# Sicherheit in industriellen Informations- und Steuerungssystemen

Entwicklung eines integrierten Vorgehensmodell für Safety und Security in IACS

## Masterarbeit

eingereicht von: Gernot Kucera

Matrikelnummer: 06026191

im Fachhochschul-Masterstudiengang Wirtschaftsinformatik der Ferdinand Porsche FernFH GmbH

zur Erlangung des akademischen Grades

**Master of Arts in Business**

Betreuung und Beurteilung: Univ.-Prof. Prof. (FH) Dipl.-Ing. Mag. Dr. Dr. Gerald Quirchmayr

Zweitgutachten: Mag. rer. soc. oec. Norbert Leitner

Wien, Mai 2021

## Ehrenwörtliche Erklärung

Ich versichere hiermit,

1. dass ich die vorliegende Masterarbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Alle Inhalte, die direkt oder indirekt aus fremden Quellen entnommen sind, sind durch entsprechende Quellenangaben gekennzeichnet.
2. dass ich diese Masterarbeit bisher weder im Inland noch im Ausland in irgendeiner Form als Prüfungsarbeit zur Beurteilung vorgelegt oder veröffentlicht habe.
3. dass die vorliegende Fassung der Arbeit mit der eingereichten elektronischen Version in allen Teilen übereinstimmt.

Wien, Datum _____

Gernot Kucera

# Kurzzusammenfassung

**Sicherheit in industriellen Informations- und Steuerungssystemen**

Informationssysteme durchdringen den Alltag und ohne deren Nutzung ist der technische Fortschritt nicht mehr vorstellbar. Dabei treten die Aspekte der Sicherheit solcher Systeme in den Vordergrund des Interesses.

In der vorliegenden Arbeit wird ein integriertes Vorgehensmodell vorgeschlagen, das die IT-Sicherheit (Security) solcher Systeme verbessert und gleichzeitig Aspekte der Arbeitssicherheit (Safety) für die in der Automatisierung verwendeten Systeme berücksichtigt.

Weil auch das Erlangen und Erhöhen von Sicherheit als ein sich ständig wiederholender Prozess betrachtet werden muss, ist das vorgeschlagene Modell zyklisch und wird dadurch an neue Anforderungen anpassbar.

**Schlüsselbegriffe**

Sicherheit in industriellen Informationssystemen, Sicherheit in industriellen Steuerungssystemen, Integriertes Vorgehensmodell, Safety und Security in IACS

# Abstract

**Security in industrial information and control systems**

Information systems are an integral part of everyday life and without their use, technical progress is inconceivable. The aspects of the security of thus becomes a focus of interest.

In this thesis, an integrated process model is proposed that improves the security of such systems while considering safety and security aspects for the systems used in automation.

As the achievement and increase of security must also be viewed as a continuous improvement process, the proposed model is cyclical and can therefore be adapted to new requirements.

**Keywords**

security in industrial information systems, security in industrial automation and systems, integrated process model, safety and security in IACS

# Danksagung

Industrielle Steuerungen begleiten nahezu meinen gesamten beruflichen Werdegang. Besonderer Dank gilt meinen Betreuern, die meine Interessen für diese Arbeit geteilt und gefördert haben.

Herrn Prof. Quirchmayr danke ich, dass er meine Arbeit durch seine Anregungen und Diskussionsbeiträge aktiv begleitet hat. Insbesondere seine Hinweise zu weiteren Quellen haben meinen Blick geschärft und damit meine Arbeit verbessert. Auch seine kritischen Fragestellungen und Anregungen haben wesentlich zur Verbesserung und zur Verständlichkeit des Textes beigetragen. Herrn Mag. Leitner danke ich für die Gespräche, seine Unterstützung und Anmerkungen, die zur Verbesserung meiner Arbeit beigetragen haben.

Meiner Familie danke ich für die mir entgegengebrachte Geduld und das Verständnis für meine Arbeit, welche neben meiner beruflichen Auslastung nicht gezählte Wochenenden und Nachtstunden in Anspruch genommen hat.

Gernot Kucera

# Inhaltsverzeichnis

# Abbildungsverzeichnis



# Tabellenverzeichnis

# 1. Einleitung

Der Trend zur Automatisierung ist ungebrochen, weil dadurch die wirtschaftliche Wettbewerbsfähigkeit der Betriebe nicht nur gestärkt, sondern erst ermöglicht wird. Es gibt vielfältige Gründe für die zunehmende Automatisierung und zum Einsatz von industriellen Automatisierungs- und Steuerungssystemen (Industrial Automation and Control Systems, IACS).[1]

IACS und die kommerziell genutzte IT werden immer enger miteinander vernetzt. Durch die Vernetzung entstehen zusätzlichen Risiken, denen entgegengewirkt werden muss. Hier sind insbesondere die Konzepte der Industrie 4.0 anzuführen, die die Automatisierungstechnik mit der Fertigungstechnik und der Informatik zu einer flexibilisierten Produktion verschränken. Industrie 4.0 wird gekennzeichnet durch Cyber Physical Production Systems (CPPS), die vereinigt eine Smart Factory bilden.[2]

Die Flexibilisierung der Produktion bringt es mit sich, dass diese ständig auf neue Anforderungen umgestellt werden muss. Die Risiken entstehen, weil auf der einen Seite die maschinelle und gerätetechnische Ausrüstung der Produktion nicht in beliebig kurzen Zeitabständen an den technologischen Fortschritt angepasst werden kann und weil die Lebensdauer dieser Einrichtungen in der Regel sehr langlebig ist. Auf der anderen Seite steht ein Zwang zur Flexibilisierung, der durch den Zusammenschluss bereits älterer Maschinen und Anlagen mit neuen oder mit Umbauten bewerkstelligt wird. Das ergibt einen Mix aus bereits veralteter Technologie als Schwachstellen in einem modernisierten System.[3]

[1] Einerseits soll durch Automatisierung die Sicherheit am Arbeitsplatz gesteigert werden, andererseits spielt die Humanisierung von Arbeitsplätzen und der zugehörigen Arbeitsbedingungen eine große Rolle. Außerdem lässt sich durch Automatisierung in der Regel die Qualität von Produkten verbessern, da Unzulänglichkeiten des Menschen, wie mangelnde Aufmerksamkeit, Ermüdung etc. entfallen. Durch Rationalisierung können vielfach Kosten reduziert werden oder erst die Expansion eines Unternehmens möglich sein, weil etwa bei hohem Automatisierungsgrad eine Produktion sowohl kosten- wie auch ressourceneffizient aufrechterhalten werden kann (vgl. [KG17]).

[2] Im Wesentlichen sind CPPS flexible, hoch automatisierte Fertigungssysteme, die in der Lage sind, mit einem Minimum manueller Eingriffe Gruppen von Komponenten zu fertigen (vgl. [RA16], vgl. [LT et.al 20]). Die „Just in Time“ Problematik ist eine Steuerungsgröße einer flexiblen Fertigung. Der Gesamtüberblick über Zusammenhänge von Systemparametern (wie z.B. Einsatz, Auslastung und Nutzung) sind Quellen für die miteingebundenen Informationssysteme, die als Konzepte und deren Umsetzung Industrie 4.0 ausmacht (vgl. [KW20]).

[3] Ausgelöst und verstärkt wird dieser Umstand, wenn bei Produktionseinrichtungen die Steuerungskomponenten ausgewechselt werden müssen, weil auch Steuerungen Innovationszyklen unterliegen und spätestens eine gewisse Zeit nach Produktneueinführungen ältere Systeme mangels Ersatzteile nicht mehr in Betrieb gehalten werden können. Steuerungen werden ersetzt und gleichzeitig modernisiert, wodurch es zu vielschichtigen Problemen im Bereich der Sicherheitstechnik kommen kann. Der Begriff Retrofit (engl. für nachrüsten, umrüsten, Nachrüstung) meint dabei das Reagieren auf die rasante technologische Weiterentwicklung im Bereich der Computertechnologien und damit einhergehend auch in der Automatisierungstechnik. Damit wird die Modernisierung oder der Ausbau bestehender meist älterer oder nicht mehr ersetzbarer Anlagen und Betriebsmittel verstanden (vgl. TW17).

## 1.1. Hintergrund und Motivation

Die Gewährleistung von Sicherheit in IACS ist ein Prozess, der ständig neu durchlaufen werden muss. Auch wenn die Lebensdauer der industriellen Steuerungssysteme durch die technologische Weiterentwicklung deutlich gesteigert worden ist und damit größer ist, als in einer typischen IT-Infrastruktur, sind die Betriebssysteme und Steuerungssoftware im Wesentlichen auf einem bestimmten Stand „eingefroren". In Bezug auf die Informationssicherheit wird bei industriellen Steuerungssystemen die Software der dort genutzten Betriebssysteme und Steuerungssoftware praktisch nicht gewartet. Existieren in diesem Bereich Schwachstellen, sind solche Systeme potenziell angreifbar. Solange solche Systeme als „Insellösungen" arbeiten, kann die Gefährdung als gering eingeschätzt werden. SCADA-Systeme[4] sind traditionell physikalisch isoliert und nutzen eine für sie speziell entwickelte Technologie. Die Grenzen der industriellen Informations- und Kontrollsysteme zu den kommerziellen Systemen verschwimmen mit der zunehmenden Integration dieser Systeme, insbesondere dann, wenn die in den Steuerungssystemen erhobenen Daten ständig kommerziell weiterverarbeitet und in die Steuerung rückgespeist werden und dazu öffentliche Netze aufgrund unterschiedlicher Standorte der Fertigungen genutzt werden müssen.

Das Risiko eines Angriffs auf solche Systeme ist damit deutlich höher geworden. Während insbesondere bei der Sicherheit für kritische Infrastruktur und beim Datenschutz bereits gesetzliche Regelungen existieren und auch das Bewusstsein für Sicherungsmaßnahmen anwächst, ist das bei IACS noch nicht so deutlich ausgeprägt, wie es eigentlich sein müsste. In dieser Arbeit soll ein Ansatz entstehen, der sich mit der Integration von Safety und Security Überlegungen für den Bereich der Informationssicherheit in IACS beschäftigt.

Fragen rund um die Sicherheit von IACS, wie diese sichergestellt, hergestellt oder aufrechterhalten werden kann, beziehen sich nicht nur auf ein rein technisches Interesse, sondern sie haben auch Einfluss auf die Wirtschaft. Mögliche Auswirkungen der Verletzung der Sicherheit sind Ausfälle, die bis hin zu katastrophalen Schäden führen können. Solche Auswirkungen oder Schadensbilder werden aber nicht weiter untersucht, da der damit verbundene Aufwand den Rahmen dieser Arbeit sprengen würde.

## 1.2. Zielsetzung

Hauptziel dieser Arbeit ist die Entwicklung eines Ansatzes, wie Überlegungen zu Safety und Security in ein Konzept für das Design von Fertigungsanlagen integriert werden kann.

Dieses Konzept wird zu einem Vorgehensmodell erweitert. Im Rahmen von repräsentativen Szenarien wird das Modell überprüft und seine Tauglichkeit anhand von Testfällen untersucht und verifiziert. Die Testfälle resultieren aus der Analyse von Schwachstellen bei typischen IACS durch die Festlegung realitätsnaher Musterkonfigurationen solcher Systeme.

[4] SCADA ist die Abkürzung für **S**upervisory **C**ontrol **a**nd **D**ata **A**cquisition. Allgemein wird unter SCADA ein Computer-System zum Überwachen und Steuern von technischen Prozessen verstanden.

## 1.3. Aufbau der Arbeit

An die Einleitung anschließende werden im zweiten Kapitel die bekannten Ansätze zur Lösung von Sicherheitsfragen aus der Literatur und Praxis untersucht. Dazu werden die Problembeschreibungen und die sich daraus ergebende Herausforderungen extrahiert und zusammengefasst. Existierende Lösungsansätze werden untersucht und bewertet, inwieweit sich Gedankengänge aus den Voruntersuchungen in die Entwicklung eines neuen Ansatzes integrieren lassen. Insbesondere wird darauf geachtet, welche Fragestellungen offengeblieben sind und ob sich Trends aus den Voruntersuchungen ablesen lassen.

Im dritten Kapitel wird basierend auf den Voruntersuchungen ein Ansatz entwickelt. Dazu werden Überlegungen zu Fragen der Sicherheit sowohl für den Bereich der Anlagen und Maschinensicherheit (Safety) als auch für den Bereich Informationssicherheit (Security) behandelt und in diesen Ansatz eingebaut.

Im vierten Kapitel wird aus dem vorher bestimmten Ansatz ein Vorgehensmodell abgeleitet und im fünften Kapitel vorgestellt. Zur Überprüfung des Modells werden im sechsten Kapitel verschiedene Testszenarien skizziert, das Modell angewendet und die Maßnahmen untersucht und verifiziert.

Das siebente Kapitel ist dem Nutzen des Vorgehensmodells für unterschiedliche praxisnahe Szenarien gewidmet. In den abschließenden Abschnitten werden durch das Gegenüberstellen der ursprünglichen Intention, die mit den erzielten Ergebnissen der Schlussfolgerungen gezogen und deren Resultate bewertet werden, Potenziale zur Verbesserung des Vorgehensmodells aufgedeckt.

## 1.4. Erwartete Ergebnisse

Als Ergebnis der Arbeit wird ein Modell erwartet, dass sich aus mehreren Teilmodellen in Form eines Modellbaukastens konfigurieren lässt.

Es gibt mehrere Gründe für diese Vorgehensweise. Zum einen besitzen industrielle Informations- und Steuerungsanlagen vielfältig unterschiedliche Konfigurationen. Die Vernetzung solcher Anlagen kann einerseits in einem örtlich gesehen unmittelbaren Nahbereich erfolgen, wo der Anteil der Nutzung öffentlicher Netze vergleichsweise gering ist. Andererseits existiert etwa bei landes- oder weltweit operierenden Unternehmen die Notwendigkeit, einzelne Werke zu Fertigungsketten zusammenzufassen, die auf die öffentliche Verbindung der Systeme angewiesen sind.

Zum anderen ist es eine praktische Überlegung, dass für kleinere Teilmodelle auch Varianten geschaffen werden können, um die individuellen Anforderungen eines Systems genauer abzubilden. Eine Konfiguration zum Gesamtmodell ist deutlich einfacher und weniger fehleranfällig, wenn nicht benötigte Parameter in Teilmodellen weggelassen werden können.

# 2. Ansätze in der Literatur und in der Praxis

Als Leitfaden hat die Swedish Civil Contingencies Agency (MSB) unter dem Titel „Guide to Increased Security in Industrial Information and Control Systems“ [SC14] Handlungsempfehlungen veröffentlicht, in der grundlegende Empfehlungen zur Erhöhung der Sicherheit in IACS zusammengestellt sind.

Es wird dort jenes Gefährdungspotenzial skizziert, von dem auch in der vorliegenden Arbeit ausgegangen wird. Es heißt dort: *„Disruptions in industrial information and control systems can lead not only to the destruction of expensive equipment, but also to the interruption of critical operations. This, in turn, can result in extensive costs and lost confidence for both the individual company and society at large.”* [SC14][5]

## 2.1. Problembeschreibung und Herausforderungen

Sicherheit in IACS hat mehrere Aspekte. Im Folgenden wird zwischen der Absicherung des Menschen vor den Gefährdungen durch Maschinen und Anlagen und der Gefährdung der Maschinen und Anlagen durch Angriffe über das Internet unterschieden.

### 2.1.1. Safety

Wird von Sicherheit im Sinne des Begriffes „Safety“ gesprochen, steht die technische Sicherheit im Mittelpunkt des Interesses.

Der Aspekt, wie und durch welche Maßnahmen die technische Sicherheit in IACS herzustellen ist, wird in dieser Arbeit nicht detailliert untersucht, sondern nur jene Beeinflussungen, die auch mit dem Bereich „Security“ im Zusammenhang stehen. Anzumerken ist, dass technische Sicherheit von Maschinen bzw. Anlagen selbst nicht statisch ist, sondern einhergehend mit dem technischen Fortschritt weiterentwickelt wird. Ausgehend von allgemeinen Schutzzielen, formuliert in Richtlinien, sind diese für die unterschiedlichen Anwendungsfälle spezifiziert. Daraus sind die zugrundeliegenden Gesetze, Richtlinien und Normen entstanden. Diese müssen nicht nur von den Betreibern solcher technischen Systeme, sondern auch von Maschinen- bzw. Anlagenbauern berücksichtigt werden, anderenfalls dürfen Maschinen oder Anlagen nicht betrieben werden. Problematisch ist dabei, dass sich auch auf Grund der technischen Weiterentwicklung die Vorschriftenlage verändert und laufend an den neuesten Erkenntnisstand angepasst wird. Was seitens der Anwender zur Verwendung und Einsatz von Sicher-

[5] Störungen in IACS können nicht nur zur Zerstörung teurer Geräte führen, sondern auch zur Unterbrechung kritischer Vorgänge. Dies kann wiederum zu erheblichen Kosten führen und sowohl für das einzelne Unternehmen als auch für die Gesellschaft zum Verlust des Vertrauens führen.

heitskomponenten zu beachten ist, wird überblicksartig in „Häufig gestellten Fragen zur Maschinenrichtlinie“ beantwortet [WKW19].[6] Die gesamte Rechtsvorschrift für die Maschinen-Sicherheitsverordnung ist im [RIS19] zusammengefasst.

### 2.1.2. Security

Auf der anderen Seite steht Sicherheit im Sinne des Begriffes „Security“. Auf diesem Aspekt liegt das Hauptinteresse dieser Arbeit.

Im Bereich „Security“ wird unterschieden zwischen den in der Industrie für Fertigungssysteme genutzten IACS und solche, die als systemrelevant und damit als kritische Infrastruktur betrieben werden.

