführung innerhalb definierter Grenzen überwachen und bei Grenzwertverletzungen Schutzaktionen ausführen, erfassen die Sensoren kontinuierliche Daten aus dem Prozess. Die Auswertung der bereits vorhandenen Sensordaten und Informationen könnte z.B. dazu verwendet werden, auch geringfügige Veränderungen im Prozess zu erkennen.

Stellen Sie sich bitte einen Durchflussmengenmesser vor, in dem zusätzliche ein Temperatursensor integriert ist. Bisher wurde lediglich der Messwert für die Durchflussmenge genutzt. Zukünftig könnte auch die Temperatur erfasst werden und zur Überwachung und Optimierung des Prozesses herangezogen werden. Ein weiteres Beispiel wäre eine Möglichkeit zur Erkennung von Leckagen in Rohrleitungen. Hierzu können Messwerte an verschiedenen Stellen im Prozess abgeglichen werden. Abweichungen können auf Optimierungsbedarf des Prozesses deuten, um eine höhere Ausbeute zu erzielen oder ein mögliches Leck in Trans-

portleitungen. Leckagen ließen sich über die Auswertung der in der Anlage bereits installierten Durchflussmessung, durch einen Abgleich mit vorangegangenen Messungen (Datenhistorie) quantifizieren, dann könnten Maßnahmen zur Qualitätssicherung getroffen werden.

Bei der Datensammlung kann es notwendig werden zusätzliche Schnittstellen einzuführen, die zu komplexen, stark vernetzten Netzwerken führen. Um die Angriffsfläche für Cyber-Angriffe zu verkleinern, sollten ungenutzte Schnittstellen speziell gegen Zugriffe geschützt und die Datenverbindungen derart ausgeführt werden, dass sie rückwirkungsfrei auf die Prozessleittechnik sind. Die spezifische Auswertung von Daten kann aber auch helfen, die Integrität von PLT-Sicherheitseinrichtung zu überwachen. Einen Ansatz zur Integritätsüberwachung kann dem Artikel „Security für die SPS-Programmierung“ (18) entnommen werden.

3.2 Feldgeräteintegration

Die Feldgeräteintegration (engl. Field Device Integration, FDI) vereinheitlicht Geräteintegration, Konfigurationswerkzeuge, Diagnose und Dokumentation unabhängig von einem Betriebssystem.

Ein bereits verbreitetes Anwendungsbeispiel ist die Kopplung digitaler Rohrleitungs- und Instrumentenschemata (R&I-Schemata) mit den Anlagendaten. Moderne Automatisierungstechnik, einschließlich der Feldgeräte, verfügt zunehmend über eingebettete Mikroprozessoren, mit denen u.a. eine digitale Feldgeräteintegration in die OT-Netzwerke ermöglicht wird. Ein standardisiertes hersteller- und systemübergreifendes digitales Datenprotokoll gestattet die erleichterte Gerätekonfiguration, den Austausch, die Wartung und die Diagnose. Wird z.B. in einer Anlage ein Messumformer durch ein anderes vergleichbares Messmittel eines anderen Herstellers ersetzt, dann können die Änderungen (Hersteller/Typwechsel) auch über FDI automatisch in der as-built-Dokumentation angepasst werden. Einige Technologieunternehmen auf dem Markt haben bereits in dieser Form FDI als Softwarelösungen für Asset Management implementiert. Die notwendige Voraussetzung zur Nutzung der in den Anlagen vorhandenen Daten ist ein einheitliches und standardisiertes Datenformat (z.B. FDI, OPC UA).

Neben den Vorteilen kann FDI jedoch auch dazu führen, dass bei unsachgemäßer Anwendung Informationen aus dem Netzwerk von Dritten leichter ausgespäht oder geändert werden. Die Datenformate verfügen alle über entsprechende Security Einstellungen, die bei sachgemäßer Anwendung und Aktualisierung mit Updates und Patches gegen Fremdzugriffe geschützt werden können. Dabei sollte überprüft werden, ob die mit der Systempflege betrauten Mitarbeitenden die Technologie hinreichend kennen und Zugang zu den benötigten Unterlagen haben. Für die sichere Nutzung von FDI sollten ungeübte Personen eine Einarbeitung für den Betrieb und die Pflege der Security-Aspekte erhalten.

3.3 Interoperabilität

Bis vor ein paar Jahren waren SPSen nicht mit viel mehr verbunden als mit ihren Ein- und Ausgängen, benachbarten Steuerungen und vielleicht einem Leitsystem – und dies schon gar nicht per Netzwerk. In Bezug auf die Nutzung der in der Anlage verfügbaren Daten für weitere Digitalisierungsanwendungen werden heute zunehmend Daten aus den unterschiedlichen Systemen vernetzt und dann in ein einheitliches Format gebracht. Ein vielversprechender Standard, der in Zukunft zunehmend Anwendung finden könnte, ist OPC UA (Open Platform Communications Unified Architecture).

> *OPC UA ist eine Sammlung von Standards für die Kommunikation und den Datenaustausch im Umfeld der Industrieautomation. Mithilfe von OPC UA werden sowohl der Transport von Machine to Machine-Daten als auch Schnittstellen und die Semantik von Daten beschrieben. Die komplette Architektur ist serviceorientiert aufgebaut. - Stefan Lummer/Nico Litzel | Autor/Redakteur | 22. März 2018 | Bigdata-insider.de*

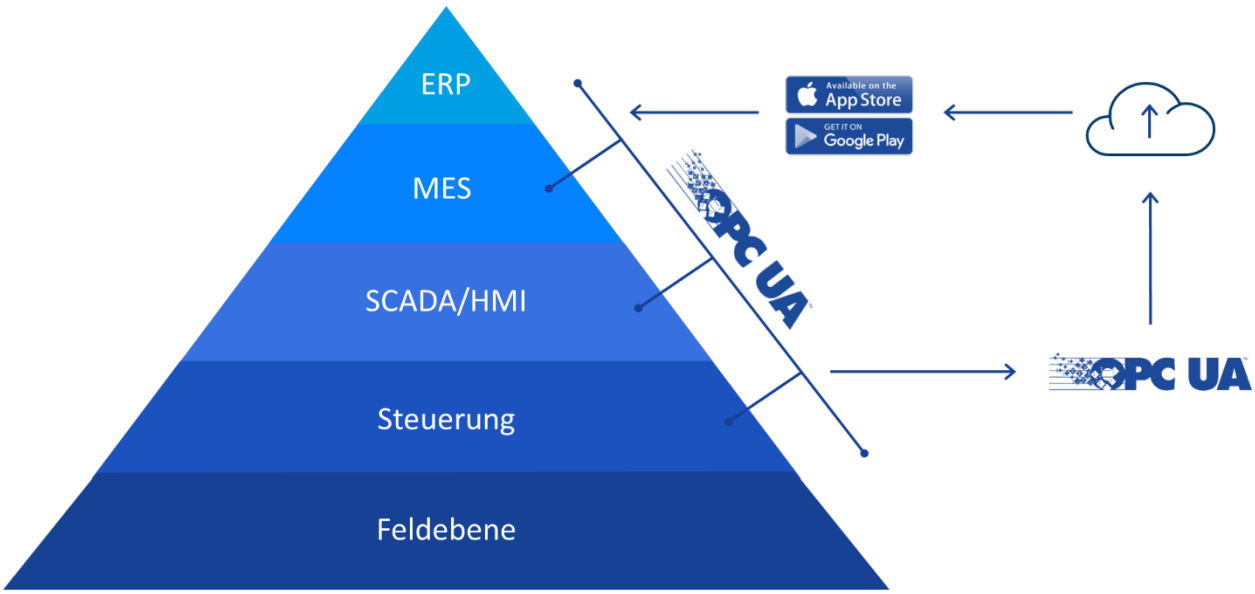

Abbildung 14 Open Platform Communications Unified Architecture

Die nach den OPC-Informationsmodellen aufbereiteten Daten gestatten die Anbindung von internen sowie auch externen Anwendungen. OPC UA ist ein standardisiertes Datenaustauschformat, das Anlagendaten (z.B. Regelgrößen, Messwerte, Parameter usw.) nicht nur transportiert, sondern auch maschinenlesbar beschreibt. Wie in Abbildung 14 dargestellt, können für den Datentransport Schnittstellen der Automatisierungspyramide genutzt werden. So können z.B. Produktions-, Qualitäts-, Instandhaltungs- und Inventarmanagement-Tools auch von smarten Anwendungen genutzt werden, die Daten in Echtzeit verarbeiten. Während die Nutzung dieser Tools aufgrund der standardisierten Datenkommunikation mittels OPC UA sehr einfach ist, sind Maßnahmen zur Absicherung schwieriger. OPC UA bietet Mechanismen zur Authentifizierung, Signierung und Verschlüsselung an. Diese werden jedoch häufig aufgrund der zusätzlichen Arbeit zur Konfiguration und Betreuung im Betrieb nicht genutzt. Eine zusätzliche Hürde stellt auch hier das fehlende Wissen der Integratoren und OT-Anwender dar, da dies bisher nicht zu ihren üblichen Aufgaben gehörte. Im Einzelfall sollte das Risiko bewertet und bei Bedarf zusätzliche Maßnahmen getroffen werden.

3.4 Vernetzung

Auf der Feldebene sind Sensoren und Aktoren in der Regel Punkt-zu-Punkt mit der Logiksteuerung verdrahtet. Von der Steuerungsebene aufwärts der Automatisierungspyramide (vgl. Abbildung 14), erfolgt die Kommunikation in den Anlagen über Ethernet-basierte Bussysteme. Zunehmend werden modulare Subsysteme in das Produktions-LAN integriert und von externen Dienstleistern, z.B. aus der Ferne, gewartet.

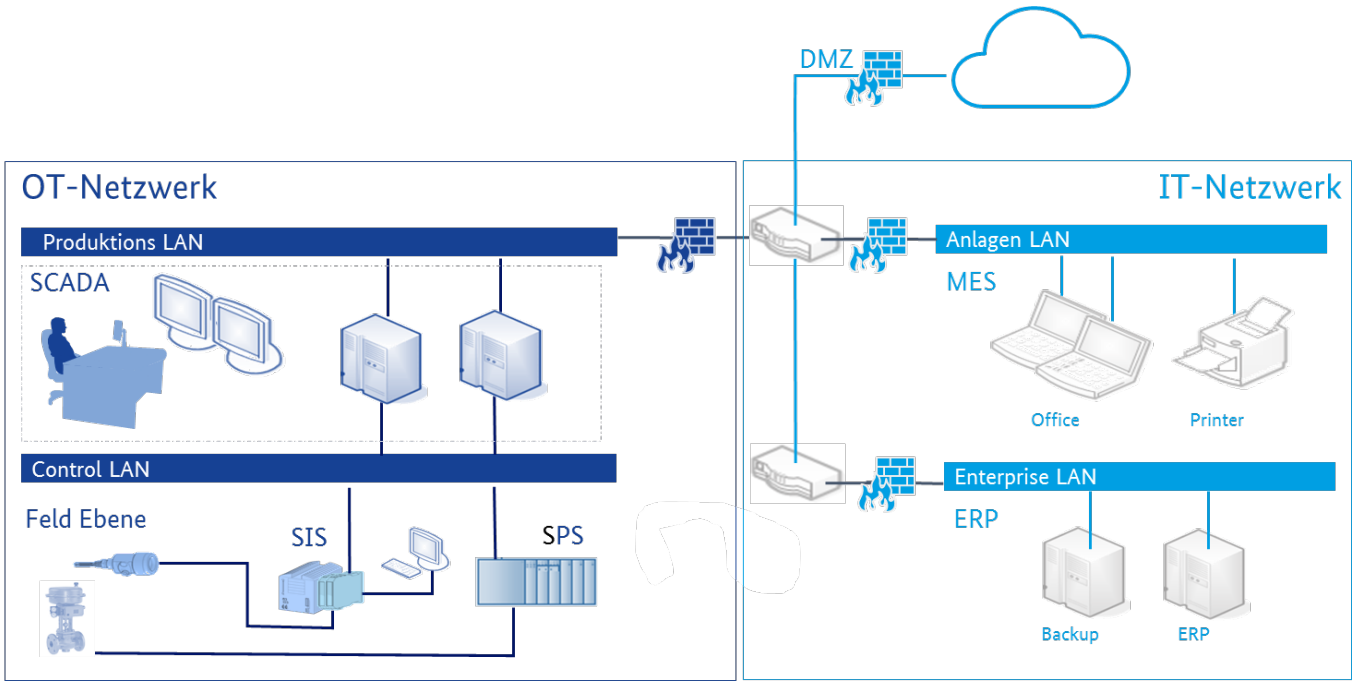

Abbildung 15 Schematischer Netzwerkplan

Sollen Daten der Feldebenen für unternehmensexterne Anwendungen (z.B. Fernwartungsdienste) verfügbar gemacht werden, dann sind diese mit dem Internet zu vernetzen. Dabei haben die Daten das Produktions-LAN, die Firewall zum Anlagen-LAN und die demilitarisierte Zone (DMZ) ins Internet zu passieren (vgl. Abbildung 15). Der Nutzen von Fernwartungszugängen für die Unternehmen soll vielfältig sein, wie in der NA 135 „Fernwartung der Automatisierungstechnik in der Prozessindustrie“ beschrieben.

> *Mit Hilfe von Fernwartung lassen sich Kosten sparen, Risiken minimieren, z.B. von Anlagen- oder Systemausfällen, und Servicelevel optimieren (z.B. Verfügbarkeit, Wiederherstellungszeit bei Ausfall). Andererseits können durch die Nutzung von Fernwartung zusätzliche Kosten entstehen (z.B. für die Bereitstellung der erforderlichen Kommunikationsinfrastruktur) und zusätzliche Risiken, etwa im Hinblick auf die Vertraulichkeit und die Integrität der gewarteten Systeme. - NA 135/ NAMUR / 24. Mai 2011 / namur.net/de/*

Um Aufwände für die Verkabelung beim Anschluss von Sensoren, Aktoren und Steuerungen zu sparen, liegt es nah, moderne Funktechniken wie W-LAN, Bluetooth, NFC / PROFIsave / WirelessHART, das 5G-Netz oder zukünftig Satelliten-Verbindungen zu nutzen. Mit 5G soll z.B. die Datenübertragung bei gleicher Reichweite zu 4G zuverlässiger und leistungsstärker werden. Und mit WLAN ausgestattete Sensoren sind bereits heute weit verbreitet.

Durch Unachtsamkeit bei der Inbetriebnahme oder aus Bequemlichkeit im Betrieb können Schnittstellen, z.B. mit Funkstandards, zu unautorisierten Kommunikationswegen im Netzwerk führen. Der Komfort wird mit einigen Einschränkungen erkauft. So sind Funkverbindungen störanfälliger und die Signale können einfacher mitgelesen werden. Mögliche Angreifer müssen keinen direkten Zugang zur Anlage mehr besitzen, sondern können ggf. auch von außerhalb des Werksgeländes auf das Funknetzwerk zugreifen. Daher ist hier besondere Vorsicht und Achtsamkeit bei Planung und Betrieb notwendig.

Wie sieht aber eine anforderungsgerechte Netzwerkstruktur aus, in die sich auch die zuvor genannten Funkstandards integrieren lassen? Die grundlegenden Anforderungen sollen bestehen bleiben: Die Produktion muss sicher, zuverlässig und effizient sein und das Bedienpersonal muss die anvertrauten Prozesse verstehen, beherrschen und bestmöglich steuern.

Der Wunsch innovative Technologien für den wirtschaftlichen Erfolg zu nutzen und diese durch entsprechende Security-Maßnahmen abzusichern, ohne die Kernautomatisierung zu beeinträchtigen, ist aktuell die größte Herausforderung der Prozessautomatisierung.

Nachfolgend werden zwei Architekturmodelle vorgestellt, die zurzeit für die Vernetzung interner und externer Dienste diskutiert werden.

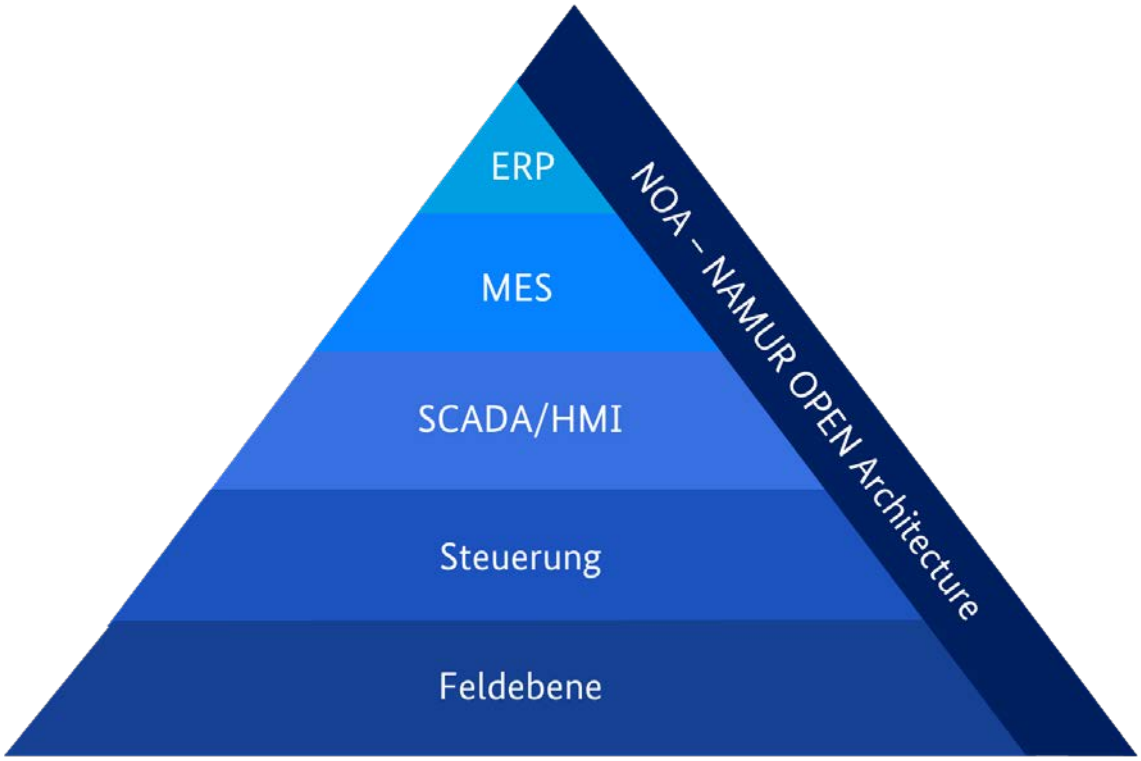

Abbildung 16 NAMUR Open Architecture (NOA) in Anlehnung an (19)

NAMUR Open Architecture (NOA) beschreibt eine zukunftsgerichtete Netzwerkarchitektur (vgl. Abbildung 16) als eine Konzeption, mit der sich IoT-Technologien rückwirkungsfrei nutzen lassen. Die klassische Automatisierungspyramide wird zu diesem Zweck um einen rückwirkungsfreien NOA-Seitenkanal erweitert. Das bestehende Automatisierungssystem bleibt unverändert. In den NOA-Seitenkanal lassen sich Daten aus allen Ebenen der Automatisierungspyramide übertragen. Hierbei werden rückwirkungsfreie Schnittstellen verwendet, die den Datenexport nur in den NOA-Seitenkanal gestatten. Ein automatischer Rückkanal soll nicht möglich sein, da es sich um eine Art Diode handelt. Diese lässt nur Datenverkehr in eine Richtung zu. Ein Rückfluss von Informationen erfordert eine explizite Freigabe.

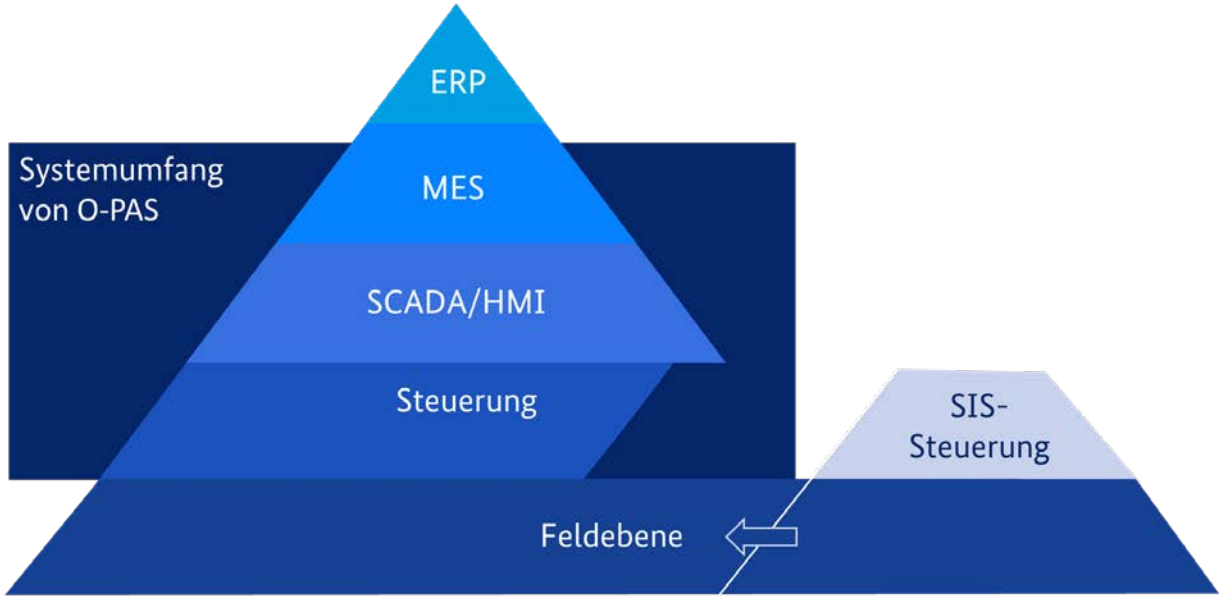

Abbildung 17 Open Process Automation Standard (O-PAS)

Eine alternative Lösung, die mehr Flexibilität bei gleichbleibender Sicherheit bietet, ist im Open Process Automation Forum in Diskussion (vgl. Abbildung 17). Im Gegensatz zu NOA wird im Open Process Automation Standard (O-PAS) das die PLT-Sicherheitseinrichtung aus dem restlichen Netzwerk herausgelöst. Auf der gemeinsamen Feldebene ließe sich dann ebenfalls mittels Datendiode eine rückwirkungsfreie, unidirektionale Kommunikation herstellen.

In den beiden Netzarchitekturmodellen O-PAS und NOA übernehmen Datendioden die Aufgabe der rückwirkungsfreien und sicheren Kommunikation. Die Datendiode und weitere OT-Security Techniken gehören somit zu den neuen Technologietrends der Prozessautomatisierung.

3.5 OT-Security

Die Integrität der Systemdaten, die Cyber-Sicherheit der Datenprotokolle, die Administration der vernetzten Systeme und deren Einbindung in segmentierte Netzwerkarchitekturen sind Aufgaben und Herausforderung der OT-Security, die sich aus den Technologietrends der Industrie 4.0 ergeben. Somit gehört die OT-Security ebenfalls zu einem wichtigen Technologietrend.

Im Geltungsbereich der 12. BImschV wurden mit dem Leitfaden „Maßnahmen gegen Eingriffe Unbefugter“ (KAS-51) von der KAS Schutzmaßnahmen gegen IT-Risiken definiert (vgl. Abbildung 18). Die Basismaßnahmen gelten für alle Störfallbetriebe. Ob darüber hinaus weitere Maßnahmen zu treffen sind, entscheidet sich in der Sicherungsanalyse. Besteht für Anlagenbereiche ein erhöhter Schutzbedarf, beschreibt die KAS-51 für diese ergänzende Maßnahmen.

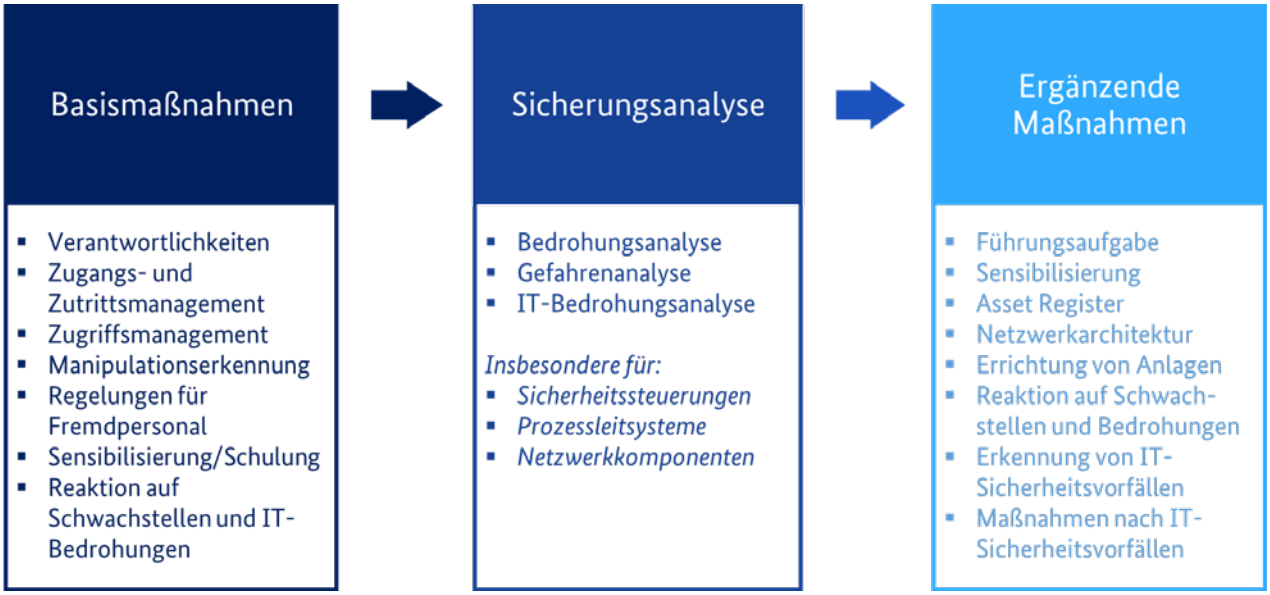

Abbildung 18 OT-Security auf Basis der KAS-51

Zur inhaltlichen Ausgestaltung der Maßnahmen verweist die KAS-51 z. B. auf die ISO 27001 (vgl. Kapitel 4.2). In Bezug auf die eingangs beschriebenen Security Herausforderungen der Industrie 4.0 liefern die KAS-51 und ISO 27001 jedoch nicht immer konkrete Anleitung, wie die OT-Security im Einzelfall auszusehen hat. Zum Schutz gegen Schadsoftware definiert die ISO 27001 zum Beispiel als Ziel: „Erkennungs-, Vorbeugungs- und Wiederherstellungsmaßnahmen zum Schutz vor Schadsoftware in Verbindung mit einer angemessenen Sensibilisierung der Benutzenden ...“ vorzusehen (20). Eine Antwort auf die Frage, welche Maßnahme dazu geeignet ist, Schadsoftware auf einer SPS zu detektieren, beantwortet die ISO 27001 nicht. Recherchen zu geeigneten OT-Security Maßnahmen - wie dieser - stellt viele Anwender vor eine große Herausforderung.

Die ISA (International Society of Automation) Global Cyber-Security Alliance hat zu diesem Zweck das “Top 20 Secure PLC Programming Practices” initiiert. Im Artikel „Security für die SPS-Programmierung“ (18) berichtet Sarah Fluchs über erste Vorschläge, die von der Projektgruppe erarbeitet wurden. In Bezug auf das hier beschriebene Problem schreibt sie:

Während Antivirenprogramme, Prüfsummen oder Hashes zur Integritätsprüfung aufgrund des Ressourcenverbrauchs für SPS ggf. ungeeignet sind, lässt sich die Plausibilität vorhandener Daten, wie die SPS Zykluszeiten, recht einfach nutzen. Plötzliche Änderungen der SPS Zykluszeiten können als Indikator für Änderungen in der SPS-Logik (z.B. durch eine Schadsoftware) genutzt werden.

Ziel des Projektes ist es OT-Security Maßnahmen, z.B. in der IEC 62443, konkreter beschreiben zu können.

Im Zuge der fortschreitenden Digitalisierung sollten folgende Fragen geklärt sein:

- Wer übernimmt die Verantwortung für den Ausbau und die Pflege der OT-Netzwerke?
- Welche Referenzarchitektur (NOA oder O-PAS) beschreibt im Unternehmen die zur Integration von IoT-Technologien angestrebte Netzwerktopologie am besten?
- Wie lassen sich die Anforderungen der KAS-51 technologisch in den bestehenden Anlagen umsetzen?

3.6 Trends und mögliche Risiken für die Anlagensicherheit

Nach den Wegbereitern für Industrie 4.0 und deren Herausforderungen werden im Weiteren zu einer Auswahl von speziellen Technologietrends die potentiellen Auswirkungen auf den Betrieb oder die Anlagensicherheit bewertet. Hierbei werden sowohl Security Einrichtungen als auch neue datenbasierte Technologien betrachtet. Bei diesen Technologien werden jeweils ihr Nutzen sowie mögliche Probleme und sich ändernde Tätigkeiten in den Blick genommen.

3.6.1 Firewall

Abbildung 19 Vor- und Nachteile von Firewalls

Firewalls sind ein sehr wichtiges Cyber-Sicherheitswerkzeug, das den Datenverkehr auf zuvor definierte Kommunikationsbeziehungen einschränkt. Mithilfe einer Firewall wird letztlich definiert, welche Komponente auf welchem Weg mit wem kommunizieren darf. In einem Industrienetzwerk fungiert eine Firewall als segmentierende Komponente, die z.B. das sensible OT-Netzwerk von dem Büronetzwerk trennt. Firewalls finden ihren Nutzen jedoch nicht nur in der Trennung des Office-Netzes vom OT-Netzwerk. Sie können auch innerhalb eines Netzwerks zur Zonierung eingesetzt werden.

Um Firewalls effektiv zu nutzen, ist es für Betreiber industrieller Anlagen sinnvoll, eine Übersicht über die zu schützenden Assets zu besitzen (Asset Management). Dies kann mit sogenannten Inventarisierungstools

relativ schnell und effizient erreicht werden. Zudem sollten Kommunikationsverbindungen der Komponenten untereinander (z.B. Datenflüsse) bekannt sein, um Firewalls entsprechend zu konfigurieren. Die Konfiguration des Regelwerks von Firewalls sollte dokumentiert werden, damit diese langfristig nachvollziehbar ist. Insbesondere sollten Änderungen nur von dazu autorisierten Personen (am besten nach dem Vieraugenprinzip), sowie basierend auf nachvollziehbaren Entscheidungen (am besten mittels Änderungsantrag), vorgenommen werden. Des Weiteren sollten im Rahmen fixer Zyklen Wartungsarbeiten durchgeführt werden. Dazu gehört, dass die Regelverwaltung hinsichtlich ihrer Aktualität geprüft wird. Darüber hinaus sollten Sicherheitsupdates, die vom Hersteller bereitgestellt werden, kurzfristig installiert werden. Im Rahmen der zyklischen Wartungsarbeiten sollten regelmäßige Backups der Firewallregeln sowie der verwendeten Firmware der Geräte erstellt werden. Die Backups werden für den Fall eines Defekts zur Neuinstallation oder für die Konfiguration eines Ersatzgeräts benötigt. Dies trägt zu einer zügigen sowie sicheren Wiederinbetriebnahme einer industriellen Anlage bei.

3.6.2 Datendiode

Abbildung 20 Vor- und Nachteile von Datendioden

Eine Datendiode bewirkt, 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 sowie 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 aus 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 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 Bereich oder Gültigkeit erfolgen.

Aufgrund des Aufwands und der Einschränkungen ist eine solche Datendiode nur für sehr sensible Anwendungsbereiche sinnvoll.

3.6.3 Public Key Infrastructure

Abbildung 21 Vor- und Nachteile von Public-Key-Infrastrukturen

Eine Public Key Infrastructure (PKI) ist ein System, welches der Ausstellung, Verteilung und Prüfung digitaler Zertifikate dient und hierarchisch aufgebaut sein kann. Ein Zertifikat bindet einen öffentlichen Schlüssel kryptographisch gesichert an die Identität der Instanz, der der zugehörige (geheim zu haltende) private Schlüssel gehört. Die Technologie der PKI bietet einen hohen Vertrauensgrad in die Datenintegrität. Diese Kombination kann zur Verschlüsselung bzw. Signierung von Daten oder zur Authentifizierung elektronischer Ausweisdokumente sowie zur Sicherstellung der Echtheit aller Einheiten in einem Netzwerk genutzt werden.

Inzwischen gibt es für den sicheren Datenaustausch zwischen Betreibern und Wartungsunternehmen auch Lösungen für den Einsatz in der Industrie. Die Kommunikation von Systemen bis hin zur automatisierten Kommunikation zwischen Maschinen, machine-to-machine communication (M2M-Communication), kann abgesichert werden. Der Einsatz von Verschlüsselungstechnologien in der Automatisierungstechnik ist bisher noch wenig verbreitet, bietet jedoch große Vorteile hinsichtlich der Wahrung der betrachteten Schutzziele Vertraulichkeit und Integrität sowie Authentizität. PKI als Lösung für die OT-Security ist jedoch aufgrund von Faktoren wie ressourcenbeschränkten Umgebungen, Bandbreitenüberlegungen und harten Echtzeit-Kommunikationsanforderungen eine Herausforderung und bedarf einer korrekten Verwaltung digitaler Zertifikate. Eine PKI-Infrastruktur für ICS-Netzwerke stellt für Unternehmen eine Herausforderung dar.

3.6.4 Intrusion Detection System / Anomaly Detection System

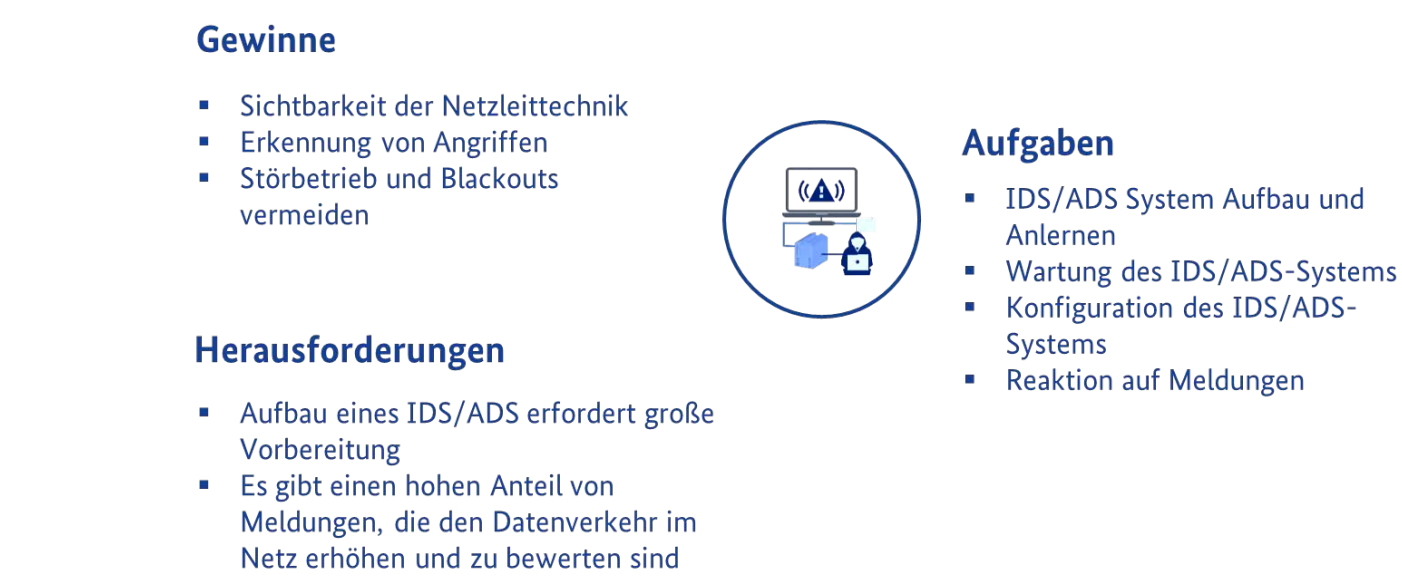

Abbildung 22 Vor- und Nachteile von IDS und ADS

Firewalls können das Netzwerk nicht vor allen Angriffen, wie u.a. Malware oder Zero-Day-Angriffen, schützen. Ein Zero-Day-Angriff ist das Ausnutzen der Schwachstellen des Systems, die den Benutzenden und Anbietenden noch nicht bekannt sind. Dazu zählt auch das Ausnutzen und Manipulieren, bevor die Schwachstelle den Benutzenden oder Anbietenden bekannt wird oder es einen wirksamen Patch oder Fix für die Beseitigung der Schwachstelle gibt. Der Schutz des Netzwerks vor solchen Exploits und solcher Malware ist ebenfalls ein notwendiger Aspekt. Ein Intrusion Detection System (IDS) ist ein System, das den Datenverkehr überwacht und die Angriffsversuche erkennt und die Administration alarmiert.

Industrielle Anomaly Detection Systeme (ADS) überwachen, als industrielles Netzwerkmonitoring mit Anomalieerkennung, die gesamte Kommunikation innerhalb der Prozess- und Netzleittechnik.

Bevor IDS bzw. ADS sinnvoll eingesetzt werden können, muss diesen Systemen der „Normalzustand“ des zu überwachenden Netzes bekannt sein. Dazu wird die Kommunikation in Lernphasen aufgezeichnet und nach der Bewertung als normal deklariert. Die Bewertung erfolgt automatisiert durch vorher festgelegte Regeln sowie manuell für Ereignisse, die vom vorhandenen Regelwerk nicht erfasst werden. Erstmalig auftretende Ereignisse stellen immer eine Anomalie dar. In der industriellen Automation ist es nicht selten, dass manche Funktionen nur wöchentlich oder monatlich ausgeführt werden, wodurch die Lernphase sich über einen längeren Zeitraum erstrecken kann. Jede Änderung am System bedingt damit aber auch eine Anpassung der Erkennungssysteme.

Mit dem Anlernen des Systems ist die Arbeit für den Betreiber jedoch nicht beendet. Die generierten Meldungen über mögliche Cyber-sicherheitskritische Ereignisse müssen auch ausgewertet werden. Es ist also eine dauerhafte, kontinuierliche Befassung damit verbunden, die sich nicht nur auf die Einrichtung und Anpassungen beschränkt. Dies sollte bei der Planung der notwendigen Ressourcen berücksichtigt werden.

3.6.5 Modulare Automation

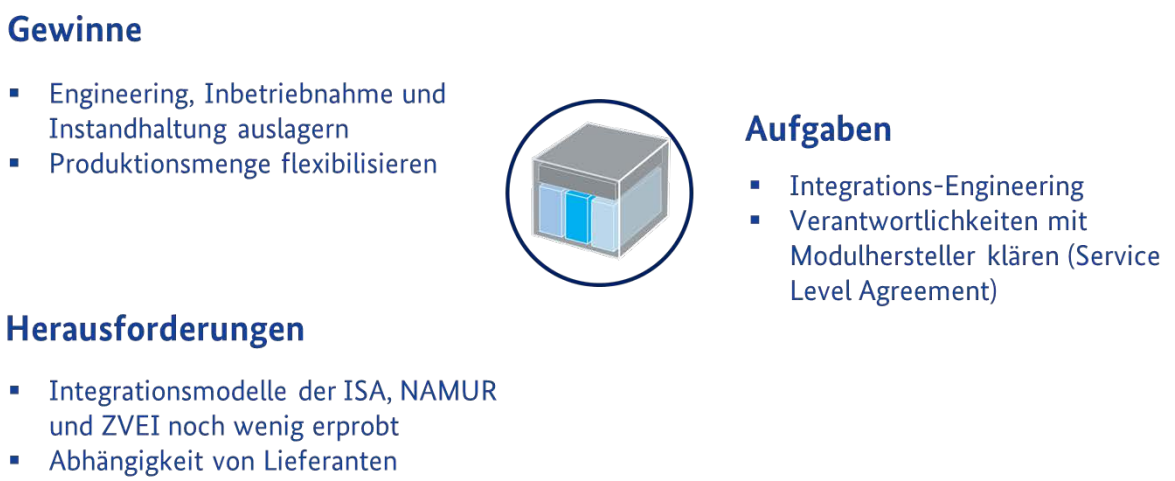

Abbildung 23 Vor- und Nachteile der Modularen Automation

Im ZVEI Whitepaper „Modulbasierte Produktion in der Prozessindustrie“ (21) ist zu lesen, dass modulare Automation durch Kapselung der verfahrenstechnischen Funktionen die Komplexität verringert sowie Aufwände für Engineering, Inbetriebnahme und Instandhaltung abnehmen. Diese positiven Eigenschaften lassen sich einfach durch die Phrase „Plug & Produce“ beschreiben. Manchen mag die Phrase an die Anfänge der Plug & Play Eigenschaft von Windows 95 erinnern. Hat „Plug & Produce“ heute schon den Reifegrad, um die zentrale Automatisierung in der durch Ansätze vorhandenen dezentralen Automatisierung abzulösen?

Die Steuerung und Regelung des Moduls im Anlagenbetrieb wird auf die Basisautomation und auf die übergeordneten Automatisierungssysteme aufgeteilt. Die Basisautomation steuert und überwacht die Prozesse des Moduls und umfasst ggf. auch ein eigenständiges PLT-Sicherheitseinrichtung. Ferner umfasst die Basisautomation eine Kommunikationseinheit, die Daten mit den übergeordneten Automatisierungssystemen des Betreibers und externen Fernwartungsdiensten austauscht.

Es existiert eine verteilte Automatisierungsintelligenz in den einzelnen Modulen. Dies spart (Engineering-)Zeit, denn bei der Inbetriebnahme ist die Software und Logik in den einzelnen Modulen bereits vorhanden und getestet. Der Nachteil dieser Lösung ist, dass momentan nur sehr wenig Erfahrung vorliegt, wie eine verteilte Automatisierungsintelligenz flexibel zu einer Gesamtapplikation zusammengefügt wird. Gerade bei Multi-Vendor-Modulen mit unterschiedlichen Automatisierungssystemen kann diese Aufgabe schnell recht komplex werden. Des Weiteren ergeben sich noch ungelöste Herausforderungen bei der Bewertung der Safety. Dazu gehört unter anderem, welche Freigaben nach dem Zusammenfügen erteilt werden. Es stellt sich die Frage, ob eine erneute Zertifizierung des „neuen“ Safety-Systems notwendig ist oder ob die der Einzelmodule ausreichen. Diese Fragestellung ist noch unbeantwortet und wird in Expertenkreisen diskutiert.

3.6.6 Fernwartung

Abbildung 24 Vor- und Nachteile von Fernwartung

Die Wartung und Pflege der automatisierten Anlagen erfolgt heute überwiegend durch den Anlagenbetreiber selbst. Bei dem Einsatz von Automatisierungsmodulen muss der Hersteller verstärkt eingebunden werden, so dass dieser entweder vor Ort präsent sein muss oder ihm umfangreiche Fernwartungsmöglichkeiten eingeräumt werden müssen. Darüber hinaus ermöglicht die Fernwartung, z.B. in Zeiten von Pandemien, den Zugriff für die Arbeitskräfte aus dem Homeoffice.

Schnittstellen für die Fernwartung und das Einbringen von Daten in das Automatisierungssystem des Moduls müssen jedoch in das IT-Securitykonzept des Betreibers integrierbar sein. Dabei muss auch sichergestellt werden, dass nur die Personen Zugriff erlangen können, die diesen auch benötigen. Hier ist auch zwischen verschiedenen Rollen zu unterscheiden. Rufen Sie sich in Erinnerung, dass erfolgreiche Cyber-Kriminelle bei einer integrierten Steuerung theoretisch Zugriff auf Funktionen des PLS und SIS haben. Dann ist es nachvollziehbar, dass Schnittstellen der Fernwartung sehr kritisch zu betrachten sind und ein erhöhter Schutzbedarf in Bezug auf das IT-Securitykonzept des Betreibers zu realisieren ist.

Im Einzelnen sind die spezifischen Anforderungen an garantierte und verfügbare Leistungen und Security Standards durch Serviceverträge mit den Herstellern bzw. Lieferfirmen abzustimmen. Die Security Lösungen zum Datenaustausch zwischen den Modulen und der Anlage, sind zusammen mit dem Hersteller im Rahmen einer Risikoanalyse zu bewerten. Remoteverbindungen, die für das Patch-Management oder insbesondere die kontinuierliche Zustandsüberwachung benötigt werden, erfordern einen hohen Schutz gegen Cyber-Bedrohungen. Fragestellungen des Datenschutzes, der Datensicherheit, unterschiedliche Akzeptanz der Arbeitskräfte, vertragliche Abstimmungen mit Lieferfirmen und Dienstleistungsunternehmen sowie unklare Verantwortlichkeiten, sind einige der hierbei zu meisternden Herausforderungen.

Hierbei können z.B. der BSI Grundschutz Baustein OPS.2.4 – Fernwartung (22) oder die acht BSI-Grundregeln zur Absicherung von Fernwartungszugängen (23) als Erkenntnisquelle herangezogen werden.

3.6.7 Integrierte Steuerung

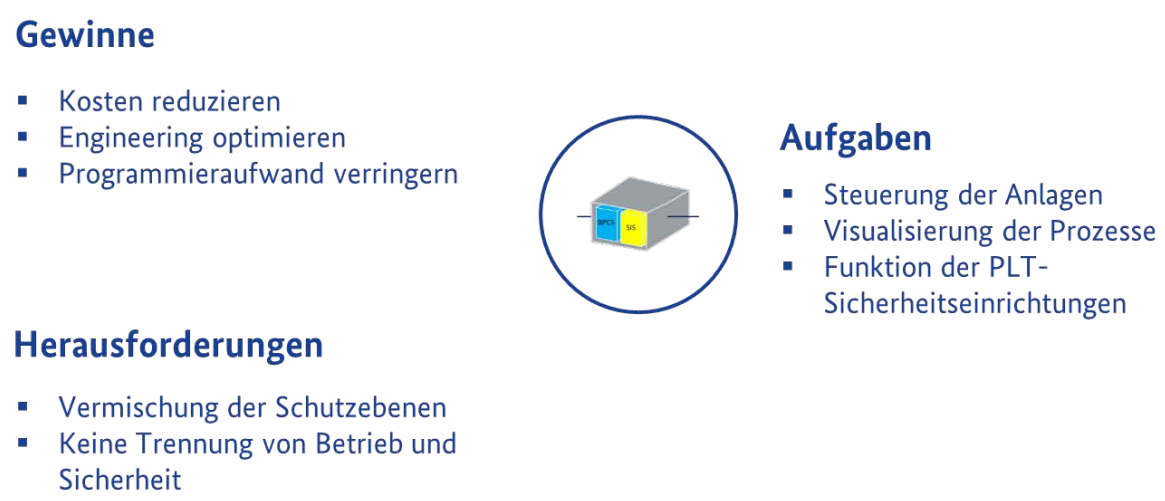

Abbildung 25 Integrierte Steuerungen

Eine integrierte Steuerung vereint in einer Komponente betriebliche Steuerungsaufgaben des PLS sowie sicherheitsrelevante Aufgaben der PLT-Sicherheitseinrichtung. In Bezug auf die einfache Ersatzteilhaltung, den geringeren Schulungsaufwand für den Programmierenden und den optimierten Platzbedarf im Schaltschrank, erfreut sich die integrierte Steuerung zunehmender Beliebtheit. Die Hardware für die integrierte Steuerung besteht aus einem oder mehreren Controllern, welche PLS- und PLT-S-Funktionen in einem Gehäuse wahrnehmen. Die Ein- und Ausgangsmodule, die als Schnittstelle zu den Feldgeräten dienen, sind hierbei mit der integrierten Steuerung verbunden. Im Allgemeinen werden betriebliche und sicherheitsrelevante Funktionen auf getrennte I/O-Module aufgeteilt. Die Trennung der Aufgaben des PLS und des PLT-S - und damit auch die rückwirkungsfreie Trennung der Schutzebenen - erfolgt in vielen integrierten Steuerungen größtenteils nur auf Basis der Software.

Diese Gerätearchitektur führt dazu, dass eine Arbeitskraft oder auch potentielle Angreifende Zugriff nur auf eine Steuerung erhalten müssen, um sowohl die betrieblichen als auch die Sicherheitsfunktionen zu manipulieren. In einem Betriebsbereich wäre es somit möglich, sowohl den Anforderungsfall einer Störung auszulösen, als auch die dafür vorgesehene PLT-Sicherheitseinrichtung zu deaktivieren, also den Zugriff auf zwei Schutzebenen zu erhalten. Zum Beispiel könnte durch das fehlerhafte Öffnen einer Regelarmatur der Auslegungsdruck in einem Behälter die zulässigen Grenzen überschreiten, was ein Bersten des Behälters zur Folge hätte. Gemäß der sicherheitstechnischen Auslegung soll die PLT-Sicherheitseinrichtung bei Überschreitung des Grenzwertes (Druck sehr hoch) zum Abschalten der Förderpumpe führen und den Schaden verhindern. Hat eine cyber-kriminelle Person einmal Zugriff auf die integrierte Steuerung erlangt, dann hat sie auch Zugriff auf die PLT-Sicherheitseinrichtung und kann diese theoretisch unwirksam machen. Der Schadensfall würde eintreten.

Eine praktische Anleitung zur Absicherung von PLT-Sicherheitseinrichtungen gegen Cyber-Risiken, ist im NAMUR Arbeitsblatt NA 163 für die klassische Trennung der Schutzebenen unter Verwendung von zwei Steuerungen (eine für das PLS und eine für das SIS) enthalten. Für Systeme mit integrierten Steuerungen funktionieren diese Konzepte allerdings nicht. Die ausschließlichen Betrachtungen aus Sicht der Normen der Funktionalen Sicherheit sind an dieser Stelle ebenfalls nicht ausreichend. Gemäß den Festlegungen der IEC 61508, IEC 61511 und dem NAMUR Arbeitsblatt NA 163 wird in diesem Zusammenhang z.B. die Normenreihe IEC 62443 referenziert. In den Teilen IEC 62443-3-2 und IEC 62443-3-3 ist eine Methode zur Durchführung von Risikobeurteilungen und Anforderungen an die OT-Security beschrieben. Schlussendlich muss diese aber in Zusammenarbeit mit dem jeweiligen Hersteller durchgeführt werden, da der Betreiber oder Integrator nicht über die notwendigen technischen Informationen verfügt.

Unabhängig von der Risikobetrachtung ergibt sich für den Betreiber ein deutlich erhöhter Aufwand sowohl in der Planung als auch im Betrieb, um Security und die Aufrechterhaltung der Safety nachzuweisen und sicherzustellen. Dies auch aufgrund der zuvor beschriebenen Möglichkeiten der Fernwartung.

3.6.8 Plant Information Management System (PIMS)

Abbildung 26 Vor- und Nachteile von PIMS

Ein Plant Information Management System kann in einem Unternehmen eine Vielzahl von Aufgaben wahrnehmen. Es kann

- zur Bereitstellung von Prozessdaten im Unternehmen dienen,
- zur Durchführung aufwendiger Berechnungen genutzt werden, die z.B. im PLS nicht möglich wären oder
- zur Langzeitarchivierung der Anlageninformationen dienen.

In Bezug auf die Cyber-Sicherheit unterhält das Plant Information Management System eine dauerhafte Verbindung zum Steuerungs- bzw. Leitsystem der Anlage oder sogar der SSPS und muss mit dem Firmennetzwerk und darüber hinaus vielleicht sogar mit dem Internet Informationen austauschen. Dadurch besteht die Möglichkeit, dass diese Infrastruktur als Einfallstor genutzt wird.

Zugriff auf das Plant Information Management System können dementsprechend auch eine größere Anzahl von (unternehmensinternen/-externen) Nutzenden haben. Die Daten werden z.B. für Anwendungen der Produktionsplanung verwendet und ggf. Arbeitsergebnisse zurück in die Steuerungs- und Leitsysteme der Anlage übertragen. In diesem Fall benötigen Abteilungen, die mit der Prozessoptimierung arbeiten, Lese- oder Schreibzugriffe.

Fehlerhafte bzw. veränderte Daten können unterschiedliche Folgen haben. Angenommen eine angreifende Person erhält über das Plant Information Management System Zugriff auf Daten, Parameter oder Softwarestände der betrieblichen Steuerung oder gar der Sicherheitssteuerung, dann kann dies relevante Auswirkungen auf die Anlagenverfügbarkeit, die Produktivität, die Produktqualität und auch auf die Anlagensicherheit haben.

Die Verwaltung von Nutzenden, die Konfiguration und die Netzwerksegmentierung erfordert intelligente Konzepte. Ein sicherer Betrieb und der Schutz gegen Angreifende erfordert systematische Analysen und eine Bewertung nicht nur des Plant Information Management Systems, sondern auch des Netzwerks, in das es eingebettet ist. Durch unter Umständen sehr komplexe Verbindungen, kann eine Bewertung sehr aufwendig werden. Wenn z.B. Daten aus der Simulation in das Produktivsystem übertragen werden sollen, ist es erforderlich sicherzustellen, dass diese keine kritischen Veränderungen enthalten.

Hierbei können z.B. der BSI Grundschutz Baustein APP.5.1 – Allgemeine Groupware oder Baustein NET.1.2 Netzwerkmanagement zur Absicherung von Plant Information Management Systemen als Erkenntnisquelle herangezogen werden (24).

3.6.9 Digitaler Zwilling

Abbildung 27 Vor- und Nachteile digitaler Zwillinge

Wenn nun nicht ausschließlich, wie bei dem Plant Information Management System, Prozessdaten digital verfügbar sind, sondern auch die zugehörige Anlagendokumentation und Prozessteuerungssoftware, dann käme dies einem digitalen Zwilling der Anlage sehr nahe. Ein digitaler Zwilling repräsentiert ein reales Objekt in der digitalen Welt. Es kann sich um materielle Teilanlagen oder immaterielle Daten und Software handeln. Die digitalen Zwillinge sind selbst aus Daten und Algorithmen aufgebaut und können über Sensoren mit der realen Welt gekoppelt sein. Der digitale Zwilling beinhaltet virtuell die Eigenschaften und das Verhalten der realen Objekte. Der Zwilling ist somit ein datenbasiertes Modell einer bestehenden oder geplanten Anlage, mit dem sich Simulationen, Analysen und Tests durchführen lassen. Derzeit sind Anwendungen in der Prozessindustrie, aufgrund des über den Lebenszyklus betrachteten hohen Aufwands zur Synchronisierung der Prozessanlage (as-built), mit dem digitalen Zwilling selten (25). Der digitale Zwilling könnte für serienmäßig gefertigte Anlagen gleicher Bauart (z.B. Package Units) bei der Entwicklung, Optimierung, Wartung und Instandhaltung von höherem Nutzen sein. Anlagendaten werden interpretiert und für den digitalen Zwilling lesbar gemacht oder sind Bestandteil eines integrierten Workflows. Basierend auf den Anlagendaten (z.B. R&I, Funktionsgruppenpläne, 3D-Modelle etc.) werden Informations- und Simulationsmodelle entwickelt, mit denen die nutzende Person über HMI interagieren kann.

Der digitale Zwilling kann somit als konsistente Anlagendokumentation zu einem wesentlichen Bestandteil des Engineering Prozesses werden. Das bedeutet auch, dass die Integrität der Daten für den sicheren Betrieb von hoher Bedeutung ist. Die Daten des Informationsmodells, als auch die der angebundenen Sensoren, sind gegen Manipulation zu schützen. Auch bedarf es einer Backupstrategie für den Fall eines Datenverlustes. Insbesondere sind Schnittstellen, über die der digitale Zwilling mit Onlinedaten aus der Real-Anlage versorgt wird, in einer Risikoanalyse zu überprüfen und zu schützen.

Zudem ist der digitale Zwilling der Anlage vor unberechtigtem Zugriff zu schützen. Angreifer können diesen aufgrund des realistischen Verhaltens auch für die Planung von Angriffen nutzen, da alle relevanten Informationen in den Modellen vorliegen. Es wäre dann möglich auch sehr komplexe Angriffe vorzubereiten.

Risiken und geeignete Security Maßnahmen können z.B. unter Verwendung des IT-Grundschutz Bausteins SYS.1.5 (22) Virtualisierung definiert werden.

4 Regelwerke, Normen und gesetzliche Anforderungen

Anlagen zur Lagerung oder zur Produktion von bestimmten Stoffen und Gütern bedürfen seit 1974 einer Genehmigung nach dem Bundes-Immissionsschutzgesetz (BImSchG). Wie im deutschen Recht üblich, ist in diesem Gesetz auch eine Ermächtigung zum Erlass von Rechtsverordnungen in § 7 BImSchG enthalten. Daraufhin wurde in der 4. Verordnung zum Bundes-Immissionsschutzgesetz (4. BImSchV) geregelt, welche Anlagen genehmigungsbedürftig sind. Für diese genehmigungsbedürftigen Anlagen gilt der Abs. 2 des § 1 des BImSchG. Danach sollen die Betreiber zum einen die Emissionen verringern oder vermeiden und zum anderen Schutz und Vorsorge gegen Gefährdung, erhebliche Nachteile und erhebliche Belästigungen, die auf andere Weise herbeigeführt werden, treffen.

Im europäischen Recht wurde nach dem folgenschweren Industrieunfall in Seveso, Italien, von 1976 im Jahr 1982 die Seveso-I-Richtlinie erlassen. Diese schreibt den Industriebetrieben vor, Schutzmaßnahmen gegen mögliche Betriebsstörungen zu treffen. Das passende Gegenstück im deutschen Recht hierzu ist die 12. BImschV (erste Version 1982), die aufgrund des § 7 im BImSchG erlassen wurde.

Die 12. BImschV bestimmt, welche Anlagen ein besonderes Gefährdungspotential besitzen, um die Menschen und die Umwelt im Störfall nachhaltig zu schädigen. Als Beispiele hierfür kann die Freisetzung von Dioxin in Seveso, der Großbrand einer Chemikalienlagerhalle bei der Fa. Sandoz in Schweizerhalle oder auch die Explosion des Kraftstofftanklagers in Buncefield herangezogen werden.

Die 12. BImschV bietet den Rahmen für alle weiteren Überlegungen. Nach dem § 3 Abs. 2 der 12. BImschV sind zur Erfüllung der Pflichten, neben den betrieblichen und umgebungsbedingten Gefährdungen, auch die Eingriffe Unbefugter zu untersuchen.

Das bedeutet nichts anderes, als dass vermutet wird, dass solche Anlagen mit besonderem Gefährdungspotential auch prinzipiell für Cyber-Angriffe in Frage kommen.

Die 12. BImschV setzt damit auch den Rahmen für die weitere Betrachtung der Cyber-Security in diesen Anlagen. Grundsätzlich gilt, dass Anlagen nach dem Stand der Technik / Stand der Sicherheitstechnik zu errichten und zu betreiben sind § 5 (1) Nr. 2 BImSchG bzw. § 3 (4) 12. BImSchV. Die Ausgestaltung dieses Rahmens unterliegt dann der nachfolgenden Erstellung von Leitfäden, Normen, Standards und Vorschriften.

Hierbei ist zu berücksichtigen, dass der Betreiber nicht an diese gebunden ist. Wenn jedoch davon abgewichen wird, muss nachgewiesen werden, das die von ihm getroffenen Maßnahmen mindestens gleichwertig zum Stand der Technik / Stand der Sicherheitstechnik sind. Dieser wird wiederum durch Leitfäden, Normen, Standards und Vorschriften definiert ist. Darüber hinaus kann es Vereinbarung mit dem Betreiber geben, sei es

- durch die Anordnung in der jeweiligen Norm selbst (z.B. Technische Regel brennbare Flüssigkeiten 100 zur Verordnung über brennbare Flüssigkeiten (VbF 80); Hier wurde eine Nachrüstpflicht für Brandschutzmaßnahmen bei Lagerung von entzündbaren Flüssigkeiten nach dem Brand bei Sandoz in Schweizerhalle festgelegt).
- durch Erwähnung in einem Genehmigungsbescheid nach BImSchG (z.B. Verwendung der VDI 2180 hinsichtlich der SIL Klassifizierung der PLT-Sicherheitseinrichtungen oder auch von Maßnahmen hinsichtlich Cyber-Angriffen) oder
- durch einen privatrechtlichen Vertrag zwischen Behörde und Betreiber.

Es besteht grundsätzlich die Verpflichtung des Betreibers den Stand der Technik, oder nach der 12. BImschV den Stand der Sicherheitstechnik, zu berücksichtigen und seine Anlagen regelmäßig darauf hin zu prüfen. Zur Bestimmung des Standes der Technik existiert unter anderem ein KAS-Leitfaden (SFK-GS 33). Die zunehmende Dynamik der technologischen Entwicklung stellt in Verbindung mit der Cyber-Sicherheit jedoch eine besondere Herausforderung dar.

Hinsichtlich der jetzt aktuellen Betrachtung der IT-/OT-Security folgt daraus, dass beispielsweise die Anwendung der DIN EN IEC 62443 in der Regel durch den Betreiber freiwillig erfolgen muss, es sei denn, es besteht die Möglichkeit der Anordnung dieser Norm, z. B. im Rahmen eines Genehmigungsverfahrens oder einer Gefahrenabwehr.

Im weiteren Verlauf sind die gesetzlichen Grundlagen nochmal zusammenfassend dargestellt.

4.1 Gesetze und Verordnungen

In den folgenden Seiten werden gesetzliche Vorgaben, die dieses Forschungsprojekt berühren, zusammenfassend dargestellt.

4.1.1 IT-Sicherheitsgesetz (IT-SiG)

Vollständiger Name: Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)

Im Juli 2015 ist das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) in Kraft getreten. Das IT-Sicherheitsgesetz ist ein Artikelgesetz, das u.a. das BSI-Gesetz ändert und ergänzt. Das IT-Sicherheitsgesetz leistet einen Beitrag dazu, die IT-Systeme und digitalen Infrastrukturen Deutschlands zu den sichersten weltweit zu machen.

Ziel des IT-Sicherheitsgesetzes ist die Verbesserung der IT-Security bei Unternehmen und in der Bundesverwaltung, sowie ein besserer Schutz der Bürgerinnen und Bürger im Internet. Neben o. g. Akteuren gelten einzelne Regelungen des IT-Sicherheitsgesetzes daher auch für Betreiber von kommerziellen Webangeboten, die höhere Anforderungen an ihre IT-Systeme erfüllen müssen. Auch Telekommunikationsunternehmen sind künftig stärker gefordert. Sie werden verpflichtet, ihre Kundschaft zu warnen, wenn sie einen Missbrauch eines Anschlusses feststellen. Zusätzlich sollen sie den Betroffenen, wenn möglich, Lösungsmöglichkeiten aufzeigen. Die zuständige Aufsichtsbehörde ist in diesen Fällen die Bundesnetzagentur. Um diese Ziele zu erreichen, wurden u. a. die Aufgaben und Befugnisse des BSI (siehe BSI-Gesetz) ausgeweitet.

Tabelle 2 Relevanz des IT-Sicherheitsgesetzes

Rolle	***Relevanz***
Integratoren	nicht relevant
Hersteller	ggf. relevant
Planung	ggf. relevant
Betreiber	relevant
Einkauf	relevant
Management	relevant
IT-Experten	ggf. relevant

4.1.2 BSI-KritisV

Name: Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz[1]

Die Verordnung unterstützt Betreiber von Anlagen, Systemen oder Dienstleistungen sowie Behörden bei der Feststellung, ob ein Betrieb als Teil der kritischen Infrastruktur anzusehen ist und besondere Anforderungen erfüllen muss. Kritische Infrastrukturen sind von wesentlicher Bedeutung für die Aufrechterhaltung der Gesundheit, Sicherheit, dem wirtschaftlichen und sozialen Wohlergehen der Bevölkerungen.

Die Verordnung wurde aufgrund der Änderungen des BSI-Gesetzes durch das ITSiG erlassen und umfasst Kriterien zur Einstufung von Anlagen der Sektoren für kritische Infrastrukturen (Energie, Wasser, Ernährung, Informationstechnik und Telekommunikation, Gesundheit, Finanz- und Versicherungswesen, Transport und Verkehr). Regelungen zur Verbesserung der Verfügbarkeit und Sicherheit der IT-Systeme, speziell im Bereich der Kritischen Infrastrukturen, sind im IT-Sicherheitsgesetz für die betreffenden Sektoren referenziert.

In Bezug auf die in dieser Studie behandelten Betriebsbereichen (gem. 12. BImSchV) hat die BSI-KritisV z.B. Relevanz für Raffinerien und Tankläger ab einer bestimmten Größe.

Tabelle 3 Relevanz der BSI-KRITISV

Rolle	*Relevanz*
Integratoren	relevant
Hersteller	nicht relevant
Planung	ggf. relevant
Betreiber	relevant
Einkauf	ggf. relevant
Management	relevant
IT-Experten	nicht relevant

4.1.3 NIS-Richtlinie

Name: Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie)[2]

Das Ziel der Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit ist es, ein höheres Niveau der Netz- und Informationssicherheit in der EU zu schaffen. Die EU-Mitgliedsstaaten mussten bis zum 09. Mai 2018 die NIS-Richtlinie in nationales Recht umsetzen. Die Richtlinie gilt für Betreiber wesentlicher Dienste, die in der EU niedergelassen sind. Ferner gilt sie für Anbietende digitaler Dienste, die Dienstleistungen für Personen innerhalb der EU anbieten. Die NIS-Richtlinie schreibt den Betreibern wesentlicher Dienste vor, geeignete technische und organisatorische Maßnahmen zur Sicherung ihrer Netzwerke und Informationssysteme zu ergreifen. Darüber hinaus sind Sicherheitsvorfälle zu verhindern oder zumindest die Auswirkungen zu verhindern, um die Geschäftskontinuität zu gewährleisten.

Mit der Richtlinie wurde ein einheitlicher Rechtsrahmen für den EU-weiten Aufbau nationaler Kapazitäten für die Cyber-Sicherheit, eine stärkere Zusammenarbeit der Mitgliedstaaten der Europäischen Union sowie Mindestsicherheitsanforderungen an und Meldepflichten für kritische Infrastrukturen geschaffen. Ferner wurde damit ein Rechtsrahmen für bestimmte Anbietende digitaler Dienste, wie Cloud-Services und Online-Marktplätze, geschaffen.

[1] https://www.gesetze-im-internet.de/bsi-kritisv/BSI-KritisV.pdf
[2] https://www.kritis.bund.de/SubSites/Kritis/DE/Aktivitaeten/Internationales/NIS_Richtlinie/NIS-Richtlinie_node.html

Tabelle 4 Relevanz der NIS-Richtlinie

Rolle	*Relevanz*
Integratoren	ggf. relevant
Hersteller	nicht relevant
Planung	nicht relevant
Betreiber	Relevant
Einkauf	nicht relevant
Management	nicht relevant
IT-Experten	nicht relevant

4.1.4 BSI-Gesetz (BSIG)

Name: Gesetz über das Bundesamt für Sicherheit in der Informationstechnik[3]

Das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) verfolgt das Ziel, die Informationssicherheit in Deutschland zu erhöhen. So fokussiert es im Kern das Bundesamt für Sicherheit in der Informationstechnik (BSI) und stattet es mit entsprechenden Rechten und Pflichten aus. Das BSIG enthält darüber hinaus Vorschriften, die sowohl Behörden als auch Unternehmen in Deutschland betreffen.

So definiert das Gesetz sogenannte kritische Infrastrukturen (KRITIS), die für die Versorgung der Bevölkerung notwendig sind. Diese unterliegen einem hohen Schutzbedarf und werden durch das Gesetz verpflichtet, Maßnahmen im Bereich der Informationssicherheit zu ergreifen. Die kritischen Infrastrukturen werden in neun Sektoren eingeteilt, zu denen u.a. der Sektor „Energie“ zählt. Die einzelnen Sektoren setzen sich aus verschiedenen Branchen zusammen, wie beispielsweise die Branchen Elektrizität, Gas, Mineralöl und Fernwärme, die den Sektor Energie bilden.

Das BSIG wird durch die „Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz“ (BSI-KritisV) ergänzt. In dieser werden die kritischen Infrastrukturen anhand von Schwellenwerten bestimmt. So sind Gasspeicher beispielsweise ab einer entnommenen Arbeit von 5.190 GWh pro Jahr als kritische Infrastruktur einzustufen.

Das BSIG schreibt vor, dass Betreiber kritischer Infrastrukturen ihre Maßnahmen zum Schutz der Informationssicherheitsziele Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit im Rhythmus von zwei Jahren von einer unabhängigen Partei prüfen lassen müssen. Die Ergebnisse müssen dem BSI vorgelegt werden. Zusätzlich sind die Betreiber dazu verpflichtet, Informationssicherheitsvorfälle einer zentralen Stelle des BSI zu melden.

Das Gesetz enthält Bußgeldvorschriften, die gegen Organisationen verhängt werden können, die das Gesetz missachten. Grundsätzlich stellt das BSIG das Pendant zur DSGVO dar. Während sich die DSGVO auf personenbezogene Daten beschränkt und Datenschutz seit Jahren gesetzlich verankert ist, ist die gesetzliche Vorgabe von Informationssicherheit neu. U.a. um die Gesetze einander bezüglich ihres Stellenwertes anzunähern, wird das BSIG derzeit überarbeitet.

[3] https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html

Tabelle 5 Relevanz des BSI-Gesetzes

Rolle	*Relevanz*
Integratoren	ggf. relevant
Hersteller	nicht relevant
Planung	ggf. relevant
Betreiber	wichtig
Einkauf	ggf. relevant
Management	wichtig
IT-Experten	wichtig

4.1.5 Bundesimmissionsschutzgesetz (BImSchG)

Name: Gesetz zum Schutz vor schädlichen Umwelteinwirkungen durch Luftverunreinigungen, Geräusche, Erschütterungen und ähnliche Vorgänge (Bundes-Immissionsschutzgesetz)[4]

Zweck dieses Gesetzes ist es, Menschen, Tiere und Pflanzen, den Boden, das Wasser, die Atmosphäre sowie Kultur und sonstige Sachgüter vor schädlichen Umwelteinwirkungen zu schützen und dem Entstehen schädlicher Umwelteinwirkungen vorzubeugen.

Soweit es sich um genehmigungsbedürftige Anlagen handelt, dient dieses Gesetz auch (...) dem Schutz und der Vorsorge gegen Gefährdungen, erhebliche Nachteile und erhebliche Belästigungen, die auf andere Weise herbeigeführt werden.

Tabelle 6 Relevanz des Bundesimmissionsschutzgesetzes

Rolle	*Relevanz*
Integratoren	relevant
Hersteller	nicht relevant
Planung	relevant
Betreiber	wichtig
Einkauf	nicht relevant
Management	relevant
IT-Experten	nicht relevant

4.1.6 12. Bundesimmissionsschutzverordnung

Name: Zwölfte Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes (Störfall-Verordnung)[5]

Betriebsbereiche, in denen bestimmte gefährliche Stoffe ab festgelegten Mengenschwellen vorhanden oder vorgesehen sind, unterliegen in Deutschland der 12. BImschV. Das gilt auch für Anlagen, bei denen davon auszugehen ist, dass solche Stoffe bei einem außer Kontrolle geratenen Prozessen, auch bei Lagerung, anfallen. Die 12. BImschV dient der Verhinderung von Störfällen und der Begrenzung von Störfallauswirkungen.

[4] https://www.gesetze-im-internet.de/bimschg/
[5] https://www.gesetze-im-internet.de/bimschv_12_2000/

Betreiber von Betriebsbereichen haben nach § 3 der 12. BImschV die Pflicht, Vorkehrungen zu treffen, um Störfälle zu verhindern. Dabei sind als Gefahrenquelle auch „Eingriffe Unbefugter“ zu berücksichtigen. Durch Eingriffe Unbefugter in IT-/OT-Systeme können Störfälle herbeigeführt werden.

In der 12. BImschV sind jedoch nur Grundsätze für die Verhinderung und die Begrenzung von Störfällen integriert. Weiterhin sind danach bei den Gefährdungen die Eingriffe Unbefugter zu betrachten.

Der Schutz vor Eingriffen Unbefugter hatte in den 1990er und 2000er Jahren nichts mit Angriffen auf die OT-/IT-Security zu tun, da zu diesem Zeitpunkt das Internet noch in den Anfängen steckte. Insoweit sind die Methoden auch nicht in der 12. BImschV beschrieben. Allerdings wurde schon in der ersten Fassung der 12. BImschV die Durchführung einer sicherheitstechnischen Gefahrenanalyse nach dem PAAG-Verfahren vorgesehen. Das Thema OT-/IT-Security ist dabei nicht explizit adressiert.

Tabelle 7 Relevanz der 12. BImschV

Rolle	*Relevanz*
Integratoren	relevant
Hersteller	nicht relevant
Planung	relevant
Betreiber	wichtig
Einkauf	relevant
Management	wichtig
IT-Experten	nicht relevant

4.2 Vorgaben Security

4.2.1 DIN ISO/IEC 27001 & 27002

Name: DIN ISO/IEC 27001 IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen & DIN ISO/IEC 27002 IT-Sicherheitsverfahren – Leitfaden für das Informationssicherheits-Management

Verfahren für Institutionen für die Implementierung und den Betrieb eines Informationssicherheitsmanagementsystems nach einer internationalen Norm.

Bei der DIN ISO/IEC 27001 handelt es sich um eine internationale Norm, mit deren Hilfe die Informationssicherheit in Organisationen wie Unternehmen, Non-Profitorganisationen oder öffentlichen Institutionen gewährleistet werden kann. Basis der Norm bildet die Beschreibung der Anforderungen zur Implementierung und zum Betrieb eines Informationssicherheitsmanagementsystems. Das System ist an die Gegebenheiten der jeweiligen Organisation anzupassen und berücksichtigt individuelle Besonderheiten.

Neben dem Informationssicherheitsmanagementsystem beschäftigt sich ISO 27001 mit der Analyse und der Behandlung von Risiken der Informationssicherheit. Im Rahmen der beschriebenen Anforderungen werden die Werte und Wertschöpfungsketten durch die Auswahl der geeigneten Sicherheitsmechanismen geschützt. Für Unternehmen bietet ISO 27001 einen systematisch strukturierten Ansatz, die Integrität der betrieblichen Daten und deren Vertraulichkeit zu schützen. Gleichzeitig sorgt sie für die Sicherstellung der Verfügbarkeit der an den Unternehmensprozessen beteiligten IT-Systeme.

Die Norm ist Teil der Normenfamilie ISO/IEC 27000 und wurde von der Internationalen Organisation für Standardisierung (ISO) veröffentlicht. Es existieren inzwischen mehrere Revisionen von ISO 27001. Die erste Revision entstand 2005, die aktuellste Ausgabe stammt aus dem Jahr 2015. ISO 27001 ist auch als DIN-Norm (Deutsches Institut für Normung) DIN ISO/IEC 27001 (IEC = International Electrotechnical Commission)

bekannt. Organisationen können sich nach ISO 27001 zertifizieren lassen und dadurch die Umsetzung und Einhaltung der geltenden Normen zur Informationssicherheit dokumentieren. ISO 27001 hat sich weltweit als Standard etabliert und ist eine der bekanntesten Normen für Informationssicherheit. Zahlreiche Unternehmen sind nach ISO 27001 zertifiziert.

Tabelle 8 Relevanz der DIN ISO/IEC 27001

Rolle	*Relevanz*
Integratoren	relevant
Hersteller	nicht relevant
Planung	ggf. relevant
Betreiber	relevant
Einkauf	ggf. relevant
Management	relevant
IT-Experten	nicht relevant

4.2.2 BSI Standard 200-2

Name: BSI-Standard 200-2 IT Grundschutz-Methodik [6]

Verfahren für Institutionen zum Aufbau eines Informationssicherheitsmanagementsystems (ISMS). Der neue Standard bildet die Basis der bewährten BSI-Methodik zum Aufbau eines soliden Managements.

Der Standard bildet die Basis der BSI-Methodik zum Aufbau eines Informationssicherheitsmanagementsystems (ISMS). Er etabliert drei Vorgehensweisen bei der Umsetzung des IT-Grundschutzes: Die Basis-Absicherung liefert einen Einstieg zur Initiierung eines ISMS. Mit der Standard-Absicherung kann ein kompletter Sicherheitsprozess implementiert werden. Diese Absicherung ist kompatibel zur ISO 27001-Zertifizierung. Die Kernabsicherung ist eine Vorgehensweise zum Einstieg in ein ISMS, bei der zunächst ein kleiner Teil eines größeren Informationsverbundes betrachtet wird.

Verantwortliche für Informationssicherheit können mit dem Standard 200-2 sowie den erforderlichen Bausteinen aus dem IT-Grundschutz-Kompendium ein ISMS in ihrer Institution aufbauen und bereits bestehende ISMS überprüfen oder erweitern. Die beiden verschlankten und modularen Vorgehensweisen Basis- und Kernabsicherung erleichtern insbesondere Verantwortlichen in kleinen und mittelständischen Betrieben den Einstieg in die Thematik

Tabelle 9 Relevanz des BSI Standard 200-2

Rolle	*Relevanz*
Integratoren	ggf. relevant
Hersteller	relevant
Planung	relevant
Betreiber	wichtig
Einkauf	ggf. relevant
Management	relevant

[6] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-2-IT-Grundschutz-Methodik/bsi-standard-200-2-it-grundschutz-methodik_node.html

Rolle	*Relevanz*
IT-Experten	wichtig

4.2.3 BSI 200-3 Risikomanagement

Name: BSI-Standard 200-3: Risikomanagement[7]

Vorgehensweise für Institutionen zur Steuerung von Informationssicherheitsrisiken. Im BSI-Standard 200-3 sind erstmals alle risikobezogenen Arbeitsschritte bei der Umsetzung des IT-Grundschutzes gebündelt dargestellt.

Der Vorteil für Anwendende ist ein deutlich reduzierter Aufwand, um ein angestrebtes Sicherheitsniveau zu erreichen.

Der BSI-Standard 200-3 gehört zu einer vierteiligen Standardreihe des BSI. Die Standards behandeln Grundlagen zum Aufbau eines ISMS sowie ausgewählte Aspekte, die vertieft werden. Dazu gehört neben dem 200-3, der das Risikomanagement behandelt, der BSI-Standard 100-4, der das Notfallmanagement thematisiert.

Das Risikomanagement zur Steuerung von Informationssicherheitsrisiken ist branchenneutral anwendbar und unabhängig von der Größe oder Art der Organisation einsetzbar.

Die Vorgehensweise gliedert sich in den Prozess des IT-Grundschutzes (vgl. insbesondere BSI-Standard 200-2) ein. Dieser erfordert eine Risikoanalyse, die wahlweise gemäß dem BSI-Standard 200-3 vollzogen werden kann.

Der Standard sieht einen vierteiligen Prozess zur Informationssicherheitsrisikoanalyse vor. Zunächst wird eine Gefährdungsübersicht erstellt. Dies wird in dem Standard durch eine Tabelle möglicher elementarer Gefährdungen unterstützt. Anschließend erfolgt die Einstufung des Risikos. Dazu wird die Eintrittshäufigkeit sowie die Schadenserhöhe eingeschätzt, sodass eine Risikobewertung vorgenommen werden kann. Im dritten Schritt wird eine Risikobehandlungsoption ausgewählt. Hier sieht der Standard vor, zwischen den vier Optionen Risikovermeidung, Risikoreduktion, Risikotransfer und Risikoakzeptanz zu entscheiden. Die aus der Risikoanalyse resultierenden zusätzlichen Maßnahmen zur Erhöhung der Informationssicherheit, bzw. Verringerung des Risikos, werden im letzten Schritt der Risikoanalyse in das Sicherheitskonzept zurückgeführt.

Tabelle 10 Relevanz des BSI Standard 200-3

Rolle	*Relevanz*
Integratoren	wichtig
Hersteller	ggf. relevant
Planung	relevant
Betreiber	wichtig
Einkauf	nicht relevant
Management	ggf. relevant
IT-Experten	relevant

[7] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-3-Risikomanagement/bsi-standard-200-3-risikomanagement_node.html

4.2.4 IT-Grundschutz-Kompendium

Name: IT-Grundschutz-Kompendium[8]

Verfahren zur Implementierung von Sicherheitsanforderungen für typische Geschäftsprozesse, Anwendungen, IT-Systeme, Kommunikationsverbindungen und Räume.

Im IT-Grundschutz-Kompendium werden Sicherheitsanforderungen für typische Geschäftsprozesse, Anwendungen, IT-Systeme, Kommunikationsverbindungen und Räume in einzelnen Bausteinen beschrieben. Ziel des IT-Grundschutzes ist es, einen angemessenen Schutz für alle Informationen einer Institution zu erreichen. Die IT-Grundschutz-Methodik zeichnet sich dabei durch einen ganzheitlichen Ansatz aus. Durch die geeignete Kombination von organisatorischen, personellen, infrastrukturellen und technischen Sicherheitsanforderungen wird ein Sicherheitsniveau erreicht, das für den jeweiligen Schutzbedarf angemessen und ausreichend ist, um geschäftsrelevante Informationen zu schützen. Darüber hinaus bilden die Anforderungen des IT-Grundschutz-Kompendiums nicht nur eine Basis für hochschutzbedürftige IT-Systeme und Anwendungen, sondern erläutern an vielen Stellen, wie ein höheres Sicherheitsniveau erreichbar ist.

Die IT-Grundschutz-Methodik nutzt das Baukastenprinzip, um den heterogenen Bereich der Informationstechnik einschließlich der Einsatzumgebung besser strukturieren und planen zu können. Die einzelnen Bausteine thematisieren typische Abläufe von Geschäftsprozessen und Bereiche des IT-Einsatzes, wie beispielsweise Notfallmanagement, Client-Server-Netze, bauliche Einrichtungen sowie Kommunikations- und Applikationskomponenten.

Die Bausteine des IT-Grundschutz-Kompendiums bilden den Stand der Technik ab, basierend auf den Erkenntnissen zum Zeitpunkt der Veröffentlichung. Die dort formulierten Anforderungen beschreiben, was generell umzusetzen ist, um mit geeigneten Cyber-Sicherheitsmaßnahmen den Stand der Technik zu erreichen. Anforderungen bzw. Maßnahmen, die den Stand der Technik abbilden, entsprechen dem, was sich zum jeweiligen Zeitpunkt einerseits technisch fortschrittlich und andererseits in der Praxis als geeignet erwiesen hat.

Es gibt zudem bereits Bausteine für den industriellen Kontext und somit wird die Nutzung des IT-Grundschutzes auch im Bereich der industriellen Automation unterstützt

Tabelle 11 Relevanz des IT-Grundschutz-Kompendiums

Rolle	*Relevanz*
Integratoren	ggf. relevant
Hersteller	ggf. relevant
Planung	relevant
Betreiber	wichtig
Einkauf	nicht relevant
Management	relevant
IT-Experten	wichtig

4.2.5 ISO/IEC 27005

Name: ISO/IEC 27005:2018: Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Risikomanagement[9]

[8] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html
[9] https://www.iso.org/standard/75281.html

Vorgaben zum Umgang mit Informationssicherheitsrisiken.

Der Standard enthält Leitlinien für ein systematisches und prozessorientiertes Risikomanagement, das gegebenenfalls auch die Einhaltung der Anforderungen an das Risikomanagement nach ISO/IEC 27001 unterstützt.

Die ISO/IEC 27005 verfolgt das Ziel Organisationen bei dem Umgang mit Informationssicherheitsrisiken zu unterstützen. Sie berücksichtigt die Grundlagen der ISO/IEC 27001 und fügt sich in deren Konzept ein. Zum Verständnis der ISO/IEC 27005 wird vorausgesetzt, dass die Hintergründe der ISO/IEC 27001 bekannt sind.

Die ISO/IEC 27005 legt den in der ISO/IEC 31000 beschriebenen generellen Umgang mit Risiken zugrunde. Dieser wird in der ISO/IEC 27005 für das Umfeld Informationssicherheit und damit verbundene Informationssicherheitsrisiken spezifiziert.

Um Informationssicherheitsrisiken zu identifizieren, einzuschätzen und diese zu überwachen, entwirft die Norm einen iterativen Prozess. Dadurch werden Zeit und Aufwände reduziert und somit die benötigten Ressourcen geschont.

Die Norm ist für alle Organisationen, die sich mit ihren Informationssicherheitsrisiken auseinandersetzen möchten, unabhängig von ihrer Größe oder der Etablierung eines Informationssicherheitsmanagementsystems, geeignet.

Tabelle 12 Relevanz der ISO/IEC 27005

Rolle	*Relevanz*
Integratoren	ggf. relevant
Hersteller	nicht relevant
Planung	ggf. relevant
Betreiber	wichtig
Einkauf	nicht relevant
Management	ggf. relevant
IT-Experten	relevant

4.2.6 ICS-Security-Kompendium

Name: ICS Security Kompendium

Grundlagenwerk für die IT- Sicherheit in industriellen Steuerungs- und Automatisierungssystemen (ICS).

Das „Industrielle Steuerungs- und Automatisierungssysteme (ICS) Security“ Kompendium stellt ein Grundlagenwerk für Cyber-Sicherheit dar. Es ermöglicht allen Fachkräften den einfachen Zugang zur IT- Security in ICS und erläutert die zur Erfassung des Themas notwendigen Grundlagen der Cyber-Sicherheit, der ICS Abläufe und der relevanten Normen. Es hilft, die für ICS entwickelten technischen und organisatorischen Maßnahmen mit Hilfe verschiedener Normen und Praxisbeispiele umzusetzen. Hierbei werden auch die Unterschiede und Lücken etablierter ICS Standards und insbesondere des IT Grundschutzes im Bereich ICS Security aufgezeigt. Eine konkrete praktikable Methodik zur Auditierung von ICS wird im ICS Kompendium beschrieben. Letztlich gibt das Kompendium Hinweise zum aktuellen Handlungsbedarf und zu zukünftigen Themen für Forschung und Entwicklung im Bereich ICS.

Tabelle 13 Relevanz des ICS-Security-Kompendiums

Rolle	*Relevanz*
Integratoren	wichtig
Hersteller	ggf. relevant
Planung	relevant
Betreiber	wichtig
Einkauf	nicht relevant
Management	ggf. relevant
IT-Experten	wichtig

4.2.7 IEC 62443-2-4

Name: IEC 62443-2-4 IT-Sicherheit für industrielle Automatisierungssysteme - Teil 2-4: Anforderungen an das IT-Sicherheitsprogramm von Dienstleistern für industrielle Automatisierungssysteme[10]

Vorgehensweise für Produktlieferfirmen und Wartungsanbietende zur Verwaltung der Cyber-Security während des Integrationsprozesses eines Produkts oder einer Lösung.

IEC 62443 ist eine internationale Normenreihe, die sich mit der Cyber-Security „industrieller Automatisierungs- und Steuerungssysteme (IACS)“ befasst. Die Reihe besteht aus Normen und technischen Reports, die das Verfahren zur Implementierung sicherer IACS definieren. Der Teil IEC 62443-2-4 spezifiziert Anforderungen an die Sicherheitsfähigkeiten, die dem Anlageneigentümer während der Integrations- und Wartungsaktivitäten einer Automatisierungslösung von Dienstleistungsunternehmen angeboten werden können.

Die Anforderungen der Norm IEC 62443-2-4 werden unter Verwendung des Konzepts der Maturity Level entworfen, wie in ihrem Kapitel 4.2 spezifiziert. Die Norm teilt die Maturity Level in vier Typen ein (siehe Tabelle 1 von IEC 62443-2-4):

- ML-1- Anfänglich - Auf dieser Ebene haben die Dienstleistungsanbietenden Unternehmen in der Regel mindestens einmal die Dienstleistung ad hoc und häufig nicht dokumentiert erbracht.
- ML-2-Managed - Auf dieser Ebene hat das dienstanbietende Unternehmen die Fähigkeit, die Lieferung und Leistung der Dienstleistung gemäß schriftlicher Richtlinien zu verwalten.
- ML-3-Definiert - Auf dieser Stufe hat das Dienstleistungsunternehmen mindestens einmal eine Dienstleistung für einen Anlagenbetreiber unter Verwendung der schriftlichen Richtlinien wie in ML-2 durchgeführt, und es kann nachgewiesen werden, dass die Leistung einer Dienstleistung der Stufe 3 in der gesamten Organisation des Dienstleistungsunternehmens wiederholbar ist.
- ML-4- Verbesserung - Auf dieser Ebene kontrollieren die dienstleistungsanbietenden Unternehmen die Effektivität und Leistung ihrer Dienstleistung und demonstrieren kontinuierliche Verbesserung.