Kritische Infrastrukturen sind solche, die für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen bedeutend sind. Wenn sie gestört sind, sind schwerwiegende Auswirkungen möglich. Im Wesentlichen zählen zur kritischen Infrastruktur Einrichtungen für die Gesundheit, Sicherheit oder das wirtschaftliche und soziale Wohl der Bevölkerung. Kritische Infrastrukturen existieren in den Bereichen Staat und Staatsverwaltung, Energie, Gesundheit, Informationstechnologie und Telekom, Transport und Verkehr, Medien und Kultur, Wasserversorgung, Ernährung und dem Finanz- und Versicherungswesen. Diesen Bereichen ist gemeinsam, dass diese ohne Datenverarbeitungsanlagen und vernetzte Systeme nicht auskommen, da sie mehr oder weniger voneinander abhängen. Dadurch werden die Risiken meist noch verstärkt.

Wurde ein Unternehmen der kritischen Infrastruktur zugeordnet, ist dieses besonderen Regelungen in Bezug auf Sicherheitsmaßnahmen unterworfen. Dort müssen Sicherheitsmaßnahmen gemäß dem NIS-Gesetz Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (NIS-G) umgesetzt und die Reporting-Funktionalität für den Fall von Cyber-Angriffen bereitgestellt werden. Das NIS-G ist die nationale Umsetzung der EU-Richtlinie 2016/1148 in innerstaatliches Recht, die die Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen (NIS) festlegt [RIS18]. Die DSGVO-Compliance ist von Beginn an ebenfalls zu berücksichtigen.

### 2.1.3. Schwachstelle „Mensch“

Die Bewusstseinsbildung der Nutzer technischer Einrichtungen ist ein wichtiger Aspekt für die IT-Sicherheit. Hauptgrund dafür ist das mangelnde Vorstellungsvermögen, was kleinere Verfehlungen oder Nachlässigkeiten im eigenen Verhalten und in der Bedienung von IT-Einrichtungen für Auswirkungen der Systemsicherheit bewirken können. Abgesehen von der rein technischen Seite der IT-Sicherheit ist der Faktor Mensch eine der Hauptrisikoquellen in einem IT-Sicherheitssystem.

[6] Die Vereinheitlichung der gesetzlichen Bestimmungen im Bereich der Sicherheitstechnik geht auf die als Maschinenrichtlinie bekannte „RICHTLINIE 2006/42/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES“ vom 17. Mai 2006 über Maschinen und der Änderung der Richtlinie 95/16/EG zurück [MRL06].

Es existieren Anforderungen an die Informationssicherheit einerseits durch die Gesetzgebung und andererseits als regulatorische Anforderungen.

Gefragt wird, wovon gehen die Anforderungen an die Informationssicherheit im Detail aus und inwieweit umfassen diese Anforderungen explizit den Bereich der Bewusstseinsbildung für die Informationssicherheit.

Es stellt sich weiter die Frage, wie und auf welche Weise diesen Anforderungen im Umfeld eines Unternehmens nachgekommen werden kann. Im Einzelnen wird es dabei um die Zertifizierung nach Standards oder Normen gehen. Eine weitere Frage ist, wie die Motivation auch außerhalb gesetzlicher und regulatorischer Anforderungen als Antrieb zur Verbesserung der Informationssicherheit dienen und wie sie gesteigert werden kann.

Dazu werden die Gesetzgebung und die regulatorischen Anforderungen unter Einbeziehung des Faktors Mensch untersucht. Der Fokus liegt dabei auf der Fragestellung, ob mit einer standardisierten Vorgehensweise menschliche Fehler verhindert werden können.

Auch der Unsicherheitsfaktor Mensch steht im Mittelpunkt von Untersuchungen. Der Fokus liegt dabei auf der Fragestellung, wie einerseits die Motivation zur Verbesserung der Informationssicherheit beginnend beim Arbeitsplatz bis hin zu Abteilungen und dem Gesamtunternehmen gesteigert werden kann.

Um die Informationssicherheit dauerhaft zu definieren, zu steuern und zu kontrollieren und danach diese aufrecht zu erhalten und zu verbessern, existieren Information Security Management Systeme (ISMS). Ähnlich solcher Systeme werden Bausteine für ein Vorgehensmodell entwickelt. Im Anschluss wird untersucht, wie das Durchsetzen von Anforderungen an die Informationssicherheit messbar gemacht werden kann.

### 2.1.4. Schwachstelle Gerätetechnik

Insbesondere die Gerätetechnik von IACS verharrt auf Grund ihrer vergleichsweise langen Lebenszeit und Einsatzdauer unverändert auf dem technischen Stand, den sie seit ihrer Ersteinführung innegehabt hatte. Software Updates sind bei laufenden Steuerungssystemen so gut wie ausgeschlossen. Damit können allfällige Sicherheitslücken bei den Betriebssystemen dieser Geräte nicht geschlossen werden und die Geräte werden damit angreifbar.

### 2.1.5. Schadsoftware

In den Jahresberichten des Bundesamtes für Sicherheit in der Informationstechnik (BSI) wird über Sicherheitsvorfälle im IT-Bereich berichtet und Maßnahmen bzw. Empfehlungen zur Erhöhung der Netzwerksicherheit vorgeschlagen. In den ausgewählten Beispielen sind jene Vorfälle skizziert, für die das geplante Vorgehensmodell die Sicherheit von automatisierten technischen Systemen verbessern soll.

**Beispiel: Schadensfall in einem Stahlwerk**

In einem Jahresbericht des BSI wird über einen Cyberangriff auf das Werksnetzwerk in einem deutschen Stahlwerk berichtet. Ein Hochofen soll dadurch massive Schäden erlitten haben.

Angreifer hatten sich über E-Mails Logins verschafft, mit denen sie auf die Kontrollsysteme im Stahlwerk zugreifen konnten. Der dadurch verursachte Ausfall von Anlagenteilen bewirkte, dass ein Hochofen nicht wie gewohnt stillgelegt werden konnte. Durch die außerplanmäßige Abschaltung des Ofens wurde ein nicht näher spezifizierter Schaden verursacht, wurde berichtet. Bei der Ursachenanalyse hat sich herausgestellt, dass sowohl gezielte E-Mails als auch Social-Engineering-Techniken eingesetzt worden waren, um über den Zugriff auf das Büronetzwerk des Werks auf die Produktionssysteme einwirken zu können.

Das Unternehmen und der Zeitpunkt des Angriffs wurden nicht bekannt gegeben. Obwohl dieser Angriff zu den wenigen bekannt gewordenen Angriffen zählt, zeigt der Bericht die Wichtigkeit geeigneter Schutzmaßnahmen (vgl. [BBC14]).

**Beispiel: Infektionen mit WannaCry-Schadsoftware**

Anfang des Jahres 2018 wurden mehrere Rechner in einer Produktionsanlage eines im Sektor Ernährung tätigen Unternehmens angegriffen, fielen häufig aus und mussten jeweils neu gestartet werden. Später wurden mehrere weitere Fälle bekannt, die mit WannaCry-Schadsoftware infiziert worden waren.

Die Schadenswirkungen waren unterschiedlich. In einem Fall waren die Rechner so konfiguriert, dass sie nach einem Neustart einen definierten Ursprungszustand eingenommen hatten. In einem anderen Fall wurde der Fehler durch ein Mobile Incident Response Team (MIRT) des BSI mit dem betroffenen Betreiber und dem betreuenden Unternehmen untersucht und zuletzt behoben. Ein Fehler in einer Netzwerkkomponente hatte die Trennung der Netzwerke nicht wie konfiguriert verhindert. In einem weiteren Fall lag der Fehler bei einem durch ein vom Hersteller zur Verfügung gestellten Testgerät, der das Schadprogramm auf die infizierten Geräte übertragen hatte (vgl. [BSI18-1]).

**Beispiel: Cyber-Angriff auf das Safety-System einer Industrieanlage**

Ein Cyber-Angriff auf das Safety-System einer Industrieanlage durch die Malware „Triton“ wurde durch eine Veröffentlichung der Firma FireEye bekannt (vgl. [BJ et.al. 17]). Beschrieben wurde der Angriff auf ein Safety Instrumented System (SIS) einer Industrieanlage. SIS werden im Regelfall getrennt vom Leitsystem aufgebaut, haben eine rein beobachtende Funktion und greifen nur im Anforderungsfall ein. Die von FireEye benannte Malware Triton ist auch unter den Aliasbezeichnungen Trisis und HatMan bekannt.

Obwohl auf Grund des Angriffsverlaufes und einer Analyse von festgestellten forensischen Artefakten davon auszugehen war, dass der Angriff lange vorbereitet worden war, war er erfolglos. Ein Safety Controller hatte im Verlauf des Angriffs eine Gültigkeitsprüfung des Applikationsprogramms durchgeführt und einen Fehler festgestellt und die Anlage durch das redundante Safety-System in den sicheren Zustand überführt (vgl. [BSI18-1]).

**Beispiel: Cyber-Angriff auf Aluminiumkonzern**

Der Angriff erfolgte auf einen norwegischen Aluminiumkonzern durch die Ransomware LockerGoga. Betroffen waren die IT-Systeme in den meisten Geschäftsfeldern. Als Reaktion wurden die Systeme vom Netz genommen und die Produktion wurde soweit wie möglich auf manuellen Betrieb umgestellt. Es wurde Lösegeld gefordert, aber das Unternehmen nutzte vorhandene Backups, um den Betrieb wiederherzustellen. Die Behebung des Schadens war langwierig (vgl. [BSI19]).

## 2.2. Existierende Lösungsansätze und Entwicklungen

In diesem Abschnitt werden bereits bekannte Ansätze untersucht und analysiert.

### 2.2.1. Zellen-basiertes Framework für Industrial Information Security

Herbert Dirnberger hat in seiner Arbeit mit dem Titel: „Entwicklung eines Zellen-basierten Frameworks für Industrial Information Security“ ein Framework für die Planung, Koordination, Inbetriebnahme, Instandsetzung und Optimierung von Informationssystemen entwickelt [DH11].

Das von Dirnberger vorgestellte Rahmenwerk (Framework) ist aus der Schnittmenge von Standards, Normen und Frameworks aus dem Gebiet der Informationssicherheit (Information Security) für den Fachbereich der industriellen Automatisierungs- und Steuerungssysteme (Industrial Automation and Control Systems) unter Berücksichtigung des Regelwerks der International Association of Classification Societies entwickelt worden. Für die Überprüfung seines Framewoks hat Dirnberger die von ihm vorgeschlagenen Maßnahmen für ein fiktives Unternehmen (RECPLAST GmbH) angewendet und untersucht.[7] Aus den Ergebnissen seiner Untersuchungen hat Dirnberger ein Informationssicherheits- und Serviceprogramm entwickelt (vgl. [DH11]).

Wird ein fiktives Unternehmen als Basis für eine Untersuchung zugrunde gelegt, hat das den Vorteil, dass die Grundsätze des Datenschutzes nicht verletzt werden können. Auf der anderen Seite stellt sich jedoch die Frage, inwieweit ein fiktives Unternehmen den Anspruch an die Realität erfüllen kann. Darüber hinaus stellt sich auch noch die Frage, ob Untersuchungsergebnisse, die mithilfe von fiktiven Unternehmen gefunden worden sind, auf andere Unternehmen ohne weiteres übertragen werden können und ob der Anspruch auf die allgemeine Gültigkeit gewährt bleibt.

### 2.2.2. Modellbasiertes Sicherheits-Engineering

In der Arbeit von Nigam et. al. „Model-Based Safety and Security Engineering” [NV et. al 18] werden Szenarien untersucht, wie Cyber-Angriffe bekämpft werden, die katastrophale Ereignisse verursachen können, wenn diese z.B. Sicherheitsmechanismen durch Angriffe aus der

[7] Das Beispielunternehmen RECPLAST GmbH hat rund 500 Mitarbeiter und stellt aus Recyclingmaterialien Kunststoffprodukte her (vgl. [BSI18]).

Ferne deaktivieren. Zur Gefahrenvermeidung werden Schritte zur Integration eines Sicherheitskonzepts mithilfe von Modellen beschrieben. Behandelt wird die Identifikation technischer Herausforderungen.

Genutzte Modelle sind die Goal Structured Notation (GSN) für den Bereich „Safety“ und Attack Defense Trees (ADT) für den Bereich „Security“. Gezeigt wird, wie sicherheitsrelevante Informationen aus Sicherheitsbewertungen automatisiert durch Übersetzung von GSN-Modellen in ADTs extrahiert werden können. Im von [NV et. al. 18] vorgeschlagenen Entwicklungsprozess werden Sicherheitsbewertungen durch schrittweise Berücksichtigung von Sicherheitsanalysen erstellt und eine Kompromissanalyse automatisiert durchgeführt, wenn Sicherheitsargumente im Widerspruch zueinanderstehen und wie man gegebenenfalls solche Widersprüche auflöst (vgl. [NV et. al. 18]).

### 2.2.3. Cybersicherheit für kritische Infrastrukturen

In der Arbeit von Ten et. al mit dem Titel: „Cybersecurity for Critical Infrastructures: Attack and Defense Modeling“ [TC et. al 10] werden für die Überwachung und Datenerfassung als Rahmen vier Hauptbereiche vorgeschlagen: 1. Echtzeitüberwachung, 2. Erkennung von Anomalien, 3. Analyse der Auswirkungen und 4. Strategien zur Schadensminderung. Die Wirkungsmechanismen werden über die Formulierung von Angriffsbäumen untersucht, um Schwachstellen auf System-, Szenario- und Blattebene zu bewerten. Die Anfälligkeit der Blätter wird genutzt, um Kennworte in Bezug auf ihre „Stärke“ zu bewerten und die Ports zu überprüfen. Daraus entstehen auf der Grundlage des von der American Electric Reliability Corporation (NERC) entwickelten Cybersicherheitsstandards Cybersicherheitsbedingungen. Damit werden festgestellte Schwachstellen indexiert und bewertet.

### 2.2.4. Industrial Security

Ein Faktenpapier vom Verband Deutscher Maschinen- und Anlagenbau e. V. (VDMA), verfasst von Steffen Zimmermann, nennt menschliches Fehlverhalten und Sabotage als die größten Bedrohungen für industrielle Sicherheit.

Bedrohungen für industrielle Sicherheit sind menschliches Fehlverhalten und Sabotage, das Einschleusen von Malware, Social Engineering und Phishing, die Infektion der Systeme mit Malware über Internet/Intranet, technisches Fehlverhalten und höhere Gewalt, (D)DoS-Angriffe, die Kompromittierung von Extranet- und Cloud-Komponenten, der Einbruch über Fernwartungszugänge, die mit dem Internet verbundenen Steuerungskomponenten und die Kompromittierung von Smartphones im Produktionsumfeld (vgl. [ZS19]).

### 2.2.5. ICS-Security-Kompendium

Das ICS-Security-Kompendium behandelt grundlegendes zu den sogenannten Industrial Control Systems (ICS) [BSI13].[8] Obwohl dieses Werk bereits 2013 veröffentlich worden ist, hat sich die Gefährdungslage seit damals nicht wesentlich verändert, sondern ist nach wie vor aktuell.

[8] ICS: industrielle Steuerungssysteme (industrial control systems)

Das ICS-Security-Kompendium benennt jene Fakten, die mit als eine Grundlage für die in der Folge angestellten Untersuchungen und daraus entwickelten Vorschlägen genutzt werden.

### 2.2.6. Anomalien in der Kommunikation

Windmann et. al. beschäftigen sich in ihrer Arbeit „Konzepte zur Erhöhung der IT Sicherheit in industriellen Automatisierungssystemen - Ansätze für die Feldebene“ [WS et. al. 16] mit der Feldebene industrieller Automatisierungssysteme. Es ist eine immer stärkere Vernetzung von Feldgeräten untereinander und zusätzlich mit Geräten auf höheren Ebenen der Automatisierungspyramide festzustellen. Anstelle von proprietären Feldbusprotokolle werden zunehmend standardisierte Netzwerkprotokolle auf der Basis des TCP/IP Kommunikations-Stacks genutzt. Diese Entwicklungen macht Automatisierungssysteme anfälliger gegenüber Cyberangriffen, die u.a. die Integrität und Verfügbarkeit cyberphysikalischer Produktionsprozesse bedrohen und sogar zu einer Gefährdung der Menschen führen können.

Auch die vorliegende Arbeit beschäftigt sich mit dieser Thematik. Windmann et. al. betrachten neben Standardmaßnahmen wie Verschlüsselung, kryptographische Hashfunktionen, Identifikationsmerkmalen und zeitlichen Merkmalen insbesondere auch neue Methoden zur automatischen Prozessüberwachung (vgl. [WS et. al. 16]).

Ziel ihrer Anomalie-Erkennung ist, durch Cyberangriffe verursachte Anomalien auch auf der Ebene von physikalischen Prozessen zu detektieren, in dem das tatsächliche mit dem erwarteten Prozessverhalten verglichen wird. Dazu müssen jedoch das Prozessverhalten und die Prozessabläufe bekannt sein (vgl. [WS et. al. 16]).

Auch der in dieser Arbeit verfolgte Ansatz ist, den Datenverkehr zu analysieren, um Anomalien im Datenaufkommen festzustellen. Zusätzlich soll der Datenverkehr durch Filtermechanismen auf das erforderliche Ausmaß eingeschränkt werden.

### 2.2.7. Cybersecurity Research: Challenges and Course of Action

Im Forschungsbericht des Frauenhofer Instituts „Challenges and Course of Action” [MQJ19] wird Cybersicherheit behandelt und werden Beispiele für Anwendungen und Technologien analysiert. Der Forschungsbericht enthält mehrere Beiträge zu den Herausforderungen und gibt Handlungsempfehlungen.

Der Beitrag „Secure Lifecycle despite of Less Trustworthy Components“ behandelt den Umstand, dass typische Architekturen einer Fertigungslinie oder einer kritischen Infrastruktur selten völliges Neuland in der Entwicklung darstellen. Deshalb wird als Lösungsansatz vorgeschlagen, sichere Systeme zu entwerfen, den Entwicklungsprozess schrittweise von den bestehenden Strukturen zu einer neuen Architektur zu verändern (vgl. [MQJ19]).

Das wird nur bei Neuanlagen möglich sein. Um einen sichereren Lebenszyklus trotz weniger vertrauenswürdiger Komponenten zu erreichen, wird als kurzfristige Maßnahme unter anderem die Entwicklung geeigneter und verwendbarer Prozesse und Tools zur Bewertung der Sicherheit von Systemen und Komponenten und die Definition von Standards für die Interoperabilität vorgeschlagen (vgl. [MQJ19]).

Der Beitrag „Remotely Unhackable PC“ diskutiert die „Secure Inter-Network Architecture“ (SINA). Diese Architektur wurde vom BSI mitentwickelt und ist als Vorbild gedacht, ein hohes Sicherheitsniveau auch für Heimanwendungen nutzbar zu machen. Ausgeführt wird, dass die Komponenten eines entfernt nicht hackbaren Systems im Idealfall keinen Einfluss aufeinander haben oder dass sie an strenge Protokolle gebunden sind, die die Interaktion steuern. Damit wird sichergestellt, dass auch wenn ein Programm kompromittiert wird, alle anderen Programme unberührt bleiben (vgl. [MQJ19]).

Stark vereinfacht bildet ein nicht hackbares System, bezeichnet als „Remotely Un-hackable Personal Computer“ (RUPC), eine zwischengestaltete Schnittstelle als vertrauenswürdige Plattform.

## 2.3. Trends und offene Fragestellungen

Dirnberger sieht eingangs als eine zentrale Aufgabenstellung seiner Arbeit *„die Zusammenarbeit der Domänen Informationstechnologie und Automatisierungstechnik zu fördern, um industrielle Informationssicherheit zu ermöglichen“* [DH11]. Die generellen Empfehlungen fordern im Gegensatz dazu, dass Zugriffe über das Internet von den rein kommerziell genutzten Bereichen zur Automatisierungstechnik strikt zu trennen und gegebenenfalls zusätzlich durch Maßnahmen abzusichern ist.[9] Das impliziert, dass die Interaktion einer kommerziell genutzten IT zum Bereich der in der Fertigung eingesetzten IT erschwert werden sollte. Um diesen Widerspruch aufzulösen hat Dirnberger die IT ganzheitlich betrachtet und in seinem Framework entsprechende Richtlinien vorgeschlagen (vgl. [DH11]).

Nigam et.al. nutzen anstelle einer verbalen Beschreibung Modelle. GSN-Modelle[10] beschreiben in einer strukturierten Notation Ziele, gemeint sind dabei Sicherheitsziele sowohl für Safety als auch für Security. ADTs[11] ähneln im Aufbau Entscheidungsbäumen (Decision Trees), die Maßnahmen zur Verhinderung oder zum Erschweren von Angriffsszenarien darstellen. Als Vorteil von Modellen sehen [NV et. al. 18], dass bei Modellen die darin enthaltene Informationsdichte höher und vor allem anschaulicher ist, als diese in verbalen Beschreibungen dargestellt werden kann. Darstellbar sind z.B. Zusammenhänge mit Komponenten, logische Beziehung von Lösungen und Gefahren unter Einbeziehung quantitativer Bewertungen. Nigam et.al. stellen in ihrer Arbeit eine Methode mit dem Ziel vor, Aspekte von Safety und Security zu vereinigen, um beiden Aspekten so gut wie möglich gerecht zu werden (vgl. [NV et. al. 18]).

Für die automatisierte Umwandlung der Modelle wird die so genannte Beta-Verteilung[12] genutzt, um den Zusammenhang eines Security GSN-Modells gegenüber den Safety Erfordernis-

[9] Diese Empfehlung steht ihrerseits im Gegensatz zur Intention von Industrie 4.0, die erst durch das aus der Produktion stammende Datenaufkommen Industrie 4.0 ermöglicht.

[10] GSN: Goal Structured Notation

[11] ADT Attack Defense Trees

[12] Die Beta-Verteilung ist eine Familie stetiger Wahrscheinlichkeitsverteilungen im Intervall [0, 1].

sen zu bestimmen. Damit soll durch eine quantitative Bewertung eines Modells aus den Variablen „Vertrauen“ (B, belive) „Kein Vertrauen“ (D, disbelive) und „Unsicherheit“ (U, uncertainly) ein mathematischer Zusammenhang beschrieben werden. Bekanntlich ist Sicherheit selbst grundsätzlich ein relativer Wert. Bei der Festlegung von Sicherheitseinstufungen werden immer Wahrscheinlichkeiten in die Bestimmung mit einbezogen, z.B. wie kritisch bestimmte Merkmale oder die Sicherheit beeinflussende Faktoren zu bewerten sind (vgl. [NV et. al. 18]).

Wesentliche Fakten, die die Fragestellungen in dieser Arbeit beeinflussen, sind in [BSI13] zusammengefasst. Wichtigster Umstand ist, dass *„der Lebenszyklus von ICS …“ „… aus dem der zugehörigen Produktionsanlagen abgeleitet“* wird. *„Dieser ist deutlich länger als die in der Office IT typischerweise anzutreffenden Zeiträume. Die Laufzeit beträgt zehn bis fünfzehn Jahre. Mitunter können es auch 20 Jahre sein. In der Office-IT sind es meist nur drei bis fünf Jahre.“* [BSI13]. Das bedeutet, dass das Informations-Sicherheitsniveau industrieller Anlagen dem Stand der Wissenschaft immer nachhinken wird.

Eine Verbesserung ist eher schwierig zu erreichen, weil in vielen *„Anwendungen […] der Betrieb der Anlagen an behördliche Auflagen gebunden ist (z. B. Anlagensicherheit). In diesen Fällen bedürfen wesentliche Änderungen, worunter auch Softwareänderungen an den eingesetzten ICS fallen können, einem dedizierten Genehmigungsprozess.*

*Aufgrund des vorgeschriebenen Prüfprozesses sind hier beispielsweise die Möglichkeiten zum zeitnahen Einspielen von Sicherheitsupdates begrenzt bzw. nicht gegeben*.“ [BSI13]

## 2.4. Forschungsfragen

Es ist grundsätzlich der richtige Weg, Maßnahmen zur Verbesserung der IT-Sicherheit an den unmittelbaren Schnittstellen des Internets zum internen IT-Netz zu treffen und nicht erst an jenen Stellen, wo der industriell genutzte Bereich der Automatisierung technischer Systeme beginnt. In dieser Arbeit wird davon ausgegangen, dass geeignete Maßnahmen zur Sicherstellung der generellen IT-Sicherheit dem Stand der Technik und dem Erkenntnisstand der Praxis bereits gegeben sind. Dennoch kann es aufgrund neuer Angriffsszenarien oder aufgrund sonstiger Fehler dazu kommen, dass der äußere Schutz überwunden worden ist und systemkritische Bereiche zusätzlich abgesichert werden müssen. Auf diesem Aspekt liegt das Hauptaugenmerk dieser Arbeit.

Zentrale Forschungsfragen dieser Arbeit werden daher sein:

„Welche zusätzlichen Sicherheitsmaßnahmen sind zum Schutz der technischen Systeme in einer Produktion implementierbar?“ Die zusätzlichen Sicherungsmaßnahmen werden dabei so gewählt, dass sie den Intentionen von Industrie 4.0 nicht widersprechen, weil Industrie 4.0 erst durch die Fähigkeit zum Austausch großer Datenmengen ermöglicht worden ist. Notwendig ist dazu der selektive Datenaustausch innerhalb des eigenen Unternehmens aber auch zwischen unterschiedlichen Unternehmen mit deren Subsystemen. Solange der Datenaus-

tausch innerhalb eines eigenen Unternehmens erfolgt, sollte dieser in Bezug auf Informationssicherheit beherrschbar sein. Schwieriger wird es sein, die Informationssicherheit auch dann noch sicherzustellen, wenn dieser Datenaustausch mit fremden Unternehmen erfolgen muss.

„Welche Möglichkeiten existieren für die technische und organisatorische Nach- bzw. Aufrüstung technischer Systeme im Bereich der Automatisierungstechnik?“ Hier werden die technischen und organisatorischen Möglichkeiten und deren Einbettung in die Automatisierungstechnik betrachtet.

„Wie kann ein Maßnahmenpaket aus Einzelmaßnahmen in einen Modellbaukasten eingeordnet werden, um bestimmte Szenarien von Beeinträchtigungen automatisierter technischer Systeme zu erkennen?“ Gefundene Einzelmaßnahmen werden sortiert zu Maßnahmenpaketen zusammengefasst. Jedes dieser Maßnahmenpakete stellt ein Teilmodell dar, dass zu einem Gesamtmodell zusammengebaut werden kann. Gefragt wird auch, inwieweit Teilmodelle in sich konsistent gestaltet werden können und ob diese gegenüber konkurrierenden Teilmodellen widerspruchsfrei sind.

„Welche Abwehrmaßnahmen können die IT-Sicherheit in technischen Systemen verbessern?“ Diese Frage richtet sich hauptsächlich auf Aspekte der technischen Umsetzbarkeit.

„Wie können einzelne Maßnahmen, Teilmodelle und Modelle zur Erhöhung der Sicherheit in Bezug auf ihre Wirksamkeit verifiziert werden?“ Mit dieser Frage wird der Nutzen hinterfragt. Die kritische Gegenüberstellung der ursprünglich aufgeworfenen Fragestellungen und Ergebnisse von Zwischenuntersuchungen sollen eine Bewertung ermöglichen.

# 3. Anforderungen an das zu entwickelnde Modell

Von der IT-Infrastruktur sind die dort eingesetzten Netzwerke das Verbindungssystem der Unternehmens IT mit der Automatisierungstechnik. Als IT-Infrastruktur wird in der Folge die Gesamtheit aller Elemente wie die genutzten Geräte und Komponenten, Kommunikationsdienste, mit eingebundene Maschinensteuerungen und Programme verstanden, die zur automatisierten Informationsverarbeitung zur Verfügung stehen. Dabei müssen die einzelnen Bestandteile an sich ändernde Anforderungen immer wieder angepasst werden. Als Grundlage der Kommunikation und der Datenverarbeitung in den einzelnen Bereichen wie Organisationseinheiten, Abteilungen bis zu den beteiligten Personen mit deren Arbeitsplätzen dienen die Netzwerke. Während einzelne Geräte von Zeit zu Zeit ersetzt werden, bleibt die generelle Netzwerkstruktur in der Regel auch für längere Zeiträume weitgehend unverändert. Insbesondere bei umfangreichen industriellen Anlagen wird die Netzwerkstruktur einen dezentralen, redundanten Aufbau aus vielen Netzwerkkomponenten aufweisen.[13]

## 3.1. Anforderungen aus der Praxis

Wird die Sicherheit in IACS untersucht, muss der typische Aufbau einer IT-Infrastruktur und insbesondere das dort eingesetzte Netzwerk für die Entwicklung eines integrierten Vorgehensmodell für Safety und Security in der Automatisierung technischer Systeme berücksichtigt werden.

Die Systemsicherheit im Sinne von Security bedeutet dabei, dass die innerhalb des Systems zu verarbeitenden Daten nicht korrumpiert werden. Im Gegensatz dazu bedeutet Systemsicherheit im Sinne von Safety, dass selbst bei einem Angriff auf die Systemsicherheit durch Verletzung der Security die Sicherheit der Anlagen und Maschinen erhalten bleibt, also dass die Safety Aspekte in jedem Fall erhalten bleiben und sichergestellt sind.

Im Prinzip gilt, falls die Gesamtheit aller Schutzmaßnahmen eines Systems bereits derart ausgereift sind, dass die Verletzung der Security praktisch unmöglich gemacht worden ist, dass dann auch keine zusätzlichen Maßnahmen zur Sicherung von Saftey-Komponenten oder Safety-Funktionen für die Maschinen und Anlagen notwendig werden. Das wäre der Idealfall. In der Realität ist es jedoch so, dass die Entwicklung der IT, sowohl für die Gerätetechnik als auch für die dort genutzte Software, so rasch weiterentwickelt wird, dass man davon ausgehen kann, dass es weder die absolut fehlerfreie Gerätetechnik noch die entsprechende Software dazu gibt.

In der Praxis bedeutet das, dass insbesondere industrielle Steuerungssysteme vor der Infektion mit Schadprogrammen besonders geschützt werden müssen. Dazu kommt, dass industrielle Steuerungssysteme in der Regel eine deutlich größere Einsatz- und Verwendungsdauer haben als kommerziell genutzte Systeme. Während in der Office-Umgebung die Komponenten auch auf Grund der rasanten Entwicklung in der Computertechnik in relativ kurzen Zeiträumen

[13] In der Veröffentlichung „7 Tipps für den idealen Aufbau Ihrer IT Infrastruktur“ werden Anregungen zum Aufbau einer IT-Infrastruktur gegeben (vgl. [SU19]).

ausgetauscht und durch neue Komponenten ersetzt werden, ist das bei industriellen Steuerungssystemen nicht der Fall. Das bedeutet aber auch, dass in der Automatisierungstechnik genutzte Systeme oft mehr als zehn Jahre in Betrieb sind. Dort verwendete Betriebssysteme werden in der Regel nicht gewartet, Software Updates oder Patches sind unüblich.

Eine Ursache dafür ist, dass gegenüber von in Office Umgebungen genutzten Geräten es deutlich weniger industrielle Steuerungssysteme gibt. Darüber hinaus haben auch unterschiedliche Hersteller solcher Systeme jeweils für diese Steuerungssysteme eigene Betriebssysteme und Programmierumgebungen entwickelt, die untereinander nicht kompatibel sind. Das Gleiche gilt auch für die Kommunikationssysteme mit der angeschlossenen Peripherie, obwohl es dort auch auf Grund von Normungen Komponenten gibt, die kombinierbar sind. [14]

## 3.2. Hierarchie in der Automatisierung

In der so genannten Automatisierungspyramide ist die in der Automatisierung typische hierarchische Struktur des Zusammenwirkens von Aufgabenstellungen und den zugehörigen Komponenten dargestellt. Die Verbindung dieser Komponenten wird dazu durch verschiedene Netzwerke hergestellt.

Zur besseren Übersicht wird in der Folge gezeigt, wo die Schnittstellen zwischen dem Office-Bereich und dem Automatisierungs-Bereich angesiedelt sind. Die Grenze ist nicht scharf definierbar, weil die Prozessleitfunktionen auch mit Industrie-PCs realisiert werden können. Während die Automatisierungsgeräte zum Teil auch direkt in einer rauen Industrieumgebung [15] eingesetzt werden können und deshalb auch direkt in die zu steuernden Maschinen oder Anlagen integriert sein können, wird die Funktion der Prozessleitung in Warten ausgeübt, wo die Umgebungsbedingungen dem Office-Bereich entsprechen.

Automatisierungsfunktionen sind die selbsttätig ausgeführten Funktionen, die weitgehend autonom ablaufen und die je nach Prozessführungsebene unterschiedliche Bedeutung und Interaktionsmöglichkeiten besitzen. Das Ebenen-Modell der so genannten Automatisierungspyramide spiegelt eine hierarchische Ordnung wider. Anzumerken ist, dass in der Literatur die Grenzen der hier genannten Ebenen auch unterschiedlich gelegt werden können, wobei 3-, 4- oder 5-Ebenen unterschieden werden. Im dargestellten 5-Ebenen-Modell (Fig. 1) existieren auch neben den funktionalen Eigenschaften zeitliche Auswirkungen. Die hierarchisch gesehen höchste Ebene, Ebene 1, wird als Führungsebene bzw. Unternehmensleitebene klassifiziert

[14] Die Inkompatibilität von Hard- und Software wird von den Herstellern meist als Alleinstellungsmerkmal genutzt. Damit können Steuerungsprogramme beim Systemwechsel nur mit größerem Aufwand von einem System in ein anderes System übertragen werden. Das geht zum Teil soweit, dass bei speicherprogrammierbaren Steuerungen des gleichen Herstellers unterschiedliche Programmiersysteme bei so genannten „Steuerungsfamilien“ notwendig sind.

[15] Unter rauer Industrieumgebung wird hier das Auftreten von Staub, Schmutz, Luftfeuchtigkeit, erhöhte Temperatur etc. verstanden. Auch die Störbeeinflussung auf Grund der Schaltvorgänge (Anlauf von Antrieben, Umrichter-Betrieb etc.) bedeutet die Möglichkeit Signale zu beeinflussen und damit eine entsprechende robustere Ausführung der in dieser Umgebung eingesetzten Bauteile und Komponenten.

(Corporate Management Level). Die wesentliche Aufgabe dort ist das Führen des Unternehmens und beinhaltet dispositive Aufgaben wie Kostenanalysen oder statistische Auswertungen. Dementsprechend langfristig sind die Auswirkungen, die im Bereich von Wochen bis Monaten liegen können (vgl. KG17]).

In Ebene 2, der Betriebsführungsebene (Betriebsleitebene, Produktleitebene, Plant Management Level, Production Management Level), liegen die Aufgabenbereiche in der Führung des Betriebes bzw. der gesamten Fabrik. Dispositive Aufgaben sind dort unter anderen die Betriebsablaufplanung, Optimierung der Kapazität einer Produktion und Auswertung der Prozessergebnisse. Der Entscheidungs- und Auswirkungszeitraum ist deutlich kürzer und liegt im Bereich von Tagen, Wochen bis zu wenigen Monaten (vgl. KG17]).