Tabelle 14 Relevanz der IEC 62443-2-4

Rolle	*Relevanz*
Integratoren	wichtig
Hersteller	wichtig
Planung	nicht relevant

[10] https://www.beuth.de/de/norm/din-en-iec-62443-2-4/321127867

Rolle	*Relevanz*
Betreiber	relevant
Einkauf	nicht relevant
Management	ggf. relevant
IT-Experten	ggf. relevant

4.2.8 IEC 62443-3-3

Name: Security für industrielle Automatisierungs- und Steuerungssysteme Teil 3-3: System Security Anforderungen und Security Levels[11]

IEC 62443 ist eine internationale Normenreihe, die sich mit der Cyber-Security „industrieller Automatisierungs- und Steuerungssysteme (IACS)“ befasst. Die Reihe besteht aus Normen und technischen Reports, die das Verfahren zur Implementierung sicherer IACS definieren.

Der Teil IEC 62443-3-3 spezifiziert Anforderungen an Sicherheitsfähigkeiten, die von einem Hersteller oder Integrator für ein System, z.B. SCADA-System, DCS usw. angeboten werden können.

Die Anforderungen der Norm IEC 62443-3-3 werden unter Verwendung des Konzepts der Security Level entworfen, wie in ihrem Kapitel 3.3 von IEC 62443-3-3 festgelegt.

Der Standard teilt die Sicherheitsstufen in vier Typen ein, und die zugehörigen vier SLs sind definiert als:

- SL-1 - Verhindern der unbefugten Offenlegung von Informationen durch Abhören oder zufällige Enthüllung.
- SL-2 - Verhindern der unbefugten Offenlegung von Informationen gegenüber einer Entität, die aktiv nach ihnen sucht, mit einfachen Mitteln und mit geringen Ressourcen, allgemeinen Fähigkeiten und geringer Motivation.
- SL-3 - Verhindern der unbefugten Offenlegung von Informationen gegenüber einer Entität, die aktiv nach ihnen sucht, indem Sie ausgeklügelte Mittel mit mäßigen Ressourcen, IACS-spezifischen Fähigkeiten und mäßiger Motivation einsetzen.

SL-4 - Verhindern der unbefugten Offenlegung von Informationen gegenüber einer Entität, die aktiv nach ihnen sucht, indem Sie ausgeklügelte Mittel mit erweiterten Ressourcen, IACS-spezifischen Fähigkeiten und hohen Ressourcen einsetzen.

Tabelle 15 Relevanz der IEC 62443-3-3

Rolle	*Relevanz*
Integratoren	wichtig
Hersteller	wichtig
Planung	ggf. relevant
Betreiber	relevant
Einkauf	nicht relevant
Management	nicht relevant
IT-Experten	wichtig

[11] https://www.beuth.de/de/norm/din-en-iec-62443-3-3/311519620

4.2.9 IEC 62443-4-1

Name: IEC 62443 IT-Sicherheit für industrielle Automatisierungssysteme - Teil 4-1: Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung[12]

IEC 62443 ist eine internationale Normenreihe, die sich mit der Cyber-Security „industrieller Automatisierungs- und Steuerungssysteme (IACS)“ befasst. Die Reihe besteht aus Normen und technischen Reports, die das Verfahren zur Implementierung sicherer IACS definieren. Der Teil IEC 62443-4-1 spezifiziert die Anforderungen an den Produktentwicklungs-Lebenszyklus in Bezug auf Cyber-Security für Produkte, die von Produktlieferfirmen zur Verwendung in einer IACS-Umgebung vorgesehen sind.

Die Anforderungen der Norm IEC 62443-4-1 werden unter Verwendung des Konzepts der Maturity Level (ML) entworfen, wie in ihrem Kapitel 4.2 spezifiziert. Die Norm teilt die Maturity Level in vier Typen ein (siehe Tabelle 1 von IEC 62443-4-1):

ML-1- Anfänglich - Auf dieser Stufe führen Hersteller die Produktentwicklung in der Regel ad hoc und oft undokumentiert (oder nicht vollständig dokumentiert) durch.

ML-2- Managed - Auf dieser Ebene ist der Hersteller in der Lage, die Lieferung und Leistung der Dienstleistung gemäß schriftlicher Richtlinien zu verwalten.

ML-3- Definiert - Auf dieser Ebene ist der vom Hersteller implementierte Entwicklungsprozess in der gesamten Organisation der Lieferfirmen praktiziert worden, und es gibt Beweise dafür, dass dies geschehen ist.

ML-4– Verbessern - Auf dieser Ebene kontrollieren die Hersteller die Wirksamkeit und Leistung des Produkts und weisen eine kontinuierliche Verbesserung des Entwicklungsprozesses nach.

Tabelle 16 Relevanz der IEC 62443-4-1

Rolle	*Relevanz*
Integratoren	relevant
Hersteller	wichtig
Planung	relevant
Betreiber	Ggf. relevant
Einkauf	Ggf. relevant
Management	Ggf. relevant
IT-Experten	Ggf. relevant

4.2.10 IEC 62443-4-2

Name: IEC 62443 IT-Sicherheit für industrielle Automatisierungssysteme - Teil 4-2: Technische Sicherheitsanforderungen an Komponenten industrieller Automatisierungssysteme

IEC 62443 ist eine internationale Normenreihe, die sich mit der Cyber-Security „industrieller Automatisierungs- und Steuerungssysteme (IACS)“ befasst. Die Reihe besteht aus Normen und technischen Reports, die das Verfahren zur Implementierung sicherer IACS definieren.

Der Teil IEC 62443-4-2 spezifiziert Anforderungen an Sicherheitsfunktionen, die von einer Produktlieferfirma für ein Produkt angeboten werden können, dass in einer IACS-Umgebung eingesetzt wird.

Die Anforderungen der Norm IEC 62443-4-2 werden unter Verwendung des Konzepts der Security Level (SL) entworfen, wie in ihrem Kapitel 3.3 der IEC 62443-4-2 angegeben.

[12] https://www.beuth.de/de/norm/din-en-iec-62443-4-1/292194568

Der Standard teilt die Sicherheitsstufen in vier Typen ein, und die zugehörigen vier SLs sind definiert als:

- SL-1 - Verhindern Sie die unbefugte Offenlegung von Informationen durch Abhören oder zufällige Enthüllung.
- SL-2 - Verhindern Sie die unbefugte Offenlegung von Informationen gegenüber einer Entität, die aktiv nach ihnen sucht, mit einfachen Mitteln und mit geringen Ressourcen, allgemeinen Fähigkeiten und geringer Motivation.
- SL-3 - Verhindern Sie die unbefugte Offenlegung von Informationen gegenüber einer Entität, die aktiv nach ihnen sucht, indem Sie ausgeklügelte Mittel mit mäßigen Ressourcen, IACS-spezifischen Fähigkeiten und mäßiger Motivation einsetzen.
- SL-4 - Verhindern Sie die unbefugte Offenlegung von Informationen gegenüber einer Entität, die aktiv nach ihnen sucht, indem Sie ausgeklügelte Mittel mit erweiterten Ressourcen, IACS-spezifischen Fähigkeiten und hohen Ressourcen einsetzen.

Tabelle 17 Relevanz der IEC 62443-4-2

Rolle	*Relevanz*
Integratoren	ggf. relevant
Hersteller	wichtig
Planung	nicht relevant
Betreiber	nicht relevant
Einkauf	Ggf. relevant
Management	nicht relevant
IT-Experten	nicht relevant

4.3 Vorgaben Safety

4.3.1 Leitfaden Maßnahmen gegen Eingriffe Unbefugter KAS-51

Name: KAS 51: Leitfaden – Maßnahmen gegen Eingriffe Unbefugter der Kommission für Anlagensicherheit[13]

Der Leitfaden unterstützt Betreiber von Betriebsbereichen dabei, sich gegen Eingriffe Unbefugter, durch die ernste Gefahren hervorgerufen werden können, zu schützen. Somit gibt er Leitlinien zur Erfüllung der in § 3 Abs. 2 Nr. 3 der 12. BImschV enthaltenen Betreiberpflicht zur Berücksichtigung von Eingriffen Unbefugter als Gefährdung.

Die Kommission für Anlagensicherheit (KAS) ist das Nachfolgegremium der Störfall-Kommission (SFK) und des Technischen Ausschusses für Anlagensicherheit (TAA). Ihre Aufgaben richten sich nach dem § 51a BImSchG. Sie schlägt unter anderem technische Regeln vor, die im Rahmen von Genehmigungsverfahren und sicherheitstechnischen Prüfungen Berücksichtigung finden.

Im Leitfaden KAS 44 vom November 2017 waren erstmals Leitsätze für die Abwehr von cyber-physischen Angriffen im Hinblick auf die Eingriffe Unbefugter nach 12. BImschV genannt. Der Leitfaden KAS-51 -Maßnahmen gegen Eingriffe Unbefugter- ist das jüngste Dokument in dieser Reihe. Er löst den Leitfaden SFK-

[13] https://www.kas-bmu.de/nachricht/kas-51.html

GS-38 ab und integriert den KAS 41 zum Schutz vor Eingriffen Unbefugter. Hiernach ist eine Sicherungsanalyse vorgesehen und die Maßnahmen werden in organisatorische Maßnahmen (Sicherungsmanagementsystem) und anlagentechnische Maßnahmen unterschieden.

Der Leitfaden beschreibt Methoden und Maßnahmen zum Schutz vor Eingriffen Unbefugter. Dazu gehören vor allem auch Gefährdungen durch Eingriffe Unbefugter auf IT-/OT-Systeme (Cyber-Angriffe).

Tabelle 18 Relevanz der Leitfaden Maßnahmen gegen Eingriffe Unbefugter KAS-51

Rolle	*Relevanz*
Integratoren	nicht relevant
Hersteller	nicht relevant
Planung	relevant
Betreiber	wichtig
Einkauf	nicht relevant
Management	relevant
IT-Experten	ggf. relevant

4.3.2 VDI/VDE 2180

Name: VDI/VDE 2180 Funktionale Sicherheit in der Prozessindustrie Teile 1-3[14]

Planung, Errichtung und Betrieb von PLT-Sicherheitseinrichtungen in chemischen Prozessanlagen.

Ansatz der chemischen Industrie in Deutschland zur Umsetzung der Anforderungen aus der DIN EN 61511.

Diese Richtlinie basiert auf der IEC 61511 und gilt für Anlagen der Prozessindustrie, z.B. der chemischen und petrochemischen Industrie. Sie stellt eine bewährte Möglichkeit dar, die Anforderungen der 12. BlmSchV an PLT-Sicherheitseinrichtungen umzusetzen. Die Richtlinie besteht aus drei Teilen:

- Blatt 1: Einführung, Begriffe, Konzeption
- Blatt 2: Planung, Errichtung und Betrieb von PLT-Sicherheitsfunktionen
- Blatt 3: Nachweis der Ausfallwahrscheinlichkeit im Anforderungsfall (PFD)

PLT-Sicherheitseinrichtungen kommen üblicherweise dann zum Einsatz, wenn andere Maßnahmen nicht anwendbar, nicht ausreichend oder bei vergleichbarer Risikoreduzierung nicht wirtschaftlich sind. Die Anwendung möglichst einfacher, überschaubarer und unmittelbar wirkender Maßnahmen (z.B. Sicherheitsventile, druckfeste Absicherung) führt in der Regel zu sicheren und gleichzeitig wirtschaftlichen Lösungen.

In dieser Richtlinie werden die allgemeinen Grundsätze für die Sicherung von Anlagen der Prozessindustrie mit Mitteln der PLT für den typischen Fall, dass eine PLT-Sicherheitsfunktion maximal einmal im Jahr angefordert bzw. benötigt wird, beschrieben.

Die VDI/VDE 2180 beschreibt einen möglichen Umgang mit PLT-Sicherheitseinrichtungen auf Basis der internationalen Normen und vereinfacht die diversen Möglichkeiten der entsprechenden Regelwerke.

Die Richtlinie verweist in ihrem Teil 1 auf die Notwendigkeit der Betrachtung von Risiken der IT-Security. Im Management der funktionalen Sicherheit müssen Aspekte der IT-Security in der Planung, der Beschaffung, der Validierung, im Betrieb, bei Änderungen und bei der Außerbetriebnahme berücksichtigt werden.

[14] https://www.vdi.de/richtlinien/details/vdivde-2180-blatt-1-funktionale-sicherheit-in-der-prozessindustrie-einfuehrung-begriffe-konzeption

Für die Komponenten und Schnittstellen zwischen Systemen ist zwingend eine IT-Risikobeurteilung erforderlich.

Tabelle 19 Relevanz der VDI/VDE 2180

Rolle	*Relevanz*
Integratoren	wichtig
Hersteller	ggf. relevant
Planung	wichtig
Betreiber	relevant
Einkauf	nicht relevant
Management	nicht relevant
IT-Experten	ggf. relevant

4.3.3 DIN EN IEC 61511

Name: Funktionale Sicherheit – PLT-Sicherheitseinrichtungen für die Prozessindustrie Teile 1-3[15][16][17]

Planung, Errichtung und Betrieb von Einrichtungen zur funktionalen Sicherheit.

Die IEC 61511-Reihe behandelt die Anwendung von PLT-Sicherheitseinrichtungen in der Prozessindustrie. Sie thematisiert außerdem die Gefahren- und Risikoanalyse des Prozesses, die durchzuführen ist, um die Spezifikation der PLT-Sicherheitseinrichtungen daraus abzuleiten. Die Beiträge anderer Sicherheitseinrichtungen werden nur im Hinblick auf die Anforderungen an die PLT-Sicherheitseinrichtung betrachtet. Die PLT-Sicherheitseinrichtung umfasst dabei alle zur Ausführung einer PLT-Sicherheitsfunktion erforderlichen Geräte vom Sensor bis zum Aktor.

Diese Norm stellt Anforderungen zur Erreichung der erforderlichen funktionalen Sicherheit auf, legt jedoch nicht fest, wer für die Erfüllung dieser Anforderungen verantwortlich ist (beispielsweise Planung, Lieferfirmen, Betreiber, Kontraktoren). Diese Verantwortlichkeit wird den Beteiligten im Rahmen der Sicherheitsplanung, der Projektplanung, des Projektmanagements oder nationaler Vorschriften zugewiesen.

Sie ist anwendbar, wenn Geräte, die den Anforderungen der IEC 61508 Serie 2010 oder IEC 61511-1:2016 [11.5] entsprechen, in ein Gesamtsystem integriert werden, das in der Prozessindustrie eingesetzt werden soll. Sie ist nicht anwendbar, wenn Hersteller die Eignung von Geräten als PLT-Sicherheitseinrichtungen in der Prozessindustrie erklären wollen (siehe IEC 61508-2:2010 und IEC 61508-3:2010).

Die IEC verweist darauf, dass eine Risikobeurteilung hinsichtlich der IT-Security durchgeführt werden muss. Es werden einige Rahmenbedingungen zur Durchführung der Risikoanalyse definiert, im Grundsatz verweist die Norm aber auf die Anwendung der ISO/IEC 27001 und IEC 62443-2-1.

Tabelle 20 Relevanz der DIN EN IEC 61511

Rolle	*Relevanz*
Integratoren	relevant
Hersteller	ggf. relevant
Planung	wichtig
Betreiber	wichtig

[15] https://www.beuth.de/de/norm/din-en-61511-1/296008238
[16] https://www.beuth.de/de/norm/din-en-61511-2/295873010
[17] https://www.beuth.de/de/norm/din-en-61511-3/295783182

Rolle	*Relevanz*
Einkauf	ggf. relevant
Management	nicht relevant
IT-Experten	ggf. relevant

4.3.4 NAMUR NA 135

Name: NAMUR NA 135 Fernwartung bei Systemen der Automatisierungstechnik in der Prozessindustrie[18]

Darlegung von technischen und organisatorischen Randbedingungen für Fernwartung in der Automatisierungstechnik - Praxisleitfaden.

Bei der Einführung von Fernwartung steht für die Betreiber meist der wirtschaftliche Nutzen im Vordergrund. Da Fernwartung aber auch mit Investitions- und Betriebskosten sowie mit Risiken im Betrieb verbunden ist, sollte am Anfang eine Wirtschaftlichkeitsbetrachtung stehen, welche den Gesamtaufwand über den Lebenszyklus des Systems berücksichtigt. Dabei sind nach Möglichkeit verschiedene technische Alternativen zu prüfen und gegenüberzustellen.

Die Betrachtung der OT-Security spielte zu dem Zeitpunkt der Herausgabe nur eine untergeordnete Rolle und es werden nur relativ allgemeine Rahmenbedingungen beschrieben. Nichtsdestotrotz bildet die Beschreibung in diesem Regelwerk eine gute Basis - insbesondere der organisatorischen Maßnahmen - für die Realisierung eines Fernwartungszugangs.

Tabelle 21 Relevanz der NAMUR NA 135

Rolle	*Relevanz*
Integratoren	wichtig
Hersteller	relevant
Planung	relevant
Betreiber	wichtig
Einkauf	nicht relevant
Management	nicht relevant
IT-Experten	wichtig

4.3.5 DVGW Informationsschriften

Name: DVGW-Informationsschriften[19]

Schutz gegen Bedrohungen der Strom- und Gasversorgung. Sammlung von Anwendungsfällen.

Um die Vorteile moderner Informationstechnik sicher nutzen zu können, wird ein angemessener Schutz gegen Bedrohungen auch im Bereich des Netzbetriebs der Strom- und Gasversorgung angestrebt. Der DVGW beschreibt in verschiedenen Veröffentlichungen sehr detailliert diverse Anwendungsfälle.

Angewendet auf den Unternehmenswert „Information“ und mit dem Ziel „Sicherheit“ ist mit diesem Prozess in Grundzügen bereits ein Informationssicherheitsmanagementsystem beschrieben. Die DIN ISO/IEC 27001 ist das entsprechende normative Regelwerk, nach dem ein solches ISMS aufgebaut werden kann. Durch den IT-Sicherheitskatalog der Bundesnetzagentur gemäß §11 Abs. 1a EnWG ist die Einführung eines

[18] https://www.namur.net/de/empfehlungen-und-arbeitsblaetter/aktuelle-nena.html
[19] https://www.dvgw.de/leistungen/publikationen/die-leistungen-des-dvgw/info-schriften/gas-information-nr-22/

ISMS auf Grundlage der DIN ISO/IEC 27001 bei allen Strom- und Gasnetzbetreibern verbindlich vorgeschrieben. Ein Nachweis muss regelmäßig erbracht werden.

Das vorliegende Dokument nimmt eine grundlegende Einordnung der bestehenden Normen und Regelwerke vor, die für den (informationstechnisch) sicheren Netzbetrieb notwendig sind. Darauf aufbauend wurde eine Analyse und ein Ausblick auf den weiteren Handlungsbedarf für die Ausgestaltung einer sicheren Informationstechnik (IT) im Netzbetrieb erarbeitet.

Tabelle 22 Relevanz der DVGW Informationsschriften

Rolle	*Relevanz*
Integratoren	relevant
Hersteller	nicht relevant
Planung	relevant
Betreiber	ggf. relevant
Einkauf	nicht relevant
Management	ggf. relevant
IT-Experten	relevant

4.3.6 PAAG-Leitfaden

Name: Das PAAG-Verfahren: Methodik – Anwendung - Beispiele[20]

Gem. Anhang III der 12. BImschV sind für Betriebsbereiche im Rahmen des Sicherheitsmanagementsystems Verfahren festzulegen, mit denen die Gefährdungen von Störfallen systematisch ermittelt werden. Ein weitverbreitetes Verfahren zur systematischen Ermittlung von Gefahren in Prozessanlagen ist das PAAG-Verfahren (Prognose von Störungen, Auffinden von Ursachen, Abschätzen der Auswirkungen, Gegenmaßnahmen), welches auf dem englischen HAZOP-Verfahren basiert. Die Broschüre gibt einen Einblick in die Methodik und die praktische Anwendung des PAAG-Verfahrens.

Die Broschüre empfiehlt, die PAAG-Studie auf prozessbedingte Gefährdungen zu beschränken. Die Betrachtung externer Gefährdungen, wie „Eingriffe Unbefugter“, sind gem. dieser Broschüre übergeordnet zu betrachten, da Maßnahmen gegen diese Ereignisse in der Regel auf Werk- bzw. Standortebene getroffen werden müssen. Dies liegt unter anderem an der Ausgestaltung des Verfahrens selbst. Die in dem PAAG Verfahren bisher verwendeten Leitworte sind nicht dafür entwickelt, Gefährdungen der OT-/IT-Security zu begegnen.

Tabelle 23 Relevanz des PAAG-Leitfadens

Rolle	*Relevanz*
Integratoren	ggf. relevant
Hersteller	ggf. relevant
Planung	relevant
Betreiber	relevant
Einkauf	nicht relevant
Management	nicht relevant
IT-Experten	nicht relevant

[20] ISBN 92-843-7037-X, ISSN 1015-8022

4.3.7 NAMUR Arbeitsblatt Nr. 163

Name: NAMUR Arbeitsblatt Nr. 163 „IT-Risikobeurteilung von PLT-Sicherheitseinrichtungen“[21]

Betriebsbereiche werden nach der 12. BImschV zunehmend intern und nach außen informationstechnisch vernetzt. Diese Netze und Systeme sind grundsätzlich als Angriffspunkte nach § 3 Absatz 2 Nummer 3 der 12. BImschV zu betrachten. Die NA 163 beschreibt ein Vorgehen, mit dem eine IT-Risikobeurteilung in nur einem Tag durchgeführt werden kann.

Wie auch die KAS-44 betrachtet die NA 163 ausschließlich potentielle Angriffe über IT-Systeme, die sicherheitstechnische Relevanz (Safety) haben. Sie besteht aus einem beschreibenden Teil und einer Checkliste. In dem beschreibenden Teil ist die Referenzarchitektur einer im OT-Netzwerk eingesetzten Sicherheitssteuerung beschrieben, für die die Methode anwendbar ist. Mit der Checkliste kann zu je einer PLT-Sicherheitssteuerung eine IT-Risikobeurteilung durchgeführt und dokumentiert werden. Bei der Durchführung der IT-Risikoanalyse festgestellte Abweichungen zu den in der Checkliste empfohlenen Maßnahmen geben direkt Aufschluss zu konkreten Verbesserungsmaßnahmen. Bei Anwendung der NA 163 kann somit ein einheitlicher Stand der IT-Security durchgesetzt werden. Berichten von Nutzenden der NA 163 zufolge hat sich eine externe Moderation bewährt.

Tabelle 24 Relevanz der NA 163

Rolle	*Relevanz*
Integratoren	relevant
Hersteller	ggf. relevant
Planung	wichtig
Betreiber	wichtig
Einkauf	ggf. relevant
Management	relevant
IT-Experten	relevant

4.3.8 DIN EN ISO 12100

Name: DIN EN ISO 12100 Sicherheit von Maschinen - Allgemeine Gestaltungsleitsätze – Risikobeurteilung und Risikominderung[22]

Die ISO 12100 spezifiziert grundlegende Anforderungen an die funktionale Sicherheit von Maschinen (z.B. Turbinen, Pumpen, Armaturenantriebe, Notstromaggregate, Rührwerke, etc.) gem. den Anforderungen der EU-Richtlinien. Wer dergleichen Anlagen oder Teile dieser Maschinen vertreibt oder ändert, wird zum Inverkehrbringer und ist an die Anforderungen gebunden. Grundlegende IT-Security Anforderungen an die Steuerungen von Maschinen sind ebenfalls definiert.

Die ISO 12100 beschreibt ein einfaches und systematisches Verfahren, um Gefahren, die von einer Maschine ausgehen, zu identifizieren und bzgl. des Risikos abzuschätzen. Zudem erfolgt eine Gegenüberstellung zu den Maßnahmen, mit denen das Risiko minimiert werden kann. Das Kapitel 6.2.11 befasst sich mit der inhärent sicheren Konstruktion von Steuerungen und kann auch auf IT-Risiken sinngemäß angewendet werden. Z.B. sind Sicherheitssteuerungen auf Grundlage der IEC 61508 auszulegen, in der u.a. eine IT-Risikoanalyse verbindlich gefordert wird. Konkret fordert die ISO 12100 die Software einer Maschine durch geeigneten Schutz unveränderlich zu halten oder den Zugriff durch Schlösser oder Passwörter zu begrenzen.

[21] https://www.namur.net/de/empfehlungen-und-arbeitsblaetter/aktuelle-nena.html
[22] https://www.beuth.de/de/norm/din-en-iso-12100/128264334

Tabelle 25 Relevanz der ISO 12100:2010

Rolle	*Relevanz*
Integratoren	wichtig
Hersteller	wichtig
Planung	wichtig
Betreiber	relevant
Einkauf	ggf. relevant
Management	ggf. relevant
IT-Experten	nicht relevant

4.3.9 Richtlinie 2006/42/EG Maschinenrichtlinie

Name: Richtlinie 2006/42/EG [...] über Maschinen und zur Änderung der Richtlinie 95/16/EG[23]

Die Richtlinie 2006/42/EG (Maschinenrichtlinie) regelt ein einheitliches Schutzniveau zur Unfallverhütung für Maschinen und unvollständige Maschinen (z.B. Turbinen, Pumpen, Armaturenantriebe, Notstromaggregate, Rührwerke, etc.) beim Inverkehrbringen oder bei Änderungen.

Die Maschinenrichtlinie regelt das Inverkehrbringen und die Änderungen von Maschinen. Wesentliche Merkmale sind die Konformitätsbewertungen nach den harmonisierten EU-Normen (z.B.: der ISO 12100 oder ISO 13849) und die CE-Kennzeichnung. Für den praktischen Gebrauch sind im Anhang I praktische Grundsätze an die Gestaltung der Maschinen definiert. Das Kapitel 1.2.5 beschreibt die Anforderungen an Steuerungs- oder Betriebsarten. Sind gefährliche Funktionen durch absichtliche oder unabsichtliche Einwirkung auf die Sensoren oder die Steuerung der Maschine möglich, „[...]so muss der Steuerungs- oder Betriebsartenwahlschalter andere Schutzmaßnahmen auslösen, die so angelegt und beschaffen sind, dass ein sicherer Arbeitsbereich gewährleistet ist.“ Dieser Passus ist grundsätzlich auch auf Cyber-Sicherheitsanforderungen anzuwenden. Den Nutzenden der Maschine ist vom Inverkehrbringenden eine technische Dokumentation zu übergeben, in der die Maschine, die Sicherheitsmaßnahmen, Restrisiken, Sicherheits- und Gesundheitsschutzanforderungen beschrieben sind. Über die Gestaltung hinaus, definiert die Maschinenrichtlinie auch Anforderungen zur Fertigungsüberwachung, zu Prüfungen durch benannte Stellen und für die Qualitätssicherung.

Tabelle 26 Relevanz der Richtlinie 2006/42/EG

Rolle	*Relevanz*
Integratoren	wichtig
Hersteller	wichtig
Planung	wichtig
Betreiber	relevant
Einkauf	relevant
Management	ggf. relevant
IT-Experten	nicht relevant

[23] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:157:0024:0086:DE:PDF

4.4 Übersicht der wesentlichen Regelwerke

Den höchsten Konkretisierungsgrad in Bezug auf die Störfallvorsorge gegen Eingriffe Unbefugter (vgl. §3 Abs. 2 Nr. 3 der 12. BImschV) besitzt derzeit der KAS Leitfaden 51. Der Leitfaden entstand vor dem Hintergrund der technologischen Entwicklungen (Digitalisierung, Automatisierung und Vernetzung) und der geänderten Bedrohungslage (Cyber-Attacken), um aus heutiger Sicht anforderungsgerechte Maßnahmen gegen Eingriffe Unbefugter festzulegen. Die Umsetzung des Leitfadens kann aus Sicht der KAS u.a. als Nachweis geführt werden, dass organisatorische und technische Maßnahmen ausreichend im Sinne von §10a der Sicherheitsüberprüfungsfeststellungsverordnung sind.

Organisatorische und technische Maßnahmen werden in vielen Unternehmen bereits auf Basis des IT-Grundschutz und ISO 27001 umgesetzt. In Abbildung 19 und in der Tabelle sind den Anforderungen der KAS-51 (Kapitel 4 bis 7 und Anhängen) die entsprechenden Kapitel der Standards und Regelwerke zugeordnet.

Die Abbildung adressiert dabei im Wesentlichen die Betreiber. Die Schnittstelle zu den Integratoren wird durch die Verbindung bei der Maßnahme „Regelungen für Fremdpersonal und fremdvergebene Dienstleistungen“ hergestellt (gestrichelte blaue Linie).

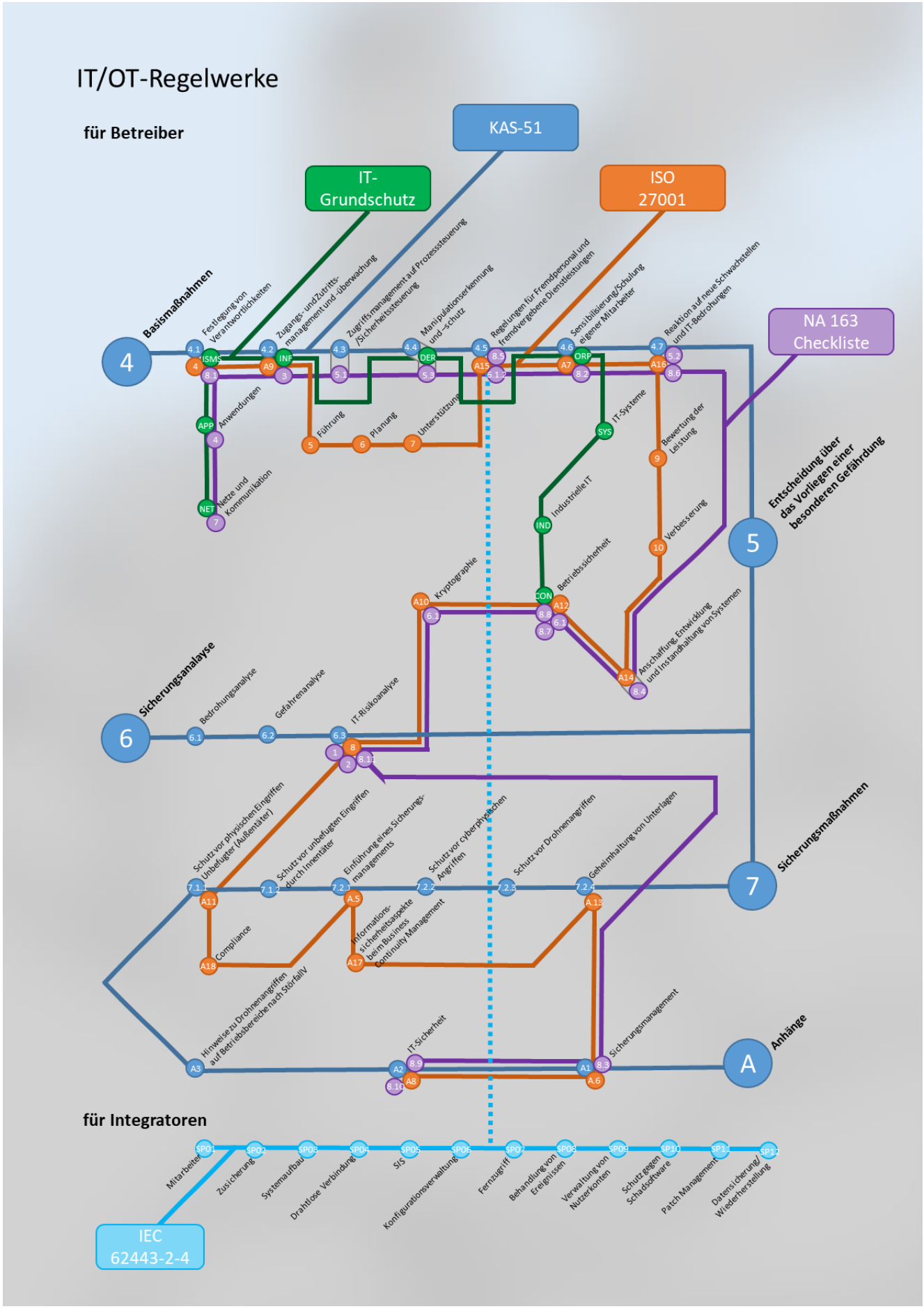

Abbildung 28 IT/OT-Regelwerk "U–Bahn Plan"

Tabelle 27 Abgleich IT/OT-Maßnahmen

Aspekte der Informationssicherheit	*KAS-51*	*ISO 27001*	*IT-Grundschutz*
Festlegung von Verantwortlichkeiten	4.1	5	ISMS.1 Sicherheitsmanagement
Zugangs- und Zutrittsmanagement und -überwachung	4.2	A.11.1	INF.1 Allgemeines Gebäude
Zugriffsmanagement und Prozesssteuerung / Sicherheitsmanagement	4.3	A.9.4	ORP.4 Identitäts- und Berechtigungsmanagement
Manipulationserkennung und -schutz	4.4	A.16	DER.1 Detektion von sicherheitsrelevanten Ereignissen
Regelungen für Fremdpersonal und fremdvergebene Dienstleistungen	4.5	A.15	OPS.2.1 Outsourcing für Kundschaft OPS.3.1 Outsourcing für Dienstleistungsunternehmen
Sensibilisierung/Schulung eigener Arbeitskräfte	4.6	A.7	ORP.3 Sensibilisierung und Schulung
Reaktion auf neue Schwachstellen und IT-Bedrohungen	4.7	A.16	DER.2.1 Behandlung von Sicherheitsvorfällen
Entscheidung über das Vorliegen einer besonderen Gefährdung	5	8	BSI Standard 200-3 Risikoanalyse auf der Basis von IT-GS
Bedrohungsanalyse	6.1	8	BSI Standard 200-3 Risikoanalyse auf der Basis von IT-GS
Gefahrenanalyse	6.2	8	BSI Standard 200-3 Risikoanalyse auf der Basis von IT-GS
IT-Risikoanalyse	6.3	8	BSI Standard 200-3 Risikoanalyse auf der Basis von IT-GS
Schutz vor physischen Eingriffen Unbefugter (Außentäter)	7.1.1	A.11.1	Bausteine der Schicht "Infrastruktur" z.B. INF.1 Allgemeines Gebäude
Schutz vor unbefugten Eingriffen durch Innentäter	7.1.2	A.9.2	ORP.4 Identitäts- und Berechtigungsmanagement
Einführung in Sicherheitsmanagement	7.2.1	A.5	ISMS.1 Sicherheitsmanagement
Schutz vor cyber-physischen Angriffen	7.2.2	A.13.1	NET.1.1 Netzarchitektur und -design
Schutz vor Drohnenangriffen	7.2.3	A.11.1	Bausteine der Schicht "Infrastruktur" z.B. INF.1 Allgemeines Gebäude
Geheimhaltung von Unterlagen	7.2.4	A.13.2	ORP.5 Compliance Management
Sicherheitsmanagement	A1	A.6	ISMS.1 Sicherheitsmanagement
IT-Security	A2	A.8	IT-GS in Gänze
Hinweise auf Drohungen auf Betriebsbereiche nach 12. BImschV	A3	-	-

5 Herausforderungen

In diesem Kapitel werden die Herausforderungen, die sich aus den gesetzlichen Anforderungen gemäß Kapitel 4 ergeben, dargestellt. Um festzustellen, wo hier die Schwerpunkte gesehen werden, wurden verschiedene Betreiber, Behörden und Sachverständigenorganisationen befragt.

Die 12. BImschV gilt für Betriebsbereiche, d.h. den unter Aufsicht eines Betreibers stehende Bereich mit Produktions- oder Lageranlagen, in denen gefährliche Stoffe in bestimmten Mengen gehandhabt werden. Bei Überschreitung einer im Anhang I der Verordnung genannten unteren Mengenschwelle (z.B. 10.000 kg Chlor) wird von Betriebsbereichen der unteren Klasse gesprochen. Bei Überschreitung einer oberen Mengenschwelle (z.B. 25.000 kg Chlor) wird hingegen von Betriebsbereichen der oberen Klasse gesprochen.

Die Betreiber aller Betriebsbereiche gemäß 12. BImschV sind verpflichtet, Vorkehrungen zur Verhinderung von Störfällen sowie Maßnahmen zur Begrenzung von Störfallauswirkungen zu ergreifen. Gemäß § 3 12. BImschV sind hierbei auch Maßnahmen zu ergreifen, die gegen Gefährdungen durch „Eingriffe Unbefugter“ wirksam sind. Zu diesen Gefährdungen durch Eingriffe Unbefugter sind mögliche Maßnahmen im Leitfaden KAS-51 zusammengefasst. Einen Schwerpunkt bilden dabei die Maßnahmen der IT- bzw. OT-Security.

5.1 Allgemeine Anforderungen

Der Leitfaden legt Basisanforderungen fest, die durch alle Betreiber von Betriebsbereichen zu erfüllen sind. Weitere Maßnahmen sind nur dann erforderlich, wenn von dem Betriebsbereich durch Eingriffe Unbefugter eine „besondere Gefährdung“ im Sinne des Leitfadens ausgehen kann. Die bei Vorliegen einer besonderen Gefährdung erforderlichen weitergehenden Schutzmaßnahmen sind aufgrund einer Sicherungsanalyse festzulegen, die ebenfalls Gegenstand des Leitfadens KAS-51 ist.

Die zuständige Behörde hat gemäß § 16 der 12. BImschV ein angemessenes Überwachungssystem einzurichten, welches eine planmäßige und systematische Prüfung der technischen, organisatorischen und managementspezifischen Systeme der betroffenen Betriebsbereiche ermöglicht. Im Rahmen dieser Prüfungen muss sich die zuständige Behörde insbesondere vergewissern, dass der Betreiber nachweisen kann, dass, im Zusammenhang mit den verschiedenen betriebsspezifischen Tätigkeiten, die zur Verhinderung von Störfällen erforderlichen Vorkehrungen ergriffen wurden. Somit ist die zuständige Behörde auch in der Pflicht zu prüfen, ob Vorkehrungen gegen Gefährdungen durch Eingriffe Unbefugter umgesetzt wurden. Dieser Verpflichtung muss die zuständige Behörde sowohl bei der regelmäßigen Überwachung als auch bei Neu- bzw. Änderungsgenehmigungen von Betriebsbereichen nachkommen.

Auch für die aufsichtsrechtlichen Pflichten in Bezug auf die Maßnahmen gegen Eingriffe Unbefugter stellt der Leitfaden KAS-51 die Basis dar. Aus dem Leitfaden ergeben sich für die Aufsichtsbehörden die folgenden Anforderungen:

- Entscheidung über das Vorliegen einer besonderen Gefährdung (Kap. 5 in KAS-51)
- Bewertung der umgesetzten Basismaßnahmen (Kap. 4 in KAS-51), sowie der ergänzenden Maßnahmen bei einer besonderen Gefährdung (Anhang 2 in KAS-51
- Plausibilitätsprüfung der Einschätzung der Bedrohungslage (Kap. 6.1 in KAS-51)
- Überprüfung der Sicherungsmanagement-Bausteine im Rahmen der Überprüfung des Sicherheitsmanagementsystems (Kap. 7.2.1 in KAS-51)
- Abstimmung mit den Betreibern über das genaue Vorgehen bzgl. der Geheimhaltung von Dokumenten (Kap. 7.2.4 in KAS-51)
- Feststellung der Notwendigkeit für Sicherheitsüberprüfungen (§ 10a SÜFV) für Betriebsbereiche der oberen Klasse (Kap. 8 in KAS-51)

5.2 Einbindung von Sachverständigen

In der Praxis werden von Betreibern oder Behörden oftmals Sachverständige damit beauftragt, sicherheitstechnische Prüfungen nach § 29a BImSchG vorzunehmen. Die Einbindung von Sachverständigen nach § 29b Abs. 1 BImSchG unterstützt Betreiber und Behörden, den Stand der Sicherheitstechnik in der Praxis festzulegen und einzuhalten.

Sachverständige nach § 29b Abs. 1 BImSchG werden auf Basis der 41. BImSchV bekanntgegeben. Aktuell sind in der Datenbank www.resymesa.de insgesamt 304 bundesweit tätige Sachverständige nach §29b Abs. 1 BImSchG bekanntgegeben. Die Anerkennung gilt für individuell bestätigte Fachgebiete und Anlagentypen. Ein spezifisches Fachgebiet zur Prüfungen von OT-Security gibt es nicht. Gleichwohl ergeben sich bei dem Thema OT-Security Bezüge zu etablierten Fachgebieten:

- Verfahrenstechnische Prozessführung
- Versorgung mit Energien und Medien
- Elektrotechnik
- MSR-/PLT
- Systematische Methoden der Gefahrenanalysen
- Betriebliche Alarm- und Gefahrenabwehrpläne
- Sicherheitsmanagement und Betriebsorganisation

Da die Sachverständigen nicht immer für alle Fachgebiete, die für die spezielle Prüfaufgabe erforderlich sind, eine Anerkennung besitzen, ist die Einbindung anderer Fachkräfte (z.B. für funktionale Sicherheit) etablierte Praxis.

Aber auch für die Sachverständigen gilt: in Bezug auf die OT-Security stellt der Leitfaden KAS-51 die Grundlage für die Überprüfung der störfallverhindernden Vorkehrungen dar, da die Umsetzung des Leitfadens aus Sicht der KAS u.a. als Nachweis geführt werden kann, dass organisatorische und technische Maßnahmen der OT-Security ausreichend sind.

5.3 Interviews mit den Verfahrensbeteiligten

Mit den Verfahrensbeteiligten wurden Interviews über deren Erfahrungen mit der Umsetzung des Leitfadens KAS-51 geführt. Dabei wurde auch und vor allem auf die sich ergebenden Herausforderungen sowie auf Praxisbeispiele und Defizite eingegangen. Die Antworten der Betreiber, Behördenvertretung und Sachverständigen auf die Interviewfragen sind in den Anhängen 1 bis 3 in anonymisierter Form dokumentiert. In den folgenden Kapiteln sind die Kernaussagen der Interviews zusammengefasst. Dabei herausgearbeitete Praxisbeispiele sind mit einem Daumensymbol gekennzeichnet, Defizite bzw. zukünftige Handlungsbedarfe sind mit einem Klemmbrettsymbol gekennzeichnet.

5.3.1 Herausforderungen aus Sicht der Betreiber

Es wurden sieben Interviews mit Betrieben bzw. Unternehmen geführt, die der 12. BImschV unterliegen. Die Befragten sind mit dem Thema IT-/OT-Security größtenteils schon vor acht bis zehn Jahren in Berührung gekommen; häufig waren dabei Änderungen bzw. Anpassungen in der Prozessleittechnik der Auslöser.

Aber auch die Mitarbeit in entsprechenden Arbeitskreisen bzw. Gremien oder Regelwerksänderungen haben zu einer Auseinandersetzung mit dem Thema geführt, zumal einige der Befragten auch unter die KritisV fallen.

Die Motivation der befragten Betreiber, sich mit dem Thema Security & Safety auseinanderzusetzen, ergibt sich somit in erster Linie aus den Anforderungen aus dem Überwachungsverfahren, Regelwerksänderungen und Unternehmensvorgaben. Aber auch „Cyber-Incidents“, Anforderungen durch Kundschaft bzw. durch Versicherungsträger sowie wirtschaftliche Gründe wurden als Motivation genannt.

Die Betreiber haben mit überwiegender Mehrheit Stabsstellen bzw. zentrale Arbeitsgruppen/Abteilungen gebildet, die sich mit dem Thema Safety & Security befassen. Über untergeordnete Organisationsstrukturen (projektbezogene bzw. lokale Verantwortlichkeiten) wird das Thema dann in die entsprechenden Abteilungen hineingetragen. Bei kleineren und mittleren Unternehmen sind in der Regel keine Stabsstellen vorhanden; hier wird das Thema meist durch einzelne Personen verfolgt.

5.3.1.1 Asset-Managementsystem

In Bezug auf das Asset-Managementsystem wurde festgestellt, dass unterschiedlicher Handlungsbedarf besteht. Während einige der Betreiber über ein zentralisiertes Asset-Managementsystem verfügen, haben andere Betreiber ein Asset-Managementsystem mit einer verteilten Datenverwaltung für Assets, Konfigurationen und Kommunikationsverbindungen.

Die Herausforderungen, die von den Betreibern gesehen werden, sind in erster Linie die Schnittstellen zwischen IT und OT mit doppelter Datenhaltung, Aktualität, Struktur und Vollständigkeit der Daten. Ein weiteres Problem besteht, wenn die Daten in unterschiedlichen Systemen gespeichert sind.

Vor diesem Hintergrund ist aus Sicht der Betreiber die Einführung eines Plant-Asset-Managementsystems ein vielversprechender Ansatz.