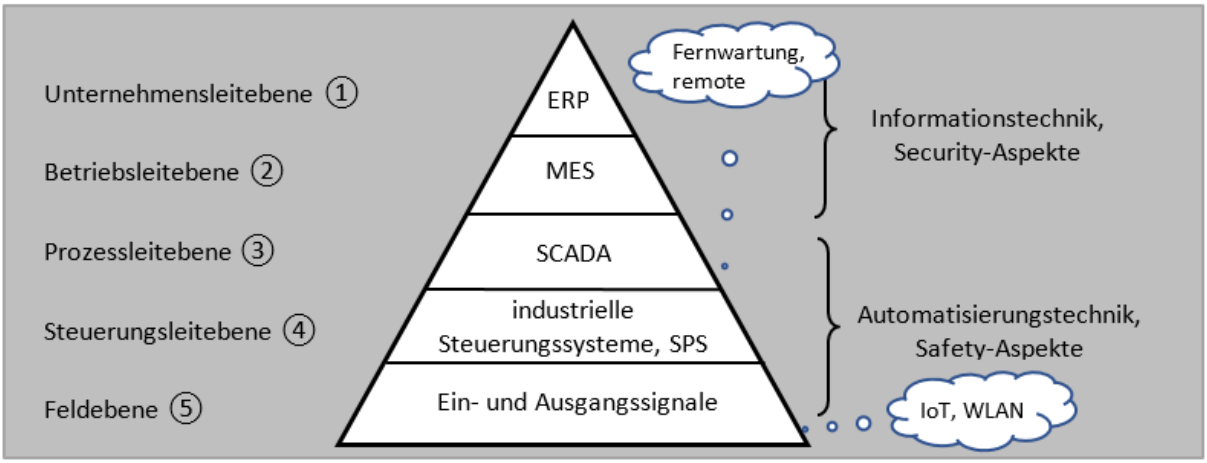



*Fig. 1: Netzwerkhierarchie in der Automatsierungspyramide, 5-Ebenen Modell (vgl. KG17])*

Ab der Ebene 3, der Anlagenführungsebene (Prozessleitebene, Process Management Level, Process Supervision Level) sind die eigentlichen Automatisierungsaufgaben zu finden. In diesen Verantwortungsbereich fallen die Führung eines oder mehrerer technischer Prozesse von Verfahrensgruppen usw. mit operativen und teilweise auch dispositiven Aufgaben, wie Prozess-Überwachung, An- und Abfahren, Störungsbehandlung, Prozessführung sowie Prozess-Sicherung. Entscheidungen müssen innerhalb von wenigen Minuten getroffen und umgesetzt werden (vgl. KG17]).

Ebene 4 wird oft mit der Ebene 5 zusammengefasst. Aufgabenbereich der Ebene 4, bezeichnet als Funktionsgruppenebene, Gruppenleitebene, MSR-Ebene bzw. Process Control Level, ist das Ausführen von Funktionen zur Regelung, Steuerung, Überwachung und Sicherung. Hinzu kommen operative Aufgaben, wie Messen, Steuern, Stellen, Regeln, Verriegeln, Not-Bedienen von Prozessgrößen, Abschalten und Schutz. Das Zeitfenster für Reaktionen ist hier bereits auf Mikro- bis Millisekunden reduziert. Ebene 5 ist die Ebene des technischen Prozesses, das so genannte Feld, als niedrigste in der Hierarchie angeordnete Ebene. Aufgaben sind das Messen von Prozessgrößen mit Sensoren, Einwirken auf den technischen Prozess mittels Stellgliedern,

also die Erfassung und Beeinflussung von Prozessgrößen mit Hilfe von Sensoren und Aktuatoren. Reaktionszeiten liegen im Bereich von wenigen Millisekunden.[16] Insbesondere bei sicherheitsrelevanten Vorgängen müssen die Steuerungssysteme unmittelbar reagieren können und insbesondere die Beeinflussung der dort ablaufenden Schaltvorgänge durch die Unternehmens IT muss ausgeschlossen sein (vgl. KG17]).

## 3.3. Abgrenzung der Bereiche „Security“ und „Safety“

In Fig. 1 ist eine Abgrenzung zwischen der gesamten System-Sicherheit gegenüber der Sicherheit im Sinne von Safety Aspekten als Maschinensicherheit in die Prozessleitebene gelegt worden. Betrachtet man Safety aus der Sicht der potenziellen Gefahrenquellen, das ist in der Regel der in einer Maschine oder Anlage ablaufende Prozess, dann sind als Sicherungselemente überwachte, gesteuerte Schutzelemente und Vorrichtungen für die Prozesssicherheit verantwortlich. Da die Prozesssicherheit durch gesteuerte Elemente sichergestellt wird, muss ausgeschlossen werden, dass Angriffe auf die vorgeschalteten Leitsysteme die Sicherheitseinrichtungen beeinflussen können. Andererseits dürfen aber die an die Steuerungssysteme angeschlossenen intelligenten Sensoren oder Aktoren auf Grund von dort eingebauten Rechnersystemen nicht als Einfallstor für Schadprogramme dienen.

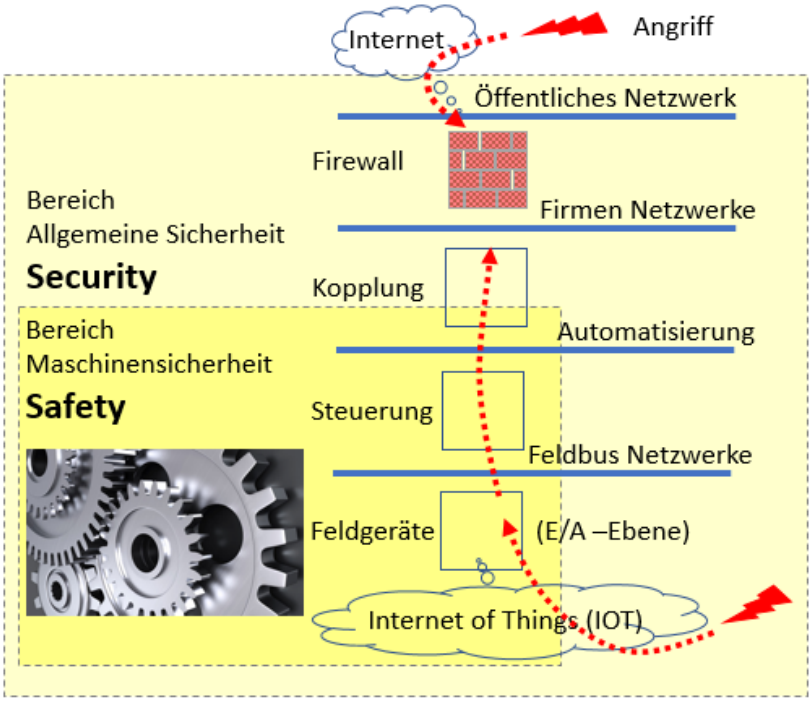



*Fig. 2: Übersicht: Safety als Teilmenge von Security*

[16] Die Reaktionszeiten sind bei Sensoren und Aktuatoren z.T. schaltungstechnisch verzögert, um externe Störbeeinflussungen zu unterdrücken. Stellglieder wie Magnetventile benötigen eine gewisse Zeit, um durch den Druckaufbau in Zylindern Bewegungsabläufe einzuleiten. Die typische Anzugsverzögerung bei Schaltschützen für Motorabzweige liegt je nach Schaltleistung im Bereich von wenigen Millisekunden. Es entstehen daher Totzeiten zwischen einem Ereignis und der Reaktion eines Steuerungssystems bzw. umgekehrt bei der Befehlsausgabe und der Reaktion der Maschine oder Anlage.

Fig. 2 symbolisiert in einer Übersicht die Abgrenzung der Bereiche Security und Safety.[17] Im Wesentlichen darf ein erfolgreicher Angriff auf das Gesamtsystem in keinem Fall Auswirkungen auf sensible und damit besonders zu schützende Bereiche einer Maschine haben. Besonders müssen auch Angriffswege gesichert werden, wenn über Peripheriegeräte der Steuerungstechnik ein Zugang zu den internen Netzwerken möglich ist. Bekannte Schwachstellen sind dabei auf Basis „Embedded Systems" entwickelte Peripheriegeräte und Funk-Verbindungen zur Datenübertragung (WLAN-Netzwerke und deren Komponenten). Sind Feldbusnetzwerke besonders ausgedehnt und reichen über Gebäudegrenzen hinweg, werden auch bei der Leitungsführung- und -legung gegebenen falls besondere Vorkehrungen notwendig werden.

Die Idee ist, die Bereiche zwischen Prozessleitebene und der Feldebene bis zu der angeschlossenen Sensorik und den Aktuatoren besonders zu schützen.

In Fig. 1 wird diese Abgrenzung als Bereich der Ebene 4 und 5 der Automatisierungspyramide festgelegt. Dort sind auch die Safety Komponenten industrieller Steuerungssysteme angeordnet, die direkt in die Maschinen- und Anlagenfunktionen eingreifen, um die Maschinensicherheit herzustellen und zu gewährleisten. Aber die Maschinensicherheit, die vordergründig den Personen und Anlagenschutz im Fokus hat, ist nur ein Aspekt. Auch die automatisierten Abläufe müssen vor Fremdbeeinflussungen geschützt werden, um die ungestörte Produktion sicher zu stellen.

## 3.4. Einflüsse durch das Industrie 4.0 Konzept

Anhand einiger Beispiele wird beleuchtet, warum durch das Industrie 4.0 Konzept auch indirekte Gefährdungen in ein System hineingetragen werden können.

**Beispiel 1**: Beim Direct-to-Customer-Vertrieb verzichten Produktionsunternehmen auf Zwischenhändler. Dazu werden ERP-Systeme eingesetzt, um multidimensionale Geschäfte genau abzubilden und alle Daten in Echtzeit zu synchronisieren. Durch die Anbindung der Produktion an IoT-Plattformen wird die vollautomatisierte Fertigung nach Kundenwunsch ermöglicht.

Damit erstreckt sich das Schutzkonzept auf den gesamten Bereich der Automatisierungspyramide nach Fig. 1.

**Beispiel 2**: Produkterweiterungen, die mit Hilfe von Industrie 4.0 Lösungen wie von IoT-Plattformen realisierbar sind, ermöglichen es auch die Produkte selbst mit einer Eigenintelligenz auszustatten. Durch geeignete intelligente Sensoriken am Produkt kann über IoT eine direkte und vollautomatische Meldung an ein ERP-System übergeben werden, wann ein Produkt Pflege oder Wartung benötigt. Die Idee dahinter ist die automatisierte Nachbestellung von z.B. Ersatzteilen, die vom gelieferten Produkt ausgelöst werden kann.

[17] Die Zahnräder symbolisieren eine Maschine. Offene Getriebe besitzen ein hohes Potenzial, Menschen zu verletzen oder wenn Teile in das Getriebe fallen, größere Schäden hervorzurufen. Überwachte und verriegelte Abdeckungen verhindern das Öffnen, solange die Maschine arbeitet.

Ein direkter Durchgriff vom Produkt via IoT an ein ERP System ist zwar bequem, aber in Bezug auf die Sicherheit problematisch, wenn die am Produkt angebrachte Sensorik nicht ausreichend gegen Fremdzugriffe geschützt ist oder geschützt werden kann.

**Beispiel 3**: Digitalisierte Nachschubversorgung, z.B. bei einer Fließbandfertigung werden diverse Materialien als just-in-time Anlieferungen automatisiert vom System angefordert. Ziel dazu ist die automatisierte Nach-Befüllung bzw. Nach-Lieferung von Produktionsmaterialien an die Produktionslinie. In diesem Fall tritt die Produktionslinie selbst als Auftraggeber auf.

Hier müssen die Meldungen des Steuerungssystems besonders geschützt werden, um etwa die Möglichkeit von Fehlbestellungen zu verhindern bzw. Anforderungen so erfolgen, dass benötigte Teile zeitgerecht zur Verfügung stehen. Auch hier muss die Fremd-Einflussnahme auf die Datenübertragung besonders geschützt werden.

# 4. Entwicklung des Ansatzes

In der Konzeption eines Modells für ein Sicherheitskonzept müssen zuerst die ablaufenden Prozesse definiert und Risikobewertungen durchgeführt werden. In erster Linie interessiert in dieser Arbeit der Datenfluss an der Schnittstelle des Bereichs Security zum Bereich Safety, wobei die auszutauschenden Daten katalogisiert und klassifiziert werden, die Häufigkeit und Notwendigkeit des Austausches betrachtet und im Rahmen einer Risikoanalyse der Schutzbedarf definiert wird.

Im folgenden Schritt muss der Schutz der Daten vor Angriffen und Missbrauch sichergestellt werden. Bei Safety Komponenten kann der Datenverlust oder die Datenmanipulation zu empfindlichen Gefährdungen von Anlagen oder auch Personen führen. Bei der Leittechnik kann es zu Betriebsstörungen oder sogar zum Betriebsstillstand kommen. Beispiele von erfolgreichen Angriffen mit Schadsoftware wurden weiter oben bereits erläutert (vgl. [BBC14], [BSI18-1], [BSI19]).

Unzulänglichkeiten im Ablauf safety-relevanter Prozesse müssen möglichst bereits im Ansatz erkannt werden. Dazu ist im dritten Schritt das Bereitstellen von Funktionalitäten für die schnelle Erkennung vorzusehen, um mögliche Auswirkungen von Schutzverletzungen gleich im Zustand eines Angriffs zu verhindern. Das wird eher selten möglich sein.

Werden Schutzverletzungen erkannt, sollen im vierten Schritt Sicherheitskomponenten diese aufzeichnen, melden und wenn möglich von sich aus gezielt eingreifen.

## 4.1. Grundlegende Ideen

Im Wesentlichen geht es beim Entwurf eines Modells für die Sicherheit in IACS darum, Gefahren und Gefährdungen durch Sicherheitsmaßnahmen vom System fernzuhalten. Ist diese Funktion nicht zur Gänze gegeben, existieren Schwachstellen im Modell.

### 4.1.1. Allgemeine Anmerkungen

Sicherheit in Unternehmen beschränkt sich in vielen Fällen auf das Bereitstellen von Technologien oder das Implementieren von sogenannten „Best-Practices“. Dabei wird im Wesentlichen bei auftretenden Problemen reagiert. Fallbezogen zu reagieren macht in der Regel ein System nicht sicher. Ein strategischer Ansatz ist es, anstelle von Kontrollmaßnahmen die Sicherheitsrisiken zu bestimmen. Entsprechend der Einstufung der Sicherheitsrisiken werden Prioritäten festgelegt und diese entsprechend ihrer Dringlichkeit bearbeitet. Absolute Sicherheit ist nicht erreichbar. Deshalb müssen Kompromisse im Zusammenhang mit zu treffenden Maßnahmen und deren Ausführung gegenüber möglichen Risiken gefunden werden.

Ansatz dafür ist ein Betriebsmodell zur Gewährleistung der Sicherheit. Das Betriebsmodell muss in einem kontinuierlichen Verbesserungsprozess immer wieder an neue Herausforderungen angepasst werden. Kern des Modells sind klar definierte Verantwortlichkeit für die Durchführung und Aufsicht. In der Regel müssen auch Geschäftsinteressen berücksichtigt werden, weil meist nur knappe Ressourcen zur Verfügung stehen, die nur entsprechend priorisiert

eingesetzt werden können. Erforderlich sind auch Mechanismen für die Überwachung, um einen objektiven Überblick über Sicherheitsrisiken, Sicherheitsmaßnahmen, Implementierung und deren Kontrolle sowie die Wirksamkeit zum Aufrechterhalten eines Sicherheits-Standards festzulegen.

Es ist die Aufgabe der Unternehmensführung zusammen mit internen und externen[18] Fachexperten sowie den in den Unternehmen betroffenen Mitarbeiter*innen ein Ausführungsmodell für die Sicherheit einzuführen. Als Basis wird ein Rahmen festgelegt, der als Orientierungshilfe die Struktur industrietauglicher Konzepte festlegt, um die besten Ansätze zu identifizieren, damit potenzielle Lücken bei der Abdeckung von Sicherheitsanforderungen geschlossen werden können. Ausgehend von den erforderlichen bzw. zur Verfügung stehenden Ressourcen müssen die Risiken abgeschätzt werden. Im Vordergrund stehen dabei kritische Sicherheitsfunktionen. Verfahren zur Messung sollen Sicherheit messbar machen, denn nur was gemessen werden kann, kann auch verbessert werden. Begleitet wird die Einführung des Modells durch Kontrolle und die Verifikation der gesetzten Maßnahmen. Die Verfeinerung des Modells entsteht durch das ständige Durchlaufen der genannten Schritte, um für neu hinzugekommene Risiken immer besser gerüstet zu sein.

### 4.1.2. Begriffsabgrenzung und Einordnung

Ganz allgemein wird unter dem Begriff „Informationssicherheit“ das Sicherstellen des Erreichens und Einhaltens von Schutzzielen verstanden. Schutzziele sind dabei Vertraulichkeit (C - Confidentiality), Integrität (I - Integrity) und Verfügbarkeit (A - Availability), sowohl von technischen als auch nicht-technischen Systemen (vgl. [BSI20]).

Standards zur Informationssicherheit sind unter der Normenreihe ISO/IEC 27000 (Information technology – Security techniques) zusammengefasst. Aufbauend auf dieser Normenreihre und weiterer Normen und Vorschriften wurde vom BSI die „Edition 2020 des IT-Grundschutz-Kompendiums“ veröffentlicht [BSI20]. Im IT-Grundschutz-Kompendium sind insgesamt 96 IT-Grundschutz-Bausteine enthalten, die im Einzelnen jeweils Auswirkungen von Schadensereignissen, deren Abwehr und Sicherungsmaßnahmen sowie typische Beispiele beschreiben.

Die in dieser Arbeit vorgeschlagenen Sicherungsmaßnahmen und Vorgehensweisen orientieren sich am vom BSI veröffentlichen IT-Grundschutzkompendium.

### 4.1.3. Informationssicherheit als Aspekt der Sicherheit

Sicherheit in IACS zu gewährleisten, ist ohne die Betrachtung der Informationssicherheit insbesondere in vernetzten Systemen nicht denkbar. Wird beispielsweise das Schutzziel Vertraulichkeit betrachtet, kommt es immer wieder vor, dass vertrauliche Mitteilungen zwischen Personen fallweise dennoch in der Öffentlichkeit bekannt werden, wenn durch unbedachte Bemerkungen Geheimnisse aufgedeckt werden. Bei der Interaktion technischer Systeme besteht

[18] Die externe Fach-Expertise soll in erster Linie zur Beratung beim Prozess der Einführung und der Implementierung und später zur Evaluierung von eingeführten Maßnahmen in Anspruch genommen werden.

die Möglichkeit, den Austausch von Daten durch Verschlüsselung abzusichern. Der Datenaustausch auf diese Art und Weise ist aber auch nur solange sicher, solange der Schlüssel nicht bekannt ist.

Die Anforderungen an das Schutzziel Vertraulichkeit unterscheiden sich für die unterschiedlichen Bereiche. So werden im Bereich der Verwaltung, der Produktion und der weiteren Abteilungen eines Unternehmens je nach Art der dort genutzten Informationen unterschiedliche Sicherheitsvorkehrungen getroffen werden müssen. Hier bietet es sich an, ein Zonenmodell zu definieren.

Die zentralen Fragen betreffen Safety und Security in Fertigungsanlagen. Deshalb wird das Schutzziel Vertraulichkeit im Sinne der Datenschutz Grundverordnung nicht näher untersucht und in die Überlegung zur Gestaltung des Sicherheitsmodells nur soweit berücksichtigt, wenn technische Aspekte betroffen sind.[19]

Mit dem Schutzziel Integrität wird die Datenintegrität angesprochen. Im Wesentlichen geht es dabei darum, dass die genutzten Daten im gesamten Lebenszyklus genau und gültig sind. Überprüfung und Validierung solcher Daten sind gängige Methoden zur Sicherung der Datenintegrität.

Betrachtet man das Schutzziel Verfügbarkeit, soll der kontinuierliche Ablauf des Geschäftsbetriebs oder der Produktion durch Bereitstellung von Systemen und Applikationen derart erfolgen, dass Systeme und deren Nutzung innerhalb definierter Zeiträume gewährleistet sind und dass darüber hinaus ein Notbetrieb im Katastrophenfall sichergestellt wird.

[19] Gemeinsamkeiten und Unterschiede von Informationssicherheit und Datenschutz:
**Unterschiede**:
Informationssicherheit hat den Schutz der Informationen zum Ziel. Der Personenbezug ist im Gegensatz zum Datenschutz nicht von Interesse.
Der Datenschutz ist gesetzlich geregelt. Innerhalb der EU gilt die Datenschutzgrundverordnung (DSGVO). Vorher gab es in Österreich Regelungen auf Grundlage des Datenschutzgesetzes 2000 (165. Bundesgesetz: Datenschutzgesetz 2000 – DSG 2000) [DSG2000]. Die Informationssicherheit selbst ist nicht klar gesetzlich geregelt. Für die Planung, Implementierung und den Betrieb eines Informationssicherheitsmanagementsystems steht die ISO 27000er Normen-Reihe zur Verfügung und Vorgehensmodelle und Standards, wie beispielsweise den BSI-Grundschutz, oder für den KMU-Bereich ISA Plus. Eine Verpflichtung zur Umsetzung besteht in Österreich nicht.
Informationssicherheit und Datenschutz können nicht voneinander isoliert betrachtet werden. Typische Maßnahmen im Bereich der Informationssicherheit sind eher technisch und organisatorisch. Der Fokus liegt dabei auf Sicherheit des Informationssystems im Sinne ihrer Vertraulichkeit, Integrität und Verfügbarkeit. Maßnahmen im Bereich des Datenschutzes sind zusätzliche weitere (und meist auch nicht-IT spezifische) Fragestellungen wie zugrundeliegende Rechtsfragen.
**Gemeinsamkeiten**:
Sowohl der Datenschutz als auch die Informationssicherheit sind Teilmengen des Informationsschutzes als Ganzes.
Bei beiden Teilmengen des Informationsschutzes ist es unerheblich, ob sich die Schutzziele auf analoge oder digitale Daten beziehen. Die Art der Daten spielt keine Rolle.
Organisatorische Regelungen und technische Maßnahmen haben den Schutz der Informationen und Daten insgesamt zum Ziel. Die beiden Aspekte des Informationsschutzes lassen sich nicht isoliert betrachten, da es ohne Informationssicherheit auch keinen Datenschutz geben kann.

Auch hier bietet es sich an zu klassifizieren. Durch Festlegungen von Kategorien kann ein Maßstab angelegt werden, welche Maßnahmen zur Sicherstellung der Verfügbarkeit getroffen werden müssen. So können Daten, die unkritisch sind, weil sie relativ leicht wiederhergestellt werden können, anders behandelt werden als solche, die bei Verlust zu Ausfällen oder Schäden führen können.

Als besonderer Aspekt der Informationssicherheit wird noch einmal der oben erwähnte „definierte Zeitraum“, innerhalb dessen die Information zur Verfügung stehen muss, hervorgehoben. Dieser Aspekt wird mit rechtzeitig bzw. mit „Echtzeit“ beschrieben. Insbesondere bei industriellen Steuerungen ist die Echtzeitfähigkeit der dort verwendeten Systeme von entscheidender Bedeutung.

### 4.1.4. Ergänzende Aspekte

Neben der Informationssicherheit existieren eine Reihe weiterer Aspekte, die bei der Modellbildung zu berücksichtigen sind. Einige diese Aspekte sind sofort einleuchtend, bei den anderen wird im Rahmen dieser Aufzählung auch kurz begründet, warum die Berücksichtigung des genannten Aspekts als notwendig erachtet wird.

**Authentizität:**

Insbesondere bei der Übertragung und Verarbeitung von sensiblen Daten muss die Authentizität der Kommunikationspartner sowie die Authentizität der Daten sichergestellt sein.

Für die Sicherheit in IACS ist es wichtig, z.B. bei remote Zugriff auf die Anlagen und Maschinen durch Fernwartung sicherzustellen, dass nur den Berechtigten der Zugriff auf die Mess- Steuer- und Regeleinrichtungen, Abfragen vom Maschinenzustand oder von Produktionsdaten und Veränderungen in den Programmen oder Rezepturen ermöglicht wird.

Zur Einordnung im Modell ist die Authentizität ein Aspekt, der jedenfalls beachtet werden muss. In Bezug auf die rein technische Sicherheit von Anlagen kommt diesem Aspekt eine entscheidende Bedeutung zu.

**Verbindlichkeit:**

Verbindlichkeit bedeutet, dass gesetzte Handlungen von Personen nachträglich nicht mehr abgestritten werden können. Der Verursacher ist verantwortlich für die gesetzten Handlungen und den daraus folgenden Konsequenzen. Für die Sicherheit in IACS trifft das z.B. bei Geschäftsabschlüssen im on-line-Vertrieb zu, z.B. Zusagen und Vereinbarungen müssen erfüllt werden (vgl. auch Nicht-Abstreitbarkeit).

Betrachtet man nur die rein technische Sicherheit, dann erschließt sich die Diskussion zu diesem Aspekt nicht unmittelbar. Die Verbindlichkeit wird deshalb dennoch als wichtig angesehen, denn die Sicherheit kann in der Regel auch dadurch erhöht werden, wenn aus Fehlern gelernt wird, und wenn die Entstehungsgeschichte, wie es zu Fehlhandlungen und Fehlern ge-

kommen ist genau rekonstruiert werden kann. Dabei steht nicht die Suche nach den Schuldigen, sondern die Verbesserung von Abläufen für die zukünftige Vermeidung oder Verhinderung im Rahmen eines Verbesserungsprozesses im Vordergrund.

**Nicht-Abstreitbarkeit:**

Eng verwandt mit der Verbindlichkeit ist die Nicht-Abstreitbarkeit. Neben der Nutzung einer Ressource im Sinne der „Zurechenbarkeit“ ist auch die konkrete Zuordnung von Datenmanipulationen zu einem eindeutigen Anwender eine zentrale Forderung für viele Bereiche.

**Zurechenbarkeit:**

Nutzung spezifischer Systemressourcen werden protokolliert. Gründe: der Nutzungsgrad einer Ressource durch die Anwender oder Anwendergruppen erlaubt Rückschlüsse auf Erfolg des Systemeinsatzes. Dazu erhöht dieser Dienst in Kombination mit der Zugriffskontrolle und Nicht-Abstreitbarkeit die Sicherheit, weil damit die unverhältnismäßig intensive oder inhaltlich auffällige Nutzung von Ressourcen aufgedeckt werden kann.

**Verlässlichkeit:**

Verlässlichkeit und die Beherrschbarkeit von Systemen hängen mit Integrität und Verfügbarkeit zusammen. Verlässlichkeit eines Systems ist die Eigenschaft, keine unzulässigen oder undefinierten Zustände anzunehmen (dependability), um damit sicherzustellen, dass spezifizierte Funktionen auch zuverlässig erbracht werden (reliability).

Die vorhandene Funktionalität muss mit der vorher bestimmten Soll-Funktionalität übereinstimmen (Funktionssicherheit).

In der Praxis werden zur Überprüfung verschiedene Testverfahren eingesetzt (z.B. Simulation).

Verlässlichkeit betrifft dabei die Sicherheit des Systems, Beherrschbarkeit die Sicherheit der Betroffenen.

Weitere Maßnahmen sind die Validierung von Eingabedaten, um mögliche Nebenwirkungen zu reduzieren und das bewusste Abfangen von ungültigen Daten.

### 4.1.5. Vereinfachtes Modell

Im vereinfachten Modell geht es um die Regelung des Datenverkehrs eines Unternehmens sowohl nach außen als auch nach innen.

Wenn von Sicherheit gesprochen wird, wird als Sicherheit jener Bereich bezeichnet, in dem das Restrisiko klein wird. In diesem Zusammenhang wird mit Wahrscheinlichkeiten gerechnet, um ein Restrisiko einschätzen zu können. Um absolute Sicherheit zu erreichen, müsse das Restrisiko daher den Wert null annehmen, was wiederum bedeutet, dass alle möglichen Risiken bekannt sein müssen, um eine solche Einschätzung machen zu können.

Um eine möglichst hohe Sicherheit zu erreichen, müssen aus diesem Grund im ersten Schritt alle Risiken bestimmt werden und im zweiten Schritt entsprechende Sicherheitsmaßnahmen

getroffen werden. An dieser Stelle schließt sich die Argumentationskette: auch Sicherheitsmaßnahmen sind nur so lange sicher, solange es keinen Weg gibt diese zu umgehen. Sicherheitsmaßnahmen können nur gegen bekannte Risiken eingeführt werden. Es bleibt der Unsicherheitsfaktor, dass unbekannte Risiken existieren, die bereits vorhandene Sicherheitsmaßnahmen unwirksam machen.

Im Aufbau wird das vorgeschlagene Modell als Schalenmodell konzipiert, bei dem für das Gesamtsystem ein generell gültiger allgemeiner Schutz gegen Angriffe von außen vorgesehen ist und innerhalb des Schutzbereichs zusätzliche Schutzzonen aufgebaut sind, die speziell auf die Bedürfnisse einzelner Bereiche abgestimmt werden.

Risiken entstehen dort, wo mögliche Gefährdungen existieren. Das hier vorgestellte Modell ist deshalb ein Vorgehensmodell für Safety und Security in der Automatisierung technischer Systeme, in denen die entsprechenden Maßnahmen zur Erhöhung der Sicherheit in IACS behandelt werden.

Das Vorgehensmodell für Safety und Security in der Automatisierung technischer Systeme soll zwei Aspekte berücksichtigen: Hauptaspekt ist die Tauglichkeit des Modells für neue Anlagen und neue Systeme. Das Ziel dabei ist es, die Sicherheit möglichst bereits beim Entwurf eines Systems zu erreichen bzw. zu steigern. Nebenaspekt ist es, Teile des Modells auch für bereits bestehende Anlagen und Systeme nutzbar zu machen.

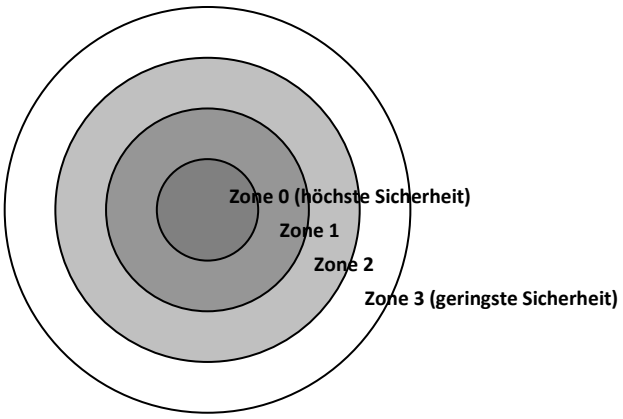



*Fig. 3: Konzentrisches Zonenmodell für Sicherheitsstufen*

Fig. 3 zeigt das konzentrische Zonenmodell für die Berechtigung von Zugriffen auf Datenbestände in einem Unternehmen. Das Modell stellt von außen nach innen die immer höher werdenden Sicherheitsstufen dar. Damit wird in der innersten Abstufung die höchste Sicherheit erreicht. Die Übergänge zwischen den Zonen stellen dabei z.B. die Hindernisse bei Angriffen von außen nach innen dar.[20] Besser ist der Vergleich der Zonengrenzen mit Berechtigungen,

[20] Ein derartiges Zonenmodell ist vergleichbar mit einer Befestigungsanlage, wie diese aus dem Mittelalter bekannt sind (Burgen, Stadtmauern, Zitadellen etc.). Ähnliche Modelle werden z.B. bei der Konzeption von Berechtigungen des Betriebssystems bei der Speicherverwaltung des Arbeitsspeichers genutzt, um zu bestimmen, welche Zonen vor Schreibzugriffen geschützt sind. Voller Zugriff für Schreiben und Lesen von Speicherinformationen ist nur bei der geringsten Sicherheitseinstufung möglich.

Informationen zwischen den einzelnen Bereichen auszutauschen. Bezieht man das Ganze auf ein Modell für die Sicherheit in IACS, müsste die Abstufung anders erfolgen.

In Fig. 4 ist ein Zonenmodell mit individuellen Sicherheitsabstufungen dargestellt. Für diese Darstellung gilt, dass bereits die äußere Zone das Gesamtunternehmen symbolisieren soll und den unberechtigten Zugriff von außen bereits vollkommen abblocken können muss. Die innen dargestellten Bereiche stellen in diesem Fall Abstufungen als Berechtigungen dar, welchen Geschäfts-Bereichen bzw. Personen im Unternehmen der Zugriff auf Datenbestände besonders geschützter Zonen zugestanden werden kann. Derartige Berechtigungen können hierarchisch geordnet sein. In beiden Modellen sind vereinfachend vier Zonen vorgesehen worden. Bezogen auf ein reales Unternehmen können auch weitere Untergliederungen notwendig werden.

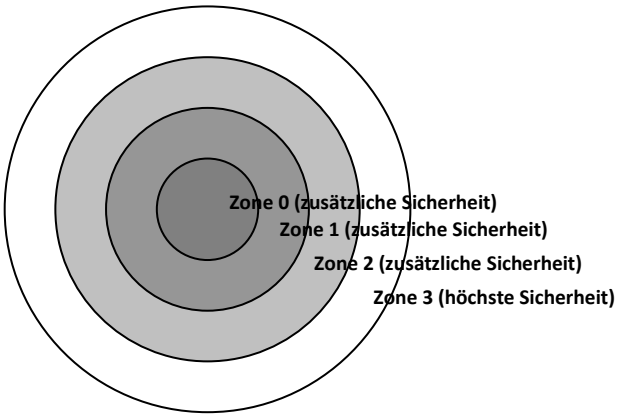



*Fig. 4: Zonenmodell für individuelle Sicherheitsstufen*

Als Interpretation des Zonenmodells kann angenommen werden, dass die zu definierenden Grenzen dieser Zonen im Wesentlichen Zugriffsberechtigungen zur Datennutzung beschreiben. Dabei ist angedacht, Berechtigungen restriktiv auf ein unbedingt erforderliches Ausmaß einzuschränken. Die hier skizzierten Ansätze können auch insoweit kombiniert werden, wenn z.B. ein hierarchisches Modell (ähnlich Fig. 3) als Teilbereich für eine automatisierte Fabrikation genutzt wird, das in ein Gesamtmodell (ähnlich Fig. 4) mit individualisierten Sicherheitsstufen eingebettet worden ist.

### 4.1.6. Steuerung des Modells

Für die Steuerung des Modells ist ein Informationssicherheitsmanagementsystem (ISMS) angedacht. Nach dem BSI-Standard 200-1 besteht ein ISMS aus vielen Bausteinen. In der Folge werden wesentliche Bausteine kurz beschrieben und deren Bedeutung aus Sicht der Informationssicherheit beleuchtet. Insbesondere interessieren die Rollen von bereits genannten Schutzzielen und deren Einordnung in ein Modell.