5.3.1.2 Ressourcen und fachliche Kompetenz

Die Ressourcen im Bereich der IT-/OT-Security für Betreiber stellen eine große Herausforderung dar. Während der Befragung wurde festgestellt, dass die meisten Betreiber keine feste Zuweisung von Arbeitsaufgaben haben, die zum Thema IT-/OT-Security gehören. Meistens haben die Arbeitskräfte doppelte Aufgaben und daher ist die Konzentration auf IT-/OT-Security eine Herausforderung. Es ist schwierig, IT-/OT-Security-Fachkräfte zu bekommen, weil es an Ausbildung in diesem Bereich mangelt. Die Einstellung neuer Arbeitskräfte und deren Schulung ist eine große Herausforderung für Betreiber.

Aus der Sicht der Betreiber sind Schulungen und Erfahrungsaustausche ein vielversprechender Ansatz.

5.3.1.3 Festlegung von Verantwortlichkeiten

Gemäß KAS-51 sollten folgende grundlegende Maßnahmen zur Definition von Verantwortlichkeiten von den Betreibern umgesetzt werden:

- Verantwortlichkeit für die Maßnahmen zum Schutz vor Eingriffen Unbefugter muss eindeutig zugewiesen sein.
- Effektive Maßnahmen zum Schutz vor Eingriffen Unbefugter festlegen und dokumentieren.
- Regelmäßige Überprüfung der Maßnahmen.

- Vertraulichkeit bezüglich der getroffenen Schutzmaßnahmen sicherstellen.

Während der Interviews wurde festgestellt, dass die oben genannten Maßnahmen der KAS-51 bei den meisten Betreibern bekannt waren, aber noch nicht erfolgreich umgesetzt wurden. Die Betreiber sind dabei, diese Maßnahmen umzusetzen.

Aus der Sicht des Betreibers ist die Festlegung der Verantwortlichkeiten ein vielversprechender Ansatz und sollte als Teil des OT-Security-Managements definiert werden.

5.3.1.4 Manipulationserkennung und Schutz

Gemäß KAS-51 sollten folgende grundlegende Maßnahmen zur Definition von Manipulationserkennung und zum Schutz von Betreibern umgesetzt werden:

- Sicherung der Anlagen vor Auslösung von Störfällen durch Unbefugte ohne interne Kenntnisse.
- Frühzeitige Erkennung bzw. Verhinderung von Manipulationen an Systemen (z.B. Maßnahmen zum Schutz vor bzw. zur Erkennung von Schadsoftware, Maßnahmen gegen Fehlbedienung).
- Implementierung von Maßnahmen zum physischen Schutz (z.B. Integritätsüberwachung der Zäune und Schlösser, Zutrittsschutz, ggf. Kameraüberwachung).

Während der Interviews wurde festgestellt, dass die oben genannten Maßnahmen der KAS-51 bei den meisten Betreibern bekannt waren und die Maßnahmen von den Betreibern überwacht worden sind.

Aus der Sicht des Betreibers ist Manipulationserkennung und der Schutz davor ein vielversprechender Ansatz und sollte als Teil des Rollen- und Berechtigungsmanagements definiert werden.

5.3.1.5 Awareness

Gemäß KAS-51 sollten folgende grundlegende Maßnahmen zur Definition von Sensibilisierung/Schulung eigener Arbeitskräfte von den Betreibern umgesetzt werden:

- Zielgruppenorientiertes und risikobasiertes Schulungskonzept gegen Eingriffe Unbefugter und zur IT-Security umsetzen.
- Motivation zur Meldung von Abweichungen bzgl. des physischen Schutzes und der IT-Security fördern. Die Meldung sollte über ein betriebliches Meldesystem sichergestellt werden.

Während der Befragung wurde festgestellt, dass einige Betreiber Awareness-Schulungen zur Cyber-Security durchführen.

Aus der Sicht des Betreibers ist Awareness ein gewinnbringender Ansatz und sollte entsprechend konzeptioniert und umgesetzt werden.

5.3.2 Herausforderungen aus Sicht der Behörden

Es wurden sechs Interviews mit Überwachungsbehörden geführt. Die Befragten sind aufgrund sehr unterschiedlicher Auslöser mit dem Thema IT-/OT-Security in Berührung gekommen: teilweise wurde das Thema durch die direkte Arbeit mit den Störfallbetrieben aktuell (Änderungsanzeige zur Migration des PLS, Überwachung, Vorfall in einem Störfallbetrieb), teilweise wurden aber auch interne Projekte oder Gremienarbeit als Auslöser für die Befassung mit dem Thema genannt. Insgesamt lässt sich sagen, dass eine vertiefte Auseinandersetzung mit dem Thema vor allem in den letzten 2-4 Jahren stattgefunden hat.

Bei den mit der Störfallvorsorge betrauten Behörden wurde vielerorts eine Unterstützungsstelle oder eine zentrale Arbeitsgruppe/Abteilung gebildet, die sich mit dem Thema Safety & Security befasst und für die Sachbearbeiter entsprechende Arbeitshilfen erarbeitet. Außerdem stehen diese Stellen den Sachverständigen für Fragen sowie unterstützend zur Verfügung.

5.3.2.1 Fachliche Kompetenz / Qualifikation der Arbeitskräfte

Alle befragten Arbeitskräfte von Behörden nannten übereinstimmend den Aufbau von fachlicher Kompetenz im Themenkomplex IT-/OT-Security als eine der größten Herausforderungen. Die fachliche Kompetenz sei bei den Arbeitskräften der Störfallreferate nicht bzw. nicht im erforderlichen Umfang vorhanden, da das Thema bisher nur eine untergeordnete Rolle gespielt habe. Für den Aufbau der fachlichen Kompetenzen sind aus Sicht der Befragten umfangreiche Schulungen bzw. Weiterbildungen erforderlich. Bezüglich der Schulungsinhalte besteht dabei jedoch teilweise eine Unsicherheit, da nicht klar ist, welche Kompetenzen im Einzelnen für die Arbeitskräfte der mit der Störfallvorsorge befassten Behörden überhaupt notwendig sind. In diesem Zusammenhang wurde auch der Wunsch nach Unterstützung durch das BSI geäußert.

5.3.2.2 Ressourcen

Auch die für die Auseinandersetzung mit dem Thema IT-/OT-Security notwendigen Ressourcen stellen aus Sicht der Befragten eine sehr große Herausforderung dar. Die Auslastung der mit der Störfallvorsorge befassten Behörden ist ohnehin schon groß; die Auseinandersetzung mit zusätzlichen (neuen) Themenkomplexen ist allein aus Kapazitätsgründen schon schwierig. Zeit für erforderliche Fort- bzw. Weiterbildungen ist kaum vorhanden.

Laut einer Studie von McKinsey (26) wird sich dieses Problem in den nächsten Jahren noch weiter verschärfen: bis 2030 ergibt sich durch das altersbedingte Ausscheiden von Arbeitskräften sowie fehlenden Nachwuchskräften eine Personallücke von rund 730.000 Beschäftigten im öffentlichen Sektor in Deutschland.

Ein Mangel an Fachkräften aus dem Bereich IT-/OT-Security insgesamt wurde in diesem Zusammenhang nicht nur von den Behörden beklagt; auch die befragten Betreiber und Sachverständigen berichteten von Problemen, entsprechende Fachkräfte zu rekrutieren.

5.3.2.3 Bewertungsmaßstäbe

Auch der Umgang mit den Bewertungsmaßstäben wird von einigen der befragten Behörden als große Herausforderung betrachtet. Dabei wird vor allem mit Blick auf die KAS-51 beklagt, dass der Leitfaden zwar die Anforderungen vorgibt, jedoch keinerlei Aussage über die Qualität der Umsetzung trifft. Weiterhin wurden Probleme mit der Vielzahl an unterschiedlichen Regelwerken genannt, die von den Betreibern referenziert wurden. Durch die uneinheitliche Umsetzung der Anforderungen aus der KAS-51 wird der aufsichtsrechtliche Vollzug erschwert.

In diesem Zusammenhang wurde von mehreren Befragten der Wunsch geäußert, die Bewertungsmaßstäbe zu vereinheitlichen.

Mit Blick auf die speziellen Herausforderungen, die sich aus den Anforderungen der KAS-51 für die Aufsichtsbehörden ergeben, wurden die Plausibilitätsprüfung der Einschätzung der Bedrohungslage, die Prüfung von Sicherungsmanagementbausteinen gem. Anhang I des Leitfadens KAS-51 sowie die Feststellung

einer besonderen Gefährdung genannt. Eine weitere Konkretisierung bzgl. der Umsetzung dieser Anforderungen erscheint somit dringend erforderlich.

5.3.2.4 Herausforderungen mit Blick auf die Betreiber

Mit Blick auf die Betreiber von Betriebsbereichen sehen die Vertreter der Aufsichtsbehörden die größten Herausforderungen bei der Koordinierung der Schnittstelle PLT und IT. Diese Bereiche agieren vielerorts noch völlig unabhängig voneinander. Hier muss ein gemeinsames Verständnis entwickelt werden.

Als problematisch wird zudem die Umsetzung der Basisanforderungen aus der KAS-51 in kleinen und mittleren Unternehmen (KMU) gesehen. Hier fehlen aus Sicht der Befragten häufig schlicht die personellen Kapazitäten, um das Thema anzugehen.

Ein Lösungsansatz könnte hier die Vereinheitlichung der Regelwerke sowie die Erarbeitung einer Handreichung für KMU durch die Branchenverbände oder das BSI sein.

5.3.3 Herausforderungen aus Sicht der Sachverständigen

Es wurden Interviews mit insgesamt sechs Sachverständigen geführt. Die Befragten haben in Abhängigkeit vom Alter und fachlichen Schwerpunkten, auf unterschiedlichen Wegen zu dem Thema OT-Security gefunden. Markante Einstiegspunkte waren Technologiewechsel (wie Einführung von SPS oder Fernwartungszugängen), die sie in Anlagen überprüft haben und Regelwerksänderungen (IEC 61511, VDI/VDE 2180 und KAS-51). Da das Thema erst in den letzten Jahren an Relevanz gewonnen hat, besitzen derzeit noch nicht alle Sachverständige praktische Erfahrungen.

5.3.3.1 Prüfgrundlage

In der Praxis wird das Thema OT-Security noch sehr unterschiedlich gehandhabt. Zum Beispiel wird in einigen Änderungsverfahren von Behörden eine Überprüfung der OT-Security gefordert oder in Anlageninspektionen abgefragt. Einige der Befragten gaben an, dass sie die OT-Security Fragestellungen im Rahmen ihrer Prüfaufgabe bei den Betreibern ansprechen oder diese in ihren Berichten schriftlich darauf hinweisen, dass eine Überprüfung der OT-Security mangels Angaben des Betreibers nicht vorgenommen werden konnte. Bei auskunftswilligen Betreibern erfolgt in der Regel eine Abfrage von Basisanforderungen der OT-Security. Technische Prüfungen zur Cyber-Sicherheit sind derzeit noch nicht die gängige Prüfpraxis.

Zwei der Befragten sehen Defizite im Regelwerk als Ursache für die Unklarheiten bezüglich der Prüfumfänge, Prüftiefe und den Bewertungsmaßstäben. Klarstellungen in der 12. BImschV bzw. der Seveso-Richtlinie und/oder den Prüfungsbereichen für Sachverständige, wurden als mögliche Maßnahmen benannt.

5.3.4 Aus- und Weiterbildung

Der Aufbau von Ressourcen auf Seiten der Sachverständigenorganisationen ist aufgrund von Unklarheiten bzgl. der rechtlichen Grundlage, Anforderungen an die Qualifikation und zukünftiger Nachfrage an Security Prüfungen noch verhalten. Aus Sicht einzelner Sachverständiger ist das Sammeln erster Erfahrungen mit dem Thema in Konformitäts-Assessments zur KAS-51 ein vielversprechender Ansatz. Der für Konformitäts-Assessments notwendige Schulungsaufwand für Arbeitskräfte ist gering, da für den Einstieg und Zugang zu dem Thema Cyber-Security zunächst die Vermittlung von Grundlagen ausreicht.

Für § 29b-Sachverständige und Prüfer der Funktionalen Sicherheit umfassen Grundlagenschulungen die Vermittlung von Begriffen und Methoden, wie diese u.a. im ICS-Security-Kompendium (24) zusammengestellt sind. Im Rahmen von Erfahrungsaustauschen wird das Thema dann inhaltlich mit den Konformitäts-Assessments und praktischen Erfahrungen verknüpft. Praxisbeispiele zu Schulungsformaten sind im Kapitel 6.5 zusammengestellt.

Ferner halten einige der Sachverständigen die Mitarbeit in Arbeitskreisen zur Regelwerkserstellung für eine gute Chance, um sich in das Thema tiefer einzuarbeiten. Zur Zeit tauschen sich beim Verband der Technischen Überwachungs-Vereine (VdTÜV) Vertreter der TÜV darüber aus, wie und in welchem Umfang zukünftig einheitlich Cyber-Sicherheitsaspekte in Anlagen überprüft werden sollen. In einem BSI-Projekt wird mit Vertretenden der NAMUR ein Grundschutzpapier „Chemie“ abgestimmt, das Anforderungen an den Schutz gegen Cyber-Risiken bei typischen OT-Netzwerkstrukturen definiert.

Die größte Herausforderung sehen die Befragten beim Aufbau von Sachverständigenressourcen mit dem erforderlichen Spezialwissen. Der Wissensaufbau notwendiger verfahrenstechnischer und prozessleittechnischer Kenntnisse ist bereits recht groß und zusätzlich sind Expertisen auf dem Gebiet der Cyber-Sicherheit erforderlich. Aufgrund der Gerätevielfalt und der herstellerspezifisch unterschiedlichen Ansätze zur OT-Security, ist der Umfang an notwendigem Wissen für Cyber-Sicherheit sehr groß.

Von Seiten der Hersteller liegen außerdem nicht zu allen in den Anlagen eingesetzten Sicherheitssteuerungen auch Handbücher/Dokumentation zur Cyber-Sicherheit vor. So gesehen sind wesentliche Informationen zur sicheren Integration (z.B. Anforderungen an das Netzwerk der Betreiber), den sicheren Betrieb (z.B. Anforderung an Updates und Patches) und der sicheren Entsorgung (z.B. Löschung von sensiblen Daten) nur unvollständig verfügbar und damit nicht direkt prüfbar.

5.3.5 Austausch unter den Beteiligten

Unterschiedliche Arbeitskreise u.a. die NAMUR und der VdTÜV befassen sich mit den Themen Cyber-Risikoanalyse, Grundschutz von Automatisierungstechnik der chemischen Industrie und Prüfung der Cyber-Sicherheit von überwachungsbedürftigen Anlagen. Der Austausch zwischen den Beteiligten wurde von den Sachverständigen als gute Möglichkeit angesehen, um das Thema besser zu durchdringen. Nicht jeder der 304 § 29b-Sachverständigen oder Prüfer der Funktionalen Sicherheit kann aktiv in den Arbeitskreisen mitarbeiten.

Daher sahen einige Sachverständige es für zielführend an, wenn eine Liste von Ansprechpersonen zu verschiedenen Fragestellungen existieren würde.

6 Praxisbeispiele aus den Interviews

Innerhalb der Interviews wurden neben Herausforderungen auch Bereiche evaluiert, in denen die Befragten besonders gute Erfahrungen gemacht haben. Diese werden in den folgenden Kapiteln vorgestellt, damit Sie von den Erfahrungen anderer Betreiber, Behörden oder Sachverständiger profitieren und in diesem Umfeld Anregungen für die eigene Organisation mitnehmen können.

In Abbildung 29 sind mehrfach von Interviewten genannte Aspekte den verschiedenen Abschnitten der ISO 27001 zugeordnet. Weitere anregende Praxisbeispiele, die einzelne Interviewte benannt haben, sind in der Auswertung der Interviews im Anhang 1-3 enthalten.

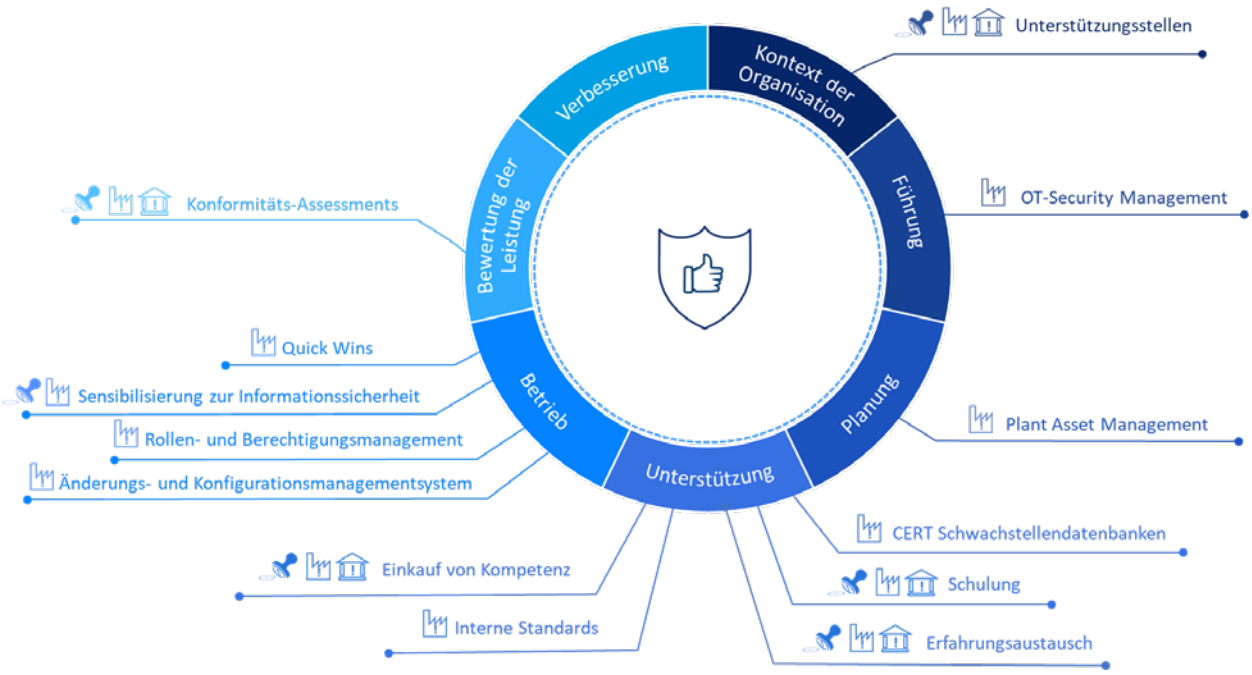

Abbildung 29 Praxisbeispiele zugeordnet auf die Abschnitte der ISO 27001

6.1 Unterstützungsstellen / Stabsstellen

Sowohl Betreiber als auch Arbeitskräfte von Behörden und Sachverständige haben im Interview berichtet, dass sie positive Erfahrungen mit der Einrichtung von zentralen Unterstützungsstellen, Stabsstellen oder auch internen Arbeitskreisen zum Themenbereich IT-/OT-Security gemacht haben. Dabei wurde vor allem die Unabhängigkeit einer solchen Stelle herausgestellt sowie die Ausstattung mit einem eigenen Budget.

Die Bildung einer solchen Unterstützungsstelle liefert eine Reihe von Vorteilen: so führt die Einrichtung einer Unterstützungsstelle zur Entlastung einzelner Instanzen, vor allem der Führungskräfte. Entscheidungen werden sorgfältiger getroffen, da eine intensivere Auseinandersetzung mit dem Thema Security erfolgt. Zudem verfügen solche Stellen über ein hohes Fachwissen; durch die Stablinienorganisation findet ein Ausgleich zwischen dem Fachwissen der Stäbe und dem Überblick der Linieninstanzen statt.

Die Interviews haben gezeigt, dass derartige Unterstützungsstellen bereits eine weite Verbreitung haben. Diese Stabsstellen erarbeiten vielerorts interne Standards oder auch Arbeitshilfen für die Mitarbeitenden in den einzelnen Bereichen des Unternehmens.

Sinnvoll ist sicherlich die Ausstattung solcher Stellen mit einem eigenen Budget, da sie so unabhängig werden und zudem auch von den einzelnen Bereichen zu bestimmten Fragestellungen konsultiert werden.

6.2 OT-Security-Management

Das wachsende Cyber-Risiko in OT-Netzwerken veranlasst viele Betreiber zu einem proaktiven Ansatz im Umgang mit den Cyber-Risiken der OT-Systeme und -Netzwerke durch die Umsetzung eines OT-Security-Managements. Ziel des OT-Security-Managements ist es, die OT-Security zu managen, zu kontrollieren, aufrechtzuerhalten und kontinuierlich zu verbessern.

Anleitungen zur Implementierung und Struktur eines OT-Security-Management finden sich u.A. in:

- IEC 62443 Cyber-Sicherheit von „industriellen Automatisierungs- und Steuerungssystemen (IACS)“
- ISO/IEC 2700x Informationssicherheitsmanagementsysteme
- BSI IT Grundschutz Kompendium
- VDI/VDE 2182 Richtlinie zur Informationssicherheit in der industriellen Automatisierung

Obwohl der Prozess der Implementierung eines Managementsystems im OT-Netzwerk dem eines IT-Netzwerks (ISMS) ähnelt, gibt es einige wichtige Punkte, die beachtet werden müssen:

- Der erste und wichtigste Punkt ist die Priorisierung von Cyber-Sicherheitsmaßnahmen. In IT-Netzwerken wird die Vertraulichkeit der Informationen als oberste Priorität angesehen, während im OT-Netzwerk die Integrität des Systems und der Komponenten, sowie die Verfügbarkeit der PLT-Sicherheitseinrichtungen, als oberste Priorität angesehen werden.
- Das System und die Komponenten in OT-Netzwerk sind im Vergleich zu denen im IT-Netzwerk komplexer. Alle technischen Eigenschaften der Systeme (z.B. Temperatur, Druck usw.) müssen beobachtet werden.

In Bezug auf diese Punkte ist die wichtigste Aufgabe bei der Implementierung eines OT-Security-Managementsystems das Bewerten und Behandeln von Risiken. Das Risikomanagement hilft dem Betreiber, Risiken, die das System birgt, zu erkennen und entsprechende Gegenmaßnahmen zu definieren. Die Beschreibung einer detaillierten Cyber-Risikoanalyse ist in den folgenden Kapiteln dieser Studie enthalten.

Eine weitere wichtige Aufgabe für die sichere Umsetzung des OT-Security-Managementsystems ist die klare Verteilung der Verantwortlichkeiten unter den Mitarbeitenden für die OT-Security. Beim OT-Security-Management ist es wichtig, die Rollen zwischen IT und OT aufzuteilen, z.B. durch Benennung einer verantwortlichen Person für OT-Security, die alle für die Cyber-Sicherheit relevanten Informationen im Büronetzwerk verwaltet, und einer verantwortlichen Person für OT-Security, die gute Kenntnisse über die im OT-Netzwerk verwendeten Systeme hat und somit die Cyber-Sicherheit dieses Systems verwaltet.

Ein Beispiel für die Verteilung von Rollen und Verantwortlichkeiten unter den Mitarbeitenden in verschiedene Teams ist in der nachfolgenden Abbildung 21 dargestellt.

Abbildung 30 Rollen und Verantwortlichkeiten der OT-Security in Anlehnung an (27)

Aus der Abbildung 30 ist ersichtlich, dass die Rollen und Verantwortlichkeiten des OT-Security-Managements in sechs Teams aufgeteilt sind, wobei das untere Dreieck (Yellow, Red, Blue) eher die technische Ebene und das obere Dreieck (Purple, Green, Orange) eher die organisatorische Ebene charakterisiert (28).

Abbildung 21 teilt die Teams grundsätzlich in verschiedene Farben ein, sodass der Name der Teams entsprechend dieser Farben vergeben wird:

- Das „Red Team“ besteht aus internen oder externen Stellen, die für die Prüfung (z.B. Penetrationstest) der Verwundbarkeit eines Systems und die Prüfung der Wirksamkeit der Cyber-Sicherheitsmaßnahmen verantwortlich sind.
- Das „Blue Team“ besteht aus Stellen, die für die innere Cyber-Sicherheit verantwortlich sind und sowohl gegen echte Angreifende als auch gegen das Red Team verteidigt. Diese Stellen sind dafür verantwortlich, auf Cyber-Angriffe so schnell wie möglich zu reagieren.
- Das „Purple Team“ bezieht sich auf Stellen, die dafür verantwortlich sind, die Effektivität des Red Teams und des Blue Teams zu gewährleisten und zu maximieren.
- Das „Yellow Team“ bezieht sich auf Stellen, die für die Administration der im OT-Netzwerk vorhandenen Komponenten zuständig sind.

- Das „Green Team“ ist dafür zuständig, nach der Entdeckung eines Angriffs daran zu arbeiten, den Schaden zu reduzieren. Das Green Team arbeitet mit dem Yellow Team und dem Blue Team zusammen.
- Das „Orange Team“ ist verantwortlich für die Umsetzung von Änderungen, die aufgrund der Ergebnisse der vom Red Team durchgeführten Cyber-Sicherheitstests notwendig werden. Das Orange Team arbeitet mit dem Yellow Team und dem Red Team zusammen.

Das Zusammenspiel aller Teams macht die Praktiken und das Vorgehen hinsichtlich des Security-Managements, der Analyse und der Konformität aus. Hier werden die aus echten Angriffen gewonnenen Erkenntnisse umgesetzt.

6.3 Plant Asset Management

Einige der Betreiber äußerten positive Erfahrungen mit der Nutzung eines Plant-Asset-Managements.

Der Begriff Asset-Management leitet sich aus dem in der Volks- und Betriebswirtschaft verwendeten Begriff der Vermögensverwaltung ab und beschreibt in Bezug auf IT-Systeme die strategische Verwaltung von Software- und Hardware-Assets. Dies umfasst den gesamten Lebenszyklus (Planung, Engineering, Beschaffung, Inbetriebnahme, Betrieb, Wartung und Instandhaltung, Austausch und Entsorgung) mit dem Ziel, ihren Geschäftswert zu maximieren. Hierbei wird auch von „ITAsset Management“ (ITAM) gesprochen.

Das Plant-Asset-Management stellt bezogen auf die betrachteten Assets eine Erweiterung des ITAM dar. Gemäß VDI 2651 Blatt 1 bedeutet Plant-Asset-Management die Verwaltung von Vermögenswerten (Assets) in Form von Anlagegütern eines Unternehmens, die speziell für die Produktion eingesetzt werden. Dies sind, auf der Ebene des Anlagenteils:

- Static Equipment, z.B. Behälter, Rohrleitungen, Wärmetauscher
- Rotating Equipment, z.B. Pumpen, Verdichter, Rührer
- Maschinen, z.B. Verpackungsmaschinen
- Feldgeräte der Automatisierungstechnik, z.B. Ventil, Umrichter, Sensorsystem, Motor
- Hardware der Automatisierungskomponenten, z.B. Kommunikationsnetzwerk, SPS, Bediengerät
- Software der Automatisierungskomponenten, z.B. Prozessmodell, Regelungsfunktion, Softsensor

Im Gegensatz zum ITAM liegt der Fokus beim Plant-Asset-Management auf der Phase des Anlagenbetriebs inklusive der Instandhaltung, die gleichzeitig die längste Phase im Lebenszyklus darstellt.

Durch die zunehmende Digitalisierung im Sinne einer Industrie 4.0 muss das Plant-Asset-Management zunehmend auch Bestandteile des ITAM berücksichtigen, da Werte der Cyber-Sicherheit wie Vertraulichkeit, Integrität und Verfügbarkeit für den Betrieb verfahrenstechnischer Anlagen an Bedeutung gewinnen. Plant-Asset-Management dient u.a. der Effizienzsteigerung der Produktionsprozesse, d.h. Produktionsmittel im Sinne des Einsatzes und der Erträge zu optimieren. Somit ist das Ziel der Verfügbarkeit im Sinne der Cyber-Sicherheit sicherlich im Schwerpunkt mitberücksichtigt, durch die Eingrenzung auf den reinen Produktionsprozess und den Betrieb inklusive Instandhaltung der Anlage fehlt aber die Berücksichtigung der Kriterien des ITAM.

Damit ein Plant-Asset-Management gewinnbringend eingesetzt werden kann, müssen sowohl die Komponenten der IT als auch die der OT integriert werden. Konzepte der IT, wie beispielsweise Patchzyklen, Härtung und Schwachstellenmanagement, sollten auf die Komponenten der OT übertragen und im Plant-Asset-Management berücksichtigt werden.

Zusammenfassend ist die Ausweitung des ITAM auf das Plant-Asset-Management aufgrund der unterschiedlichen Anforderungen und Interessen eine Herausforderung. Allerdings kann die Vernetzung industrieller Fertigungsanlagen und -prozesse nur unter höchsten Absicherungen gelingen, da die finanziellen Schadwirkungen und Gefahren für Leib und Leben hoch sind.

Ein umfassendes Plant-Asset-Management, das sowohl Komponenten der IT als auch der OT integriert, erhöht die Anlagensicherheit durch die Identifikation und Überwachung der Einzelbestandteile.

Umfassende Beschreibungen zur Implementierung eines Plant-Asset-Managements können Sie den folgenden Veröffentlichungen entnehmen:

- der VDI Richtlinie 2651 Plant Asset Management (PAM) in der Prozessindustrie
  - Blatt 1: Definition, Modell, Aufgabe, Nutzen
  - Blatt 2: Spezifikationen und Methoden
- Der NAMUR-Empfehlung NE 129 Plant Asset Management

6.4 CERT Schwachstellendatenbanken

Zwei der befragten Betreiber empfinden eine Datenbank mit bekannten Risiken und Schwachstellen als hilfreich. Daher werden nachfolgend einige entsprechende Angebote kurz vorgestellt.

Über den Warn- und Informationsdienst (WID) des "Computer Emergency Response Teams" der Bundesverwaltung (CERT-Bund) werden Informationen zu neuen Schwachstellen und Sicherheitslücken sowie aktuelle Bedrohungen für IT-Systeme publiziert[24]. In erster Linie ist die von CERT-Bund mit diesem Dienst angesprochene Zielgruppe die Bundesverwaltung. Kurzinformationen, die in der Regel die ursprünglichen Sicherheitsempfehlungen / -informationen der Hersteller referenzieren, können aber auch von Unternehmen kritischer Infrastrukturen, CERTs sowie Bürgerinnen und Bürgern abgerufen werden und zur Absicherung ihrer Systeme genutzt werden.

Wenn das herstellende Unternehmen nicht ausreichend oder nicht rechtzeitig eigene geeignete Maßnahmen ergriffen hat, erstellt das BSI formale BSI-Warnungen gem. § 7 BSIG[25].

Ein ähnliches, jedoch spezifischeres Angebot wird durch das „Industrial Control Systems Cyber Emergency Response Team“ (ICS-CERT) zur Verfügung gestellt. Das ICS-CERT ist Teil des „United States Computer Emergency Readiness Team“ (US-CERT) der „Cyber-Security and Infrastructure Security Agency“ (CISA), die dem „Department of Homeland Security (DHS)“ untergeordnet und unter anderem speziell für die Sicherheit von industriellen Steuerungssystemen und kritischen Infrastrukturen zuständig ist. ICS-CERT unterstützt Hersteller, Integratoren sowie Betreiber von industriellen Steuerungssystemen bei der Identifizierung von Sicherheitslücken und der Entwicklung solider Strategien zur Schadensbegrenzung[26]. Die Informationen sind frei zugänglich und in folgende Rubriken unterteilt:

- „Alerts“ warnen Betreiber kritischer Infrastrukturen zeitnah über Bedrohungen.
- „Advisories“ bieten Informationen zu aktuellen Sicherheitsproblemen, Schwachstellen und Exploits.
- „Reports“ umfassen Berichte, die den Schutz industrieller Steuerungssysteme adressieren.

In Deutschland wird ein entsprechendes Angebot speziell für kleine und mittlere Unternehmen (KMU) im Bereich Industrieautomation durch den Verband der Elektrotechnik, Elektronik und Informationstechnik (VDE) unter dem Namen „CERT@VDE“ zur Verfügung gestellt[27].

Eine Internetrecherche zum Thema „Schwachstellendatenbanken“ liefert eine Vielzahl weiterer Ergebnisse, so dass eine Auswahl aufgrund verschiedener Kriterien wie Branche, Größe der Organisation oder auch aufgrund der eingesetzten Produkte zu treffen ist.

[24] https://www.cert-bund.de/wid
[25] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Technische-Sicherheitshinweise-und-Warnungen/Warnungen-nach-Par-7/warnungen-nach-par-7_node.html
[26] https://us-cert.cisa.gov/ics
[27] https://cert.vde.com/de-de

Sinnvoll erscheint vor diesem Hintergrund, ebenfalls die Security Warnhinweise der Hersteller von im Betrieb eingesetzten Automatisierungslösungen zu abonnieren.

6.5 Schulung

Um die Mitarbeitenden auf ihre Aufgaben vorzubereiten und sie zu befähigen diese zu erfüllen, müssen Mitarbeitende entsprechend geschult werden. Dabei ist zu berücksichtigen, dass insbesondere die Personen mit Schnittstellenfunktionen sowohl mit Aspekten der OT als auch mit Aspekten der IT vertraut gemacht werden sollten. Beide Welten werden zukünftig immer stärker verschmelzen. Daher sollte dieser Ansatz auch für Mitarbeitende verfolgt werden, die sich schwerpunktmäßig in einer der beiden Welten bewegen, um sich in der jeweils anderen zurechtzufinden. So wird die Kommunikation der Teammitglieder verbessert und Missverständnissen vorgebeugt.

Für den Bereich IT sollten Schulungen besucht werden, die vergleichbar mit einer der nachfolgenden Schulungen sind:

- Einführung / Implementierung der ISO/IEC 27001
- TeleTrusT Information Security Professional
- IT-Sicherheitsbeauftragte (ITSiBe) / Chief Information Security Officer (CISO)
- Certified Information Security Manager (CISM)

Für den Bereich OT sollten Schulungen besucht werden, die thematisch den folgenden Aspekten entsprechen:

- Cyber-Security in der Industrieautomatisierung (ISO/IEC 62443)
- ICS Security-Manager gemäß IEC 62443, ISO 27001 und BSI IT-Grundschutz

Für den Bereich Anlagensicherheit in Störfallbetrieben bieten sich folgende Schulungen als Grundbausteine an:

- Störfallbeauftragte nach § 58a BImSchG
- Sicherheitsmanagementsystem nach Anhang III der 12. BImschV

Darüber hinaus sollten schwerpunktspezifische Schulungen rollenabhängig besucht werden, wie beispielsweise:

- IT-Notfallmanagement / Business Continuity Management (BCM)
- Notfallübungen in Betriebsbereichen und Organisationsstrukturen
- IT-Security in öffentlichen Verwaltungen
- Der Mensch als IT-Security-Faktor

Die Kenntnisse aus den Schulungen sollten ins Unternehmen getragen werden. Dazu bedarf es einer Kultur im Unternehmen, die sich durch Offenheit für Neues und als lernbereit charakterisiert.

6.6 Erfahrungsaustausch

Sowohl die befragten Betreiber als auch Behörden und Sachverständige gaben an, dass ihnen der Erfahrungsaustausch mit Personen oder Organisationen, die einer ähnlichen Fragestellung unterliegen oder an dieser arbeiten, weitergeholfen hat.

Ein Erfahrungsaustausch kann dabei auf verschiedenen Ebenen stattfinden:

- horizontal mit anderen Organisationen des gleichen Umfelds – Behörden mit anderen Behörden, Betreiber mit anderen Betreibern oder Sachverständige mit anderen Sachverständigen,
- vertikal über Behörden, Sachverständige und Betreiber hinweg oder
- intern zwischen verschiedenen Personen, Funktionen oder Abteilungen.

Dabei haben sich in der Praxis für horizontale Erfahrungsaustausche bereits unterschiedliche Schwerpunkte wie beispielsweise kritische Infrastrukturen etabliert. Es bietet sich an, sich bei Behörden oder Branchenverbänden zu einem passenden Kreis zu informieren.

Für den internen Erfahrungsaustausch müssen entsprechende Freiräume (zeitlich, ggf. auch räumlich) geschaffen werden, die sowohl einen informellen als auch einen formellen Erfahrungsaustausch zwischen verschiedenen Beteiligten ermöglichen. Zudem muss ersichtlich sein, welche Person bei bestimmten Fragestellungen angesprochen werden kann.

Sowohl horizontal als auch vertikal erfolgt ein Erfahrungsaustausch, auch auf Messen oder Fachtagungen. Bei einem Besuch der gängigen Messen, wie beispielsweise der it-sa in Nürnberg (jährlich im Oktober) oder der SPS Smart Production Solutions (früher SPS IPC Drives, jährlich im November in Nürnberg) werden sowohl Wissen durch die Vorträge in den Foren vermittelt als auch interessante Kontakte im persönlichen Gespräch geknüpft.

Für unterschiedliche Schwerpunkte, wie beispielsweise Schulung und Awareness (Take Aware, jährlich im Frühjahr) oder kritische Infrastrukturen (Protekt, jährlich im November) gibt es kleinere Fachtagungen, in denen ein Erfahrungsaustausch ermöglicht wird.

6.7 Interne Standards

Eine der befragten Organisationen hat gute Erfahrungen mit der Einführung von internen Standards gemacht. Andere Betreiber bemängeln das Fehlen von internen Standards oder haben Schwierigkeiten bei einer konzernweiten Umsetzung.

Interne Standards unterstützen Organisationen grundsätzlich durch die Vereinheitlichung von Prozessen, um u.a. die Kosteneffizienz und den Wissenstransfer zu steigern. Auch ermöglicht die Definition von Anforderungen an einen Prozess oder eine Anlage eine spätere Überprüfung der Prozesse, die zu einer kontinuierlichen Verbesserung beiträgt.

Der Einsatz von standardisierten Geräte mit Verfahrensanweisungen erhöht die Verfügbarkeit durch leichteren Ersatz und macht weniger abhängig von personellen, individuellen Spezialwissen der Mitarbeitenden.

Allerdings wird die Standardisierung durch den Grad der Diversifikation der Produkt- und Prozesstiefe, sowie durch technische Unterschiede der Produktionsanlagen, erschwert.

Daher sollte die Einführung interner Standards durch die Geschäftsführung initiiert werden. Als förderlich hat sich dafür der Aufbau einer Organisation oder Organisationseinheit zur Koordinierung und Vereinheitlichung erwiesen. Bei internationalen Organisationen besteht zudem eine Herausforderung darin, unterschiedliche nationale Anforderungen zu berücksichtigen.

6.8 Einkauf von Kompetenz

In den Interviews stellte sich heraus, dass einige der befragten Organisationen sehr vom Einkauf von Kompetenz profitieren. Dies traf gleichermaßen auf Betreibende, Behörden und Sachverständige zu. Da das IT/OT Umfeld sehr komplex und vielschichtig ist, ist es sinnvoll - insbesondere für spezielle Fragestellungen - externe Fachkräfte mit entsprechendem Fachwissen hinzuzuziehen, sofern diese in der Organisation oder Unternehmung nicht verfügbar sind. Nachdem ein Überblick der anstehenden Aufgaben erstellt worden ist,

können diese Aufgaben auch gut an externe Firmen vergeben werden. Es ist empfehlenswert auf Unternehmen zu vertrauen, mit denen Sie selbst oder andere Organisationen derselben Branche bereits positive Erfahrungen gemacht haben. Nichtsdestotrotz sollten Sie den Anbietenden, je nach Fachgebiet, nach einem gewissen Zeitraum wechseln, da sich eine gewisse Betriebsblindheit auch bei externen Beratern einstellen kann.

Neben einem Beratungsunternehmen, das den Aufbau der Organisation in Bezug auf Informationssicherheit generell betreut, werden nachfolgend einige Bereiche vorgestellt, in denen sich die Unterstützung durch externe Kompetenz in den Interviews als empfehlenswert herausgestellt hat:

- Durchführung von Penetrationstests
  Durch Penetrationstests werden zuvor definierte Systeme oder Komponenten hinsichtlich deren technischer Absicherung geprüft. Durch den definierten Umfang lassen sich diese gut extern beauftragen. Insbesondere die Komponenten, die von außen erreichbar sind sowie diejenigen, die einem hohen Schutzbedarf unterliegen, sollten regelmäßig und insbesondere nach Änderungen einem Penetrationstest unterzogen werden.
- Security Operations Center (SOC)
  In einem SOC bzw. Cyber-Abwehrzentrum wird die Angriffslage auf die Organisation überwacht. Im Gegensatz zur eigenen Organisation erfolgt die Überwachung durch ein SOC 24/7. Angriffe können so frühzeitig entdeckt und ihnen entgegengewirkt werden.
- Patchdienste durch Hersteller
  Insbesondere beim Einkauf von Komponenten sollte darauf geachtet werden, dass diese auch zukünftig mit Updates und Patches versorgt werden. Die Unternehmen, die die Produkte herstellen, sollten somit auch zukünftig Patches für diese bereitstellen, um Schwachstellen zu beseitigen. Darüber hinaus bieten viele Herstellende einen Patchdienst an, durch den sie die Organisationen dabei unterstützen, die Patches einzuspielen. Dabei kann der Grad der Unterstützung zuvor vertraglich vereinbart werden. Die Bandbreite reicht von der reinen Möglichkeit der Kontaktaufnahme „im Fall der Fälle“ bis hin zum vollständigen Einspielen der Patches durch den Hersteller.
- Incident Response
  Sollte die Organisation trotz zahlreicher proaktiver Vorkehrungen erfolgreich infiltriert worden sein und es zu einem Cyber-Sicherheitsvorfall kommen, bieten zahlreiche Unternehmen Unterstützung zur Behebung des Cyber-Sicherheitsvorfalls an. Es ist durchaus sinnvoll, sich bereits im Vorfeld mit der Beauftragung eines Unternehmens auseinanderzusetzen. Die Verträge können derart gestaltet werden, dass beispielsweise eine Zeitspanne definiert wird, innerhalb der das Unternehmen aktiv werden muss, um bei der Behebung des Cyber-Sicherheitsvorfalls zu unterstützen.

Zum Vergleich von unterschiedlichen Anbietenden bietet sich neben einer gängigen Marktrecherche, ein Blick in die aktuelle Gartner-Studie[28] (Magic Quadrant) zu dem entsprechenden Aspekt an.

6.9 Änderungs- und Konfigurationsmanagementsystem

Einer der befragten Betreiber eines Betriebsbereichs hat gute Erfahrungen mit der Einführung eines Änderungsmanagements hervorgehoben.

Das Änderungsmanagement definiert ein Vorgehen zur Erfassung, Bewertung, Entscheidung, Umsetzung und Nachverfolgung von Änderungen. Es ist eine bewährte Methode, mit der Anlagensicherheits-, Gesundheits- und Umweltrisiken und -gefährdungen im Zusammenhang mit Änderungen an Einrichtungen, Betrieben oder Personal eines Unternehmens kontrolliert werden. Ein ordnungsgemäß umgesetztes Änderungsmanagement vermindert ein erhöhtes Risiko für aktuelle Gefährdungen und schützt vor der Einführung neuer Gefährdungen.

[28] https://www.gartner.com/en/information-technology/research/magic-quadrant

Die Anforderungen an den Prozess „Änderungsmanagement“ sind für verschiedene Managementsysteme ähnlich und lassen sich (grob) wie folgt zusammenfassen:

1. Beschreibung der Änderung (Änderungsantrag).
2. Umfang der Änderung analysieren.
3. Auswirkungen (Risiko) abschätzen.
4. Änderungen zur Realisierung freigeben.
5. Änderungen realisieren und durchführen.
6. Änderungen qualifizieren / testen.
7. Änderung freigeben.
8. Änderung in Produktivumgebung implementieren.
9. Änderungsprozess abschließen.

Ein Änderungsmanagement ist auch für industrielle Automatisierungssysteme zu installieren, da sich durch Änderungen an diesen Systemen ggf. Einfallstore für Angreifende öffnen. Auf der anderen Seite ergibt sich aus der immer schnelleren Entwicklung in der IT/OT die Notwendigkeit, die Komponenten der industriellen Automatisierungssysteme korrekt und zeitnah zu aktualisieren, z.B. um ggf. vorhandene Cyber-Sicherheitslücken zu schließen.

In diesem Zusammenhang wird häufig der Begriff Konfigurationsmanagement oder Konfigurationsverwaltung verwendet. Gem. DIN EN IEC 62443-2-4, Tabelle A.1, SP.06.XX, bezeichnet die Konfigurationsverwaltung die Dokumentation der genauen logischen und physischen Infrastruktur der Automatisierungslösung, einschließlich ihrer Netzwerkkomponenten und internen und externen Schnittstellen. Als Ergebnis muss es möglich sein, mit der Konfigurationsverwaltung die Geräte und ihre Einstellungen zu prüfen und zu verifizieren.

Das Änderungsmanagement ist in diesem Zusammenhang Teil des Konfigurationsmanagements und kann außerdem auch Bestandteil des Asset-Managements sein.

Das IT-Grundschutz-Kompendium hebt außerdem das Patch-Management als Teilbereich des Änderungsmanagements hervor. Der Begriff Patch-Management bezeichnet die strategische Steuerung zum Einspielen von sogenannten Patches, mit denen erst nach der Markteinführung erkannte Cyber-Sicherheitslücken in Softwareanwendungen geschlossen werden. Ein Patch (deutsch „Flicken“) stopft die Cyber-Sicherheitslücke, behebt Programmfehler und verhindert so den Erfolg von Malware-Angriffen.

Anforderungen an ein Änderungsmanagement sowie Anregungen zur Einführung entsprechender Prozesse, ergeben sich übergeordnet aus den Anforderungen an Managementsysteme, wie z.B.:

- Qualitätsmanagementsystem gem. DIN EN ISO 9001, Kapitel 8.5.6: Überwachung von Änderungen,
- Sicherheitsmanagementsystem gem. Anhang III 12. BImschV, Ziffer 3: Sichere Durchführung von Änderungen,
- Informationssicherheitsmanagementsystem gem. DIN EN ISO/IEC 27002, Kapitel 12.1.2: Änderungssteuerung.

Weitere Konkretisierungen, z.B. bezüglich der Modifikation von PLT-Sicherheitseinrichtungen oder der Änderung von industriellen Steuerungssystemen, können Sie den folgenden Normen und Richtlinien entnehmen:

- DIN EN 61511-1 Funktionale Sicherheit – PLT-Sicherheitseinrichtungen für die Prozessindustrie – Teil 1: Allgemeines, Begriffe, Anforderungen an Systeme, Hardware und Anwendungsprogrammierung, Kapitel 17: Modifikation der PLT-Sicherheitseinrichtung.

- VDI 2180 Blatt 2 Funktionale Sicherheit in der Prozessindustrie – Planung, Errichtung und Betrieb von PLT-Sicherheitsfunktionen, Kapitel 10: Änderungen an PLT-Sicherheitseinrichtungen.
- IT-Grundschutz-Kompendium, Baustein OPS.1.1.3: Patch- und Änderungsmanagement.

Einen Good-Practice-Vorschlag stellt in diesem Zusammenhang die IT Infrastructure Library (ITIL) dar. ITIL ist eine Sammlung vordefinierter Prozesse, Funktionen und Rollen, wie sie typischerweise in jeder IT-Infrastruktur mittlerer und großer Unternehmen vorkommen. Die ITIL enthält u.a. einen Prozess für das Änderungsmanagement.

Die Erfahrung zeigt, dass Prozesse zum Änderungsmanagement im Sinne eines Sicherheitsmanagementsystems gem. 12. BImschV bei einem Großteil der Betreiber von Betriebsbereichen installiert und umgesetzt sind. Auch ein Konfigurationsmanagement für die IT-Systeme ist in den meisten Betriebsbereichen vorhanden und umgesetzt. Sowohl aus der Erfahrung der Projektbeteiligten als auch aus den Interviews ergibt sich jedoch ein Mangel bei der Ausweitung des Konfigurationsmanagements auf den OT-Bereich sowie bei der Umsetzung eines integrierten Managementsystems, das auch alle Schnittstellen und Systeme betrachtet.

6.10 Rollen- und Berechtigungsmanagement

In den Interviews mit Betreibern stellte sich heraus, dass die Definition von Zugriffsrechten in einem konzeptionellen Rollen- und Berechtigungsmanagement einen Mehrwert für den Schutz von Informationen im Bereich IT und OT bietet. Durch ein Rollen- und Berechtigungsmanagement kann die Manipulation technischer Einrichtungen eingeschränkt werden, indem Zugriffsregeln für die Daten eines Systems aufgestellt werden.

Der Begriff Zugriff wird in der Informationssicherheit gemäß BSI wie folgt definiert:

Mit Zugriff wird die Nutzung von Informationen oder Daten bezeichnet. Über Zugriffsberechtigungen wird geregelt, welche Personen im Rahmen ihrer Funktionen oder welche IT-Anwendungen bevollmächtigt sind, Informationen, Daten oder auch IT-Anwendungen zu nutzen oder Transaktionen auszuführen.

Die bestehenden IT-Securitykonzepte bezüglich Rollen- und Zugriffsmanagement lassen sich nicht 1:1 auf Produktionsumgebungen übertragen.

Dies kann auf mehrere Gründe zurückgeführt werden:

- Zudem erheben unterschiedliche Normen, wie ISO 27001, TISAX oder IEC 62443, verschiedene Anforderungen an ein Rollen- und Berechtigungsmanagement.
- Im industriellen Umfeld kommen häufig sogenannte „Package Units“ zum Einsatz, die mit einem eigenen Automatisierungssystem ausgestattet sind. Die Anwendung eines zentralen Rollen- und Berechtigungssystems auf solche Package Units ist nur mit einem relativ großen Aufwand möglich.

Die Umsetzung eines durchgängigen Rollen- und Berechtigungsmanagements ist aus den vorgenannten Gründen daher häufig schwierig. Um einheitliche Standards zu etablieren ist es notwendig, unterschiedliche innerbetriebliche Unternehmenskulturen in Produktion und Büro-IT zu vereinheitlichen. Hierbei können die strukturierten Standards aus der IT auch auf die OT übertragen werden.

Grundsätzlich sollte ein übergreifendes, einheitliches Berechtigungskonzept für IT und OT erstellt werden. Anregungen hierzu können Sie dem BSI IT-Grundschutz entnehmen. Im Baustein ORP.4 Identitäts- und Berechtigungsmanagement sind diverse Anforderungen formuliert. Unterstützend ist ein Blick in die jeweiligen Umsetzungshinweise empfohlen, die die Implementierung der Anforderungen erleichtern.

Auch in den gängigen Normen wie der ISO 27001 oder der IEC 62443 sind Vorgaben zum Rollen- und Berechtigungsmanagement enthalten. Die ISO/IEC 29146 fokussiert die Thematik sogar. Wichtig ist, dass Sie sowohl die Rahmenbedingungen der IT als auch die der OT berücksichtigen und somit ein übergreifendes Konzept entwickeln.

6.11 Sensibilisierung zur Cyber-Sicherheit

In den Interviews mit Organisationen, die einem Störfallbetrieb zugeordnet sind, wurde das Format „Learn at Lunch“ als Erfolgskonzept für die Sensibilisierung von Beschäftigten aufgeführt. Innerhalb eines „Learn at Lunch“ werden Inhalte und Verhaltensweisen mit dem Bezug Cyber-Sicherheit in einem informellen, spielerischen Rahmen und mit Bezug zum Privaten vermittelt.

Die Thematik „Sensibilisierung“ bzw. auf Englisch „Awareness“ grenzt sich insofern von Schulungen ab, dass die Vermittlung von Wissen innerhalb von Sensibilisierung nur einen Aspekt darstellt. Es geht gemäß (8) in erster Linie darum ein Gleichgewicht zwischen den Bereichen „Wissen“, „Können“ und „Wollen“ herzustellen. Zur Veranschaulichung dient das Beispiel einer Phishing-E-Mail: Mitarbeitende müssen wissen, anhand welcher Anzeichen sie die E-Mail als Phishing-E-Mail erkennen können. Anschließend müssen sie organisatorisch dazu in der Lage sein, wie gewünscht reagieren zu können. Das kann beispielsweise bedeuten, dass sie Verfahren haben, mit dem sie den Helpdesk kontaktieren können. Zuletzt müssen die Mitarbeitenden auch sicherheitskonform handeln wollen. Das heißt beispielsweise, dass den Beschäftigten keine Strafe oder kein Nachteil daraus entstehen sollte, dass ein Phishing-Angriff gemeldet wird.

Durch Sensibilisierung, also die Herstellung des Bewusstseins für Schwachstellen oder Cyber-Sicherheitsereignisse, werden die Mitarbeitenden aufmerksam und sind in der Lage die Organisation gemeinsam zu schützen. Dabei muss Sensibilisierung als Gesamtkonzept verstanden werden, das von unterschiedlichen Perspektiven entwickelt wird. Dazu gehören neben Cyber-Sicherheit und Datenschutz auch die interne Unternehmenskommunikation, Personalwesen, physische Sicherheit, IT-Betrieb, Helpdesk sowie Geschäftsführung. Durch einzelne Maßnahmen, wie beispielsweise die Simulation eines Phishingangriffs, werden die drei oben genannten Aspekte – wissen, können, wollen – nicht berücksichtigt. Stattdessen sollte ein Konzept entwickelt werden, das Inhalte, Kommunikationskanäle, Zielgruppen und Zeiträume gegenüberstellt. Zudem sollten die Organisationsspezifika berücksichtigt werden (Aufteilung auf Standorte, Länderspezifika, Hierarchien, Kommunikationsart etc.).

Durch Sensibilisierung als Gesamtkonzept werden Mitarbeitende dazu motiviert, sich mit Aspekten der Cyber-Sicherheit auseinanderzusetzen. Ein Bezug zum Privaten erleichtert die Identifikation mit den oftmals abstrakten Inhalten. So lässt sich beispielsweise sehr gut nachvollziehen, dass eine E-Mail von der eigenen Bank mit der dringlichen Aufforderung die Zugangsdaten zu ändern, mit Vorsicht zu genießen ist. Der gleiche Mechanismus – Dringlichkeit in einer E-Mail, Aufforderung zur Eingabe von Zugangsdaten – sollte auch im geschäftlichen Umfeld zu dem Ergebnis „Vorsicht“ führen. Durch die Verknüpfung des privaten und geschäftlichen Raums, werden die Maßnahmen verständlich und die gewünschten Reaktionen können auf beide Bereiche angewendet werden.

Falls Sie Anregungen für die Umsetzung suchen, bietet sich ein Besuch der fachspezifischen Tagungen „Take Aware“ (jährlich im Frühjahr) sowie dem „SANS Security Awareness Summit“ (halbjährlich im Dezember und Sommer) oder die Lektüre des Buchs „Security Awareness: Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung“ von Dietmar Pokoyski und Michael Helisch (29) an.

6.12 Quick Wins

Vor allem bei den kleineren und mittleren Unternehmen steckt die Umsetzung von OT-Security-Maßnahmen oft noch in den Kinderschuhen. Dies ergibt sich sowohl aus den Interviews mit den Betreibern als auch aus den Interviews mit den Behörden, die dies explizit als Defizit herausgestellt haben.

Die Einführung entsprechender Maßnahmen stellt einen Veränderungsprozess für die entsprechenden Unternehmen dar. In diesem Zusammenhang wird häufig die Erarbeitung frühzeitiger, greifbarer Erfolge – sogenannter „Quick-Wins“ – empfohlen. Quick-Wins sind kleine Erfolge, die mit wenig Aufwand zu erzielen sind, aber eine große Wirkung haben.

Für einen langfristigen Veränderungsprozess sind Quick-Wins sehr wichtig, da sie schnelle Resultate zeigen und das positive Momentum zu Beginn einer Veränderung nutzen.

Als Grundlage für die Erarbeitung solcher Quick-Wins im Zusammenhang mit der Einführung von OT-Security kann die BSI-Veröffentlichung „Industrial Control System Security – Top 10 Bedrohungen und Gegenmaßnahmen 2019“ (23) herangezogen werden. Die Veröffentlichung fasst die zehn kritischsten und am häufigsten auftretenden Bedrohungen für industrielle Automatisierungssysteme zusammen und benennt für jede dieser zehn Bedrohungen mögliche Gegenmaßnahmen. Einige dieser Gegenmaßnahmen sind – im Verhältnis zum Nutzen – einfach umsetzbar. Dabei ergibt sich der große Nutzen vor allem aus der Eliminierung oder zumindest der Minderung der kritischsten und am häufigsten auftretenden Bedrohungen.

Im Folgenden sollen beispielhaft zwei solcher Quick-Wins aus der Veröffentlichung herausgearbeitet werden:

- Als eine TOP Bedrohung für ICS benennt die Veröffentlichung das Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware.
  Als Gegenmaßnahmen werden eine Reihe einfach umzusetzender organisatorischer und technischer Lösungen angeführt. Hierunter sind zum Beispiel physische Sperren gegen (unbefugtes) Anschließen von USB-Geräten durch z.B. Kunstharz, USB-Schlösser oder Ablöten auf Platinen. Zudem kann über eine Organisationsanweisung ein Virenscan für mitgebrachte Notebooks oder Wechseldatenträger vorgeschrieben werden.
- Als eine weitere TOP Bedrohung wird der Einbruch über Fernwartungszugänge genannt.
  Als Gegenmaßnahme wird z.B. die Nutzung von hinreichend sicheren Authentifizierungsverfahren wie z.B. Pre-Shared-Keys, Zertifikate, Hardwaretoken, Einmalpasswörter oder Mehr-Faktor-Authentisierung durch Besitz und Wissen oder die Freischaltung von Fernzugängen durch internes Personal nur für die Dauer und den Zweck der Fernwartung vorgeschlagen. Auch diese Maßnahmen sind vergleichsweise einfach umzusetzen und haben große Auswirkungen auf die Security des ICS.

6.13 Konformitäts-Assessments

Im Rahmen der Interviews wurde die Durchführung normenbezogener Konformitäts-Assessments als vorteilsbringend erwähnt. Konformitätsbewertungen sind Tätigkeiten des Auswählens und Bewertens allgemeiner bzw. dedizierter Anforderungen entlang einer Norm. Sie finden sowohl freiwillig auf rechtlich ungeregelter Basis statt - etwa als entwicklungsbegleitende Prüfung oder als Bestätigung von Eigenschaften in einem Vertragsverhältnis - als auch auf der Grundlage gesetzlicher Regelungen. Wiederkehrende verpflichtende Assessments werden im Rahmen von Zertifizierungsverfahren durch Zertifizierungsstellen durchgeführt. Im Bereich der industriellen Automatisierungstechnik wird in der Praxis gern die IEC 62443 herangezogen.

Sowohl freiwillige als auch verpflichtende Assessments ermöglichen Betreibern das Einholen der Expertise von außen zur Unterstützung der Selbsthilfe.

Assessments werden auf Grundlage von ausgewählten Standards oder Vorgaben durchgeführt, um eine Vergleichbarkeit der Ergebnisse mit dem Soll-Zustand zu gewährleisten. Während die häufig in den Betrieben umgesetzten Anforderungen gemäß ISO 27001 oder NIST (National Institute of Standards and Technology) Cyber-Security Framework grundlegende Aspekte eines Informationssicherheitsmanagementsystems betrachten, fokussieren andere Normen, wie die KAS-51 oder die IEC 62443, spezielle Bereiche. So kann zur Grundlage eines Assessments auch die KAS-51 dienen, die Anforderungen für OT-Systeme sowie PLT-Sicherheitssysteme adressiert. Das Assessment erleichtert damit den Betreibern den Nachweis der Konformität zur KAS-51 und den Behörden deren Überprüfung.

7 Defizite und Handlungsbedarf aus Sicht der Verfahrensbeteiligten

Aus den Befragungen lassen sich folgende Defizite und zukünftige Handlungsbedarfe ableiten:

Tabelle 28 Übersicht der Defizite

Defizit	*Beschreibung*
Defizit 1	Sowohl Betreiber als auch Behörden beklagen die vielerorts noch vorhandene strikte Trennung von IT (Büro) und OT (Betrieb, Produktion). Hier ist eine engere Zusammenarbeit wünschenswert. Im Bereich IT ist das Bewusstsein für Anwendungen im Bereich der OT zu stärken und umgekehrt.
Defizit 2	Alle Befragten beklagen die mangelnde Verfügbarkeit von qualifizierten Arbeitskräften. Der zukünftige Handlungsbedarf liegt in der Aus- und Weiterbildung von Fachkräften.
Defizit 3	Bei den Behörden fehlt derzeit noch die fachliche Kompetenz, um die ergriffenen Maßnahmen in Genehmigungs- und Aufsichtsverfahren beurteilen zu können. Eine Unterstützung durch das BSI ist gewünscht; entweder durch Begleitung der Verfahren oder durch Unterstützung beim internen Aufbau von Kompetenzen.
Defizit 4	Sowohl Behörden als auch Betreiber wünschen sich eine Vereinheitlichung der Anforderungen (NIST, NA-163, KAS-51, BSI Grundschutz-Kataloge, ISO 27001). D.h. in behördlichen Leitfäden sollten zu den genannten Anforderungen Verweise auf die Kapitel der Standard-Regelwerke gegeben werden, mit denen die Anforderungen erfüllt werden können.
Defizit 5	Die Behörden sehen Probleme bei der Umsetzung von Safety & Security in kleineren und mittleren Unternehmen (KMU). Diese haben in der Regel keine Kapazitäten, um sich dieses Themas intensiv anzunehmen. Hier sind ggf. Lösungsansätze durch die Branchenverbände und das BSI zu erarbeiten.
Defizit 6	Einige der befragten Sachverständigen sehen Defizite im Regelwerk als Ursache für die Unklarheiten bezüglich der Prüfumfänge, Prüftiefe und den Bewertungsmaßstäben. Klarstellungen in der 12. BImschV, der europäischen Seveso Richtlinie wurden als mögliche Maßnahmen benannt.
Defizit 7	Von Seiten der Hersteller liegen nicht zu allen in den Anlagen eingesetzten Sicherheitssteuerungen auch Security Handbücher vor. So gesehen sind wesentliche Informationen zur sicheren Integration (z.B. Anforderungen an das Netzwerk der Betreiber), zum sicheren Betrieb (z.B. Anforderung an Updates und Patches) und zur sicheren Entsorgung (z.B. Löschung von sensiblen Daten) nur unvollständig verfügbar.
Defizit 8	Behördenseitig (z.B. BSI, Unterstützungsstellen der Länder, Polizei und Gewerbeaufsichtsämter) und bei Verbänden (NAMUR, VdTÜV) gibt es inzwischen viele Initiativen und Informationsbroschüren zum Thema Cyber-Security. Seitens der Befragten bestand der Wunsch, diese unter Benennung der betreffenden Ansprechpersonen systematisiert aufzubereiten.
Defizit 9	Nach Aussage der Behörden gibt es derzeit noch keinen einheitlichen Ansatz zu Forderungen und Bewertung der Cyber-Sicherheitsmaßnahmen in Genehmigungsverfahren.
Defizit 10	Die Betreiber beklagen, dass bei den Lieferfirmen von PLT-Komponenten keine Auseinandersetzung mit dem Thema erfolgt. Hier wird eine Unterstützung durch das BSI bzw. eine Entwicklung von Standards für Systemlieferfirmen (Sicherheitskennzeichen für Komponenten) gewünscht.

Defizit	*Beschreibung*
Defizit 11	Einer der befragten Betreiber wünscht sich Inspektionen bzw. Audits durch das BSI, verbunden mit Empfehlungen.
Defizit 12	Einer der befragten Betreiber wünscht sich praktische Empfehlungen durch das BSI bzgl. der Ausführung von Interfaces zwischen PLS und SIS (rückwirkungsfreie Schnittstelle) sowie Blueprints für optimale Architekturen. Eine verbindliche Herstellerverpflichtung lässt sich derzeit nicht aus dem Produktsicherheitsgesetz ableiten, um entsprechende Festlegungen in der Gebrauchs- und Bedienungsanleitung zu fordern.
Defizit 13	Die in den Interviews von den Befragten genannten Praxisbeispiele wurden durch die Autoren dieser Studie den einzelnen Abschnitten der ISO 27001 zugeordnet. Dabei fällt auf, dass keine Praxisbeispiele aus dem Bereich „Verbesserung“ genannt wurden. Der zukünftige Handlungsbedarf liegt in der Entwicklung von Prozessen zur kontinuierlichen Verbesserung der Security für IT und OT Netzwerke.

8 Fallbeispiel Gasspeicheranlage

Um das Vorgehen der Cyber-Risikoanalyse nach dem Standard IEC 62443-3-2 an einem realen Objekt durchzuführen, wurde das Vorgehen an einer Kavernen-Gasspeicheranlage angewandt.

Kavernenspeicher sind große, künstlich angelegte Hohlräume in unterirdischen Salzstöcken. Die physikalischen Eigenschaften der Salzschicht garantieren eine natürliche Dichtheit der Kavernen, denn der umgebende Salzstock ist eine gasundurchlässige Barriere. Kavernenspeicher werden durch einen Solprozess bergmännisch angelegt. Die Aussolung erfolgt über Tiefbohrungen durch kontrollierte Wasserzufuhr. So entstehen Hohlräume von bis zu 500 Metern Höhe, in denen Erdgas gespeichert werden kann. Die Tiefbohrung wird nach entsprechender Ausrüstung später zur Ein- und Auslagerung des Gases genutzt. Die Ein- und Ausspeicherleistung von Kavernenspeichern ist vergleichsweise höher als die von Porenspeichern. Der Grund dafür ist einfach: Bei Porenspeichern muss das Erdgas zunächst durch das poröse Gestein zur Bohrung strömen, während die Kavernen über eine Tiefbohrung direkt mit den obertägigen Speicheranlagen verbunden sind.

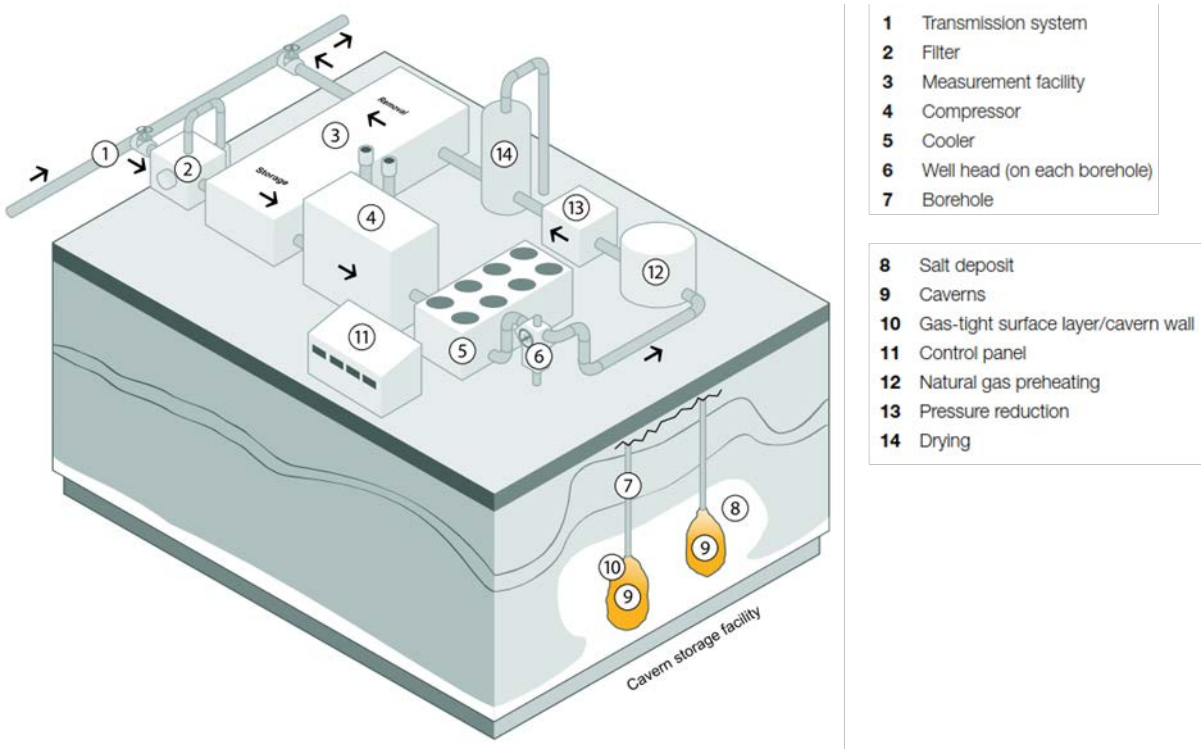

Abbildung 31 Gasspeicheranlage (Quelle: „Brochure Cavern Storage“)

In dem Fallbeispiel wird das einzulagernde Gas über das Fernleitungsnetz zur Verfügung gestellt und über Verdichter auf das für die Einlagerung notwendige Druckniveau angehoben, um in die Kavernen einzulagern. Für die Ein- und Auslagerung des Speichermediums werden zusätzlich noch Anlagenteile zur Reinigung und Trocknung benötigt sowie für die Kühlung bzw. Erwärmung des Gases. Schlussendlich existiert noch eine Fackelanlage, über die im Notfall einzelne Anlagenteile oder die Gesamtanlage entleert werden können.

Die Steuerung der Anlage erfolgt über ein betriebliches Leitsystem und eine sicherheitsgerichtete Steuerung des gleichen Herstellers. Die Steuerungskomponenten sind vollständig vor Ort installiert und in separaten Räumen untergebracht.

Am Standort ist eine Leitwarte vorhanden, die aber im Normalbetrieb nicht verwendet wird. Die ständig besetzte Warte befindet sich in ca. 300 km Entfernung und ist über eine VPN-Verbindung angekoppelt. Der Standort ist zu den normalen Arbeitszeiten besetzt, außerhalb dieser Zeiten und am Wochenende erfolgt die Überwachung unter anderem per Videoüberwachung aus der zentralen Warte. Die Feuerwehr oder andere

Einsatzkräfte haben die Möglichkeit, die Anlage vor Ort durch das beschriebene NOT-AUS-System über die SSPS in den sicheren Zustand zu versetzen.

8.1 Vorgehen im Rahmen der Risikoanalyse gemäß IEC 62443-3-2

Im Rahmen der Cyber-Sicherheitsrisikobewertung der in dieser Studie betrachteten Gasspeicheranlage fand die IEC 62443-3-2 Anwendung. Die durchgeführten Schritte zur Cyber-Sicherheitsrisikobewertung werden im Folgenden näher erläutert.

Eine Möglichkeit zur Durchführung der Cyber-Sicherheitsrisikobewertung für die Industrie ist in der IEC 62443-3-2 definiert. Die Norm IEC 62443-3-2 beschreibt eine Vorgehensweise, um Organisationen durch den Prozess der Risikobewertung in industriellen Automatisierungs- und Steuerungssystemen (IACS) zu führen und die Gegenmaßnahmen zu identifizieren und anzuwenden. Dabei geht es um die Reduktion der identifizierten Risiken, bei dem die gesetzlichen Vorgaben eingehalten und wirtschaftliche Schäden für das Unternehmen auf ein tolerierbares Maß begrenzt werden. Es gibt mehrere aufeinander aufbauende Schritte, die als „Zonen, Conduits und Risikobewertungsanforderungen“ (ZCR) bezeichnet werden, die die Cyber-Sicherheitsrisikobewertung gemäß IEC 62443-3-2 definieren

Diese sind:

1. ZCR 1 - SUC (System under Consideration) identifizieren:
   In diesem Schritt würde das zu betrachtende System (sog. Scope) identifiziert werden. Dieser umfasst alle Informationen, Assets, Inventare, Architekturdiagramme und Datenflüsse, die im Zusammenhang mit dem SUC stehen.
2. ZCR 2 - Initiale Cyber-Sicherheitsrisikobewertung:
   Ziel dieses Schrittes ist die Durchführung einer initialen Cyber-Sicherheitsrisikobewertung. Ferner wird überprüft, ob eine frühere Cyber-Sicherheitsrisikobewertung anwendbar ist. Innerhalb der Cyber-Sicherheitsrisikobewertung werden die Risiken identifiziert, die zu einer Beeinträchtigung, Unterbrechung oder Deaktivierung kritischer IACS Operationen führen. Die initiale Cyber-Sicherheitsrisikobewertung soll ein erstes Verständnis für das Worst-Case-Risiko bezogen auf Gesundheit, Sicherheit, Umwelt, Betriebsunterbrechung, Produktionsausfall usw. vermitteln. Die Ergebnisse der Gefahrenanalyse (PHA) und der Bewertung der Funktionalen Sicherheit können als Teil der anfänglichen Cyber-Sicherheitsrisikobewertung herangezogen werden, um die Auswirkungen im schlimmsten Fall zu ermitteln.
3. ZCR 3 - Aufteilung des SUC in Zonen und Conduits:
   An dieser Stelle werden das IACS und die zugehörigen Assets in Zonen und Conduits gruppiert. Die Gruppierung muss auf dem Ergebnis der anfänglich durchgeführten Cyber-Sicherheitsrisikobewertung basieren. Andere Kriterien wie z. B. die Kritikalität der Assets, die betriebliche Funktion, der physische oder logische Standort usw. können bei der Gruppierung von IACS in Zonen und Conduits ebenfalls berücksichtigt werden. Die Absicht der Segmentierung von IACS und deren Assets in Zonen und Conduits ist es, diejenigen Assets zu identifizieren, die gemeinsame Cyber-Sicherheitsanforderungen haben und die Identifizierung gemeinsamer Cyber-Sicherheitsmaßnahmen zur Risikominderung zu ermöglichen.
4. ZCR 4 - Risikovergleich:
   Schritt 4 umfasst den Vergleich der in ZCR 2 durchgeführten initialen Cyber-Sicherheitsrisikobewertung mit dem tolerierbaren Risiko der Organisation. Wenn das initiale Risiko das tolerierbare Risiko übersteigt, muss eine detaillierte Cyber-Sicherheitsrisikobewertung durchgeführt werden.
5. ZCR 5 - Durchführung einer detaillierten Cyber-Sicherheitsrisikobewertung:
   In diesem Schritt ist eine detaillierte Risikobeurteilung durchzuführen, wenn das in ZCR 2 gefundene initiale Risiko das tolerierbare Risiko überschreitet. In der detaillierten Cyber-Sicherheitsrisikobewertung müssen Bedrohungen und Schwachstellen identifiziert, die Wahrscheinlichkeit der identifizierten Bedrohungen, sowie das ungeminderte Cyber-Sicherheitsrisiko bewertet werden. Am Ende ist das Ziel (Security Level-Targets (SL-T)) festzulegen und Gegenmaßnahmen zu identifizieren.

6. ZCR 6 - Dokumentation der Cyber-Sicherheitsanforderungen, Annahmen und Einschränkungen:
   Hier sind alle Cyber-Sicherheitsanforderungen, Annahmen und Einschränkungen innerhalb des SUC zu dokumentieren, die zur Erreichung des definierten SL-T erforderlich sind.
7. ZCR 7 - Genehmigung des Asset Owners der Anlage:
   In diesem Schritt ist die Genehmigung der Ergebnisse der Risikobeurteilung von der Leitung des Eigentümers der Anlage, der für die Anlagensicherheit, Integrität und Zuverlässigkeit des kontrollierten Prozesses verantwortlich ist, einzuholen. Das Konzept der Cyber-Sicherheitsrisikobewertung nach IEC 62443-3-2 ist die Anwendung von IACS-Sicherheitszonen und Conduits.

Es handelt sich in dem Fallbeispiel zwar nicht um eine KRITIS-relevante Anlage. Jedoch befinden sich viele Gasspeicheranlagen im KRITIS-relevanten Bereich, so dass die Autoren sich entschlossen haben, weitere gesetzliche Anforderungen für KRITIS-relevante Anlagen zu berücksichtigen. Somit ist es erforderlich, die Vorgaben des IT-Sicherheitskatalogs zu berücksichtigen. Dem IT-Sicherheitskatalog gemäß § 11 Absatz 1b Energiewirtschaftsgesetz folgend steht die Segmentierung des Geltungsbereichs in sechs Zonen im Vordergrund. Alle im Geltungsbereich befindlichen Assets, wie z.B. Anwendungen, Systeme und Komponenten, sind entsprechend ihrer Kritikalität zusammenzufassen und geeignete Maßnahmen zu treffen. Die am Fallbeispiel analysierten Risiken und die möglichen Behandlungsoptionen werden in den nächsten Kapiteln beschrieben.

8.2 Die Bedrohungsanalyse - Analyse der umgebungsbedingten Faktoren

Der Betrieb einer verfahrenstechnischen Anlage kann durch technisches Versagen, durch Bedienungsfehler sowie durch natur- oder umgebungsbedingte Faktoren derart gestört werden, dass es zu sicherheitsrelevanten Auswirkungen auf Mitarbeiter, Umwelt und Nachbarschaft kommen kann.

Für die Betreiber von Betriebsbereichen gemäß Störfallverordnung ist daher die Festlegung und Anwendung von Verfahren zur systematischen Ermittlung der Gefährdungen von Störfällen sowie die Abschätzung der Wahrscheinlichkeit und der Schwere solcher Störfälle durch die 12. BImSchV verbindlich vorgeschrieben. Aus einer solchen systematischen Gefahrenanalyse lassen sich dann die erforderlichen Maßnahmen für einen sicheren Betrieb der Anlagen ableiten.

Ein in Deutschland etabliertes und behördlich anerkanntes Verfahren zur systematischen Gefahrenanalyse ist das so genannte HAZard and OPerability-(HAZOP-)Verfahren. Das in Großbritannien bei der Firma ICI entwickelte Verfahren wurde im deutschsprachigen Raum unter dem Begriff „PAAG-Verfahren“ erstmals 1978 veröffentlicht. „PAAG“ steht dabei für „Prognose von Störungen“, „Auffinden der Ursachen“, „Abschätzen der Auswirkungen“ und „Gegenmaßnahmen“. Das Verfahren hat in Form der IEC 61882 – „Hazard and Operability studies (HAZOP studies) – Application guide“ auch Einzug in die internationale Normung gefunden.

Der grundlegende Ansatz, den diese Methode verfolgt, wird durch die deutschsprachige Interpretation „PAAG“ (s.o.) beschrieben. Anhand einer Kombination aus Parametern und Leitworten (z.B. Füllstand zu hoch) werden Abweichungen vom bestimmungsgemäßen Betrieb (Störungen) prognostiziert (z.B. Überfüllen eines Behälters), die möglichen Ursachen ermittelt (z.B. Versagen der Füllstandsmesseinrichtung), die Auswirkungen abgeschätzt (z.B. Umwelt- oder Brandgefahr) und zuletzt die erforderlichen Gegenmaßnahmen (z.B. Installation einer Überfüllsicherung) festgelegt.

Die Durchführung des Verfahrens erfolgt in der Regel durch ein Team von Experten verschiedener Fachrichtungen, vornehmlich aus der Belegschaft des Betreibers und/oder des Anlagenplaners und wird durch einen HAZOP-Leader moderiert, der die Einhaltung der systematischen Vorgehensweise gewährleistet.

Die betrachtete Anlage bzw. das betrachtete System wird in funktionale Einheiten zergliedert, für die jeweils eine Sollfunktion formuliert wird und die dann einzeln anhand der vorher festgelegten Kombinationen aus Parameter und Leitwort betrachtet und analysiert werden.

Die sich aus der Durchführung dieses Verfahrens ergebenden Gegenmaßnahmen können sowohl technischer (z.B. Druckentlastungseinrichtungen, PLT-Sicherheitseinrichtungen) als auch organisatorischer (z.B. Betriebsanweisungen, Alarmpläne) Natur sein.

Im Rahmen dieser Studie liegt der Fokus auf den PLT-Sicherheitseinrichtungen, da im Rahmen dieser Systeme der Einsatz IT-basierter Technologien und die zunehmende Vernetzung von Systemen Maßnahmen der Security erforderlich machen. Die Anforderungen an PLT-Sicherheitseinrichtungen ergeben sich aus der Basisnorm für die „Funktionale Sicherheit sicherheitsbezogener elektrischer/ elektronischer/ programmierbarer elektronischer Systeme - IEC 61508“ sowie aus der daraus für die Prozessindustrie abgeleiteten Norm „Funktionale Sicherheit – PLT-Sicherheitseinrichtungen für die Prozessindustrie – DIN EN 61511“, die in der VDI 2180 „Funktionale Sicherheit in der Prozessindustrie“ konkretisiert wird. Bereits die Basisnorm empfiehlt die Durchführung einer Cyber-Risikobeurteilung und verweist dabei für eine Anleitung auf die Normenreihe IEC 62443. Diese wiederum empfiehlt „als Teil der allgemeinen Cyber-Sicherheitsrisikoanalyse“ die Bezugnahme der Ergebnisse der systematischen Gefahrenanalyse sowie der Beurteilung der Funktionalen Sicherheit, um Auswirkungen im ungünstigsten Fall zu identifizieren. Somit kann die HAZOP sowie die daraus resultierende Beurteilung der Funktionalen Sicherheit als Basis für die Cyber-Sicherheitsrisikoanalyse herangezogen werden.

8.2.1 Anwendung in der Studie

Eine Cyber-Sicherheitsrisikoanalyse gem. IEC 62443-3-2 wurde im Rahmen dieser Studie beispielhaft für eine Gasspeicheranlage durchgeführt. Eine umfangreiche HAZOP für die Anlage lag aus der Planungsphase der Anlage vor, so dass die Risiken für den Ausfall einer PLT-Sicherheitseinrichtung oder das Auftreten eines Fehlers, sowie die daraus abgeleiteten Maßnahmen aus dieser herausgearbeitet werden konnten.

Die betrachteten Anlagen dienen zur Speicherung sowie zur Aufbereitung und Konditionierung von Erdgas. Das größte Risiko der Anlagen ergibt sich aus einer Freisetzung von Erdgas, aus der sich durch Zündung eine Explosion und / oder Brand entwickeln kann. Daher liegt der Fokus der Anlagensicherheit auf der Verhinderung einer Freisetzung von Erdgas. Als mögliche Ursache für eine Freisetzung ist vor allem das Versagen von Umschließungen (z.B. Rohre, Ventile und Tanks) infolge eines Druck- oder Temperaturanstiegs über das zulässige Maß hinaus zu betrachten. Ein solcher Anstieg kann sich zum Beispiel aus dem Versagen eines Reglers oder aus einer Fehlstellung von Armaturen ergeben.

Für die Cyber-Sicherheitsrisikoanalyse wurden zwei PLT-Sicherheitseinrichtungen ausgewählt, die sowohl in den Anlagen des betrachteten Gasspeichers als auch allgemein bei Betreibern von Gasspeicheranlagen verbreitet zum Einsatz kommen: „High-integrity pressure protection systems (HIPPS)“ zur Verhinderung einer Überdruckbeaufschlagung von Komponenten oder Systemen und „Emergency Shut-Down System (ESD)“ zur Überführung der Anlagen bzw. einzelner Komponenten in einen sicheren Zustand im Notfall.

8.3 Bedrohungen aufgrund der Anlagenplanung

Das Thema Sicherheit, unabhängig ob Anlagensicherheit, Funktionale Sicherheit oder Cyber-Sicherheit, muss bereits in frühen Stadien der Anlagenplanung (z.B. HIPPS und ESD) berücksichtigt und implementiert werden. Hierbei ist eine besondere Sorgfalt erforderlich, denn bereits in der frühen Planungsphase enthaltene Fehler wirken sich auf die weiteren Abschnitte des Lebenszyklus aus und können dort weitreichende Folgen haben. Eine Bereinigung dieser Fehler ist i.d.R. kosten- bzw. ressourcenintensiv.

Ein sicherlich äußerst prominentes Beispiel für planerische Fehlleistungen ist der Bau des neuen Flughafens in Berlin. Hier haben verschiedene Planungsfehler und gravierende Änderungen während der Umsetzung des Projekts zu einem nicht unerheblichen Zeitverzug sowie enormen Mehrkosten geführt. Regelwerke wurden teilweise nicht angemessen beachtet. Auch haben sich gesetzliche Anforderungen und Vorschriften bereits während der langen Planungs- und Umsetzungsphase geändert. Die Kommunikation und auch an-

dere Schnittstellen waren nicht eindeutig definiert, wodurch Änderungen in der Planung nicht an alle Gewerke oder Teams weitergegeben wurden. Dazu kam noch ein immenser Kostendruck, der bei der Planung von Maßnahmen das Umsetzen sinnvoller Lösungen teilweise blockierte. Eine ähnliche Geschichte ist von einem Stahlwerk in Brasilien bekannt. Hier führten wirtschaftliche Einflüsse und unzureichende geologische Untersuchungen zu Problemen im Bau und im Folgenden zu einer Kostenexplosion. So führten auch da Planungsfehler und sich ändernde Rahmenbedingungen dazu, dass das Projekt in Bezug auf Kosten und Terminen völlig aus dem Ruder lief.

Solche Beispiele lassen sich dementsprechend als Grundlage für weitere Überlegungen nutzen. Dafür ist es erforderlich, dass die weiteren Vorgehensweisen strukturiert werden. Einerseits können schon im Konzept und in der Basisplanung eine Reihe von Vorgaben erfolgen, die später Auswirkungen haben. Daher sollte der Start zur Entwicklung von Konzepten und Verfahren zur OT-Security bereits so früh wie möglich erfolgen und in einem OT-Sicherheitskonzept beschrieben werden. Andererseits besteht insbesondere bei langlaufenden Projekten die Problematik, dass sich rechtliche, technische oder organisatorische Rahmenbedingungen ändern. Hier kennen viele sicherlich die Änderungen, die sich für die Industrie über Änderungen oder Einführung von Normen in den vergangenen Jahren ergeben haben oder neue Anforderungen, die mit Gesetzen und Verordnungen (welche z.B. die europäischen Richtlinien in nationales Recht überführen) Anpassungsbedarf mit sich brachten. Grundsätzlich erfolgt dies, um auf neue Sachverhalte oder Bedrohungen zu reagieren. Dies kann jedoch den Ablauf eines Projektes empfindlich stören. Darüber hinaus kann es auch dazu kommen, dass Änderungen zu Fehlern führen und diese Fehler sich anschließend nur sehr schwer beheben lassen bzw. diese gar nicht erkannt werden. Daher ist es notwendig, die Konzepte so flexibel wie möglich zu gestalten, dass auf solche Einflüsse im Projektstadium und auch später im Betrieb der Anlage reagiert werden kann.

Werden Erfahrungen aus diesen oder ähnlichen Beispielen auf den Bereich der OT-Security und im speziellen auf die Anlagenplanung übertragen, zeichnen sich schnell Punkte ab, die auch auf die Planung der OT-Systeme übertragbar sind. Ungeklärte Schnittstellen in der Projektabwicklung und Projektkommunikation aber auch technische Schnittstellen (z.B. WLAN, USB) können schnell zu Sicherheitslücken führen, wenn diese beispielsweise aufgrund einer unklaren Aufgabenteilung nicht oder nur unzureichend berücksichtigt werden. Fehlende Kommunikation zwischen einzelnen Teilprojekten oder Abteilungen kann somit ein Einfallstor für Fehler oder Sicherheitslücken im System, wie z.B. die unzureichende Abstimmung über Kommunikationsschnittstellen, sein. Dies erhöht in der Folge die Problematik, dass keine oder nur ungenügenden Sicherungsmaßnahmen getroffen werden. Darüber hinaus können Zeit- und Kostendruck zu unzureichenden Gefahrenanalyse oder Maßnahmen führen.

Es ist wichtig, schon zum Anfang einer Planung mit der Gefahrenanalyse zu starten und ein übergeordnetes Konzept aufzustellen, hierbei ist es essentiell, alle beteiligten Komponenten und Schnittstellen zu identifizieren. Dabei muss der spätere Umfang der Anlage sowie die erforderlichen Funktionen betrachtet werden. Eingesetzte Geräte und die Planung der Systeme müssen sich diesem Konzept unterordnen. Ist dies nicht möglich, ist es erforderlich wieder am Anfang anzusetzen und das Konzept anzupassen oder zu erweitern. Dabei muss aber darauf geachtet werden, das bereits umgesetzte Teile weiter funktionieren. Wenn an dieser Stelle bereits die OT-Security berücksichtigt wird, können deren Anforderungen beispielsweise mit in die Produktauswahl oder in die Auswahl der zu nutzenden Übertragungsprotokolle einfließen.

Der Problematik sich ändernder Rahmenbedingungen lässt sich leider nicht immer aus dem Weg gehen. Ob es sich nun um Normen und technische Regeln oder um Gesetze und Verordnungen handelt, die einzige Möglichkeit dem vorzubeugen ist es, mit Weitsicht zu planen. Dabei sollte man sich an der technischen Erfahrung orientieren, um eine gute Lösung zu erarbeiten. Sollten sich die Rahmenbedingungen dann ändern, hat man gute Chancen, dass die gewählte Lösung beibehalten oder mit wenig Aufwand angepasst werden kann.

Bei der Wahl der Partnerfirmen und Lieferanten sollte darauf geachtet werden, dass dort bereits erprobte Verfahren vorhanden sind. Planungsfirmen, Integratoren und Hersteller, die bereits ein ISMS nach DIN EN 27001 oder IEC 62443 eingeführt haben, sind am Markt vorhanden. Insbesondere bei der Entwicklung und

Herstellung von Produkten und Software ist es wichtig, einen Security-by-Design-Ansatz zu fahren. Hierzu zählen auch die Versorgung mit Sicherheitsupdates und die Reaktion auf Schwachstellen über die Lebenszeit der Komponenten (in der Anlage). Dies sollte bereits bei der Planung und Umsetzung berücksichtigt werden.