Die einzelnen Bausteine für ein ISMS sind laut dem BSI-Grundschutz in Bereiche gegliedert. Diese betrachten im Einzelnen die Organisation und Personal, wo allgemeine und übergreifende Anforderungen im Bereich Organisation behandelt werden, die Konzeption und Vorgehensweisen, die sich mit der Erstellung von Datensicherungskonzepten beschäftigt, der Betrieb, der die ordnungsgemäße IT Administration sicherstellt, Detektion und Reaktion, die das

systematische Vorgehen für das Sammeln und Auswerten von Informationen behandelt und wie sicherheitsrelevante Ereignisse zu detektieren sind, Anwendungen, wo es um den Schutz von Informationen geht die mittels Software bearbeitet werden, IT-Systeme, wo die Hardware in den Vordergrund gestellt wird, die Industrielle IT, wobei hier komponentenübergreifende, konzeptionelle und architektonische Sicherheitsanforderungen behandelt werden, Netze und Kommunikation, wobei die Informationssicherheit als integraler Bestandteil der Netzarchitektur und des Netzdesigns gesehen wird und die Infrastruktur, wo die Anforderungen an z.B. Räume und Gebäude aus Sicht der Informationssicherheit behandelt werden (vgl. [BSI20-1]).

Die wesentlichen Bereiche eines ISMS betreffen das Risikomanagement, das Richtlinienmanagement, Auditprogramme, Awareness und Schulungsprogramme, das Kennzahlenmanagement, das Sicherheitsvorfallmanagement und zuletzt das IT-Notfall- und Krisenmanagement.

Das Risikomanagement umfasst die Identifikation, Bewertung und die Behandlung von bestehenden Sicherheitsrisiken mithilfe geeigneter technischer und organisatorischer Maßnahmen.

Beim Richtlinienmanagement in Bezug auf die Informationssicherheit geht es darum, bestehende rechtliche Vorgaben einzuhalten und diese in eigene, innerorganisatorische Vorschriften umzusetzen.

Auditprogramme beschreiben die Planung und Durchführung von System- und Prozessaudits sowie jene von Sicherheitsanalysen (Penetrationstests).

Awareness- und Schulungsprogramme beschreiben die Durchführung von Mitarbeiter*innenschulungen, um deren Awareness gegenüber möglichen Sicherheitsrisiken zu sensibilisieren.

Beim Kennzahlenmanagement geht es um die Kontrolle und Überwachung der getroffenen Maßnahmen, sowie die Messung der Sicherheitsmaßnahmen auf ihre Wirksamkeit und die Bestimmung des Reifegrades von Sicherheitsprozessen.

Sicherheitsvorfallmanagement umfasst die Prüfung und Behandlung von Sicherheitsvorfällen und kritischen Sicherheitsschwachstellen.

Beim IT-Notfall- und Krisenmanagement geht es um die Festlegung und Umsetzung der Notfallvorsorge, das Erstellen von Notfallplänen und Abhalten von Notfallübungen (vgl. [BSI20-1]).

Die einzelnen Bestandteile eines ISMS beschreiben als Ganzes betrachtet einen sich ergänzenden Gesamtprozess.

Dasselbe trifft auch auf die drei Grundsätze der CIA Schutzziele zu (Vertraulichkeit, Integrität, Verfügbarkeit).

Wird das ISMS zusammen mit den CIA Schutzzielen betrachtet, erkennt man, dass sich diese Prozesse und die Schutzziele gegenseitig unterstützen und ergänzen. Wie bereits weiter oben beschrieben, ist es wichtig, eine ausgewogene Mischung der einzelnen Prozesse zu finden und auf die jeweiligen Tätigkeitsbereiche anzupassen.

Betrachtet man zum Beispiel den Bereich Awareness- und Schulungsprogramme, wird es in der Regel unterschiedliche Intensitäten dieser Schulungen für die einzelnen Bereiche geben, wie zum Beispiel Bürodienst in der Verwaltung im Gegensatz zu Mitarbeiter*innen in der Forschung und Entwicklung. Ein Zusammenhang zwischen diesen beiden doch recht unterschiedlichen Bereichen kann durch das Risikomanagement hergestellt werden, wo es um die Identifikation, Bewertung und Umsetzung von Maßnahmen gegen mögliche Sicherheitsrisiken geht. Aufgrund der Definition von bereichsbedingten CIA Schutzzielen können die entsprechenden Schutzziele identifiziert und in Schutzkategorien oder Schutzklassen eingeteilt werden. Die Kriterien dafür sind, welche Informationen bzw. auch Daten immer verfügbar sein müssen, um bei den Änderungen jederzeit nachvollziehbar zur Verfügung zu stehen und zusätzlich welche Mitarbeiter*innen für das Einpflegen oder Verändern zuständig sind. Als weiterer Punkt müsste noch festgelegt sein, welche Zugangsberechtigungen zur Nutzung dieser Daten bestehen, da diese nicht für jeden zugänglich sein dürfen.

**Anmerkung**

Auf die genannte Art und Weise hätte man bei der Bewertung des Risikomanagements auch die CIA Schutzziele mit einbeziehen können. Es lassen sich damit die Risikobewertungen genauer durchführen und die notwendigen und passenden Veränderungen und Verbesserungen umsetzen. Im Falle des genannten Beispiels ergänzen sich Prozesse und Schutzziele gut, das wird jedoch nicht immer so eindeutig der Fall sein.

### 4.1.7. Normen

Zu den relevanten Normen und Standards zur Implementierung eines ISMS zählen die ISO 2700x-Reihe, BSI-Standards sowie IT-Grundschutzkataloge des BSI.

**ISO 2700x**

Die ISO 27000 gibt einen allgemeinen Überblick über ISMS und Zusammenhänge der verschiedenen Standards der ISO 2700x Reihe. Beschrieben sind darin die grundlegenden Prinzipien, Begriffe, Konzepte und Definitionen für ISMS.

Die ISO 27001 ist für das Management von Informationssicherheit der erste internationale Standard, da damit eine Zertifizierung möglich ist. Diese Norm enthält allgemeine Empfehlungen für die Einführung, den Betrieb und der Verbesserung eines dokumentierten ISMS unter der Berücksichtigung von Risiken. Zur praktischen Umsetzung sind keine Hilfestellungen enthalten.

Die ISO 27002 hat zum Ziel, ein Rahmenwerk für das ISMS zu definieren. Sie beschreibt die erforderlichen Schritte, um ein funktionierendes Sicherheitsmanagement aufzubauen und dieses in eine Organisation zu integrieren. Die ISO 27002 dient als Empfehlung für die Management-Ebene und enthält kaum konkrete technische Hinweise.

Die ISO 27005 enthält die Rahmenempfehlungen zum Risikomanagement für Informationssicherheit. Sie unterstützt die Umsetzung aus den Anforderungen der ISO 27001. Auch hier fehlen spezifische Methoden (vgl. [EX18]).

**Zusammenfassung**

Die ISO 2700x ist eine theoretische Zusammenstellung der Parameter, die zur Erstellung eines ISMS benötigt werden. Beispiele für die praktische Umsetzung fehlen weitgehend.

### 4.1.8. BSI-Standards

Der BSI-Standard 200-1 beschreibt Schritt für Schritt, was ein erfolgreiches ISMS ausmacht und welche Aufgaben der Leitungsebene in Behörden und Unternehmen dabei zukommen (vgl. [BSI20-2]). Eine wesentliche Rolle spielen die CIA Schutzziele in den Prozessschritten Initiierung des Sicherheitsprozesses, bei der Erstellung der Leitlinien zur Informationssicherheit und bei der Erstellung und Umsetzung einer Sicherheitskonzeption.

Der BSI-Standard 200-1 löst den BSI-Standard 100-1 ab. Darin werden die allgemeinen Anforderungen an ein ISMS beschrieben. Der Standard ist vollständig kompatibel zur ISO-27001 und berücksichtig Empfehlungen der ISO-27000 und 27002. Dadurch wird der BSI-Standard 200-1 zu einer einfachen, verständlichen und systematischen Anleitung. Diese Anleitung ist unabhängig von den genutzten Methoden, mit denen die Anforderungen umgesetzt werden. Die Inhalte des ISO-Standards sind damit in einem eigenen BSI-Standard übernommen worden, wo auf einzelne Themen genauer und ausführlicher eingegangen worden ist. Auch Fragen, wie die Informationssicherheit im laufenden Betrieb gewahrt und verbessert werden kann, werden im BSI-Standard 200-1 behandelt (vgl. [BSI20-2]).

Der BSI-Standard 200-2 (IT-Grundschutz-Vorgehensweise) beschreibt Schritt für Schritt, wie ein ISMS in der Praxis aufgebaut werden kann und wie es funktioniert. Der Standard geht sehr genau darauf ein, wie ein Sicherheitskonzept in der Praxis erstellt werden kann, wie Sicherheitsmaßnahmen ausgewählt werden und was bei der Umsetzung des Konzeptes zu beachten ist (vgl. [BSI-20-3]).

Die Zielsetzung für die Umsetzung eines ISMS wird vom BSI als *„… den Aufwand im Informationssicherheitsprozess zu reduzieren …“* beschrieben. *„Dazu werden bekannte Ansätze und Methoden zur Verbesserung der Informationssicherheit gebündelt und kontinuierlich aktualisiert.“* [BSI-20-3] BSI nutzt als Beispiel die RECPLAST GmbH.[21] Dort wird beginnend bei der Initialisierung bis zur Zertifizierung nach ISO 27000 die Vorgehensweise schrittweise dargestellt.

Diesem Standard zu folgen bietet sich an, weil aus der Reihe von Vorschlägen jene, die am besten genutzt werden können, an die Gegebenheiten einer Firma angepasst werden können.

Um mit standardisierten Sicherheitsmaßnahmen ein Sicherheitsniveau für Geschäftsprozesse sicherzustellen, müssen diese Prozesse einzeln beurteilt werden. Da die Abläufe etwa in der

[21] Die RECPLAST GmbH ist ein fiktives Unternehmen. Sie dient als Beispiel, wie Maßnahmen eingeführt und umgesetzt werden können (vgl. [BSI18]).

Verwaltung sich von jenen in der Fertigung oder Entwicklung stark unterscheiden, muss entsprechend des Umfeldes für jeden der identifizierten Bereiche die Festlegung organisatorischer, personeller, infrastruktureller und technischer Maßnahmen für sich erfolgen.

Der BSI-Standard 200-3 ist eine Methode zur Risikoanalyse. Dieser Standard löst den BSI-Standard 100-3 ab und hat auf Grund von Anwender*innenkommentaren einige Begriffe der Vorversion präzisiert und ersetzt.

Dieser Standard bietet sich allgemein für Unternehmen an, die bereits erfolgreich den IT-Grundschutz umgesetzt und eingeführt haben. Die dort vorgeschlagene Risikoanalyse ermöglicht nahtlos die ergänzende Sicherheitsanalyse und vervollständigt damit die Grundschutz-Analyse (vgl. [BSI-20-4]).

Wie bereits weiter oben erwähnt, hat auch das BSI eine Musterfirma modelliert, die RECPLAST GmbH, und zeigt anhand dieser Firma die Modellierung und den Aufbau eines Teilnetzes für den Datenaustausch in der Administration. Daher können die in [BSI-20-4] veröffentlichten Gedankengänge mit kleinen Adaptionen auch in einem allgemeinen Sicherheitsmodell als Grundlage für die Einführung und Umsetzung genutzt werden.

Im BSI-Standard 100-4 wird eine Methodik zum unternehmensweiten Notfallmanagement erläutert.

Diese Methodik baut auf dem BSI-Standard 100-2 auf und ergänzt diesen. Der neue Standard befindet sich in Überarbeitung und soll als BSI-Standard 200-4 den alten Standard ersetzen. Für den neuen BSI Standard 200-4 ist geplant, ein Stufenmodell einzuführen. Es soll 4-stufig sein und in einer vereinfachten Einstiegsstufe die Eintrittsbarrieren senken und so den Einstieg erleichtern (vgl. [BSI-20-5], [BSI-20-6]).

**Zusammenfassung**

Die Nutzung der BSI-Standards bieten sich an, weil auch die ISO Normenreihe 2700x mit aufgenommen worden ist. Darüber hinaus ist in der aktuellen Version bereits die vom BSI vorgestellte Musterfirma als Grundlage für die Überlegungen und die Entwicklung eines ISMS innerhalb des geplanten Modells genutzt worden.

### 4.1.9. IT-Grundschutzkataloge

Die IT-Grundschutzkataloge (Stand 2016) wurden vom BSI herausgegeben und geben auf 5082 Seiten eine Übersicht zu einem Modell, das Schichten, Gefährdungen und zugehörige Maßnahmen beschreibt.

Die Schichten sind als Bausteinkataloge untergliedert.

Beispiel zur Verdeutlichung des Aufbaus: Die Schicht 1 enthält 18 Bausteine. Der Baustein B1.5 ist der Schicht 1 zugeordnet und behandelt den Datenschutz aus der Sicht von übergreifenden Aspekten. Der Baustein B2.5 ist der Schicht 2 zugeordnet und behandelt das Datenträgerar-

chiv. Dazu sind jeweils Gefährdungen beschrieben, die ebenfalls in Form von Katalogen dargestellt sind. Um das Beispiel zum Datenschutz fortzusetzen wird unter G2.174 die „Fehlende oder unzureichende Datenschutzkontrolle“ genannt.

Der Mangel ist offensichtlich organisatorischer Natur (Katalog G2). Geeignete Maßnahmen, zusammengefasst in den Maßnahmenkatalogen, sind z.B. das Datenschutzmanagement (M2.501). Die Maßnahme „Datenschutzmanagement“ wird in weiterer Folge ausführlich im Maßnahmenkatalog behandelt.

Trotz des Umfanges des Dokuments können die einzelnen Details rasch aufgerufen werden, da man durch einfaches Anklicken schnell innerhalb des Dokuments navigieren kann (vgl. [BSI20-7]). Fig. 5 zeigt die Schichten und Kataloge für den BSI Grundschutz.

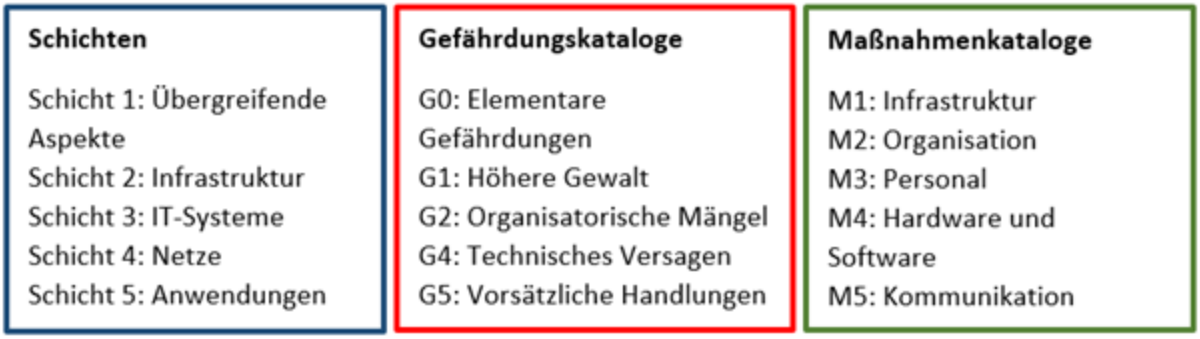



*Fig. 5: Aufbau des BSI-Grundschutzkatalogs nach [BSI20-7]*

### 4.1.10. Einfluss durch das Industrie 4.0 Konzept

Oliver Bendel klassifiziert „Industrie 4.0“ als einen Marketingbegriff. Industrie 4.0 zeichnet sich durch die Individualisierung der Produktion aus. Dabei beginnt die Individualisierung bzw. Hybridisierung der Produkte bereits in der Serienfertigung und die Kunden und Geschäftspartner werden in die Geschäftsprozesse integriert (vgl. [BO19]). Aus diesem Grund sind die Bereiche der Geschäftsprozesse und der Produktion praktisch als „System Industrie 4.0“ zu einer Gesamteinheit zusammengeschlossen. Damit gehen auch die Grenzen zwischen Produktions-IT, Logistik des Vertriebes und der Zulieferindustrie weitgehend verloren, da Produktion und Vertrieb praktisch nahtlos ineinander übergehen. Das bedeutet, dass die unterschiedlichen Sicherheitsanforderungen der betroffenen Bereiche miteinander und zueinander abgestimmt werden müssen. Das betrifft insbesondere die Vernetzung unterschiedlicher Systeme.

Dabei eröffnet die Vernetzung potenziellen Angreifern neue Möglichkeiten, in Systeme einzudringen und auch im Bereich der physischen Welt, z.B. bei Produktionsmaschinen und Anlagen Schäden hervorzurufen, insbesondere dann, wenn bei den Maschinensteuerungen Fernwartungszugriffe notwendig werden.

Die neuen Ansätze für Sicherheitsmodelle trennen den kommerziellen Bereich vom Bereich der Produktion nicht ab, sondern sehen die Sicherheitsmodelle als Gesamtkonzept. Auf der anderen Seite müssen Schäden im Bereich der Produktion deshalb höher bewertet werden,

weil insbesondere bei Produktionsmaschinen und Anlagen auch die dort beschäftigten Personen durch das Versagen von Sicherheitseinrichtungen gefährdet sein können.

Aus diesem Grund beschäftigt sich das in dieser Arbeit vorgestellte Vorgehensmodell insbesondere auch mit zusätzlichen Maßnahmen, die in erster Linie die Produktion und die dort genutzten Sicherheitseinrichtungen besonders schützen sollen. Das bedeutet eine gewisse Abkehr von der Betrachtungsweise von allgemeingültigen Sicherheitsmodellen im Gegensatz zu Modellen, die einzelne Zonen vorsehen, in denen spezifische Sicherheitsmaßnahmen angepasst an die dort herrschenden Gegebenheiten vorgesehen sind.

Im Gegensatz zum offenen Modell soll im Zonenmodell der mögliche Datenverkehr entsprechend eingeschränkt werden. Das Modell sieht vor, dass der Datenaustausch auf die benötigten Daten und Informationen durch entsprechende Filtermechanismen eingeschränkt wird. Die Idee der Filtermechanismen ist, eine Art von Berechtigungen vorzusehen, durch die der Datenaustausch selektiv gesteuert wird.

## 4.2. Schrittweise Verfeinerung

Das IT-Grundschutz-Kompendium [BSI20] ist ein Sammelwerk. Im Kapitel „Elementare Gefährdungen“ werden diese aufgezählt und entsprechende Maßnahmen zur Abwehr bzw. auch zur Schadensminderung diskutiert. Das Kapitel „Prozessbausteine“ ist in Abschnitte untergliedert. Der erste Abschnitt betrachtet den Prozessbaustein „ISMS“ Sicherheitsmanagement allgemein. Dazu werden die Schritte vorgestellt, wie ein Informations-Sicherheits-Managementsystem eingerichtet und weiterentwickelt werden kann. Der zweite Abschnitt „ORP“ beschäftigt sich mit Organisation und Personal, der dritte, „CON“ mit Konzepten und Vorgehensweisen. Das Kapitel „OPS“ behandelt den Betrieb, „DER“ die Detektion und Reaktion. Das Kapitel „System-Bausteine“ ist ebenfalls untergliedert in die Abschnitte „Anwendungen“, „IT-Systeme“, „Industrielle IT“, „Netze und Kommunikation“ und „Infrastruktur“ (vgl. [BSI20]).

Grundsätzlich trägt das Kompendium generell zum hier vorgestellten Modell bei, jedoch sind aufgrund der Fokussierung auf ein Vorgehensmodell für Safety und Security in der Automatisierung technischer Systeme in erster Linie die im Kompendium beschriebenen Themen zu „Industrielle IT“ bzw. „Netze und Kommunikation“ Hauptschwerpunkte in der folgenden Betrachtung.

### 4.2.1. Industrielle IT

Aufgabe der Betriebstechnik ist es, Hard- und Software zu überwachen und zu steuern. Kritische Bereiche sind dabei Lösungen und Automatisierungsaufgaben bei Steuerungs- und Regel Funktionen, bei denen die dort beschäftigten Menschen zu Schaden kommen können. Weil sich der Trend zur Optimierung von Fertigungsprozessen immer mehr beschleunigt, insbesondere getrieben durch die Konzepte von Industrie 4.0, wird die Betriebstechnik der klassischen IT der Administration immer stärker mit der innerbetrieblichen Steuerungstechnik vernetzt.

Das sich daraus ergebende Problem ist, dass sich die Anforderungen an die Verfügbarkeit und Integrität unterscheiden. Störungen in der Betriebstechnik sind in der Regel nicht durch den

Neustart der Anlagen im Gegensatz zu den in Administration verwendeten Geräten möglich (vgl. [BSI20-IND]).

In BSI20-IND sind die entsprechenden Bedrohungen und sich daraus ergebende mögliche Schwachstellen aufgezählt. Als Vorgehensmodell für Safety und Security in der Automatisierung technischer Systeme liegt der Schwerpunkt in dieser Arbeit auf den rein technischen Aspekten. Im Modell werden daher technische Maßnahmen vorgeschlagen, die insbesondere zur Erhöhung der Sicherheit in der Betriebstechnik beitragen.

Die Einführung eines Zonenkonzepts wird auch in BSI20-IND vorgeschlagen. Innerhalb der Zonengrenzen werden dazu entsprechende Maßnahmen zur gegenseitigen Abschottung in das Modell aufgenommen.

In BSI20-IND werden darüber hinaus auch die elektronischen Komponenten, die Maschinen oder Anlagen steuern bzw. regeln, betrachtet und zugehörige Anforderungen an die Sicherheitstechnik gestellt. Durch Referenztabellen werden Zuordnungen von elementaren Gefährdungen zu den entsprechenden Anforderungen hergestellt. Ebenso werden als wichtigster Baustein für die Automatisierung industrieller Anlagen speicherprogrammierbare Steuerungen sowie Sensoren und Aktoren behandelt.

BSI20-IND behandelt auch die technischen Vorrichtungen (Maschinen), die mithilfe von z.B. speicherprogrammierbaren Steuerungen bestimmte vordefinierte Funktionen durchführen. Vielfach sind diese Vorrichtungen jedoch parametrierbar und können durch Fernzugriffe gesteuert werden. Daraus ergeben sich insbesondere bei der Fernwartung Anforderungen an die Sicherheit, die im Modell besonders berücksichtigt werden müssen.

BSI20-IND behandelt sicherheitsgerichtete Steuerungssysteme in einem eigenen Abschnitt. Sicherheitsgerichtete Steuerungssysteme entstehen durch das Zusammenwirken von Sensoren, Aktoren und den zugehörigen Steuerungskomponenten. Im einfachsten Fall sind das Not-Abschaltsysteme, bei denen entsprechende Geber und Auswertegeräte das sichere Abschalten durch Trennen der Energiezufuhr gewährleisten. In der Regel sind aber solche Steuerungssysteme als sicherheitsgerichtete speicherprogrammierbare Steuerungen ausgeführt.

Einfache Not-Abschaltsysteme sind eher unkritisch, Systeme in Verbindung mit sicherheitsgerichteten speicherprogrammierbaren Steuerungen meistens deshalb nicht, weil diese Systeme meist über Kommunikationsverbindungen mit den übrigen Anlagen verbunden sind und interagieren. Von besonderer Bedeutung sind folgende Schwachstellen:

- Die Manipulation des Logiksystems, bei dem das Anwenderprogramm beeinflusst werden kann. Dabei kann unterschieden werden, ob die Sicherheitsfunktion die Steuerung auslöst, also die Manipulation erkennt, oder nicht.
- Neben der Manipulation des Logiksystems spielt auch die verwendete Software eine besondere Rolle. Als wesentliche Funktion des Automatisierungssystems müssen die Betriebszustände der ablaufenden Prozesse ausreichend überwacht werden. Werden die entsprechenden Überwachungsmöglichkeiten programmtechnisch nicht vorgesehen,

werden ungewöhnliche bzw. auch sicherheitsrelevante Ereignisse nicht entsprechend erkannt. In solchen Fällen kann auch eine sicherheitsgerichtete Steuerung nicht adäquat reagieren (vgl. [BSI20-IND]).

### 4.2.2. Sicherheit für Maschinen und Anlagen, Maschinenrichtlinie

Maschinensicherheit wird durch gesetzliche Regelungen und zugehörige Normen bestimmt. Die „Maschinenrichtlinie“ 2006/42/EG ist in ihrer aktualisierten 2. Auflage ein Leitfaden, der seit dem Ende 2009 verpflichtend anzuwenden ist.

Sicherheitseinrichtungen für maschinelle Anlagen müssen entsprechend dieses Leitfadens insbesondere für neue Anlagen vor dem Inverkehrbringen von Maschinen und Anlagen vorgesehen sein.

Dieser „Leitfaden für die Anwendung der Maschinenrichtlinie 2006/42/EG Auflage 2.2 – Oktober 2019 (Aktualisierung der 2. Auflage)“ [EK19] ist die Grundlage für die Ausrüstung von Maschinen und Anlagen. Das darin beschriebene Modell und die Vorgehensweise bildet die Grundlage zum Aufbau und zur Gestaltung des Sicherheits-Modells.

### 4.2.3. Netze und Kommunikation

Geschäftsprozesse benötigen Daten aus der Produktion und die Produktion wird aufgrund der Ergebnisse von Geschäftsprozessen gesteuert. Aus dem Wechselspiel der Kommunikation und den technologischen Fortschritten in der Messtechnik stehen immer mehr Daten zur Verfügung. Damit ist der Stellenwert des Datenaustausches und der Datennutzung in der industriellen IT stark angewachsen.

Daraus bedingt sind zur Sicherstellung eines hohen Sicherheitsniveaus zusätzliche sicherheitsrelevante Aspekte zu berücksichtigen. Im weiter oben skizzierten Schalenmodell können die unterschiedlichen Gerätegruppen z.B. derart voneinander getrennt werden, dass nur erforderliche Daten ausgetauscht werden können, um die Sicherheit zu erhöhen.

Im IT-Grundschutz Kompendium ist den Netzen und der Kommunikation ein eigener Abschnitt gewidmet. [BSI20-NET] Dort werden Gefährdungen und entsprechende Maßnahmen sowohl die Geräte Technik als auch die Kommunikationstechnik entsprechend behandelt. Insbesondere wird die Separierung von Infrastrukturdiensten und die Zuweisung definierter Subnetze empfohlen. Bei hoch verfügbaren Komponenten wie diese in der Sicherheitstechnik für Maschinen und Anlagen eingesetzt werden, lautet die Empfehlung Redundanzen vorzusehen.

Um den Datenaustausch zwischen den einzelnen Subnetzen zu regeln, werden Firewalls eingesetzt. Diese dienen dazu die Datennetze sicher zu koppeln. Mithilfe einer entsprechenden Firewall-Struktur wird der Informationsfluss entsprechend vorher festgelegten Regeln eingeschränkt (vgl. [BSI20-NET]).

## 4.3. Ansatz

Das IT-Grundschutz Kompendium zeigt für denkbare Gefährdungen in der Form von Empfehlungen Möglichkeiten, die IT-Sicherheit sicherzustellen bzw. zu erhöhen. Dabei ist die Gliederung sehr detailliert gewählt, sodass alle Eventualitäten abgedeckt werden können. Handlungsempfehlungen zeigen dabei Wege zur Verbesserung und werden in praktikable Sicherheitsempfehlungen überführt (vgl. [BSI20]).

Der Ansatz orientiert sich an der so genannten „Defense-in-Depth-Strategie“. Dieser Begriff sagt aus, man sollte Angreifer mit möglichst vielen Verteidigungslinien hindern. Das entspricht den weiter oben diskutierten Zonen. Dazu werden Daten-, Informations- und operationelle Sicherheit umfassend und in der Tiefe betrachtet. Dieses Konzept kann bereits als ein Standard betrachtet werden. Damit kann ein solcher Standard auch angepasst an die Aufgabenstellungen der Prozessleittechnik für Anlagen und Maschinensteuerungen im industriellen Umfeld genutzt werden.[22]

Sicherheit in der industriellen IT unterscheidet sich zum Teil von der kommerziellen. Grundsätzlich muss die Sicherheitsstrategie einer Organisation jene Werte schützen, die als erfolgskritisch betrachtet werden müssen. Während der kommerzielle Bereich hauptsächlich von der Vertraulichkeit der Geschäftsprozesse abhängig ist, sind es im Bereich der Anlagen und Maschinensicherheit die Sicherheit der dort beschäftigten Personen, Sachgütern und der Umwelt. Damit stehen im industriellen Umfeld die Verfügbarkeit und die Korrektheit der dort genutzten Anwenderprogramme im Vordergrund des Interesses.

Das Aneinanderreihen von Sicherheitsstufen muss mit der Überwachung, Erkennung und Reaktion auf bestimmte Ereignisse einhergehen. Cyber-Angriffe können grundsätzlich nicht verhindert werden, deshalb ist die rasche Erkennung mit darauffolgender Isolierung und Abwehr die wichtigste Aufgabe. Dazu muss kommen, dass mögliche Folgen weitgehend gemindert werden.

Das Defense-in-Depth Konzept muss einzelne Technologien und die Software-Applikationen vereinigen. Dazu werden alle Ressourcen und deren Zusammenwirken als Schutz zur Überwachung und zur Reaktion gegen Cyber-Bedrohungen benötigt. Innerhalb des Konzepts müssen folgende Bereiche berücksichtigt werden:

- Bedrohungen und Schwachstellen müssen erhoben bzw. bestimmt werden. Hier sind es die möglichen Absichten der Angreifer, deren Fähigkeiten und die möglichen Gelegenheiten für Angriffe.
- In Bezug auf den Betrieb, des Personals und der Technologie müssen Sicherheitsstandards mit den zugehörigen Kontrollmaßnahmen definiert werden. Dazu kommen noch die entsprechenden Gegenmaßnahmen, die vorgesehen werden sollen. Im Wesentlichen fallen

[22] Der Verband Schweizerischer Elektrizitätsunternehmen (VSE) hat in seiner Veröffentlichung „Handbuch Grundschutz für «Operational Technology» in der Stromversorgung“ [VSE18] sein Defense in Depth Konzept für Storm Versorgungsnetze in der Schweiz vorgestellt.

in diesen Bereich die Kontrollen, Überwachung, das Festlegen von Richtlinien und Prozessen. Darüber hinaus ist die Sensibilisierung der betroffenen Beteiligten z.B. durch Unterweisung und Schulungsmaßnahmen notwendig.

Bei der Implementierung müssen die Unterschiede zwischen dem kommerziellen IT-Umfeld und dem Bereich der Fertigung beachtet werden. Auch bei Abteilungen wie Forschung und Entwicklung sind spezielle Erfordernisse zu berücksichtigen. So sind z.B. kritische Daten und kritische Informationen als Geschäftsdaten, Finanzdaten und Personaldaten, anders zu bewerten als Daten aus Leitsystemen, Sensordaten und Daten aus Abteilungen wie Forschung und Entwicklung. Ähnlich ist es bei der Verfügbarkeit: diese ist im kommerziellen Bereich wenigstens während des Bürobetriebs sicherzustellen, während in der Fertigung die Verfügbarkeit in Echtzeit und praktisch 24 Stunden pro Tag gegeben sein muss. Ein wesentlicher Unterschied besteht in der genutzten Technologie bzw. in der Lebensdauer der verwendeten Geräte. Automatisierungsgeräte haben eine Lebensdauer von zehn und mehr Jahren und werden innerhalb ihrer Lebensdauer in der Regel nicht ersetzt. Dementsprechend bleibt deren Stand in Bezug auf die Informationssicherheit gegenüber den neu hinzukommenden Bedrohungen konstant auf einem mit der Zeit veraltetem Stand der Technik und bedingt zusätzliche Sicherheitsmaßnahmen. Der Ersatz älterer Einheiten ist teilweise aus technischen Gründen nicht einfach möglich oder wirtschaftlich vertretbar. Demgegenüber können die kommerziell genutzten Geräte in kürzeren Zeiträumen relativ kostengünstig ersetzt werden.

Bei der Umsetzung werden organisatorische und technische Maßnahmen koordiniert eingesetzt.

Zu den organisatorischen Maßnahmen zählen das Bestimmen von Verantwortlichen sowohl für die Organisation und die Kontrolle. Es werden Richtlinien bestimmt und die zugehörigen Handlungsanweisungen. In den Handlungsanweisungen werden auch die Prozesse für das Einrichten und das Aufrechterhalten von Sicherungsmaßnahmen festgelegt. In weiterer Folge wird das genutzte Inventar bestimmt. In Bezug auf das Inventar wird z.B. auch festzulegen sein, in welchen Zeiträumen Geräte zu ersetzen sind. Risiken sind durch das Aufstellen von Bedrohungsszenarien und Schwachstellenanalyse zu identifizieren, einzuschätzen und zu bewerten. Mit Hilfe von Maßnahmen, die eventuell katalogisiert sein können, wird die Umsetzung und Überprüfung gesteuert. Ein wesentlicher Faktor ist der Mensch. Organisatorisch sind Trainings, Schulungen und Unterweisungen und vor allen die Sensibilisierung der betroffenen Personen und Personengruppen einzuplanen.

Organisatorische Maßnahmen sind die Voraussetzungen zur Erlangung der Basissicherheit. Die zugehörigen technischen Maßnahmen sind abhängig von der Art der Unternehmen und deren Ausstattung. Im Bereich der Technik und im Betrieb geht es um die physische Sicherheit und um die Architektur der genutzten Netzwerke (Grundlegendes, Einzelelemente, Gruppierungen und Kommunikationsschnittstellen). Hauptpunkte in Bezug auf die technische Sicherheit sind das Festlegen von Grundsätzen für Übergänge von Zonen, Authentifizierung und Feststellen von Berechtigungen insbesondere auch bei Remotezugriff. Ein Grundsatz für die technische Sicherheit ist auch das Management von Back-ups.

Kommt es zu Sicherheitsvorfällen müssen diese entsprechen behandelt werden.

Als Vorgehensmodell für Safety und Security soll der Grundschutz für alle Bereiche eines betrachteten Unternehmens gelten, also für Verwaltung, Fertigung, Vertrieb und Logistik, Forschung und Entwicklung. Die Anforderungen in den genannten Bereichen sind unterschiedlich und damit auch die zu treffenden Maßnahmen. Je nach Art des Betriebes werden die Anforderungen etwa für IT-Sicherheit in der Verwaltung ähnlich sein, in den anderen Bereichen sich aber aufgrund unterschiedlicher Produkte stark unterscheiden. Speziell für den Bereich der Fertigung, wo es um die Automatisierung technischer Systeme geht, sind entsprechende Anpassungen an die dort hergestellten Produkte notwendig.

**Diskussion**

Der Fokus dieser Arbeit liegt bei einem Vorgehensmodell für Safety und Security in der Automatisierung technischer Systeme. Bezogen auf den oben diskutierten Ansatz kann festgestellt werden, dass bei neu zu errichtenden Anlagen oder maschinellen Einrichtungen entsprechende Konzepte vergleichsweise einfacher erstellt werden können als bei bestehenden. Bei bestehenden Anlagen oder maschinellen Einrichtungen ergibt sich die Schwierigkeit, dass Gegebenheiten zu berücksichtigen sind, die bestimmte Maßnahmen möglicherweise erschweren oder nicht zulassen. In solchen Fällen muss der Ansatz entsprechend adaptiert werden.

Um ein neues Sicherheitsmodell zu erstellen oder ein vorhandenes zu verbessern wird schrittweise vorgegangen. Diese Schritte sollten zur kontinuierlichen Verbesserung regelmäßig überprüft und gegebenen falls neu eingeordnet und wiederholt werden.