Die jeweiligen Anforderungen für die OT-Security werden vom Auftraggeber oder einem damit beauftragten Unternehmen in einem oder mehreren Lastenheften beschrieben. Diese können den gesamten Projektumfang oder nur Teilbereiche betreffen. Hierbei sind die Aufgaben, Rahmenbedingungen und Anforderungen an die OT-Security klar und eindeutig zu spezifizieren, so dass der Integrator später alle notwendigen Informationen besitzt, um im Rahmen seiner Planung und der ggf. anschließenden Umsetzung

- die Anforderungen zu berücksichtigen,
- die richtige Technik (Hardware und Software) auszuwählen,
- die erforderlichen Cybersicherheitsmaßnahmen zu integrieren und
- Pflichten für den sicheren Betrieb zu formulieren.

Die jeweiligen (Unter-)Auftragnehmer besitzen in seltenen Fällen einen ausreichenden Gesamtüberblick über das Projekt, um die Gesamtsicherheit der erforderlichen Maßnahmen zu bewerten. Daher ist es notwendig, dass der Auftraggeber seinerseits die Rahmenbedingungen für die neue Anlage oder den neuen Anlagenteil beschreibt und festlegt und im Anschluss die Pflichtenhefte der Dienstleister genauestens prüft und die geplanten und beschriebenen Maßnahmen mit dem Gesamtkonzept abgleicht. Der Integrator kennt i.d.R. lediglich seine eigenen Aufgaben und ist darauf angewiesen, dass äußere Einflüsse und Schnittstellen korrekt beschrieben sind. Auftretende Abweichungen sind im Gesamtkontext zu betrachten und zu bewerten, ggf. notwendige Ersatzmaßnahmen sind festzulegen und zu beschreiben sowie Korrekturmaßnahmen einzuleiten. Dementsprechend ist es die Pflicht des Auftragnehmers, die Pflichten für den Betrieb der Anlage im Rahmen der Bedienungsanleitung detailliert zu beschreiben. Auf Basis des erforderlichen Niveaus der Funktionalen Sicherheit sind Tätigkeiten bei der Inbetriebnahme notwendig, wie beispielsweise das Ändern der Default-Passwörter, um einen sicheren Betrieb zu gewährleisten. Solche Vorgänge funktionieren jedoch nur wenn eine umfassende Beschreibung vorhanden ist.

9 Risiken aus Errichtung und Betrieb einer industriellen Anlage

Bei der Errichtung, Digitalisierung und dem Betrieb eines modernen Betriebsbereichs ergibt sich, dass eine Vielzahl an Fehlermöglichkeiten besteht, die in der „analogen Zeit“ keine Beachtung fanden oder in dieser Zeit nicht existierten. Bei Planungen von Steuerungssystemen wurden in der Vergangenheit Ereignisse ausgeschlossen, da ein Zusammentreffen mehrerer Fehler hinreichend sicher zu vernachlässigen war. Im Falle von smarten Bauteilen und Geräten muss hier aber aufgrund der fortschreitenden Digitalisierung ein Umdenken stattfinden. Der zufällige Ausfall kann zwar weiterhin weitestgehend ausgeschlossen werden, jedoch rücken an dieser Stelle gezielte Manipulationen in den Vordergrund. Ein Angreifender kann durch die Vernetzung ohne weiteres mehrere Geräte manipulieren. Dies war vorher nicht oder nur mit sehr hohem Aufwand möglich.

9.1 Errichtung

Beim Bau von Anlagen steht verständlicherweise auch der finanzielle Aspekt im Fokus, so dass bei der Errichtung gerne an Gerätetechnik und Platz gespart wird. So werden heute teilweise Systeme eingesetzt, die sowohl das betriebliche Leitsystem als auch die sicherheitsgerichtete Steuerung in einem Gerät vereinen oder zumindest zu einem System/Netzwerk zusammenfassen und sich eine zentrale Konfigurationsschnittstelle teilen. Dabei muss beachtet werden, dass bei der sicherheitstechnischen Betrachtung der Anlage meist eine strikte Trennung der beiden Systeme vorausgesetzt wird bzw. die Rückwirkungsfreiheit auf die SSPS zu gewährleisten ist. Im zweiten Fall kann der Beweis sehr schwierig sein und daher ist eine strikte Trennung oftmals der „bevorzugte“ Ansatz. Das bedeutet, man geht davon aus, dass bei einem Fehler des PLS die SSPS immer noch eingreifen kann. Die Wahrscheinlichkeit eines Fehlers im Anforderungsfall ist also nur von der Zuverlässigkeit der Sicherheitseinrichtung abhängig. Wenn nun aber beide Systeme (PLS und SSPS) über den gleichen Angriffsvektor verfügen (z.B. eine gemeinsam genutzte Komponente wie ein Konfigurationsgerät), existiert hier ein zentraler Angriffspunkt. Über diesen Weg können beide Systeme manipuliert werden, was bei einer Kompromittierung durch Dritte ein hohes Gefahrenpotential birgt. Hier ist auf logische oder (ebenfalls) physische Trennung zu achten.

Darüber hinaus sind hier die Hersteller selbst gefordert, um sichere Lösungen für den Einsatz ihrer Produkte anzubieten. Dabei ist es erforderlich, dass auch in diesem Bereich eine hohe Transparenz herrscht, um dem Anwender die Möglichkeit zu geben seine Anwendung auch vollständig zu bewerten.

Ein ähnlicher Sachverhalt ergibt sich auch bei der Sensorik und Aktorik. Grundsätzlich ist die Standardisierung, z. B. durch die Verwendung von einheitlichen und erprobten Geräten ein erstrebenswerter Zustand. Im Hinblick auf die Anlagensicherheit kann es an einzelnen Stellen sinnvoll sein, durch Diversität bei der Geräteauswahl die sicherheitstechnische Verfügbarkeit zu erhöhen. Darüber hinaus muss die Mitbenutzung von Geräten sowohl für betriebliche Zwecke als auch für Sicherheitseinrichtungen noch mal anders betrachtet werden als schon aus Sicht der Funktionalen Sicherheit. Je nachdem, welche Struktur für die Errichtung gewählt wird, können sich hier Risiken ergeben, die beachtet werden müssen.

Ein anderer Faktor kann auch im Bereich der Energieversorgung liegen. Mögliche Szenarien für den gleichzeitigen Ausfall aller Energiesysteme sind üblicherweise nicht Betrachtungsgegenstand.

Besonders kritisch wird es, wenn Energie dafür erforderlich ist, die Anlage in den sicheren Betrieb zu versetzen. Insbesondere wenn es sich dabei um elektrische Energie handelt. Denn auch dort sind digitale Systeme im Einsatz, z. B. für die Steuerung oder Fernwartung. Es gilt daher auch die Zusammenhänge und Abhängigkeiten der Systeme oder Anlagen untereinander zu berücksichtigen.

9.2 Betrieb

Im Betrieb gehört sicherlich die Organisation der Sicherheit (in jeglicher Form) zu den wichtigsten Herausforderungen. Bei einer prozesstechnischen Anlage hat man es regelmäßig mit Änderungen zu tun, sei es durch Defekte einer Komponente, die nicht bau- oder funktionsgleich ausgetauscht werden kann, oder dass Modifikationen an der Anlage vorgenommen werden müssen. Werden solche Vorgänge nicht geplant und strukturiert durchgeführt, ergeben sich Sicherheitslücken, die vorher noch nicht bedacht wurden. Gerade im Zuge von Störungen werden gerne Ad-hoc-Maßnahmen veranlasst, die dann im Anschluss nicht zurückgenommen werden. Auch provisorische Lösungen, z.B. im Rahmen von Störungsbeseitigungen, bleiben oft lange bestehen, getreu dem Motto: „Nichts hält so lange wie ein gut gebautes Provisorium“.

Auch ist das Thema Zugriffsschutz sehr differenziert zu betrachten. Es ist sicher notwendig, alle Systeme mit einem Zugriffsschutz zu versehen. In diesem Zusammenhang müssen einheitliche Codes für alle Geräte oder Herstellereinstellung (Default-Passworte) vermieden werden. Dafür sollten für das Personal handhabbare Lösungen gefunden werden, da sonst die Maßnahmen umgangen werden.

Ein weiteres Risiko kann durch das Auftreten von Mehrfachfehlern oder verbundenen Fehlern auftreten. Bisher war das gleichzeitige Versagen von mehreren Geräten bzw. verschiedenen Komponenten nicht im Fokus der Sicherheitsbetrachtung. Es kann durch einen Cyber-Angriff dazu kommen, dass im Anlagenbereich HIPPS Messwerte dahingehend manipuliert werden, dass diese trotz Vorherrschen eines kritischen Zustandes Normalwerte anzeigen. Dadurch kann der Bediener dazu veranlasst werden, die Anlage unbewusst in einen unzulässigen Bereich zu fahren. Die Integrität der Daten wird an dieser Stelle verletzt. Es sollten Maßnahmen ergriffen werden, die Integrität der Daten und Informationen zu schützen.

Ein weiteres Szenario wäre bei Steigerung des Zulaufs einer Kolonne und gleichzeitiger Maximierung der Beheizung denkbar. Wenn nun das mechanische Sicherheitsventil auf jeweils eine der beiden Störungen, aber nicht auf das gleichzeitige Auftreten ausgelegt ist, kann dies zu einem Schadensereignis führen. In diesem Beispiel könnte sogar ein Szenario ohne Kompromittierung der Sicherheitstechnik zu einem Ereignis führen.

Ein weiterer wichtiger Themenkomplex ist der Austausch oder die Änderung von Komponenten oder Systemen. Wie geht man damit um, wenn ein Sensor getauscht oder ergänzt werden muss und das ursprüngliche Modell nicht mehr verfügbar ist? Dabei ist die Gefährdung zu betrachten, dass bisher verwendete Schnittstellen nicht mehr verfügbar sind, oder dass die Geräte über neue Schnittstellen, wie z.B. Bluetooth/WLAN, verfügen. Durch den Einsatz neuer vorher noch nicht genutzter Technologien ergeben sich möglicherweise zusätzliche Gefährdungen. Dies ist analog auf Komponenten von SPS-/PLS-Systemen anwendbar. PLS- und SPS-Systeme bedürfen außerdem weiterer Updates und Patches, die nach einer gewissen Zeit nicht mehr verfügbar sind, da der Hersteller den Support eingestellt hat. Daher ist es für Betreiber einer industriellen Anlage wichtig, den Einsatz neuer Systeme bzw. Technologien im Rahmen einer Risikoanalyse zu bewerten und aus dieser gegebenenfalls entsprechende Maßnahmen abzuleiten.

Darüber hinaus ist zu beachten, dass sich die Technik weiterentwickelt und immer neue Bedrohungen entstehen.

10 Cyber-Sicherheitsrisiken am Beispiel des Kavernenspeichers

Die zuvor dargestellten Bedrohungen und Risiken für industrielle Anlagen werden in diesem Kapitel im Kontext des konkreten Fallbeispiels analysiert. Die nächsten Kapitel dieser Arbeit widmen sich den erkannten Cyber-Sicherheitsrisiken und deren Behandlungsoptionen unter Zuhilfenahme des IT-Grundschutzkompendiums des BSI. Jedes identifizierte Risiko umfasst eine Beschreibung und stellt die wichtigsten Behandlungsoptionen vor. In den zugehörigen Tabellen werden die gewichteten Behandlungsoptionen dargestellt, um Betreibern eine Anleitung an die Hand zu geben, um dem jeweiligen Risiko mit ersten Schritten zu begegnen. Im Anhang dieser Studie befinden sich weitere entsprechende Anforderungen aus den Bausteinen des IT-Grundschutzkompendiums, die eine ausführliche Behandlung der Risiken erlauben.

10.1 Abbruch der Verbindung zur Remote-Leitwarte

Im Rahmen der initialen Risikobewertung, in Schritt ZCR 3 gemäß IEC 62443-3-2, wurde die Verbindung zur Remote-Warte als kritisch eingestuft. Die Gasspeicheranlage, die der Studie als Fallbeispiel dient, wird durch ein Remote-Leitsystem von einem mehrere hundert Kilometer entfernten Standort gesteuert. Dieser ist 24/7 besetzt. Die Gasspeicheranlage kann auch mittels eines Leitsystems vor Ort gesteuert werden. Dazu sind in den üblichen Wochenarbeitszeiten Mitarbeitende vor Ort. Außerhalb der Geschäftszeiten kann die Steuerung im Notfall über ein Bereitschaftsnotebook übernommen werden.

Als ein Risiko für eine Beeinträchtigung der Funktion aus der Befragung des Gasspeicherbetreibers, wurde der Abbruch der Verbindung der Remote-Leitwarte genannt.

Im Wesentlichen sollten hierzu technische und organisatorische Maßnahmen getroffen werden, um den Übertragungsweg vor beispielsweise Man-in-the-Middle-Angriffen zu schützen und eine Steuerung des Gasspeichers gewährleisten zu können.

Um grundlegende Verantwortlichkeiten festzulegen, sollte dieses auch von der Unternehmensleitung bestimmt und den verantwortlichen Personen und Rollen zugewiesen werden. Um im Notfall funktionieren zu können, muss auch 24/7 gewährleistet sein, dass sowohl vor Ort als auch in der Remote Leitwarte ausreichend qualifizierte Mitarbeitende zur Verfügung stehen und zwar ggf. so lange, bis der Betrieb wieder läuft. Ereignisse im Münsterland 2005 haben gezeigt, dass eine Stromversorgung eventuell auch über mehrere Tage ausfallen kann. Grundsätzliche arbeitsrechtliche Voraussetzungen sollten auch den 24/7 Betrieb berücksichtigen. Geeignete Mitarbeiter müssen zu Bereitschaften verpflichtbar und entsprechend in die erforderliche Technik und in die Notfallprozesse eingewiesen sein. Sollten zu der Wiederherstellung der Verbindung zum Leitsystem unterstützend Dienstleister benötigt werden, müssen diese in einem Notfallkonzept und in den Verträgen mitberücksichtigt werden. Bei einem Abbruch der Verbindung müssen generelle Kommunikationswege festgelegt sein. Bei Krisenfällen sollten Eskalationen und Kaskaden zu abhängigen interessierten Parteien (z.B. Katastrophenschutz) festgelegt sein.

Um beim Abbruch der Verbindung erneuten Remotezugriff erlangen zu können, ist es wichtig, das Thema „Ausfall der Fernwartung“ in den Notfallplan zu integrieren. Da bei einem 24/7 Betrieb die Anforderungen an die Verfügbarkeit hoch sind, müssen sich Gedanken über dezidierte Systeme zur Fernwartung und Redundanzen bei den Kommunikationswegen gemacht werden.

Da eine hohe Verfügbarkeit der Leitwarte zu gewährleisten ist, ist es ratsam, die Remoteverbindung auch permanent zu überwachen. Bei sicherheitsrelevanten Ereignissen, wie Abbruch der Remote Verbindung, sollten Automatismen greifen. Auch sollten die Protokolle der Fernwartung regelmäßig von geeignetem Personal ausgewertet und ggf. entsprechende Maßnahmen abgeleitet werden. Häufig wird der Aufwand für die Überwachung, Auswertung und Reaktion auf Probleme nicht berücksichtigt.

Alle oben geschilderten Maßnahmen sollten in einem Notfallhandbuch ausreichend dokumentiert sein.

Bei den Netzkomponenten ist eine sichere Planung zum Einsatz nötig. Entscheidend für den Einsatz von Systemen ist hier die Hochverfügbarkeit, die durch Redundanzen abgesichert werden kann. Neben dem Einsatz der Netzkomponenten spielen alle weiteren Kommunikationsmittel eine wichtige Rolle. Diese sollten auch mehrfach redundant zur Verfügung stehen, um eine Verbindung mindestens zwischen Remote-Leitzentrale, der eigentlichen Leitzentrale vor Ort und dem Bereitschaftsdienst gewährleisten zu können.

10.1.1 Anforderungen IT-Grundschutz zur Reduzierung des Risikos zum „Abbruch der Verbindung zur Remote-Leitwarte“

- ORP.1 Organisation (B, inklusive Umsetzungshinweise)
  - ORP.1.A1 Festlegung von Verantwortlichkeiten und Regelungen
  - ORP.1.A2 Zuweisung der Verantwortung
- ORP.2 Personal (B, inklusive Umsetzungshinweise)
  - ORP.2.A1 Geregelte Einarbeitung neuer Mitarbeiter
  - ORP.2.A3 Festlegung von Vertretungsregelungen
  - ORP.2.A5 Vertraulichkeitsvereinbarungen für den Einsatz von Fremdpersonal
  - ORP.2.A6 Überprüfung von Kandidaten bei der Auswahl von Personal
  - ORP.2.A7 Überprüfung der Vertrauenswürdigkeit von Mitarbeitern
  - ORP.2.A8 Aufgaben und Zuständigkeiten von Mitarbeitern
  - ORP.2.A9 Schulung von Mitarbeitern
- ORP.3 Sensibilisierung und Schulung (B, inklusive Umsetzungshinweise)
  - ORP.3.A3 Einweisung des Personals in den sicheren Umgang mit IT
- ORP.4 Identitäts- und Berechtigungsmanagement (B, I, H, inklusive Umsetzungshinweise)
  - ORP.4.A5 Vergabe von Zutrittsberechtigungen
  - ORP.4.A6 Vergabe von Zugangsberechtigungen
  - ORP.4.A7 Vergabe von Zugriffsrechten
- CON.9 Informationsaustausch (B)
  - CON.9.A1 Festlegung zulässiger Empfänger
  - CON.9.A3 Unterweisung des Personals zum Informationsaustausch
- OPS.1.2.5 Fernwartung (B, I, H, inklusive Umsetzungshinweise)
  - OPS.1.2.5.A21 Erstellung eines Notfallplans für den Ausfall der Fernwartung
  - OPS.1.2.5.A14 Dedizierte Systeme bei der Fernwartung
  - OPS.1.2.5.A22 Redundante Kommunikationsverbindungen
- DER.1 Detektion von sicherheitsrelevanten Ereignissen (B, I, H)
  - DER.1.A6 Kontinuierliche Überwachung und Auswertung von Protokolldaten
  - DER.1.A14 Auswertung der Protokolldaten durch spezialisiertes Personal
  - DER.1.A16 Einsatz von Detektionssystemen nach Schutzbedarfsanforderungen
  - DER.1.A17 Automatische Reaktion auf sicherheitsrelevante Ereignisse
- DER.2.1 Behandlung von Sicherheitsvorfällen (B)

  - DER.2.1.A3 Festlegung von Verantwortlichkeiten und Ansprechpartnern bei Sicherheitsvorfällen
  - DER.2.1.A5 Behebung von Sicherheitsvorfällen
  - DER.2.1.A6 Wiederherstellung der Betriebsumgebung nach Sicherheitsvorfällen
  - DER.2.1.A7 Etablierung einer Vorgehensweise zur Behandlung von Sicherheitsvorfällen
  - DER.2.1.A9 Festlegung von Meldewegen für Sicherheitsvorfälle
  - DER.2.1.A13 Einbindung in das Sicherheits- und Notfallmanagement
- DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle (B, I, H, inklusive Umsetzungshinweise)
  - DER.2.3.A1 Einrichtung eines Leitungsgremiums
  - DER.2.3.A2 Entscheidung für eine Bereinigungsstrategie
- DER.4 Notfallmanagement (B)
  - DER.4.A1 Erstellung eines Notfallhandbuchs
- NET.3.1 Router und Switches (B, I, H)
  - NET.3.1.A22 Notfallvorsorge bei Routern und Switches
  - NET.3.1.A23 Revision und Penetrationstests
  - NET.3.1.A26 Hochverfügbarkeit
- NET.3.2 Firewall (B, I, H)
  - NET.3.2.A2 Festlegen der Firewall-Regeln
  - NET.3.2.A5 Restriktive Rechtevergabe
  - NET.3.2.A24 Revision und Penetrationstests
  - NET.3.2.A29 Einsatz von Hochverfügbarkeitslösungen
- NET.3.3 VPN (B, I, H)
  - NET.3.3.A1 Planung des VPN-Einsatzes
  - NET.3.3.A4 Sichere Konfiguration eines VPN
- NET.4.1 TK-Anlagen (B, I, H)
  - NET.4.1.A14 Notfallvorsorge für TK-Anlagen
  - NET.4.1.A15 Notrufe bei einem Ausfall der TK-Anlage
  - NET.4.1.A19 Redundanter Anschluss

10.2 Arbeiten aus dem Home-Office

Im Rahmen der Cyber-Risikobewertung wurde die Zone des Home-Office betrachtet. Die Zonierung fand in ZCR 3 der Risikobetrachtung gemäß IEC 62443-3-2 statt.

Wenn es erforderlich ist, die Bedienung für einen Störfallbetrieb aus dem Home-Office (mittels des Bereitschaftsnotebooks) zu übernehmen, sind besondere Sorgfaltspflichten zu berücksichtigen. Im Gegensatz zu Tätigkeiten in der reinen Büro-IT können die Schäden durch Prozess- und Steuerungs-IT von erheblich größerer Schadwirkung sein. Die Nutzung von betriebseigenen IT-Systemen kann im privaten Umfeld problematisch sein. So könnte beispielsweise Familienmitgliedern der Zugang zu IT-Systemen ermöglicht sein. Ferner ist es möglich, dass die Nutzung starker Verschlüsselungstechnologien im heimischen WLAN

nicht jedem Mitarbeiter geläufig bzw. technisch möglich ist. Wenn es unbedingt notwendig ist, dass Mitarbeitende von Betriebsbereichen remote arbeiten, sollten Unternehmen technische sowie organisatorische Regelungen für das Arbeiten im Home-Office treffen. Der Remote-Zugriff auf die Netze von Betriebsbereichen sollte zweckgebunden sein und technisch dem Stand der Technik entsprechen. Sämtliche Zugriffe sollten protokolliert und dieses auch den Mitarbeitenden kommuniziert werden.

In vielen Unternehmen gibt es Regelungen zur Telearbeit. Zu unterscheiden ist hier Teleheimarbeit (gesamte Arbeitszeit Zuhause), alternierende Telearbeit (wechselweises Arbeiten im Büro und Zuhause) und mobile Telearbeit (z. B. auf Dienstreise). Auch der Begriff des Home-Office ist geläufig, sollte aber auch differenziert werden. In aktuellen Krisenzeiten sind kurzfristig viele flexible Lösungen im gemeinsamen Interesse zwischen Arbeitnehmenden und Arbeitgeber möglich gemacht worden oder nötig gewesen. Daher sollte der Begriff Telearbeit nach den Anforderungen differenziert werden. Dies fordert von den Unternehmen, sich mit den neuen Gegebenheiten generell und natürlich auch speziell für jeden Arbeitnehmenden und somit dessen Zugriff auseinanderzusetzen. Dabei gilt es die entstehenden Risiken bei den unterschiedlichen Arten zu betrachten und entsprechend zu berücksichtigen.

Hierzu ist es wichtig, dass die Unternehmen klare Regelungen und Abgrenzungen schaffen und diese kommunizieren. Die strikte Trennung von Beruflichem und Privatem ist hierbei als Maßstab anzusetzen. In diesem Zusammenhang sollte auch das Thema „Bring your own device“ kritisch hinterfragt werden und die entstehenden Risiken betrachtet werden.

Sorgen Sie für eindeutige Kontaktstellen und Kommunikationswege, die von den Beschäftigten verifiziert werden können und Klarheit schaffen.

Es stellt sicherlich eine Herausforderung dar, die physische Sicherheit in den Bereichen Zutritt und Zugriff im Home-Office genauso zu gewährleisten, wie es am Arbeitsplatz im Unternehmen möglich ist. Eine verpflichtende Kontrolle oder Begutachtung des Home-Office von den Kollegen der IT oder Informationssicherheit wie im Unternehmensgebäude ist schwierig, da hier die Privatsphäre berührt wird. Es sollten dennoch hier unverbindliche Angebote geschaffen werden, um die Umgebung des Home-Office aus Cyber-Sicherheitsaspekten im gegenseitigen Interesse begutachten zu lassen. Auch könnten hier Merkblätter oder Checklisten mit Tipps und Tricks hilfreich sein. Eine Nutzung der Hardware ohne die Überwachungsmechanismen im firmeneigenen LAN stellt eine Schwachstelle dar. Sollten die gleichen Cyber-Sicherheitsstandards und Perimeter im Home-Office nicht umsetzbar sein, sollte dieses zumindest bekannt sein und nach alternativen Lösungen gesucht werden. Leitlinien zum aufgeräumten Arbeitsplatz, Clean-Desk oder Sichtschutz sollten auch hier möglich sein und einen Mindeststandard definieren.

Gerade gelegentliches Arbeiten aus dem Home-Office, wie bei Störungs-und Bereitschaftsdiensten, bringt erhöhte Cyber-Sicherheitsanforderungen mit sich, da oftmals aus dem Home-Office nicht nur überwacht, sondern auch geschaltet oder administriert wird. Hierzu ist es wichtig, die Rollen und Rechte in den Systemen mit erhöhter Cyber-Sicherheitssensibilität zu begutachten. Das Need-to-Know-Prinzip sollte hier höchste Priorität haben.

Bei der Planung der technischen Voraussetzungen für das Home-Office, sollten sich über Verbindungsaufbau über private oder firmeneigene Kommunikationslösungen Gedanken gemacht werden. Ein Aufbau einer Verbindung aus einem ungeschützten WLAN oder aus einem gemeinschaftlich genutzten WLAN stellt eine potentielle Gefährdung dar.

Die erforderliche und nötige Hardware und Software sollte definiert werden und deren Nutzung eingeschränkt werden. Möglichkeiten der Administration des Telearbeitclients entsprechend des Büroarbeitsplatzes von Netzwerk- und weitere Schnittstellen zur Verbindung mit Speicherlaufwerken, Wechseldatenträgern und anderen Peripheriegeräten wie Drucker oder Scanner sollten genutzt werden. Eine Mischung und gemeinsame Nutzung von privat genutzter und beruflicher Hardware ist zu vermeiden.

Beim Verbindungsaufbau ins Firmennetz sollte ein gesicherter, verschlüsselter Verbindungsaufbau per VPN-Tunnel mit einer Multi-Faktor-Authentifizierung der Standard sein. Weiterhin sind bei Client- Serverinstallationen eine Installation über Terminalserver oder virtualisierte Clients zu bevorzugen.

10.2.1 Anforderungen IT-Grundschutz zur Reduzierung des Risikos „Arbeiten im Home-Office“

- ORP.1 Organisation (B)
  - ORP.1.A5 Vergabe von Berechtigungen
- ORP.3 Sensibilisierung und Schulung (B)
  - ORP.3.A2 Ansprechpartner zu Sicherheitsfragen
  - ORP.3.A3 Einweisung des Personals in den sicheren Umgang mit IT
- ORP.4 Identitäts- und Berechtigungsmanagement (B)
  - ORP.4.A5 Vergabe von Zutrittsberechtigungen
  - ORP.4.A6 Vergabe von Zugangsberechtigungen
  - ORP.4.A7 Vergabe von Zugriffsrechten
- CON.9 Informationsaustausch(B)
  - CON.9.A1 Festlegung zulässiger Empfänger
  - CON.9.A2 Regelung des Informationsaustausches
- OPS.1.2.4 Telearbeit (B)
  - OPS.1.2.4.A1 Regelungen für Telearbeit
  - OPS.1.2.4.A2 Sicherheitstechnische Anforderungen an den Telearbeitsrechner
  - OPS.1.2.4.A5 Sensibilisierung und Schulung der Telearbeiter
  - OPS.1.2.4.A7 Regelung der Nutzung von Kommunikationsmöglichkeiten bei Telearbeit
- DER.4 Notfallmanagement (B, I)
  - DER.4.A1 Erstellung eines Notfallhandbuchs
  - DER.4.A8 Integration der Mitarbeiter in den Notfallmanagement-Prozess
  - DER.4.A12 Dokumentation im Notfallmanagement-Prozess
  - DER.4.A14 Regelmäßige Überprüfung und Verbesserung der Notfallmaßnahmen
- SYS.3.1 Laptops (B, I, H)
  - SYS.3.1.A1 Regelungen zur mobilen Nutzung von Laptops
  - SYS.3.1.A2 Zugriffsschutz am Laptop
  - SYS.3.1.A6 Sicherheitsrichtlinien für Laptops
  - SYS.3.1.A7 Geregelte Übergabe und Rücknahme eines Laptops
  - SYS.3.1.A8 Sicherer Anschluss von Laptops an Datennetze
  - SYS.3.1.A9 Sicherer Fernzugriff
  - SYS.3.1.A12 Verlustmeldung
  - SYS.3.1.A13 Verschlüsselung von Laptops
  - SYS.3.1.A14 Geeignete Aufbewahrung von Laptops
  - SYS.3.1.A16 Zentrale Administration von Laptops
  - SYS.3.1.A18 Einsatz von Diebstahl-Sicherungen

- NET.2.2 WLAN-Nutzung (B, I, H)
  - NET.2.2.A1 Erstellung einer Benutzerrichtlinie für WLAN
  - NET.2.2.A2 Sensibilisierung und Schulung der WLAN-Benutzer
  - NET.2.2.A3 Absicherung der WLAN-Nutzung in unsicheren Umgebungen
  - NET.2.2.A4 Verhaltensregeln bei WLAN-Sicherheitsvorfällen
- NET.3.3 VPN
  - NET.3.3.A1 Planung des VPN-Einsatzes
- INF.8 Häuslicher Arbeitsplatz (B)
  - INF.8.A1 Sichern von dienstlichen Unterlagen am häuslichen Arbeitsplatz
  - INF.8.A2 Transport von Arbeitsmaterial zum häuslichen Arbeitsplatz
  - INF.8.A3 Schutz vor unbefugtem Zutritt am häuslichen Arbeitsplatz
  - INF.8.A6 Umgang mit dienstlichen Unterlagen bei erhöhtem Schutzbedarf am häuslichen Arbeitsplatz
- INF.9 Mobiler Arbeitsplatz (B)
  - INF.9.A1 Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes
  - INF.9.A2 Regelungen für mobile Arbeitsplätze
  - INF.9.A3 Zutritts- und Zugriffsschutz
  - INF.9.A5 Zeitnahe Verlustmeldung
  - INF.9.A6 Entsorgung von vertraulichen Informationen
  - INF.9.A10 Einsatz von Diebstahlsicherungen
  - INF.9.A11 Verbot der Nutzung unsicherer Umgebungen

10.3 Angriffe von innen

Bedrohungen, welche sich von innen gegen die Anlage richten, sind ein ernstzunehmender Angriffsvektor für die Anlagenbetreiber. Ein Innentäter kann durch seine Nähe zum Angriffsobjekt in besonderem Maße Schaden anrichten. Der Innentäter hat meist ausreichend Zeit, Zugang zu Informationen, möglichweise auch die nötigen Rechte und technischen Zugänge, um seinen Angriff zu planen.

Der Täter kann am effektivsten die Systeme manipulieren, welche für ihn zugänglich sind. Eine in einer höheren Sicherheitszone liegende Anlagensteuerung kann schon eine effektive Hürde darstellen bzw. durch den fehlenden Zugang den Angriff verhindern.

Hat ein Angreifender physischen Zugang zu einem Netzwerk und Datenleitungen, kann er Geräte oder Programme installieren, die den Datenverkehr manipulieren.

Im Hinblick auf einen Störfallbetrieb ist dieser Angriff als kritisch einzuschätzen, da es durch eine Manipulation der Steuerungsdaten zu ungewünschten Zuständen der Anlage kommen kann. Es könnten auch Alarmmeldungen oder Sensordaten fehlgeleitet, geblockt oder manipuliert werden, so dass ein Fehlerzustand spät oder gar nicht erkannt werden kann und es zu einem Schaden kommt.

Um das Risiko zu verringern, kann durch zusätzliche Maßnahmen entweder die Schadenshöhe beeinflusst werden oder die Wahrscheinlichkeit, dass der Fall eintritt, reduziert werden. Hierbei sind Sie als Betreiber

(B), als Hersteller (H) sowie als Integrator (I) gefragt. Die Buchstaben in Klammern werden im Folgenden genutzt, um auf Verantwortlichkeiten hinzuweisen. Maßnahmen für Betreiber sind mit (B) versehen. Eine mehrfache Verantwortung ist ebenfalls möglich.

Ein ausgereifter Prozess zur Auswahl von Mitarbeitern (B), Dienstleistern (B) und einer durchdachten Rechtevergabe (B) kann die Möglichkeiten des Angreifenden entsprechend einschränken. Die Arbeiten Externer sind zu begleiten (B) und nach Möglichkeit zu überwachen (I, B), um eine Manipulation zu erkennen. Zugangs-, Zugriffs- und Zutrittsberechtigungen und deren effektive Umsetzung hindern schon im Ansatz einen erfolgreichen Angriff. Zonierung von Bereichen und eine restriktive Vergabe und Überwachung von Berechtigungen unterstützen dabei.

Alternative Verbindungswege (H, I, B) in die Anlagen sollten abgesichert werden und den gleichen Standards entsprechen wie die Hauptverbindungen (I, B). Unterstützende Maßnahmen sind z.B. geeignete Verschlüsselung der Kommunikationsverbindungen (H, I), Beobachten von Systemaktivitäten (B), Validierung von Daten (H, B) sowie eine Minimierung der Zugriffspunkte (H, I, B).

Sollte es zu einem Angriff kommen, ist es unbedingt erforderlich diesen zu erkennen und angemessen darauf zu reagieren. Dabei unterstützen Prozesse zu Cyber-Sicherheitsvorfällen (I, B), Notfallpläne (I, B), Monitoring (I, B), Logging (I, B) sowie forensische Maßnahmen (I, B). Die daraus abgeleiteten Maßnahmen sollten zur Verbesserung der Cyber-Sicherheit (B) und Vermeidung zukünftiger Vorfälle (I, B) genutzt werden.

10.3.1 Anforderungen IT-Grundschutz zur Reduzierung des Risikos „Angriff von innen“

- ORP.1 Organisation (I, B)
  - ORP.1.A13 Sicherheit bei Umzügen
  - ORP.1.A14 Kontrollgänge
- ORP.2 Personal (I, B)
  - ORP.2.A7 Überprüfung der Vertrauenswürdigkeit von Mitarbeitern
- ORP.4 Identitäts- und Berechtigungsmanagement (I, B)
  - ORP.4.A5 Vergabe von Zutrittsberechtigungen
  - ORP.4.A6 Vergabe von Zugangsberechtigungen
  - ORP.4.A7 Vergabe von Zugriffsrechten
- CON.1 Kryptokonzept (H, I, B)
  - CON.1.A3 Verschlüsselung der Kommunikationsverbindungen
  - CON.1.A4 Geeignetes Schlüsselmanagement
  - CON.1.A16 Physische Absicherung von Kryptomodulen
- CON.4 Auswahl und Einsatz von Standardsoftware (H, I, B)
  - CON.4.A1 Sicherstellen der Integrität von Standardsoftware
  - CON.4.A3 Sichere Installation und Konfiguration von Standardsoftware
- CON.5 Entwicklung und Einsatz von Individualsoftware
  - CON.5.A1 Festlegung benötigter Sicherheitsfunktionen der Individualsoftware
- CON.9 Informationsaustausch
  - CON.9.A8 Verschlüsselung und Signatur

- OPS.1.1.2 Ordnungsgemäße IT-Administration
  - OPS.1.1.2.A4 Beendigung der Tätigkeit als IT-Administrator
- OPS.1.1.4 Schutz vor Schadprogrammen
  - OPS.1.1.4.A2 Nutzung systemspezifischer Schutzmechanismen
  - OPS.1.1.4.A5 Betrieb und Konfiguration von Virenschutzprogrammen
- DER.1 Detektion von sicherheitsrelevanten Ereignissen
  - DER.1.A3 Festlegung von Meldewegen für sicherheitsrelevante Ereignisse
  - DER.1.A9 Einsatz zusätzlicher Detektionssysteme
- DER.2.1 Behandlung von Sicherheitsvorfällen
  - DER.2.1.A5 Behebung von Sicherheitsvorfällen
  - DER.2.1.A9 Festlegung von Meldewegen für Sicherheitsvorfälle
  - DER.2.1.A10 Eindämmen der Auswirkung von Sicherheitsvorfällen
- DER.2.2 Vorsorge für die IT-Forensik
  - DER.2.2.A3 Vorauswahl von Forensik-Dienstleistern
- DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle
  - DER.2.3.A5 Schließen des initialen Einbruchswegs
  - DER.2.3.A7 Gezielte Systemhärtung
  - DER.2.3.A10 Umbauten zur Erschwerung eines erneuten Angriffs durch denselben Angreifer
- SYS.1.1 Allgemeiner Server
  - SYS.1.1.A1 Geeignete Aufstellung
  - SYS.1.1.A13 Beschaffung von Servern
- SYS.2.1 Allgemeiner Client
  - SYS.2.1.A15 Sichere Installation und Konfiguration von Clients
- IND.2.1 Allgemeine ICS-Komponente
  - IND.2.1.A8 Schutz vor Schadsoftware
- NET.1.1 Netzarchitektur und –design
  - NET.1.1.A4 Netztrennung in Sicherheitszonen
  - NET.1.1.A6 Endgeräte-Segmentierung im internen Netz
- NET.1.2 Netzmanagement
  - NET.1.2.A4 Grundlegende Authentisierung für den Netzmanagement-Zugriff
- INF.1 Allgemeines Gebäude
  - INF.1.A7 Zutrittsregelung und -kontrolle
- INF.2 Rechenzentrum sowie Serverraum
  - INF.2.A6 Zutrittskontrolle
- INF.5 Raum sowie Schrank für technische Infrastruktur
  - INF.5.A3 Zutrittsregelung und -kontrolle

10.4 Manipulation der Aktorik

Die Cyber-Risikoanalyse im Fallbeispiel des Gasspeichers gemäß IEC 62443-3-2, identifizierte in Schritt ZCR 5 das Risiko der Manipulation der Aktorik.

Für eine Manipulation der in der Gasspeicheranlage befindlichen Aktorik gibt es diverse Angriffsvektoren. Mit dem Internet vernetzte Aktoren können (extern) aus dem Internet angegriffen werden. Nicht mit dem Internet verbundene Aktoren sind über das LAN und Bussystem des Kavernenspeichers einem potenziellen Angriff ausgesetzt. Ferner können Informationen von Aktoren mit lokalem Zugriff manipuliert werden.

Fehlzustände in der Aktorik der betrachteten Gasspeicheranlage können eine direkte Auswirkung im Sinne eines Schadereignisses haben. Es besteht jedoch auch die Möglichkeit, dass ein Aktor, zum Beispiel ein Absperrventil, manipuliert wird, ohne dass es zu einer Störung kommt. Erst ein Fehlerzustand eines angebundenen oder des gleichen Systems, kann den Fehlerzustand des Ventils aufdecken. Solche sog. „schlafende Fehler“, oder in der Funktionalen Sicherheit „gefährlichen Fehler“, sind ebenso zu behandeln.

In den kommenden Abschnitten widmet sich diese Arbeit den Anforderungen und Maßnahmen des IT-Grundschutzkompendiums, um unter anderem o.g. Risiken zu begegnen. Zunächst sind für den OT-Bereich organisatorische wie technische Maßnahmen umzusetzen. Die Anbindung von OT-Geräten sollte in die Cyber-Sicherheitsorganisation der Institution eingebunden werden (B). Zusätzlich sollte das Betriebs- und Wartungspersonal hinsichtlich der sicheren Verfahrensweisen im Lebenszyklus der Aktoren sensibilisiert und geschult werden (B, I). Aufgrund der im OT-Umfeld typischen hohen Verfügbarkeitsanforderungen und der oft extremen Umgebungsbedingungen wie Hitze oder Kälte, Staub, Vibration oder Korrosion sollten Aktoren als robuste Geräte mit hoher Zuverlässigkeit und langer Lebensdauer konstruiert werden. Darüber hinaus sind Einschränkungen z. B. bezüglich Ex-Schutz, Brandschutz oder Medieneigenschaften (abrasiv, selbstzersetzend etc.) zu beachten. Ferner sollte der Zugriff auf Konfigurations- und Wartungsschnittstellen eingeschränkt werden (B, H). Wie eingangs erwähnt, können Aktoren über ein Bussystem oder das lokale Netzwerk der Anlage angebunden sein. Daher sollten zur Wartung und Konfiguration sowie zur Übertragung von Steuerdaten der Aktoren sichere Protokolle verwendet werden (B, I, H). Des Weiteren sollten die Kommunikationsbeziehungen der Aktoren sowie weiterer ICS-Komponenten dokumentiert sein (B). Für Herstellung und Integration der Aktoren sollten Besonderheiten im Betrieb, wie z. B. Sicherung, Regelwartungsmaßnahmen, Austausch und Wiederherstellung von Komponenten oder Leistungen Dritter, sowie die Möglichkeiten zur Systemverwaltung, wie z. B. Fernzugriffe, dokumentiert werden. Diese erweiterte Systemdokumentation sollte aktuell gehalten werden (I, H). Neben der Betriebsdokumentation sollte eine geeignete Inbetriebnahme der Aktoren sichergestellt sein (I). So sollten sie den technischen Spezifikationen entsprechen. Als Nächstes sollten sie in die bestehenden Betriebs- und Informationssicherheits-Prozesse eingebunden (z.B. als Asset inventarisiert) werden (B, I). Zur physikalischen Absicherung von Aktoren sollte ein Schutz vor unberechtigtem Zutritt, Zugang und Zugriff in Form von Perimeterschutz getroffen werden (B). Zutritte sollten kontrolliert, überwacht und protokolliert werden. Sofern Aktoren eingehaust sind, sollten die Gehäuse verschließbar (B) sein. Ein zugrundeliegendes Schlüsselmanagement und Berechtigungsmanagement regelt den kontrollierten und befugten Zutritt und Zugang zur Aktorik und deren Systemen. Unbefugte Zutritte oder Zugriffe sollten zeitnah erkannt werden, z.B. durch Auslösen von Alarmen (B). Die industrielle Anlage sollte einen Prozess etablieren, um Benutzerzugänge und zugeordnete Berechtigungen für den Zugriff auf die OT zu verwalten. Die Berechtigungsverwaltung sollte den Prozess, die Durchführung und die Dokumentation für die Beantragung, Einrichtung und den Entzug von Berechtigungen umfassen (B). Die Berechtigungsverwaltung sollte gewährleisten, dass Berechtigungen nach dem Minimalprinzip vergeben und regelmäßig überprüft werden.

Standard-Benutzer und –Passwörter auf Systemen sind oft bekannt und dokumentiert, beispielsweise in Handbüchern, die oft über das Intenet zugänglich sind. Daher sollten Standard-Benutzer mindestens deaktiviert (B, I), besser gelöscht werden. Voreingestellte Passwörter in Systemen und Anwendungen sollten bei der Installation in sichere Passwörter geändert werden (B, I). Falls möglich sollte jeder Mitarbeiter über ein

eigenes Benutzerkonto verfügen (B). Bei erhöhtem Schutzbedarf sollten drahtlose Verwaltungsschnittstellen nicht benutzt werden. Alle nicht benutzten Kommunikationsschnittstellen sollten deaktiviert werden (B, I).

Aktoren sollten durch Redundanz gegen Ausfälle geschützt werden (B). Um Veränderungen an Aktoren Rechnung zu tragen, sollte über die Bereitstellung einer Testumgebung nachgedacht werden (I). Durch diese Maßnahme wird der Produktivbetrieb der Anlage nicht gefährdet.

Im Folgenden sind Anforderungen bzw. Maßnahmen aus dedizierten IT-Grundschutzbausteinen aufgeführt, die das Risiko einer Manipulation der Aktorik behandeln können.

10.4.1 Anforderungen IT-Grundschutz zur Reduzierung des Risikos „Manipulation der Aktorik“:

- INF.1 Allgemeines Gebäude (B)
  - INF.1.A1 Planung der Gebäudeabsicherung [Planer]
  - INF.1.A7 Zutrittsregelung und –kontrolle
  - INF.1.A12 Schlüsselverwaltung
  - INF.1.A22 Sichere Türen und Fenster
  - INF.1.A23 Bildung von Sicherheitszonen
  - INF.1.A26 Pförtner- oder Sicherheitsdienst
  - INF.1.A27 Einbruchschutz
- IND.1 Betriebs- und Steuerungstechnik
  - IND.1.A1 Einbindung in die Sicherheitsorganisation (B)
  - IND.1.A3 Schutz vor Schadprogrammen (B)
  - IND.1.A5 Entwicklung eines geeigneten Zonenkonzepts
  - IND.1.A6 Änderungsmanagement im OT-Betrieb
  - IND.1.A7 Etablieren einer Berechtigungsverwaltung
  - IND.1.A10 Monitoring, Protokollierung und Detektion [Bereichssicherheitsbeauftragter]
  - IND.1.A14 Starke Authentisierung an OT-Komponenten
  - IND.1.A15 Prüfung und Überwachung von Berechtigungen
  - IND.1.A16 Stärkere Abschottung der Zonen
- IND 2.3 Sensoren und Aktoren
  - IND.2.3.A3 Drahtlose Kommunikation
- IND 2.4 Maschine
  - IND.2.4.A1 Fernwartung durch Maschinen- und Anlagenbauer (B)

10.5 Nicht autorisierter Zugriff auf IT-Systeme

Ein nicht autorisierter Zugriff auf IT-Systeme einer industriellen Anlage kann Einfluss auf den sicheren Betrieb einer Anlage haben. Daher wurde dieses Risiko während der Cyber-Risikoanalyse im Rahmen der Durchführung des Schrittes ZCR 5 identifiziert.

Als IT-System werden an dieser Stelle Engineering-Workstations (Clients), Server sowie weitere Netzwerkkomponenten verstanden. Im Rahmen eines Angriffs auf die genannten Systeme können Informationen verfälscht, gelöscht oder gestohlen werden. Derartige Angriffe können aufgrund vorsätzlicher Fehlparametrisierung durch den Angreifenden in der Anlage bzw. Anlagenteilen zu schweren Unfällen mit Verletzten oder gar Toten führen. Um diesen Bedrohungen entgegenzuwirken, werden geeignete umzusetzende Anforderungen aus Sicht von Betreibern, Herstellern und Integratoren aus dem IT-Grundschutz aufgezeigt. Die Auswahl der Maßnahmen soll die Eintrittswahrscheinlichkeit des Risikos reduzieren.

Um IT-Systeme zu kompromittieren, sind verschiedene Angriffsvektoren denkbar. IT-Systeme können sowohl physikalisch als auch logisch manipuliert werden. Zur physikalischen Absicherung von IT-Systemen sollten Absicherungen gegen unberechtigten Zutritt, Zugang und Zugriff in Form von Perimeterschutz getroffen werden (B). Dies gilt insbesondere für Gebäude, Räume und Schränke. Zutritte sollten kontrolliert, überwacht und protokolliert werden. Gehäuse und Schränke sollten verschließbar (B) sein. Für den Schutz gegen unbefugten Zutritt sollte es eine Zutrittskontrolle (B) geben. Weiterhin können äußere Bedingungen Einfluss auf die Funktionsweise von IT-Systemen haben. Daher sollte sichergestellt werden, dass die Lufttemperatur und Luftfeuchtigkeit (B) im IT-Betriebsbereich innerhalb der Spezifikationen der Systeme bleibt. Jedes IT-System sollte über eine Benutzerauthentisierung (I, H) verfügen, die dem Schutzbedarf des jeweiligen Systems angemessen ist. Die Verwendung von Multi-Faktor-Authentisierung ist ebenso möglich, bei erhöhtem Schutzbedarf der IT-Systeme sogar notwendig. Soweit möglich, sollte - ebenso für die installierten Fachanwendungen - auf netzbasierte Authentisierungsdienste (z.B. LDAP) zurückgegriffen werden. Zugriffsrechte auf Informationen, die auf IT-Komponenten gespeichert sind, sollten restriktiv vergeben werden. Jeder Benutzende sollte nur auf diejenigen Dateien zugreifen können, für die er organisatorische Berechtigung innehat (I). Deshalb sollte ein Berechtigungskonzept vorliegen (B). Um das Risiko von Angriffsmöglichkeiten auf Schwachstellen von Diensten zu minimieren, sollten nicht benötigte Dienste und Kennungen deaktiviert werden (I). Auch nicht benötigte Funktionen, sofern möglich, sollten in der Firmware deaktiviert werden (I). Organisatorisch könnte hier ein Härtungskonzept für IT-Systeme entwickelt werden (B). Administratoren eines IT-Systems sollten sich im Rahmen eines Schwachstellenmanagements (B, I, H) regelmäßig über bekannt gewordene Schwachstellen der Firmware, Betriebssysteme und eingesetzter Anwendungen bei den Herstellern informieren. Im Zuge dessen ist im Rahmen eines Patchmanagements (B) dafür Sorge zu tragen, dass die aufgedeckten Schwachstellen so schnell wie möglich behoben werden. Hersteller von IT-Systemen sollten aktiv auf Meldungen von Schwachstellen reagieren. Neben notwendigen internen Vorbereitungen wie z.B. der Erstellung einer Leitlinie, in welcher der Hersteller den Umgang mit Schwachstellen definiert (Vulnerability Handling Policy), sollten entsprechende Prozesse (z.B. Incident Management Prozess) etabliert werden (H, I, B). Des Weiteren sollten Hersteller diverse Kommunikationskanäle zum Schwachstellenmanagement bedienen. Um Angriffe und den Befall durch Schadsoftware zu erkennen, ist der Einsatz von Virenschutz-Programmen anzuraten. Die entsprechenden Signaturen eines Virenschutz-Programms und das Virenschutz-Programm selbst sollten regelmäßig aktualisiert werden (I). Eine weitere Maßnahme zur Reduktion des Risikos des Befalls durch Schadsoftware ist die Einbindung eines IT-Systems in Systemüberwachungs- und Monitoringkonzepte (I). Damit wird die Funktionsfähigkeit eines Systems und der darauf betriebenen Dienste laufend überwacht und Fehlerzustände sowie die Überschreitung definierter Grenzwerte an das Betriebspersonal gemeldet (B). Um Fehlerzustände zu erkennen und entsprechend zu handeln ist das Personal zu schulen (B).

10.5.1 Anforderungen IT-Grundschutz zur Reduzierung des Risikos „Nicht autorisierter Zugriff auf IT-Systeme“:

- INF.1 Allgemeines Gebäude (B)
  - INF.1.A1 Planung der Gebäudeabsicherung
  - INF.1.A7 Zutrittsregelung und -kontrolle
  - INF.1.A9 Sicherheitskonzept für die Gebäudenutzung

  - INF.1.A12 Schlüsselverwaltung
  - INF.1.A23 Bildung von Sicherheitszonen
  - INF.1.A26 Pförtner- oder Sicherheitsdienst
  - INF.1.A27 Einbruchschutz
- INF.2 Rechenzentrum sowie Serverraum (B, I)
  - INF.2.A3 Einsatz einer unterbrechungsfreien Stromversorgung
  - INF.2.A5 Einhaltung der Lufttemperatur und -feuchtigkeit
  - INF.2.A6 Zutrittskontrolle
  - INF.2.A7 Verschließen und Sichern
  - INF.2.A12 Perimeterschutz für das Rechenzentrum
  - INF.2.A24 Einsatz von Videoüberwachungsanlagen
- SYS.1.1 Allgemeiner Server (B, I, H)
  - SYS.1.1.A2 Benutzerauthentisierung an Servern
  - SYS.1.1.A3 Restriktive Rechtevergabe
  - SYS.1.1.A4 Rollentrennung
  - SYS.1.1.A5 Schutz der Administrationsschnittstellen
  - SYS.1.1.A6 Deaktivierung nicht benötigter Dienste und Kennungen
  - SYS.1.1.A7 Updates und Patches für Firmware, Betriebssystem und Anwendungen
  - SYS.1.1.A9 Einsatz von Virenschutz-Programmen
  - SYS.1.1.A18 Verschlüsselung der Kommunikationsverbindungen
  - SYS.1.1.A34 Festplattenverschlüsselung
- SYS.2.1 Allgemeiner Client (B, I, H)
  - SYS.2.1.A1 Sichere Benutzerauthentisierung
  - SYS.2.1.A3 Aktivieren von Autoupdate-Mechanismen
  - SYS.2.1.A5 Verwendung einer Bildschirmsperre
  - SYS.2.1.A6 Einsatz von Viren-Schutzprogrammen
  - SYS.2.1.A9 Festlegung einer Sicherheitsrichtlinie für Clients
  - SYS.2.1.A14 Updates und Patches für Firmware, Betriebssystem und Anwendungen
  - SYS.2.1.A19 Restriktive Rechtevergabe
  - SYS.2.1.A28 Verschlüsselung der Clients
  - SYS.2.1.A29 Systemüberwachung und Monitoring der Clients
  - SYS.2.1.A32 Einsatz zusätzlicher Maßnahmen zum Schutz vor Exploits
  - SYS.2.1.A37 Verwendung von Mehr-Faktor-Authentisierung
- SYS.3.1 Laptops (B, I, inklusive Umsetzungshinweise)
  - SYS.3.1.A2 Zugriffsschutz am Laptop
  - SYS.3.1.A3 Einsatz von Personal Firewalls

  - SYS.3.1.A4 Einsatz von Antivirenprogrammen
  - SYS.3.1.A9 Sicherer Fernzugriff
  - SYS.3.1.A13 Verschlüsselung von Laptops
  - SYS.3.1.A15 Geeignete Auswahl von Laptops
- SYS.3.2.1 Allgemeine Smartphones und Tablets (B, I)
  - SYS.3.2.1.A3 Sichere Grundkonfiguration für mobile Geräte
  - SYS.3.2.1.A4 Verwendung eines Zugriffschutzes
  - SYS.3.2.1.A5 Updates von Betriebssystem und Apps
  - SYS.3.2.1.A11 Verschlüsselung des Speichers
  - SYS.3.2.1.A14 Schutz vor Phishing und Schadprogrammen im Browser
  - SYS.3.2.1.A20 Auswahl und Freigabe von Apps
  - SYS.3.2.1.A26 Nutzung von PIM-Containern
- SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte (B, I)
  - SYS.4.1.A2 Geeignete Aufstellung und Zugriff auf Drucker, Kopierer und Multifunktionsgeräte
  - SYS.4.1.A22 Ordnungsgemäße Entsorgung ausgedruckter Dokumente
  - SYS.4.1.A18 Konfiguration von Druckern, Kopierern und Multifunktionsgeräten
  - SYS.4.1.A14 Authentisierung und Autorisierung bei Druckern, Kopierern und Multifunktionsgeräten
- DER.1 Detektion von sicherheitsrelevanten Ereignissen (B)
  - DER.1.A9 Einsatz zusätzlicher Detektionssysteme
  - DER.1.A10 Einsatz von TLS-/SSH-Proxies
  - DER.1.A15 Zentrale Detektion und Echtzeitüberprüfung von Ereignismeldungen
  - DER.1.A17 Automatische Reaktion auf sicherheitsrelevante Ereignisse
- DER.2.1 Behandlung von Sicherheitsvorfällen (B, I, H)
  - DER.2.1.A4 Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen
  - DER.2.1.A7 Etablierung einer Vorgehensweise zur Behandlung von Sicherheitsvorfällen
  - DER.2.1.A15 Schulung der Mitarbeiter der zentralen Anlaufstelle des IT-Betriebs zur Behandlung von Sicherheitsvorfällen
- NET.1.1 Netzarchitektur und –design (B)
  - NET.1.1.A4 Netztrennung in Sicherheitszonen
  - NET.1.1.A5 Client-Server-Segmentierung
  - NET.1.1.A8 Grundlegende Absicherung des Internetzugangs
  - NET.1.1.A9 Grundlegende Absicherung der Kommunikation mit nicht vertrauenswürdigen Netzen
  - NET.1.1.A10 DMZ-Segmentierung für Zugriffe aus dem Internet
  - NET.1.1.A11 Absicherung eingehender Kommunikation vom Internet in das interne Netz
  - NET.1.1.A18 P-A-P-Struktur für die Internet-Anbindung
  - NET.1.1.A23 Trennung von Sicherheitssegmenten
  - NET.1.1.A34 Einsatz kryptografischer Verfahren auf Netzebene

- NET.3.1 Router und Switches (B, I, H)
  - NET.3.1.A1 Sichere Grundkonfiguration eines Routers oder von Switches
  - NET.3.1.A2 Einspielen von Updates und Patches
  - NET.3.1.A3 Restriktive Rechtevergabe
  - NET.3.1.A11 Beschaffung eines Routers oder Switches
  - NET.3.1.A12 Erstellung einer Konfigurations-Checkliste für Router und Switches
  - NET.3.1.A24 Einsatz von Netzzugangskontrollen
  - NET.3.1.A28 Einsatz von zertifizierten Produkten
- NET 3.2 Firewall (B, I, H)
  - NET.3.2.A2 Festlegen der Firewall-Regeln
  - NET.3.2.A3 Einrichten geeigneter Filterregeln am Paketfilter
  - NET.3.2.A4 Sichere Konfiguration der Firewall
  - NET.3.2.A5 Restriktive Rechtevergabe
  - NET.3.2.A11 Einspielen von Updates und Patches
  - NET.3.2.A15 Beschaffung einer Firewall
  - NET.3.2.A16 Aufbau einer „P-A-P“-Struktur
  - NET.3.2.A17 Deaktivierung von IPv4 oder IPv6
  - NET.3.2.A18 Administration über ein gesondertes Managementnetz
  - NET.3.2.A23 Systemüberwachung und -auswertung
  - NET.3.2.A31 Einsatz von zertifizierten Produkten
- CON.1 Kryptokonzept (B)
  - CON.1.A1 Auswahl geeigneter kryptografischer Verfahren
  - CON.1.A3 Verschlüsselung der Kommunikationsverbindungen
- CON.5 Entwicklung und Einsatz von Individualsoftware (B, I, H)
  - CON.5.A1 Festlegung benötigter Sicherheitsfunktionen der Individualsoftware
  - CON.5.A3 Sichere Installation von Individualsoftware
- ORP.4 Identitäts- und Berechtigungsmanagement
  - ORP.4.A5 Vergabe von Zutrittsberechtigungen
  - ORP.4.A6 Vergabe von Zugangsberechtigungen
  - ORP.4.A7 Vergabe von Zugriffsrechten
  - ORP.4.A8 Regelung des Passwortgebrauchs
  - ORP.4.A9 Identifikation und Authentisierung
  - ORP.4.A22 Regelung zur Passwortqualität
  - ORP.4.A10 Schutz von Benutzerkennungen mit weitreichenden Berechtigungen
  - ORP.4.A14 Kontrolle der Wirksamkeit der Benutzertrennung am IT-System bzw.Anwendung
  - ORP.4.A17 Geeignete Auswahl von Identitäts- und Berechtigungsmanagement-Systemen

- ORP.4.A18 Einsatz eines zentralen Authentisierungsdienstes
- ORP.4.A21 Mehr-Faktor-Authentisierung

10.6 Nicht autorisierter Zugriff auf steuernde OT-Komponenten

Sollte es einem unautorisierten Dritten möglich sein, auf die steuernden OT-Komponenten zuzugreifen, kann das unvorhersehbare Folgen für die Anlage nach sich ziehen. Dabei ist es unerheblich, ob der nicht autorisierte Zugriff von einem Angreifenden oder internen Mitarbeitern durchgeführt wird. Beispielsweise könnte eine speicherprogrammierbare Steuerung ohne Zugangssicherung versehentlich, unwissentlich oder absichtlich manipuliert werden und einen Vorfall verursachen, verschlimmern oder mitigierende Maßnahmen verhindern. Sollten bei diesem Zugriff Safety-Funktionen umgangen werden, könnte es im schlimmsten Fall zum Versagen dieser Einrichtungen kommen – mit katastrophalen Auswirkungen.

Um das Risiko zu verringern, kann durch zusätzliche Maßnahmen entweder die Schadenshöhe beeinflusst werden oder die Wahrscheinlichkeit, dass der Fall eintritt, reduziert werden. Hierbei sind Sie als Betreiber (B), als Hersteller (H) sowie als Integrator (I) gefragt.

Schon bei der Planung (H, I) und Einrichtung (H, I) der OT-Komponenten sollten die Möglichkeiten zum unautorisierten Zugriff minimiert werden. Es sollten nach Möglichkeit zertifizierte Komponenten (H) verwendet werden. Dazu ist bei der Planung und Beschaffung besonderes Augenmerk auf die Hersteller (B, I) und Lieferanten (H, I) zu legen. Es sollten klare Vorgaben an die Komponenten entsprechend ihres Einsatzgebietes gemacht werden (B, I). Die verwendete Hardware sollte den technischen Anforderungen entsprechen und vor der Nutzung in Form von Integrationstests und Penetrationstests geprüft werden (H, I). Diese Überprüfungen sollten in Rahmen von Audits oder Revisionen (I, B) regelmäßig wiederholt werden.

Während des Betriebs ist der Zugang (B, I) durch geeignete Schutzmaßnahmen sicherzustellen (B, I). Diese Maßnahme ist besonders bei Komponenten wirksam, welche keine externen Schnittstellen bereitstellen und einen direkten Zugriff voraussetzen. Geeignete Maßnahmen sind z.B. ein Perimeterschutz, sichere Türen, Sicherheitszonen oder Technikschränke (B, I). Wartungspersonal und Externe sollten begleitet (B) und ihre Arbeiten überwacht werden.

Es sollte durch geeignete Maßnahmen sichergestellt sein, dass kein unautorisierter Zugriff auf die Komponenten durch Unwissenheit interner Mitarbeiter geschieht. Dabei unterstützen Schulungen (B) sowie technische Einrichtungen wie Rollen und Rechtekonzepte (B). Dies kann als eine Mindestabsicherung gegen versehentlichen Zugriff gesehen werden.

Komponenten mit externen Schnittstellen oder IoT-Funktionalitäten sind darüber hinaus durch verschiedenste Angriffe gefährdet. Dabei muss unterschieden und betrachtet werden, in welchen Einsatzgebieten (H, B, I) die Komponenten verwendet werden. Es sollte geprüft werden, in wie weit Sicherheitskonzepte (H, B, I) und Regelungen erstellt werden müssen, um klare und praktikable Maßnahmen zu definieren. Die beschlossenen Maßnahmen sollten durch geschultes (B, I) und geeignetes Personal (B, I) umgesetzt und eingehalten werden. Netzverbindungen (H, B, I) und Schnittstellen sollten abgesichert und die Komponenten angemessen gehärtet (H, I) werden.

Eine Manipulation der Komponenten sollte nach Möglichkeit erkannt werden (B), damit entsprechende Gegenmaßnahmen ergriffen werden können. Dazu ist ein Monitoring und eine Loggingstruktur einzurichten. Die erkannten Vorfälle sollten in geeigneter Weise gemeldet (B), nachhaltig bearbeitet (B) und Maßnahmen zur zukünftigen Verhinderung (B, I) abgeleitet werden.

Es werden zunehmend Systeme aus der Ferne (I, B) genutzt und verwaltet. Beim Zugriff auf die OT-Komponenten aus der Ferne sind besondere Sicherungsmaßnahmen (B) für das System sowie den Zugriffspunkt zu definieren. Es ist zu vermeiden, dass Maßnahmen zur Fernsteuerung die Cyber-Sicherheit der Komponente oder des gesamten Systems schwächen.

10.6.1 Anforderungen IT-Grundschutz zur Reduzierung des Risikos „Nicht autorisierter Zugriff auf steuernde OT-Komponenten“:

- ISMS.1 Sicherheitsmanagement
- ISMS.1.A17 Abschließen von Versicherungen
- ORP.1 Organisation (B)
- ORP.1.A3 Beaufsichtigung oder Begleitung von Fremdpersonen
- ORP.1.A5 Vergabe von Berechtigungen
- ORP.3 Sensibilisierung und Schulung (I, B)
- ORP.3.A3 Einweisung des Personals in den sicheren Umgang mit IT
- CON.1 Kryptokonzept (H, I, B)
- CON.1.A1 Auswahl geeigneter kryptografischer Verfahren
- CON.1.A6 Bedarfserhebung für kryptografische Verfahren und Produkte
- CON.4 Auswahl und Einsatz von Standardsoftware
- CON.4.A1 Sicherstellen der Integrität von Standardsoftware
- CON.4.A10 Implementierung zusätzlicher Sicherheitsfunktionen
- CON.5 Entwicklung und Einsatz von Individualsoftware
- CON.5.A1 Festlegung benötigter Sicherheitsfunktionen der Individualsoftware
- CON.5.A4 Heranführen von Benutzerinnen und Benutzern an Individualsoftware
- OPS.1.1.2 Ordnungsgemäße IT-Administration
- OPS.1.1.2.A5 Nachweisbarkeit von administrativen Tätigkeiten
- OPS.1.1.2.A18 Durchgängige Protokollierung administrativer Tätigkeiten
- OPS.1.1.5 Protokollierung
- OPS.1.1.5.A3 Konfiguration der Protokollierung auf System- und Netzebene
- OPS.1.1.6 Software-Tests und –Freigaben
- OPS.1.1.6.A14 Durchführung von Penetrationstests
- OPS.1.2.5 Fernwartung
- OPS.1.2.5.A3 Absicherung der Schnittstellen zur Fernwartung
- OPS.1.2.5.A17 Authentisierungsmechanismen bei der Fernwartung
- OPS.2.2 Cloud-Nutzung
- OPS.2.2.A7 Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung
- DER.1 Detektion von sicherheitsrelevanten Ereignissen
- DER.1.A3 Festlegung von Meldewegen für sicherheitsrelevante Ereignisse
- DER.1.A5 Einsatz von mitgelieferten Systemfunktionen zur Detektion
- DER.1.A6 Kontinuierliche Überwachung und Auswertung von Protokolldaten
- DER.1.A16 Einsatz von Detektionssystemen nach Schutzbedarfsanforderungen
- DER.1.A17 Automatische Reaktion auf sicherheitsrelevante Ereignisse

- DER.2.2 Vorsorge für die IT-Forensik
- DER.2.2.A7 Auswahl von Werkzeugen zur Forensik
- DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle
- DER.2.3.A7 Gezielte Systemhärtung
- DER.2.3.A9 Hardwaretausch betroffener IT-Systeme
- DER.4 Notfallmanagement
- DER.4.A10 Tests und Notfallübungen
- SYS.1.1 Allgemeiner Server
- SYS.1.1.A1 Geeignete Aufstellung
- SYS.1.1.A2 Benutzerauthentisierung an Servern
- SYS.1.1.A18 Verschlüsselung der Kommunikationsverbindungen
- SYS.1.1.A23 Systemüberwachung und Monitoring von Servern
- SYS.2.1 Allgemeiner Client
- SYS.2.1.A1 Sichere Benutzerauthentisierung
- SYS.4.3 Eingebettete Systeme
- SYS.4.3.A16 Tamper-Schutz bei eingebetteten Systemen
- SYS.4.4 Allgemeines IoT-Gerät
- SYS.4.4.A2 Authentisierung
- SYS.4.4.A22 Systemüberwachung
- IND.1 Betriebs- und Steuerungstechnik
- IND.1.A7 Etablieren einer Berechtigungsverwaltung
- IND.1.A10 Monitoring, Protokollierung und Detektion
- IND.2.1 Allgemeine ICS-Komponente (B, H, I)
- IND.2.1.A1 Einschränkung des Zugriffs für Konfigurations- und Wartungsschnittstellen
- IND.2.1.A2 Nutzung sicherer Protokolle für die Konfiguration und Wartung
- IND.2.1.A4 Deaktivierung nicht genutzter Dienste, Funktionen und Schnittstellen
- IND.2.1.A3 Protokollierung
- IND.2.1.A5 Deaktivierung nicht genutzter Benutzerkonten
- IND.2.1.A6 Netzsegmentierung
- IND.2.1.A8 Schutz vor Schadsoftware
- IND.2.1.A12 Beschaffung von ICS-Komponenten
- IND.2.1.A13 Geeignete Inbetriebnahme der ICS-Komponenten
- IND.2.2 Speicherprogrammierbare Steuerung (SPS)
- IND.2.2.A2 Benutzerkontenkontrolle und restriktive Rechtevergabe
- NET.1.1 Netzarchitektur und –design
- NET.1.1.A4 Netztrennung in Sicherheitszonen

- NET.1.1.A31 Physische Trennung von Sicherheitssegmenten
- INF.1 Allgemeines Gebäude
- INF.1.A7 Zutrittsregelung und -kontrolle
- INF.1.A33 Anordnung schützenswerter Gebäudeteile
- INF.4 IT-Verkabelung
- INF.4.A4 Anforderungsanalyse für die IT-Verkabelung
- INF.5 Raum sowie Schrank für technische Infrastruktur
- INF.5.A3 Zutrittsregelung und -kontrolle
- INF.5.A4 Schutz vor Einbruch
- INF.5.A17 Inspektion und Wartung der Infrastruktur
- INF.5.A20 Schutz vor Einbruch und Sabotage

10.7 Unterbrechung oder Manipulation der Sensordaten

Es wurde in ZCR 5 festgestellt, dass ein Unterbrechen der Sensordaten, d.h. eine Unterbrechung des Datenflusses oder die Lieferung falscher Sensordaten zum Fehlverhalten der Anlage führen kann. Sensordaten liefern Informationen über den Zustand von Anlagen bzw. darin ablaufenden Prozessen und bilden somit die Grundlage zur Steuerung dieser. So wird beispielsweise die Anlage in einen sicheren Zustand gefahren, bzw. im Anwendungsbeispiel der Gasspeicheranlage in die Abschaltung, wenn definierte Grenzwerte der Sensordaten erreicht werden, um größere Schäden oder Gefährdungen zu verhindern. Diese Cyber-Sicherheitsfunktion kann durch eine Manipulation oder defekte Sensoren gezielt ausgelöst werden. Andersherum können im Extremfall durch manipulierte Sensordaten Funktionen der Anlagensicherheit umgegangen und der Anforderungsfall herbeigeführt werden, sodass es zu einer Zerstörung der Anlage kommen kann. Wenn beispielsweise der Drucksensor zu wenig anzeigt, erhöht sich der Druck immer weiter ohne den Grenzwert zu erreichen. So kann die Anlage zerstört werden, ohne dass dies zuvor bemerkt wird. Wenn zeitgleich die Sensordaten der betrieblichen Regelung beeinflusst werden, kann dieser Zustand bewusst herbeigeführt werden. Ebenso kann es sein, dass die Sensorik einem Fehler unterliegt, sodass die Anlage in einen sicheren Zustand versetzt wird, ohne dass dies tatsächlich notwendig gewesen wäre. Des Weiteren kann durch eine Manipulation einer größeren Anzahl von Sensoren auch eine Situation herbeigeführt werden, die durch die vorhandenen Sicherheitseinrichtungen nicht mehr beherrscht werden kann.

Um das Risiko zu verringern, kann durch zusätzliche Maßnahmen entweder die Schadenshöhe beeinflusst werden oder die Wahrscheinlichkeit, dass der Fall eintritt, reduziert werden. Hierbei sind Sie als Betreiber (B), als Hersteller (H) sowie als Integrator (I) gefragt.

Zum Eindämmen eines bereits entstandenen Schadens in der Anlage des Betreibers sollten im Rahmen des Notfallmanagements (B) u.a. Wiederanlaufpläne (B) entwickelt werden, sodass die Anlage ohne Verzögerungen sicher wieder hochgefahren werden kann. Diese Pläne sollten stets aktuell gehalten und regelmäßig geprüft werden. Dazu bieten sich Tests von Teilbereichen, theoretische Tests, Simulationen, aber auch ein vollständiger Testlauf an. Dadurch werden die Abläufe auf Schwachstellen hin überprüft und verbessert sowie verinnerlicht. Ein weiterer Aspekt besteht in der Einbindung und Sensibilisierung (B) der Mitarbeitenden, sodass diese erkennen was geschieht und in der Lage sind, entsprechend zu handeln. Um schnell zu erkennen, dass eine Unterbrechung des Datenflusses vorliegt, sollte dies durch ein Monitoring der Sensoren in einer automatischen Meldung resultieren. Hierzu müssen Meldewege und anschließende Handlungsanweisungen definiert und kommuniziert werden.

Um die Eintrittswahrscheinlichkeit zu reduzieren, sollte insbesondere auf die eingesetzten Sensoren geachtet werden. Hierbei ist ein Zusammenspiel von Herstellern (H), Integratoren (I) und letztlich den Betreibern

(B) nötig. Dazu ist bereits in der Beschaffung (B) ein Kriterienkatalog seitens des Betreibers zu erstellen, der Anforderungen an die Sensoren formuliert. Dazu gehört beispielsweise eine geringe Fehleranfälligkeit oder Integritätsprüfung. Die Sensoren sollten redundant (B) aufgebaut sein, sodass der Ausfall oder die Manipulation eines Sensors zwar einen Alarm auslöst, aber nicht die gesamte Anlage in den sicheren Zustand fahren lässt. Die Mitarbeitenden sollten hinsichtlich der ausgelösten Alarme geschult (B) sein, um z.B. die Alarmmeldung zu überprüfen oder den Sensor auszutauschen. Auch sollten ausreichend Ressourcen (B) vorgehalten werden, um den Alarmen nachgehen oder Sensoren austauschen zu können. Die Sensoren sollten gemäß eines dokumentierten Ablaufs konfiguriert (I) und installiert werden. Dabei sollten insbesondere nicht benötigte Funktionen (I), wie u.a. nicht benötigte drahtlose oder -gebundene Kommunikation sowie nicht genutzte Schnittstellen oder Benutzerkonten deaktiviert werden, insofern die Sensoren diese Funktionalität besitzen bzw. dies technisch möglich ist. Allgemein sollten nur diejenigen Personen Zugriff und administrierende Rechte (B, I) auf die Sensoren bekommen, die diesen wirklich benötigen. Es sollte geprüft werden, inwiefern ein Fernzugriff (B, I) auf die Sensoren (z.B. zu Wartungszwecken) notwendig ist und wie dieser realisiert wird. Dabei ist insbesondere darauf zu achten, dass nur dedizierte Verbindungen (IP-Adressen) zugelassen sind und keine unerlaubten Zugriffe erfolgen können. Alle Zugriffe sollten protokolliert (B, H, I) und erst nach einer erfolgreichen Benutzerauthentifizierung (B, H, I) ermöglicht werden. Zudem sollte regelmäßig (mindestens jährlich) eine vollständige Funktionsprüfung (B, I) u.a. des Messbereichs durchgeführt werden. Bei Bedarf ist auch eine erneute Kalibrierung (I) vorzunehmen. Um die Manipulation zu erschweren, sollten die Sensoren an einen räumlich geeigneten (B, I) Ort (u.a. zutrittsbeschränkt) angebracht und in einem separierten und geschützten Netzwerk bzw. separierten System (B) betrieben werden. Außerdem sollten Mechanismen zum Schutz vor Schadsoftware (B, H, I) ergriffen werden. Am Ende des Lebenszyklus der Sensoren sollten diese geregelt entsorgt (B) werden. Dies verhindert u.a., dass aus den Sensoren Informationen ausgelesen werden können, die Rückschlüsse auf die Beschaffenheit der Anlage oder auch die sich noch im Einsatz befindlichen Sensoren zulassen. Um dies sicherzustellen, bietet sich beispielsweise nach einer Löschung der Daten (B), insbesondere der Zugangsdaten, die physische Zerstörung (B) der Sensoren an, ggf. durch Beauftragung eines externen Entsorgungsdienstleisters (B). Bis zur Zerstörung muss die sichere Lagerung (B) der Komponenten gewährleistet sein und auch der externe Dienstleister sollte über eine sorgfältige Auswahl mittels Anforderungskatalog und einer entsprechenden Dienstleistersteuerung (B) überwacht werden. Insbesondere sollte die Zerstörung gesichert und zeitnah vorgenommen werden sowie dokumentiert sein. Auch andere Dienstleister, die mit den Sensoren in Verbindung stehen, wie beispielsweise zur Wartung oder zur Überwachung der Meldungen, sollten einer angemessenen Dienstleistersteuerung unterliegen. Diese sollte vertraglich u.a. die Möglichkeit zur Auditierung (B) umfassen, von der in regelmäßigen Abständen Gebrauch gemacht werden sollte.

10.7.1 Anforderungen IT-Grundschutz zur Reduzierung des Risikos „Abschalten der Anlage durch Unterbrechung der Sensordaten“:

- DER.4 Notfallmanagement (B)
  - DER.4.A1 Erstellung eines Notfallhandbuchs
  - DER.4.A7 Erstellung eines Notfallkonzepts
  - DER.4.A10 Tests und Notfallübungen
- ORP.3 Sensibilisierung und Schulung (B, inklusive Umsetzungshinweise)
  - ORP.3.A3 Einweisung des Personals in den sicheren Umgang mit IT [auch mit Sensoren und der Auswertung von Sensordaten]
  - ORP.3.A4 Konzeption eines Sensibilisierungs- und Schulungsprogramms zur Informationssicherheit
- DER.1 Detektion von sicherheitsrelevanten Ereignissen (B)
  - DER.1.A3 Festlegung von Meldewegen für sicherheitsrelevante Ereignisse

  - DER.1.A6 Kontinuierliche Überwachung und Auswertung von Protokollierungsdaten
- IND.2.3 Sensoren und Aktoren (B, I)
  - IND.2.3.A1 Installation von Sensoren
  - IND.2.3.A2 Kalibrierung von Sensoren
  - IND.2.3.A3 Drahtlose Kommunikation
- IND.2.1 Allgemeine ICS-Komponente (B, H, I)
  - IND.2.1.A1 Einschränkung des Zugriffs für Konfigurations- und Wartungsschnittstellen
  - IND.2.1.A4 Deaktivierung nicht genutzter Dienste, Funktionen und Schnittstellen
  - IND.2.1.A3 Protokollierung
  - IND.2.1.A5 Deaktivierung nicht genutzter Benutzerkonten
  - IND.2.1.A6 Netzsegmentierung
  - IND.2.1.A8 Schutz vor Schadsoftware
  - IND.2.1.A12 Beschaffung von ICS-Komponenten
  - IND.2.1.A13 Geeignete Inbetriebnahme der ICS-Komponenten
  - IND.2.1.A14 Aussonderung von ICS-Komponenten
- SYS.1.1 Allgemeiner Server (B, I, inklusive Umsetzungshinweise)
  - SYS.1.1.A1 Geeignete Aufstellung [bezogen auf Sensoren]
  - SYS.1.1.A28 Steigerung der Verfügbarkeit durch Redundanz [bezogen auf Sensoren]
- ISMS.1 Sicherheitsmanagement (B, inklusive Umsetzungshinweise)
  - ISMS.1.A15 Wirtschaftlicher Einsatz von Ressourcen für Informationssicherheit
  - ISMS.1.A11 Aufrechterhaltung der Informationssicherheit [zur Auditierung der Dienstleister]
- ORP.4 Identitäts- und Berechtigungsmanagement (B, I, inklusive Umsetzungshinweise)
  - ORP.4.A2 Regelung für Einrichtung, Änderung und Entzug von Berechtigungen
  - ORP.4.A5 Vergabe von Zutrittsberechtigungen
  - ORP.4.A6 Vergabe von Zugangsberechtigungen
  - ORP.4.A7 Vergabe von Zugriffsrechten
  - ORP.4.A9 Identifikation und Authentisierung
  - ORP.4.A10 Schutz von Benutzerkennungen mit weitreichenden Berechtigungen
  - ORP.4.A12 Entwicklung eines Authentisierungskonzeptes für IT-Systeme und Anwendungen
  - ORP.4.A21 Mehr-Faktor-Authentisierung
- OPS.1.2.5 Fernwartung (B, I)
  - OPS.1.2.5.A1 Planung des Einsatzes der Fernwartung
  - OPS.1.2.5.A2 Sicherer Verbindungsaufbau bei der Fernwartung von Clients
  - OPS.1.2.5.A17 Authentisierungsmechanismen bei der Fernwartung
  - OPS.1.2.5.A19 Fernwartung durch Dritte
  - OPS.1.2.5.A14 Dedizierte Systeme bei der Fernwartung

- INF.1 Allgemeines Gebäude (B, I, inklusive Umsetzungshinweise)
  - INF.1.A1 Planung der Gebäudeabsicherung
  - INF.1.A7 Zutrittsregelung und -kontrolle
  - INF.1.A26 Pförtner- oder Sicherheitsdienst
  - INF.1.A33 Anordnung schützenswerter Gebäudeteile
- NET.1.1 Netzarchitektur und –design (B)
  - NET.1.1.A4 Netztrennung in Sicherheitszonen
  - NET.1.1.A9 Grundlegende Absicherung der Kommunikation mit nicht vertrauenswürdigen Netzen
  - NET.1.1.A11 Absicherung eingehender Kommunikation vom Internet in das interne Netz
  - NET.1.1.A21 Separierung des Management-Bereichs
  - NET.1.1.A23 Trennung von Sicherheitssegmenten
  - NET.1.1.A34 Einsatz kryptografischer Verfahren auf Netzebene
- OPS.2.1 Outsourcing für Kunden (B, inklusive Umsetzungshinweise)
  - OPS.2.1.A3 Auswahl eines geeigneten Outsourcing-Dienstleisters
  - OPS.2.1.A4 Vertragsgestaltung mit dem Outsourcing-Dienstleister
  - OPS.2.1.A14 Notfallvorsorge beim Outsourcing

10.8 Versehentliches oder mutwilliges Betätigen des Not-Aus-Tasters

Als spezifisches Risiko des befragten Unternehmens wurde die Betätigung des Not-Aus-Tasters identifiziert. Dieses Risiko muss nicht zwangsläufig ebenfalls als Risiko eingestuft werden oder auftreten, es ist aber stellvertretend für ein unternehmensspezifisches Risiko zu betrachten. Überlegen Sie, welche Gegebenheiten vorherrschen, die als Risiko gelten, das aber nicht in allgemeinen Risikolisten aufgeführt wird. Haben Sie spezielle bauliche Risiken? Oder besondere Umwelteinflüsse?

Bei dem befragten Unternehmen ist der Not-Aus-Taster so installiert, dass er jeder Person zugänglich ist und leicht betätigt werden kann. Der Not-Aus-Schalter stellt das schnellste Mittel (auch als ultimatives Mittel bezeichnet) um eine im schlimmsten Fall drohende Gefahr für Leib und Leben oder andere gravierende bzw. unkalkulierbare Ereignisse zu negieren. Bei Betätigung wird (in Abhängigkeit der Stopp-Kategorie nach DIN EN ISO 13850 i.Vm. DIN EN 60204-1) die Anlage Stromlos geschaltet oder in einen vorher definierten sogenannten sicheren Zustand versetzt, was u.a. zu einem Produktionsausfall bzw. Stillstand führt. Ausgehend von den Implikationen die mit der Betätigung des Not-Aus-Taster einhergehen, sollte daher ein versehentliches oder böswilliges Auslösen vermieden werden.

Ebenfalls sollte der Not-Aus-Taster vor dem Hintergrund der Vernetzung betrachtet werden, da Angreifende möglicherweise einen Notausbefehl in das Netzwerk einspielen können. Damit würde ein gezieltes Herunterfahren der Anlage ausgelöst werden. In diesem Fall wird die Schutzfunktion für Mensch und Umwelt missbraucht, um einen finanziellen Schaden zu verursachen. Die Schutzfunktion selbst wird dabei nicht beeinträchtigt und es besteht keine Gefährdung.

Um das Risiko zu reduzieren, können entweder die Auswirkungen eingegrenzt werden oder die Eintrittswahrscheinlichkeit verringert werden. Bei diesem Risiko ist ausschließlich der Betreiber der Anlage in der Verantwortung, entsprechende Maßnahmen zur Reduzierung des Risikos zu ergreifen.

Zum Eingrenzen der Auswirkungen – also dem Herunterfahren der Anlage – können die gleichen Maßnahmen umgesetzt werden, wie beim Risiko „Unterbrechung oder Manipulation der Sensordaten“. D.h. es sollte

insbesondere fokussiert werden, dass die Anlage zügig wieder hochgefahren wird, nachdem festgestellt worden ist, dass das Abschalten unbeabsichtigt war. Diese Aspekte sind im Notfallmanagement (B) verankert und werden durch die Schulung und Sensibilisierung (B) der Mitarbeitenden gefördert.

Um die Wahrscheinlichkeit zu verringern, dass der Not-Aus-Taster versehentlich betätigt wird, sollten die Mitarbeitenden entsprechend der Auswirkungen unterwiesen sein. Auch Gäste (B) oder Fremdfirmen, die potentiell Zutritt zum Not-Aus-Taster haben, sollten entweder auf dessen Funktion hingewiesen oder beaufsichtigt werden. Baulich sollte der Taster an einem Ort angebracht (B) werden, an dem das versehentliche Betätigen erschwert wird. Beispielsweise nicht neben einer Tür, da die Verwechslungsgefahr mit einem Lichtschalter oder einer Klingel besteht. Es ist auch möglich, die Betätigung des Tasters zu einer bewussten Handlung (B) zu machen, indem z.B. erst eine Plexiglasabdeckung aufgeklappt werden muss, ehe der Schalter betätigt werden kann. Da es bei der Betätigung um eine einfache und schnelle Handlung gehen soll (Zeit ist also eine kritische Komponente), sind solche Maßnahmen mit sehr viel „Fingerspitzengefühl“ anzuwenden.

Not-Aus-Schalter sind an jedem Bedienstand sowie an Orten anzubringen, wo die Einleitung eines Stillsetzens im Notfall erforderlich sein kann (also z.B. in Leitwarten, am Steuerungsschrank, an der Maschine selbst). Eine Überwachung, um ein mutwilliges Betätigen zu verhindern, ist daher nicht in jedem Fall möglich. Wenn dies durch den Pförtner- / Wachdiensts möglich ist, sollte dieser entsprechend eingewiesen und instruiert werden. Sollte der Pförtner- / Wachdienst durch einen Dienstleister (B) erbracht werden, so ist der Dienstleister mit Bedacht auszuwählen zu unterweisen und regelmäßig zu auditieren.

10.8.1 Anforderungen IT-Grundschutz zur Reduzierung des Risikos „Abschalten der Anlage durch Unterbrechung der Sensordaten“

- DER.4 Notfallmanagement (B)
  - DER.4.A1 Erstellung eines Notfallhandbuchs
  - DER.4.A7 Erstellung eines Notfallkonzepts
  - DER.4.A10 Tests und Notfallübungen
- ORP.3 Sensibilisierung und Schulung (B, inklusive Umsetzungshinweise)
  - ORP.3.A3 Einweisung des Personals in den sicheren Umgang mit IT [auch mit dem Not-Aus-Taster]
  - ORP.3.A4 Konzeption eines Sensibilisierungs- und Schulungsprogramms zur Informationssicherheit [u.a. Umgang mit Gästen]
- SYS.1.1 Allgemeiner Server (B, inklusive Umsetzungshinweise)
  - SYS.1.1.A1 Geeignete Aufstellung [bezogen auf Not-Aus-Taster]
- INF.1 Allgemeines Gebäude (B, inklusive Umsetzungshinweise)
  - INF.1.A1 Planung der Gebäudeabsicherung
  - INF.1.A7 Zutrittsregelung und -kontrolle
  - INF.1.A16 Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile
  - INF.1.A26 Pförtner- oder Sicherheitsdienst
  - INF.1.A27 Einbruchschutz
  - INF.1.A33 Anordnung schützenswerter Gebäudeteile
- ORP.4 Identitäts- und Berechtigungsmanagement (B, inklusive Umsetzungshinweise)
  - ORP.4.A5 Vergabe von Zutrittsberechtigungen
  - ORP.4.A9 Identifikation und Authentisierung

- OPS.2.1 Outsourcing für Kunden (B, inklusive Umsetzungshinweise)
  - OPS.2.1.A3 Auswahl eines geeigneten Outsourcing-Dienstleisters
  - OPS.2.1.A4 Vertragsgestaltung mit dem Outsourcing-Dienstleister
- ISMS.1 Sicherheitsmanagement (B, inklusive Umsetzungshinweise)
  - ISMS.1.A11 Aufrechterhaltung der Informationssicherheit [zur Auditierung der Dienstleister]

11 Änderungen der Bedrohungen mit Blick auf Industrie 4.0

Im folgenden Kapitel dieser Studie wird der Aspekt Industrie 4.0 beleuchtet. Es wird die Frage aufgegriffen, inwiefern Entwicklungen aus dem Bereich Industrie 4.0 Einfluss auf die Anlagensicherheit haben.

11.1 Entwicklung in der OT-Welt

Der Trend zur Digitalisierung, Vernetzung und Automatisierung von Anlagen in der Industrie wird mit dem Synonym Industrie 4.0 beschrieben. Veränderungen durch die Industrie 4.0 steigern den Bedarf an sicheren Netzen und Informationssystemen. Diese werden für eine funktionierende Anlage immer wichtiger. Wenn die Anlagensicherheit von dieser Infrastruktur abhängen, steigen die damit auch die Anforderungen an die Verfügbarkeit und Integrität, um Störfälle zu verhindern.

Die Bedrohungen für traditionelle Anlagen werden durch die Entwicklung zu Industrie 4.0 nicht verschwinden. Die klassischen Hauptbedrohungen bleiben Brand, Explosionen, Produktaustritt. Dazu kommen Verschließ, menschliche Fehler bzw. systematische Fehler und Bedrohungen aus dem Umfeld sowie naturbedingte Extremlagen (Sturm, Hochwasser, Schnee, Erdbeben). Durch Erweiterungen oder Modernisierungen und der damit verbundenen Digitalisierung kommen vielmehr die Cyber-Bedrohungen hinzu.

Damit auch in Zukunft Störfälle vermieden werden, muss und wird sich dies niederschlagen, sowohl im normalen Betrieb mit all seinen Vorteilen und Herausforderungen, als auch den zusätzlichen Planungs- und Überwachsungsaufgaben.

11.2 Neue Gefährdungen durch Industrie 4.0

Die bisherigen Anlagen werden zunehmend durch vernetzte Systeme ausgetauscht oder aufgerüstet. Dabei müssen die neuen Bedrohungen, die eine innovative Anlage mit sich bringt, gründlich betrachtet und bewertet werden. Anbindungen an dezentrale Cloudsysteme ist ein Trend, welcher neben der Digitalisierung der Anlageninfrastruktur weitere Bedrohungen entstehen lassen kann. Das zunehmende Outsourcing einzelner Dienste und Dienstleistungen an externe Auftragnehmer verspricht auf der einen Seite mehr Effizienz, aber steigert auf der anderen Seite auch die Intransparenz für die genutzten Systeme, Dienste und Anwendungen. Beispielsweise birgt die Schaffung zusätzlicher Schnittstellen Potential für die unzulässige Nutzung der übertragenen Daten oder öffnet zusätzliche Einfallstore zur Manipulation der Informationen, was sowohl die Vertraulichkeit, als auch die Integrität der Anwendungen bzw. Anlagen beeinträchtigt.

Die Störfallbetriebe sind durch diese Neuerungen immer weniger in der Lage, eine Störung ohne Hinzuziehung von externem Sachverstand zu beheben oder auch nur einen sicheren Zustand herzustellen. Dadurch wachsen Erfordernis und Umfang, die genutzten Dienstleister in die Lösungsfindung einzubeziehen. Dabei ist eine solide Beziehung mit klaren Rechten und Pflichten zwischen den beteiligten Parteien wichtig. Definierte Kommunikationslösungen mit entsprechenden Eskalationswegen im Störfall unterstützen die rasche Problemlösung.

11.3 Änderungen bestehender Anlagen

Für bestehende Anlagen sind viele Erkenntnisse über Bedrohungen und Risiken für die Funktionale Sicherheit durch Erfahrungen mit den Anlagen gewonnen worden. Aber auch Vorfälle auf Basis der OT-Security sind bereits bekannt geworden. Diese bekannten Bedrohungen müssen bei der Entwicklung von Innovationskonzepten für Anlagen bedacht werden und in die Planung zur Verhinderung von Störfällen einfließen.

Einige Gefährdungen oder bisher nötige Maßnahmen können bei der Überarbeitung der Anlagen eliminiert werden. So kann es Szenarien geben, wo bspw. kein Mitarbeiter vor Ort für die Überwachung und Steuerung mehr nötig ist, wenn die Anlage nach der Überarbeitung über eine Fernüberwachung und -steuerung verfügt. Dafür bringen die neuen Anbindungen und Übertragungstrecken ihre eigenen Bedrohungen und Anforderungen mit sich.

Es können zudem bisher nicht alle Vorgänge digitalisiert werden. Bei verfahrenstechnischen bzw. allgemein komplexeren Anlagen ist ein wichtiges Instrument der Analgenüberwachung der „einfache Rundgang“ des erfahrenen Mitarbeiters, der über audiovisuelle Eindrücke entstehende Probleme oft bereits frühzeitig detektieren kann. Dazu kommen oftmals noch Eingriffsmöglichkeiten via Handarmaturen und dergleichen. Diese und andere Funktionen lassen sich nicht oder nur teilweise wirtschaftlich digitalisieren. Es werden daher teils Kompromisse bei der Einbindung von Industrie 4.0 in die neue Struktur akzeptiert. Somit können eigene Risiken entstehen, die beim Umsetzen zu berücksichtigen sind.

Anlagenbetreiber und Integratoren müssen dabei zum einen abwägen, ob die wirtschaftlichen Vorteilen die Investitionskosten rechtfertigen. Zusätzlich gilt es bei allen Änderungen auch den Stand der Technik/Sicherheitstechnik zu Berücksichtigen. Damit der Schutz von Mensch und Umwelt bei allen Veränderungen und Entwicklungen sichergestellt ist.

11.3.1 Industrie 4.0 Patchwork

Bestehende Anlagen werden häufig durch Technologien aufgerüstet, welche einen vermeintlichen Mehrwert bringen, aber nicht innerhalb eines Gesamtkonzepts geplant und gesteuert werden. Es wird oft ein Flickenteppich aus einzelnen Insellösungen ohne Struktur erzeugt. Diese haben meistens nach kurzer Zeit einen hohen Wartungsaufwand und haben häufig das Potential für einen Ausfall. Es lohnt sich, eine durchdachte Planung durchzuführen und einen angemessenen Einsatz innovativer Technologien zu prüfen. Gerne werden entsprechende als IoT-Geräte bezeichnete Systeme genutzt. Leider stehen Safety und Security bei diesen Geräten oft nicht an erster Stelle. Der Drang nach Innovation sollte nicht das Einfallstor für Gefährdungen werden. Eine veraltete IoT-Überwachungskamera stellt nicht nur eine Gefährdung für die Vertraulichkeit dar, sondern kann auch datenschutzrelevante Aspekte nach sich ziehen, sollte diese z.B. aus dem Internet erreichbar sein. Sie kann zudem als Einfallstor für Angreifer dienen, um in ansonsten geschützte Netzwerkbereiche einzudringen.

11.3.2 Hard- vs. Software

Bei Industrie-4.0-Anlagen werden in immer größerem Ausmaß Hardwaresysteme durch Softwarelösungen ergänzt oder ersetzt. Dabei muss in der individuellen Entwicklung der Software auf einen Mindeststandard an Cyber-Sicherheit geachtet werden, damit - im schlechtesten Fall – die Anlagensicherheit dementsprechend der vor der Neuerung entspricht. Insbesondere die steigende Komplexität in der Software und mögliche Abhängigkeiten zu anderen Softwarebibliotheken stellen eine Herausforderung dar. Denn diese müssen regelmäßig gepflegt und bei Fehlern auch mit Updates versehen werden.

Diese steigende Komplexität macht die Beurteilung der Einflüsse auf die Anlagensicherheit nicht einfacher. Die Innovationen in der Automatisierungstechnik darf keinesfalls die etablierten Ansprüche an die Anlagensicherheit senken. Vielmehr sollte darauf geachtet werden, diese weiter zu verbessern und Gefahren für Mensch und Umwelt weiter zu reduzieren.

11.4 Neue Anlagen

Bei der Errichtung neuer Anlagen kann und wird von Anfang an in geeigneter Weise nicht nur auf Safety, sondern auch auf Security geachtet. Viele Anlagenhersteller und Integratoren sind sich dieser Herausforderungen bewusst und beginnen schon in der Planungsphase Security im Konzept und Design der zu berücksichtigen.

Durch die erhöhte Komplexität der Geräte mit zusätzlichen Funktionen und Kommunikationsverbindungen wird der Aufwand zur Ermittlung potentieller Bedrohungen gegenüber konventioneller Technik weiter erhöht. Es mangelt zudem an Erkenntnissen, wie sich die neue Technologie im Notfall wirklich verhält, gerade wenn der Zustand nicht getestet werden kann. Gerade im klassischen Safety Bereich werden vor „Markteinführung“ umfangreiche Tests gefordert und auch durchgeführt. Zusätzlich gibt es diverse Vorgehensweisen zur Geräteauswahl bzw. zum Nachweis von Betriebsbewährung (z.B. via VDI 2180). In der Anlage geht es jedoch um das Zusammenspiel aller Komponenten.

11.4.1 Cloud

Der zunehmende Einsatz von Cloudsystemen für vielfältige Zwecke bringt neue Anforderungen an Betreiber mit sich. Die Betriebssicherheit der Cloud wird zum integralen Bestandteil der Infrastruktur und muss im Notfall hinreichend verfügbar sein. Zudem kommen neue Angriffsvektoren hinzu, die Gefährdungen für die Anlagensicherheit darstellen. Es gilt hier geeignete Lösungen zu prüfen und angemessen umzusetzen.

Verschlüsselungstechnologien und redundante Systeme helfen bei der Sicherstellung der Vertraulichkeit und Verfügbarkeit der in der Cloud angesiedelten Daten und Dienste. Gesetzliche und vertragliche Anforderungen wie Nachweisbarkeitspflichten können für den Störfall relevant werden und sollten bekannt sein.

Für die Auswahl geeigneter Cloud-Anbieter kann der Cloud Computing Compliance Criteria Catalogue (C5)[29] des BSI genutzt werden. Darin werden Mindestanforderungen an sicheres Cloud Computing spezifiziert und bildet die Grundlage, um ein betreiberseitiges Risikomanagement durchführen zu können.

11.4.2 Personaleinsatz

Das bisherige Betriebspersonal wird zunehmend reduziert und durch automatisierte Lösungen ersetzt. So sind auch im Notfall oft automatische Systeme die erste Instanz zur Regulierung. Doch geraten diese Systeme an ihre Grenzen, so müssen fachlich geschulte Mitarbeiter übernehmen. Diese Spezialisierung und Reduzierung des Personals bringt in Bezug auf Verfügbarkeiten neue Gefährdungen mit. Konnte früher noch auf eine große Personenzahl mit vielseitigen Fähigkeiten zurückgegriffen werden, ist heute meist nur die gerade nötige Menge an Personal eingesetzt und verfügbar. Der Ausfall von Kernpersonal kann bei der Schadensverhinderung oder -minimierung hinderlich sein, da viele Eigenschaften der Anlage in den Köpfen der Mitarbeiter nicht vorhanden sind, weil durch die Automatisierung dies im Normalbetrieb nicht mehr erforderlich ist. Dies schlägt sich auch in Notfallprozeduren nieder, die ggf. nicht umfassend genau beschrieben sind.

11.4.3 Management und Änderungskonzept

Managementsysteme unterstützen die internen Prozesse und erhöhen die Reaktionsfähigkeit im Notfall. Es werden klare Vorgaben bereitgestellt und vermittelt. Getestete Abläufe können der entscheidende Faktor für das erfolgreiche Bewältigen einer Krise, ohne Reduzierung der Anlagen- und Cyber-Sicherheit, sein.

Es finden immer Änderungen in Anlagen statt. Durch die Industrie 4.0 hat dies aber noch an Geschwindigkeit zugenommen. Ein kontrollierter Rahmen ist für den sicheren Betrieb unabdingbar. Das heißt auch, dass Änderungen gut geplant und fachlich richtig umgesetzt werden müssen. Nur so behält sich die Übersicht und Wartbarkeit bei.

[29] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html

11.4.4 Business Continuity Management

Ein zunehmend an Bedeutung gewinnendes Thema ist das „Business Continuity Management“(BCM). Gerade für moderne Anlagen ein entscheidendes Werkzeug, um die Wettbewerbsfähigkeit zu wahren. BCM dient in erster Linie dem geplanten Vorgehen im Notfall. Die in Industrie-4.0-Anlagen bestehenden Gefährdungen können durch ein geeignetes BCM-Konzept so betrachtet werden, dass ein Cyber-Sicherheitsvorfall nur wenige oder keinerlei Auswirkungen auf die kritischen Prozesse hat. Mit den Veränderungen an Technik und Prozesse durch die Innovationen, bietet sich die Möglichkeit auch die Reaktionsfähigkeit auf Not- und Krisenfälle zu integrieren und zu stärken.

12 Fazit

Im Auftrag des BSI wurde in dieser Studie untersucht, welcher Umsetzungstand in Bezug auf OT-Security bei den beteiligten Parteien (Betreibern, Integratoren, Herstellern, Behörden und Sachverständigen) besteht. Durch den zunehmenden Einsatz von mit der IT-Welt vernetzten OT-Komponenten entstehen neue Angriffsvektoren. Zugleich erhöht sich die Diversität der Schwachstellen, da die vielfältigen OT-Komponenten nun auch aus dem Cyber-Raum angegriffen werden können. Aus diesem Grund wurden u.a. in der KAS-51 Anforderungen zum Schutz der Anlagenintegrität und der Verfügbarkeit von Sicherheitseinrichtungen gegen Cyber-Angriffe definiert. Die KAS-51 bildet die Grundlage der Minimalanforderungen an Cyber-Sicherheit in Störfallbetrieben. Es wurde evaluiert, ob diese Basis, unter Berücksichtigung weiterer Regelwerke, hilfreich für die beteiligten Parteien ist. In Interviews mit einzelnen Vertretern der Parteien wurde deutlich, dass das Thema OT-Security bei allen Verantwortlichen auf der Agenda steht. Es existieren bereits bei größeren Institutionen und Unternehmen Organisationsstrukturen sowie erste OT-Security-Prozesse. Kleinere Institutionen und Betriebe agieren noch weniger organisiert.

Ferner gibt die Studie einen Überblick zu aktuellen Technologietrends und deren mögliche Auswirkungen auf die OT-Security. Es ist ein Managementrahmen aufzubauen, um den OT-Security-Prozess zu steuern. Die Studie gibt praktische Anregungen, um die Zusammenarbeit zwischen IT und OT zu moderieren. Durch eine Risikoanalyse ist zu evaluieren, welche zusätzlichen OT-Security Maßnahmen vorzusehen sind. Die Studie enthält eine Risikoanalyse, die anhand des Beispiels einer Gasspeicheranlage durchgeführt worden ist. Des Weiteren wird die Kombination der Risikoanalyse gemäß IEC 62443 und der Auswahl geeigneter Maßnahmen des BSI IT-Grundschutzes veranschaulicht. So sollte beispielsweise vor der Integration neuer Technologien in einem Cyber-Sicherheitskonzept eruiert werden, wie diese in die bestehende Netzwerkarchitektur integriert werden können.

Anforderungen und Maßnahmen zur IT- und OT-Security gibt es bereits in vielen Regelwerken und Standards. Die Studie enthält einen Abgleich der Inhalte und Anforderungen zu einschlägigen Regelwerken und stellt die Gemeinsamkeiten und Unterschiede der KAS-51, ISO 27001 und des BSI IT-Grundschutzes dar. Dies soll Ihnen den Nachweis zur Umsetzung verschiedener Regelwerke erleichtern.

Positive Erfahrungen interviewter Institutionen und Unternehmen sind in der Studie als Praxisbeispiele aufgeführt und sollen als Inspiration dienen. Dazu gehören z.B. Positiverfahrungen zum Plant-Asset-Management, zu der Organisation von Rollen und Berechtigungen sowie zum Aufbau und zur Verteilung von Wissen. Auf der anderen Seite wurde innerhalb der Studie deutlich, dass in einigen Bereichen noch Handlungs- und Entwicklungsbedarf besteht. So wurde aufgezeigt, dass beispielsweise oft das fachliche Know-how und die Ressourcen fehlen. Ferner wünschen sich die Interviewten u.a. eine engere Zusammenarbeit zwischen IT und OT, eindeutige Bezüge zwischen den anzuwendenden Regelwerken, Blueprints für Best-Practice-Konzepte und Security-Handbücher zu den OT-Komponenten.

Die Studie wird dem Ziel einer Bestandsaufnahme der OT-Security in Organisationen gerecht. Durch die Mitarbeit zahlreicher Beteiligter der unterschiedlichen Parteien konnten verschiedene Perspektiven eingebracht und evaluiert werden. Es zeigt sich, dass durch das bestehende Regelwerk eine Basis vorhanden ist, um in Störfallbetrieben das Thema OT-Security zu adressieren. Gleichermaßen fehlt es noch an Routine, da die Übertragung von IT-Security-Gedanken auf die OT-Welt noch sehr jung ist. Aus diesem Grund wünschen sich die Beteiligten mehr in der Praxis anwendbare Anleitungen sowie verbindliche Maßstäbe zur Bewertung der getroffenen Maßnahmen. Einige sind in die Studie bereits in Form von Inspirationen und Praxisbeispielen eingeflossen. So enthält sie u.a. einen Blueprint zur Risikoanalyse, Ideen zur Zusammenarbeit zwischen IT und OT sowie eine Übersicht und Bezüge zwischen den anzuwendenden Regelwerken.

Nutzen Sie die Erkenntnisse der Studie und profitieren Sie von den zahlreichen Anregungen sowie den Austausch mit anderen Beteiligten, um die Cyber-Sicherheit in ihrer Organisation zu erhöhen.

Viel Erfolg bei der Umsetzung.

13 Begriffsbestimmungen

Tabelle 29 Begriffstabelle

Begriff	*Inhaltsbestimmung / Definition*
Advanced Persistent Threat (ATP)	Ambitionierter, in der Regel technisch aufwändiger Angriff auf IT-Systeme, oft als langfristige Operation angelegt.
air-gapped	Als Air Gap (englisch für „Luftspalt“) wird in der Informatik ein Prozess bezeichnet, der zwei IT-Systeme voneinander physisch und logisch trennt, aber dennoch die Übertragung von Nutzdaten durch einen transportablen physischen Datenträger zulässt. [Quelle: wikipedia.org]
„as-built“ englisch für „wie-gebaut“	Korrekte und vollständige Beschreibung des tatsächlich ausgeführten Zustands in einer Dokumentation oder einem Datenmodell. Die as-built Dokumentation basiert in der Regel auf der Spezifikation und wird als Bestandteil der Revisionsdokumentation vereinbart. Die Fortschreibung erfolgt bis zur Übergabe im Rahmen der Inbetriebnahme an den Betreiber durch den Integrator.
Asset	Ein Asset ist ein Element, ein Gegenstand oder eine Einheit, das (der) (die) einen möglichen oder tatsächlichen Wert für eine Organisation besitzt. Dieser Wert variiert zwischen verschiedenen Organisationen und ihren Stakeholdern und kann materieller oder immaterieller Art, finanzieller oder nichtfinanzieller Art sein. [Quelle: ISO 55000]
Asset-Management	Asset-Management ermöglicht einer Organisation, den Bedarf und die Performance von Assets und Asset-Systemen auf unterschiedlichen Ebenen zu untersuchen. Das ermöglicht außerdem die Anwendung analytischer Ansätze hinsichtlich des Managements eines Assets über verschiedene Phasen seines Lebenszyklus. [Quelle: ISO 55000]
Awareness	Bewusstsein; in diesem Kontext Sensibilität.
Bluetooth	Funktechnologie zur Datenübertragung über kurze Entfernungen, i.d.R. wenige Meter.
Commercial off-the-shelf (COTS)	Als commercial off-the-shelf oder auch components off-the-shelf (englisch für Kommerzielle Produkte aus dem Regal), kurz COTS, werden seriengefertigte Produkte aus dem Elektronik- oder Softwaresektor (vgl. Standardsoftware) bezeichnet, die in großer Stückzahl völlig gleichartig (ugs. „von der Stange“) aufgebaut und verkauft werden. Dies kann beispielsweise bei Office-Produkten oder Warenwirtschaftssystemen praktiziert werden.

Begriff	*Inhaltsbestimmung / Definition*
Cyber-Sicherheit (engl.: Cyber-Security)	Cyber-Sicherheit befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik. Das Aktionsfeld der klassischen IT-Security wird dabei auf den gesamten Cyber-Raum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein. [Quelle: bsi.bund.de]
Defense in Depth	„Defense in Depth“ bedeutet einen koordinierten Einsatz mehrerer Sicherheitsmaßnahmen, um die Datenbestände in einem Unternehmen zu schützen. Die Strategie basiert auf dem militärischen Prinzip, dass es für einen Feind schwieriger ist, ein komplexes und vielschichtiges Abwehrsystem zu überwinden als eine einzige Barriere.
Engineering Workstation	Die Engineering Workstation ist ein einzelner Arbeitsplatz für alle Engineering-Aufgaben wie z.B. Konfiguration der graphischen Darstellung, Entwurf von Steuerungsanwendungen, Konfiguration des Steuersystems sowie der Feldgeräte und Instrumentierung.
Exploit	Systembedingte Möglichkeit der Ausnutzung von Schwachstellen in der IT.
Funktionale Sicherheit	Die „Funktionale Sicherheit“ betrachtet Gefährdungen für Bedienpersonal und andere Menschen, die Umwelt oder die Anlage selbst, die durch Zufall und Unfall entstehen. Aus Fehlfunktionen von Automatisierungssystemen können Gefährdungen auch für nicht-digitale Objekte resultieren. Dem wird mit „sicherheitsgerichteten Steuerungen“ begegnet, deren Wirkung hinsichtlich der Einwirkung von Cyber-Angriffen sicherzustellen ist. [Quelle: NA 169]
Gateway	Ein Gateway ist ein Hardware-Gerät, das als "Tor" zwischen zwei Netzwerken fungiert. Ein Gateway kann z.B. ein Router, eine Firewall, ein Server oder ein anderes Gerät sein, das den Datenverkehr in das Netzwerk hinein und aus dem Netzwerk heraus ermöglicht.
Gap-Analyse	Gap-Analyse bedeutet die Darstellung von Abweichungen zwischen - auf unterschiedlichen Annahmen basierenden - zukünftigen Entwicklungsverläufen des Geschäfts. [Quelle: wirtschaftslexikon.gabler.de]

Begriff	*Inhaltsbestimmung / Definition*
HACKED	Das engl. Wort „to hack“ bedeutet: In etwas eindringen. In der Informatik gilt ein Hacker bzw. eine Hackerin als Person, die Freude an Erstellung bzw. Veränderung von Software oder Hardware hat. Der Begriff wird im Zusammenhang mit Kriminalfällen für Personen verwendet, die solche Lücken in fremden Systemen unerlaubt für eigene, oft kriminelle Zwecke wie den Diebstahl von Informationen nutzen. "Echtes" hacking bedeutet: Einbruch in Computer bzw. Computernetze. [Quelle: wirtschaftslexikon.gabler.de]
I/O-Module	In der Prozessindustrie werden noch viele Sensordaten und Steuerungssignale (z.B. Auf-/Zu-Befehl für Armaturen) über Punkt zu Punkt verbundene Kupferleitungen übertragen. Die Leitungen aus den Feldgeräten (Sensoren/Aktoren) werden über Ein- und Ausgangskarten (I/O-Module) mit den Industriesteuerungen verbunden.
Informationstechnologie (IT)	Informationstechnologie (IT) umfasst im eigentlichen Sinne alle technischen Ressourcen, die der Generierung, Speicherung, Archivierung, Verwendung und Verarbeitung digitaler Informationen dienen. Im weiteren Sinne gehört auch die Übertragung der Informationen mittels Kommunikationstechnologie dazu. [Quelle: wirtschaftslexikon.gabler.de]
inhärent sicher	Inhärent sichere Konstruktion ist der erste und wichtigste Schritt im Prozess der Risikominderung. Dabei handelt es sich um konstruktive Maßnahmen zum Schutz vor potentiellen Gefährdungssituationen, die nicht oder nur mit hohem Aufwand manipuliert oder umgangen werden können. Ebenso ist ein Nichtbeachten oder Vergessen nicht möglich.[vgl.: ISO 12100]
Konfigurationsmanagement	Verfahren zur Identifikation der Komponenten eines sich in der Entwicklung befindenden (Hardware- und Software-) Systems zum Zwecke der Kontrolle von Veränderungen an diesen Komponenten und zur Aufrechterhaltung von Kontinuität und Zurückverfolgbarkeit während des Lebenszyklus. [Quelle: IEC 61511-1]
Local Area Network (LAN)	Local Area Network ist ein Rechnernetzwerk mit oft nur wenigen angeschlossenen Computern. Meist sind LANs auf einzelne Büros oder Gebäude beschränkt. [Quelle: Whatls.com/de]
Malware	Schadsoftware bzw. Software, die Schäden in Anwendungen oder Systemen begünstigt, ermöglicht oder bewirkt.

Begriff	*Inhaltsbestimmung / Definition*
Messwarte	Ein Leitstand (auch Leitwarte, Schaltwarte oder Messwarte genannt) ist eine technische Einrichtung (Leiteinrichtung), die den Menschen bei der Leitung eines Prozesses unterstützt. Er ist Teil eines Leitsystems. In diesem Zusammenhang ist Leiten „die Gesamtheit aller Maßnahmen, die einen im Sinne festgelegter Ziele erwünschten Ablauf eines Prozesses bewirken“. [Quelle: DIN V 19222]
Mitbenutzung	Mitbenutzung im Sinne der Funktionalen Sicherheit bedeutet, dass einzelne Geräte sowohl für betriebliche als auch für Sicherheitsfunktionen genutzt werden. Dies Bedarf in der Regel einer gesonderten Betrachtung, da dadurch zusätzliche Risiken oder die Verletzung einer Schutzebene auftreten kann.
Nebenbestimmungen	Die Nebenbestimmung stellt ein Handlungsinstrument des deutschen Verwaltungsrechts dar. Es handelt sich um einen Zusatz zu einem Verwaltungsakt, der dessen Regelungsinhalt erweitert oder beschränkt. Regelmäßig kommen Nebenbestimmungen etwa bei einer Baugenehmigung zum Einsatz. [Quelle: wikipedia]
Operational Technology (OT)	Als „Operational Technology“ (OT) wird „Hard- und Software, die eine Änderung von Prozessen und Ereignissen im Unternehmen durch die direkte Überwachung und / oder Steuerung der physischen Geräte erkennt oder bewirkt“ bezeichnet [Gartner 2016]. Damit ist die Automatisierungstechnik oder Automation Technology (AT) Teil der OT. Sie umfasst Systeme wie z.B.: PLS, SIS, SPS, SCADA, AMS und Feldgeräte. [Quelle: NA 169]
PLT-Sicherheitseinrichtung	PLT-Sicherheitseinrichtungen (früher PLT-Schutzeinrichtungen) sind Einrichtungen der Prozessleittechnik (PLT) respektive der Mess-, Steuer und Regeltechnik (MSR), die das Erreichen eines unzulässigen Fehlbereiches durch einen selbsttätigen Eingriff in den Prozess verhindern oder, im Fall des Eintritts eines unerwünschten Ereignisses, die möglichen Auswirkungen dieses Ereignisses begrenzen. [Quelle: VdTÜV-Merkblatt Druckbehälter 372]. PLT-Sicherheitseinrichtungen sind Bestandteil der Funktionalen Sicherheit.
Programmiersprache mit eingeschränktem Funktionsumfang (LVL)	LVL (limited variability language) ist eine Programmiersprache für kommerzielle und industrielle elektronische Steuerungen mit einer Reihe von begrenzten Fähigkeiten, die im zugehörigen Sicherheitshandbuch beschrieben sind. Die Schreibweise dieser Sprache kann textorientiert oder graphisch sein oder Elemente aus beiden Varianten beinhalten.

Begriff	*Inhaltsbestimmung / Definition*
Proprietäre Software	Proprietäre Software bezeichnet eine Software, die das Recht und die Möglichkeiten der Wieder- und Weiterverwendung sowie Änderung und Anpassung durch Nutzende und Dritte stark einschränkt. [Quelle: https://de.wikipedia.org/]
Prozessleitsystem (PLS)	PLS werden meist für größere verfahrenstechnische Anlagen eingesetzt und bestehen üblicherweise aus einem Paket, das folgende Mechanismen beinhaltet: Prozessnahe Komponenten zur Steuerung von Aktoren und Aufnahme der Messwerte, Alarmsystem, Anlagenvisualisierung, Kurvenaufzeichnung von analogen Messwerten, Verwaltung der Nutzenden, Möglichkeiten des Engineerings sowie eine zentrale Datenhaltung. [Quelle: ICS-Security-Kompendium]
Prozessrisiko	Risiko, das sich aus Prozesszuständen ergibt, die durch außergewöhnliche Ereignisse verursacht werden (einschließlich Fehlfunktionen des PLS). [Quelle: IEC 61511-1]
Ransomware	Ransomware bezeichnet Arten von Schadprogrammen, die den Zugriff auf die Daten oder das System einschränken beziehungsweise komplett unterbinden. Entweder sperrt die Software den kompletten Zugriff auf das System oder sie verschlüsselt bestimmte Daten. Für die Freigabe wird dann ein Lösegeld (englisch: ransom) verlangt. [Quelle: bsi.bund.de]
Recovery	Recovery bedeutet bei Datenbanksystemen die Wiederherstellung eines definierten konsistenten Zustands der Datenbasis (Datenbank) nach einem Hardware- oder Software-Fehler. [Quelle: wirtschaftslexikon.gabler.de]
Response Team	Ein Computer Emergency Response Team (CERT), ist eine Gruppe von EDV-Sicherheitsfachleuten, die bei der Lösung von konkreten IT-Sicherheitsvorfällen als Koordinator mitwirkt bzw. sich ganz allgemein mit Computersicherheit befasst. [Quelle: wikipedia.org]
Risiko	Kombination der Wahrscheinlichkeit des Auftretens eines Schadens und des Schweregrades dieses Schadens. [Quelle: IEC 61511-1]
Schadensbegrenzungs-maß-nahme (engl.: mitigation)	Maßnahme zur Verringerung der Auswirkung(en) eines gefahrbringenden Ereignisses. [Quelle: IEC 61511-1]
Scriptkiddie	Der Begriff beschreibt vornehmlich Computernutzende, die trotz mangelnder Grundlagenkenntnisse versuchen, in fremde Computersysteme einzudringen oder sonstigen Schaden anzurichten. [Quelle: wikipedia.org]

Begriff	*Inhaltsbestimmung / Definition*
Security	Die deutsche Entsprechung des englischen Begriffes „Security“ ist „Angriffssicherheit“. Aufgabe der Security ist es, materielle wie immaterielle Dinge, die für den Eigentümer/Besitzer einen Wert darstellen, vor Bedrohungen zu schützen. Neben den klassischen Schutzzielen der IT-Security (Verfügbarkeit, Integrität und Vertraulichkeit) ist bei der Automation Security immer auch der Aspekt der Betriebssicherheit oder „Safety“ mit zu betrachten, da Teile der Automatisierungseinrichtungen u.a. auch Funktionen des Personenschutzes, der Anlagensicherheit, des Umweltschutzes oder des Schutzes wertvoller Güter übernehmen. [Quelle: NA 169]
Security-Management	Die Etablierung eines umfassenden IT-Sicherheitsmanagements ist eine anspruchsvolle Aufgabe, weil Planungsfehler und unpraktikable Regelungen nur schwer wieder zu korrigieren sind und Sicherheitsprobleme unter Umständen nicht wirkungsvoll verhindert werden. Es gibt inzwischen eine Reihe von Standards und Regelwerken, zum Beispiel BS 7799-2, ISO 17799, ISO/IEC TR 13335 und die IT-Grundschutz-Kataloge des BSI, die Anleitungen für ein effektives IT-Sicherheitsmanagement bieten. [Quelle: bsi.bund.de]
Security by obscurity (dt: Sicherheit durch Unklarheit)	Security by obscurity ist ein Prinzip in der Computer- und Netzwerksicherheit. Es versucht, die Sicherheit eines Systems oder eines Verfahrens zu gewährleisten, indem seine Funktionsweise geheimgehalten wird. Das Gegenkonzept dazu ist Sicherheit durch weitestgehende Transparenz, als „Kerckhoffs’ Prinzip“ oder „Full disclosure“ bezeichnet. Ausgehend von der Kryptologie wird hierbei vorgeschlagen, so wenig wie möglich geheim zu halten, um dieses dann umso leichter schützen und gegebenenfalls ersetzen zu können. [Quelle: Wikipedia]
Sensor	Gerät oder Gerätekombination, die eine Zustandsgröße des Prozesses erfasst (z. B. Messumformer, Übertrager, Grenzwertschalter, Endschalter). [Quelle: IEC 61511-1]
Sicherheit	Freiheit von unvertretbaren Risiken. [Quelle: IEC 61511-1]
Sicherheitsfunktion	Funktion, die von einem SIS, einem sicherheitsbezogenen System anderer Technologie oder von externen Einrichtungen zur Risikominderung ausgeführt wird mit dem Ziel, unter Berücksichtigung eines festgelegten gefährlichen Vorfalls einen sicheren Zustand für den Prozess zu erreichen oder aufrecht zu erhalten. [Quelle: IEC 61511-1]
Sicherheitsgerichtete speicherprogrammierte Steuerung (S-SPS, SSPS)	Logiksystem zur Ausführung von Programmen, die sicherheitstechnische Funktionen beinhalten. Die SSPS ist die zentrale Komponente eines sicherheitstechnischen Systems (z. B. des PLT-S) und hat dadurch einen sehr hohen Schutzbedarf.

Begriff	*Inhaltsbestimmung / Definition*
Sicherheits-Instrumentierten Systems (SIS)	Sicherheits-Instrumentierten Systems zur Ausführung einer oder mehrerer sicherheitstechnischer Funktionen. Ein SIS besteht aus Sensor(en), Logiksystem und Aktor(en). [Quelle: IEC 61511-1]
Stakeholder	Anspruchsberechtigte Person oder Gruppe, die ein berechtigtes Interesse am Verlauf oder Ergebnis eines Prozesses oder Projekts hat. [Quelle: Wikipedia]
Supervisory Control and Data Acquisition (SCADA)	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). [Quelle: ICS-Security-Kompendium]

14 Abkürzungsverzeichnis

Tabelle 30 Abkürzungstabelle

Abkürzung	*Bedeutung*
4G	Mobilfunknetz der vierten Generation, enthält die Technologien GSM, UMTS, LTE
5G	Mobilfunknetz der fünften Generation – Weiterentwicklung des 4G-Netzes
ADS	Anomaly Detection System
AMS	Asset Managementsystem (SIS und auch Konfigurationsstationen und Handhelds bzw. mobile Konfigurationsgeräte)
ATP	Advanced Persistent Threat (fortgeschrittene andauernde Bedrohung durch Cyber-Attacken, meist ambitionierter Angriff mit langer Operationsdauer)
BASF	Badische Anilin- und Soda-Fabrik
BitKom	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BSI	Bundesamt für Sicherheit in der Informationstechnik
BImSchG	Bundes-Immissionsschutzgesetz
BMAS	Bundesministerium für Arbeit und Soziales
CERT	Computer Emergency Response Team (Computersicherheits-Notfall-Reaktionsteam)
CISA	Cyber-Security & Infrastructure Security Agency (Behörde für Cyber-Security und Infrastruktur-Security in den USA)
CISM	Certified Information Security Manager
CISO	Chief Information Security Officer (Verantwortlicher im Unternehmen für Informations- und Datensicherheit)
COO	Chief Operation Officer
CSMS	Cyber Security Management Systems (Bezeichnung aus der IEC 62443, um Aufgaben und Verantwortlichkeiten der OT durch eine eigene Begrifflichkeit von denen des Informationssicherheitsmanagementsystems – kurz ISMS - zu trennen)
CT	Magazin für Chemie Technik (Fachzeitschrift)
DHS	Department of Homeland Security (Ministerium für Heimatschutz in den USA)
DIN	Deutsches Institut für Normung
DMZ	Demilitarisierte Zone
EMSR	Elektrische Mess-, Steuer- und Regelungstechnik (Automatisierungstechnik)
ERP	Enterprise Resource Planning (Methode zur Unternehmenssteuerung)
FDI	Field Device Integration (Feldgeräteintegration)
GB	Gigabyte
HAZOP	HAZard and OPerability – englisches Akronym zu PAAG

Abkürzung	*Bedeutung*
HMI	Human-Machine Interface (Mensch-Maschine Schnittstelle)
I(A)CS	Industrial (Automation and) Control Systems (Industrielle Automatisierungs- und Steuerungssysteme)
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IoT	Internet of Things
ISA	International Society of Automation
ISMS	Informationssicherheitsmanagementsystem
ISO	International Standards Organization (Internationale Organisation für Normung)
IT	Informationstechnologie
ITAM	IT Asset Management
ITIL	IT Infrastructure Library
ITSiBE	IT-Sicherheits-Beauftragte
ITSiG	IT-Sicherheitsgesetz
KAS	Kommission für Anlagensicherheit (beim Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit)
KritisV	Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz
LAN	Local Area Network
M2M	Machine-to-Machine (Communication)
MES	Manufacturing Execution System
ML	Maturity Level (Reifegrad von Organisationen gem. IEC 62443)
NA	NAMUR Arbeitsblatt
NFC	Near Field Communication – Drahtlose Kommunikation über sehr kurze Entfernungen, i.d.R. wenige Zentimeter
NIST	National Institute of Standards and Technology
NOA	NAMUR Open Architecture
NVD	National Vulnerability Database
O-PAS	Open Process Automation Standard
OPC UA	Open Platform Communications Unified Architecture
OT	Operational Technology (Produktionsnahe Automatisierungs- und Steuerungstechnik)
PAAG	Prognose von Störungen, Auffinden von Ursachen, Abschätzen der Auswirkungen, Gegenmaßnahmen
PAM	Plant-Asset-Management
PFD	Probability of Failure (Ausfallwahrscheinlichkeit im Anforderungsfall)

Abkürzung	*Bedeutung*
PIMS	Plant Information Management System (sammelt und integriert Informationen über den Produktionsprozess)
PLT	Prozessleittechnik (Industrie-Automation)
Prio	Priorität
ProdSG	Produktsicherheitsgesetz
R&I	Rohrleitungs- und Instrumentenfließschema
RTU	Remote Terminal Unit (Fernbedienungsterminal)
SCADA	Supervisory Control and Data Acquisition (Fernwirk- und Überwachungsanlage)
SIS	Safety Instrumented System (Sicherheitstechnisches System)
SOC	Security Operations Center
SPS	Speicherprogrammierbare Steuerung
SSPS	Sicherheitsgerichtete Speicherprogrammierbare Steuerung, auch mit S-SPS abgekürzt.
TAA	Technischer Ausschuss für Anlagensicherheit
VdTÜV	Verband der Technischen Überwachungs-Vereine
W-LAN	Wireless Local Area Network – Drahtloses lokales Netzwerk
WID	Warn- und Informationsdienst

Literaturverzeichnis

1. **Kriminologisches Forschungsinstitut Niedersachsen e.V.** *Cyberangriffe gegen Unternehmen in Deutschland.* 2020. Forschungsbericht Nr. 152.

2. **Bundesamt für Sicherheit in der Informationstechnik.** *Recognizing Anomalies in Protocols of Safety Networks: Schneider Electric's TriStation (RAPSN SETS).* [Web] Bonn : s.n., 2012. https://www.bsi.bund.de/DE/Themen/ICS/Tools/RAPSN_SETS/RAPSN_SETS_node.html.

3. **Bundesamt für Sicherheit in der Informationstechnik .** Die Lage der IT-Sicherheit in Deutschland. *https://www.bsi.bund.de.* [Online] 2019. https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html.

4. **Bitkom.** Angriffsziel deutsche Wirtschaft: mehr als 100 Milliarden Euro Schaden pro Jahr. [Online] 16. 11 2019. https://www.bitkom-research.de/de/pressemitteilung/angriffsziel-deutsche-wirtschaft-mehr-als-100-milliarden-euro-schaden-pro-jahr.

5. **Strohm, Oliver und Eberhard, Ulich.** *Unternehmen arbeitspychologisch bewerten.* Zürich : vdf Hochschulverlag AG an der ETH Zürich, 1997.

6. **VCI.** Auf einem Blick, Chemische Industrie 2019. [Online] https://www.vci.de/vci/downloads-vci/publikation/chemische-industrie-auf-einen-blick.pdf.

7. **statista.** IT Budgets als Anteil am Umsatz nach Branchen im Jahr 2015. [Online] https://de.statista.com/statistik/daten/studie/75779/umfrage/it-budgets-als-anteil-am-umsatz-nach-branchen/.

8. **Polke, Heidi und Aschoff, Daniel.** Allianz Risk Barometer 2020. [Online] Allianz, 15. Januar 2020. https://www.allianz.com/de/presse/news/studien/200115_Allianz-Risk-Barometer-2020.html.

9. **IT-daily.net.** Ransomware: Fünf Tipps, wie Firmen die Schäden erfolgreicher Angriffe stärker eingrenzen können. [Online] 3. Juli 2020. https://www.it-daily.net/it-sicherheit/cyber-defence/24611-ransomware-fuenf-tipps-wie-firmen-die-schaeden-erfolgreicher-angriffe-staerker-eingrenzen-koennen.

10. **Gartner.** *Gartner Security Rist Mangement Summit 2018.* London : s.n., 10.09.2018.

11. **Netzwelt, Der Spiegel.** *Hackerangriff auf Industrieanlagen.* [Onlineartikel] https://www.spiegel.de/netzwelt/web/saudi-arabien-cyberangriff-auf-kraftwerk-auch-in-deutschland-wiederholbar-a-1201410.html : s.n., 2018.

12. **Forescout.** Fail to plan, plan to fail. [Online] November 2017. https://www.forescout.com/iot_forrester_study/.

13. **McCall, Thomas.** Gartner Identifies How Security Leaders Can Be Empowered to Drive Results. [Online] Gartner, 4. Juni 2018. https://www.gartner.com/en/newsroom/press-releases/2018-06-04-gartner-identifies-how-security-leaders-can-be-empowered-to-drive-results.

14. **Berufsgenossenschaft Rohstoffe und Chemische Industrie.** *Muster-Freigabeschein für sicherheitsrelevante Arbeiten.* [Webseite] 2008.

15. **Bundesanstalt für Arbeitsschutz und Arbeitsmedizin.** TRBS 1112 „Instandhaltung". 2019. Bde. Art.-Nr. 56396913, G 3191 A, – Bek. d. BMAS v. 14.3.2019 – IIIb5 – 35650 –.

16. **Berufsgenossenschaft Rohstoffe und Chemische Industrie.** *Maßnahmen der Prozesssicherheit in verfahrenstechnischen Anlagen.* 2015.

17. **DECHEMA.** Whitepaper Digitalisierung in der Chemieindustrie. [Online] 2016. https://dechema.de/dechema_media/Downloads/Positionspapiere/whitepaper_digitalisierung_final-p-20003450.pdf.

18. **Fluchs, Sarah.** Security für die SPS-Programmierung. [Online] 29. Juli 2019. https://medium.com/@fluchsfriction/security-f%C3%BCr-die-sps-programmierung-6b7af27343e8.

19. **NAMUR.** *NAMUR Hauptsitzung 2019 - NAMUR Open Architecture.* Bad Neuenahr : s.n., 2019.

20. **ISO.** ISO/IEC 27001:2013 Information technology - Seurity techniques - Information security management systems - Requirements. [Online] 2019. https://www.iso.org/standard/54534.html.

21. **ZVEI.** Modulbasierte Produktion in der Prozessindustrie – Auswirkungen auf die Automation im Umfeld von Industrie 4.0. [Online] 18. März 2015. https://www.zvei.org/presse-medien/publikationen/white-paper-modulbasierte-produktion-in-der-prozessindustrie/.

22. **Bundesamt für Sicherheit in der Informationstechnik.** IT-Grundschutz-Kompendium. [Online] 20. Juli 2020. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html.

23. —. Grundregeln zur Absicherung von Fernwartungszugängen. [Online] 11. Juli 2018. https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_054.html.

24. —. ICS-Security-Kompendium. [Online] 25. November 2013. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.html.

25. **Schüller, Andreas et al.** Der Digitale Zwilling in der Prozessindustrie . [Online] http://ojs.di-verlag.de/index.php/atp_edition/article/view/2396.

26. **McKinsey.** Die Besten, bitte: Wie der öffentliche Sektor als Arbeitgeber punkten kann. [Online] April 2019. https://www.mckinsey.com/de/~/media/mckinsey/locations/europe%20and%20middle%20east/deutschland/news/presse/2019/2019-04-03%20die%20besten%20bitte/20190402_die%20besten%20bitte_studie%20fachkrftemangel%20ffentlicher%20sektor.ashx.

27. **Daniel Miesslers „Der Unterschied zwischen Roten, Blauen und Lila Teams“.** The Difference Between Red, Blue, and Purple Teams. [Online] 04. 04 2020. [Zitat vom: 24. 03 2021.] https://danielmiessler.com/study/red-blue-purple-teams/.

28. **Miessler, Daniel.** The Difference Between Red, Blue, and Purple Teams. [Online] 4. April 2020. https://danielmiessler.com/study/red-blue-purple-teams/.

29. **Helisch, Michael und Pokoyski, Dietmar.** *Security Awareness: Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung.* 2009.

Abbildungsverzeichnis

Tabellenverzeichnis