**Schritt 1: Priorisieren und Bestimmung des Umfangs**

Es werden die Geschäftsziele und übergeordneten organisatorischen Prioritäten identifiziert. Mit diesen Informationen wird strategisch entschieden, wie bezüglich der Implementierung der Sicherheit und des bestimmten Umfangs der Systeme und Ressourcen ausgewählte Geschäftsbereiche oder Prozesse unterstützt werden. Das Modell kann angepasst werden, um die unterschiedliche Geschäftsanforderungen und die damit verbundene Risikotoleranz festzulegen.

**Schritt 2: Orientierung**

Orientierung ist der Umfang des Programms für die Bestimmung der Sicherheitsbereiche für Geschäftsbereiche oder Unternehmensprozesse. Diese werden bestimmt und regulatorische Anforderungen festgelegt. Es werden dazu Bedrohungen und Schwachstellen für die Definition eines Sicherheitsmodell gesucht.

**Schritt 3: Erstellen eines Profils**

Es wird ein aktuelles Profil für das Unternehmen erstellt, indem angegeben wird, welche Ergebnisse in Bezug auf die Sicherheit aktuell erzielt werden können.

**Schritt 4: Risikobewertung**

Die Risikobewertung sollte sich am gesamten Risikomanagementprozess des untersuchten Falles oder an früheren Aktivitäten zur Risikobewertung orientieren. Es wird das Betriebsumfeld analysiert, um die Wahrscheinlichkeit eines Sicherheitsvorfalles und dessen Auswirkungen zu ermitteln. Es ist wichtig, dass Unternehmen versuchen, aufkommende Risiken sowie Daten zu Bedrohungen und Schwachstellen zu berücksichtigen, um ein solides Verständnis der Wahrscheinlichkeit und der Auswirkungen von Sicherheitsvorfällen zu ermöglichen.

**Schritt 5: Zielprofil**

Für das Unternehmen wird ein Zielprofil erstellt, das sich auf die Bewertung konzentriert und die gewünschte Zielvorstellung zum Erreichen oder zur Erhöhung der Sicherheit beschreibt. Bezüglich der Kategorisierung können auch eigene und zusätzliche Kategorien oder Unterkategorien entwickelt werden, um eindeutige organisatorische Risiken zu berücksichtigen.

**Schritt 6: Bestimmen, analysieren und priorisieren von Lücken**

Zum Bestimmen, Analysieren und Priorisieren von Lücken werden für das Unternehmen das aktuelle Profil und das Zielprofil verglichen, um Unterschiede bzw. Lücken zu ermitteln. Darauf wird ein priorisierter Aktionsplan erstellt, um diese Lücken zu schließen. Es ist auch eine Kosten-Nutzen-Analyse notwendig. Damit werden die erforderlichen Ressourcen bestimmt. Das Nutzen von Profilen erleichtert fundierte Entscheidungen der Unternehmensführung, kostengünstige und zielgerichtete Verbesserungen zu ermöglichen.

**Schritt 7: Aktionsplan**

Der Aktionsplan legt für ein Unternehmen fest, welche Maßnahmen in Bezug auf die Lücken zu ergreifen sind. Falls solche vorhanden sind, wurden sie im vorherigen Schritt identifiziert. Anschließend wird die aktuelle Sicherheit anhand des Zielprofils überwacht. Die Standards, Richtlinien und Praktiken, einschließlich von branchenspezifischen, die am besten geeignet sind, werden von der Unternehmensleitung unter Mitwirkung der Fachexperten festgelegt.

Für das Vorgehensmodell bedeutet das, dass zielgerichtet Sicherheitslücken gesucht werden müssen. Für solche Lücken werden in der Form von typischen Lösungsansätzen Bausteine vorgeschlagen, die als Vorlage dienen, spezielle, von der jeweiligen Konfiguration abhängige Lücken zu schließen. Ein neu erstelltes Sicherheitskonzept setzt sich aus der Summe solcher Einzelmaßnahmen zusammen und muss nach der Einführung evaluiert werden.

Das Schließen von Sicherheitslücken und Verbesserungsmaßnahmen zur Erhöhung der Sicherheit können sehr kostenaufwändig sein, so dass auch das Kosten-Nutzen Verhältnis in die Überlegungen mit aufgenommen werden muss. Die Entscheidung für die Umsetzung ist abhängig vom Restrisiko zu treffen und der Geschäftsleitung zu überlassen. Die Kostenfrage bleibt in dieser Arbeit unberücksichtigt. Dazu zählt der Aspekt, wenn etwa Maßnahmen zur Erhöhung der Sicherheit auch den Arbeitsablauf beeinträchtigen. Ein Beispiel dafür ist, wenn bei Einstell- oder Wartungsarbeiten an einer Maschine oder Anlage es notwendig wird, Produktionsabläufe aus Sicherheitsgründen teilweise zu unterbrechen.

# 5. Vorgehensmodell

Hauptforderung an das Vorgehensmodell ist, dass der Rahmen dafür in seiner Struktur industrietauglich ist. Bei der Modellentwicklung stehen die Sicherheitsanforderungen deshalb an erster Stelle. Bei einer allgemeinen Abschätzung von Risiken bleiben erforderliche bzw. zur Verfügung stehende Ressourcen außer Betracht. Berücksichtigt wird jedoch die Frage nach der Messbarkeit, damit die Wirksamkeit von Maßnahmen eingeordnet werden kann.

Um das Modell anpassbar und vor allem auch erweiterbar zu machen, werden Teilmodelle beschrieben, die maßgeschneidert auf unterschiedliche Anforderungen zu einem individualisierten Modell zusammengestellt werden können.

Insbesondere die Erweiterbarkeit ist notwendig, um das Modell flexibel zu gestalten. Nichtzutreffende oder noch nicht behandelte Sicherheitsanforderungen sollen dazu ohne wechselseitige Beeinflussung der Gültigkeit der Modellannahmen ergänzt oder weggelassen werden können.

## 5.1. Entwicklung des Modells

Die Modellannahmen sind zu definierende Sicherheitsrisiken. Dazu müssen die Risiken bewertet werden.

Die ISO/IEC 27005 - Leitfaden für das Informationssicherheits-Risikomanagement ist ein kostenpflichtig erwerbbarer Leitfaden für das Informationssicherheits-Risikomanagement. Die ISO 31000 Serie ist eine Norm für Risiko Management. Einen guten Überblick zu den erforderlichen Schritten zur Risikobewertung zeigt Fig. 6.

Fig. 6 zeigt den Prozess zur Beurteilung von Risiken. Risiken sind immer im Kontext mit seiner Umgebung zu bewerten (Fig. 6 (2)) und ist ein schrittweiser Prozess. Risiken müssen identifiziert, analysiert und bewertet werden (Fig. 6 (3.1 bis 3.3), wobei bei jedem Teilschritt die Einflüsse aus Überwachung (Fig. 6 (1)) und Kommunikation (Fig. 6 (5)) in die Überlegungen mit aufgenommen werden müssen. Die erkannten Risiken müssen dann entsprechend behandelt werden (Fig. 6 (4)). Risiken können sich ändern, deshalb ist der Prozess der Risikoanalyse immer wieder neu zu durchlaufen. Auch die ISO 31000 Serie ist nicht frei verfügbar.

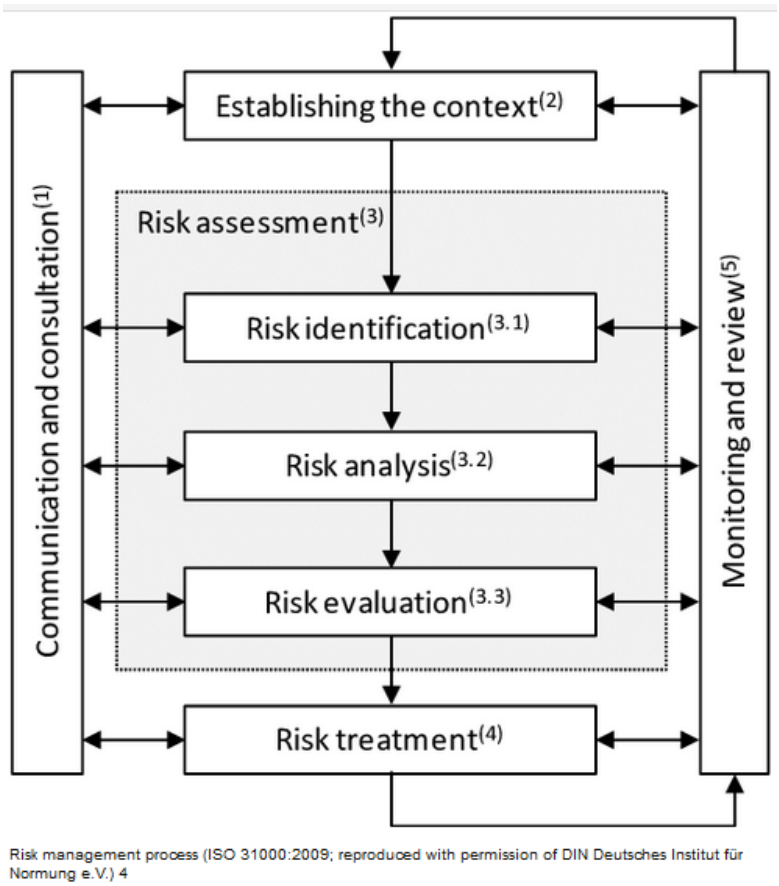



*Fig. 6: Risikomanagementprozess nach ISO 31000:2009 [Marija Bertovic] [BM15]*

In diesem Abschnitt wird stattdessen auf frei verfügbare Quellen zurückgegriffen. Der vom BSI herausgegebene „Gefährdungskatalog Elementare Gefährdungen“ [BSI11] beschreibt 46 mögliche elementare Gefährdungen und gibt Beispiele dazu an. In [BSI20] ist neben den genannten noch eine weitere Gefährdung als „G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe“ klassifiziert worden.

Entsprechend dem Aufbau des BSI-Grundschutzkatalogs nach [BSI20-7] werden die dort beschriebenen Gefährdungskataloge in die weiteren Betrachtungen mit eingebunden. Dabei werden in das Modell in erster Linie Verbesserungsmaßnahmen im Bereich der Organisation, der Technik und in jenen, wo Personen die Sicherheit wesentlich beeinflussen können, aufgenommen. Weitere Gefährdungen werden nur der Vollständigkeit halber am Rande erwähnt.

Elementare Gefährdungen sind z.B. Naturkatastrophen. Die Eintrittswahrscheinlichkeit für Naturereignisse ist vom Standort abhängig. Standorte müssen bereits bei der Planung berücksichtigt werden. Es sollte angenommen werden, dass aufgrund der Standortwahl diese Wahrscheinlichkeit gering sein sollte. Dennoch kann es zu katastrophalen Zwischenfällen kommen (z.B. Fukushima). Die Folge war der Ausfall der Stromversorgung, die katastrophale Folge war der Ausfall der Kühlsysteme (Folgeursache einer kausalen Kette von Ereignissen). Elementare Ereignisse sind aber auch z.B. Feuer, Wasser, Verschmutzung etc., die einen Betrieb gefährden und wo z.B. durch entsprechende bauliche Maßnahmen die Sicherheit erhöht werden kann.

Ernst zu nehmen ist die Gefährdung durch Ausfall oder Störung der Stromversorgung. Trotz der hohen Versorgungssicherheit kann es immer wieder zu Ausfällen oder Störungen kommen, die insbesondere die IT-Infrastruktur beeinträchtigen können. Schon eine Unterbrechung über mehrere Minuten hinweg ist geeignet, nicht nur die von der Informationstechnik abhängigen Prozesse und Vorgänge entscheidend zu stören. Störfaktoren sind dabei der Ausfall der Beleuchtung, der Gebäudeinfrastruktur, der gesamten IT, der Kommunikationseinrichtungen und in der Fertigung die gesamte Produktion. Gegenmaßnahmen gegen den Ausfall sind je nach Wichtigkeit der gefährdeten Bereiche unterbrechungsfreie Stromversorgungen bzw. Notstromaggregate.

Störungen könnten durch Netzschwankungen verursacht werden (z.B. durch Überspannungen). Dabei kann es zu Fehlfunktionen bis hin zur Beschädigung elektrischer Geräte kommen (vgl. auch [BSI11]).

Besonders hervorzuheben ist die Gefahr des Datenverlustes, ausgelöst durch Defekte in der Stromversorgung, die in der Folge die Zerstörung von Geräten oder Datenträgern verursachen kann.

Ausfall oder Störung von Kommunikationsnetzen: nahezu alle Geschäftsprozesse (in der Organisation, Verwaltung aber auch im Betrieb) sind von der Möglichkeit des Datenaustausches abhängig.

Abhängig vom Datenaustausch sind z.B. Geschäftsprozesse, wo benötigte Informationen als Basis für Entscheidungen meist sehr rasch gebraucht werden und nicht direkt abgerufen werden können. Aufträge z.B. können nicht angenommen, bearbeitet oder abgeschlossen werden. Aber auch die Produktion ist von der Kommunikation abhängig, wenn Daten von der Sensorik nicht mehr an die zentralen Recheneinheiten geliefert werden können und im schlechtesten Fall eine Produktion teilweise oder zur Gänze stilllegen. Ähnliches gilt für die Lagerlogistik, wenn die produzierten Waren weder ein- noch ausgelagert werden können bzw. wenn der Lagerort von Waren nicht mehr festgestellt werden kann und damit die Abwicklung von damit zusammenhängenden Geschäftsprozessen gehemmt oder verhindert wird (vgl. auch [BSI11]).

Ausfall oder Störung von Versorgungsnetzen: diese Art von Gefährdung summiert eine ganze Reihe unterschiedlicher Bereiche, die im Wesentlichen in den Bereich der Gebäudeinfrastruktur fallen. Die Art der möglichen Störungen ist sehr vielfältig und diese überdecken oder ergänzen sich zum Teil mit bereits genannten Beispielen (vgl. auch [BSI11]). Diese sind zwar im Hinblick auf Verbesserungen der Sicherheit als Vorsorgemaßnahmen wichtig, werden hier aber nicht weiter im Detail behandelt.

Elektromagnetische Störstrahlung: die elektromagnetische Verträglichkeit von Geräten auf der einen Seite und die Emission elektromagnetischer Störstrahlung durch Geräte auf der anderen Seite findet oft zu wenig Beachtung. Insbesondere Netzgeräte wandeln die Netzspannung in die erforderlichen Versorgungsspannungen um und erzeugen dabei Abstrahlung und Rückwirkungen in das Versorgungsnetz, die die empfindliche Elektronik in IT-Einrichtungen

stören und zerstören kann. In der Produktionsanlage von Firmen werden Drehzahlregelungen von Antrieben vielfach über Frequenzumformer realisiert, die aufgrund ihrer Arbeitsweise starke Rückwirkungen auf das Versorgungsnetz haben. In diesem Zusammenhang spricht man oft von „versauten“ Netzen. Aber nicht nur die Produktion selbst, sondern auch die Verwendung von drahtlosen Verbindungen (z.B. Funknetze) beeinflussen durch ihre Abstrahlung empfindliche Elektronik, weil entsprechend der Sendeleistung in den elektrischen Verbindungen Spannungen induziert werden können, die bis zur Zerstörung von Bauteilen reichen kann (vgl. [KG12]).

Ausspähen von Informationen und Spionage: dieser Punkt ist für Firmen von besonderer Bedeutung, weil Kundenbeziehungen, Geschäftsabläufe, Abläufe in der Produktion, Vorhaben in Forschung und Entwicklung zu den wichtigsten Geschäftsgeheimnissen zählen. Bei den Kundenbeziehungen sind es Daten wie Liefer- und Zahlungskonditionen und Zahlungsverhalten der Kunden, bei den Geschäftsabläufen Interna zur Organisation, bei der Produktion besondere Produktionsmethoden und bei Forschung und Entwicklung Vorhaben für neue Produktionen, Verbesserung von Produktionen und die Entwicklung von Produkten.

Sofern es sich dabei auf Angriffe auf die IT-Systeme handelt, müssen dazu entsprechende Sicherheitsmaßnahmen getroffen werden, die an die Firma angepasst sind (vgl. auch [BSI11]).

Diebstahl von Geräten, Datenträgern und Dokumenten: das sollte durch die entsprechenden organisatorischen Maßnahmen bereits gesichert sein. Ähnlich ist es mit den weiteren Punkten, wobei z.B. bei dem Ausfall von Geräten oder Systemen entsprechende Redundanzen vorgesehen werden müssen. Wichtig ist es auch entsprechende Vorkehrungen gegen Fehlfunktionen von Geräten oder Systemen zu treffen.

Menschliche Fehlhandlungen: IT-Systeme können durch fehlerhafte Nutzung beeinträchtigt werden. Es gibt Mängel aufgrund unzureichender Regelungen von Zuständigkeiten und von Kontrollen, wie z.B. Passwortsicherheit, unkontrollierte Vergabe von Rechten und fehlerhafte Administration von IT-Systemen.

Technisches Versagen: Zum technischen Versagen zählt z.B. der Ausfall von Datenträgern (Datenverlust), keine oder fehlerhafte Backups, defekte Datenträger in der Langzeitarchivierung etc.

Ein nicht zu unterschätzender Risikofaktor sind die handelnden Personen. Sie können fahrlässig oder vorsätzlich Handlungen setzen. Social Engineering ist das gezielte Aushorchen oder Manipulieren von Mitarbeitern (online über die sozialen Netzwerke oder offline durch persönlichen Kontakt) meist zum Ausspähen spezifischer Unternehmensinformationen. Social Engineering ist oft die Vorstufe eines Angriffs auf das IT-System.

Missbrauch von Fernwartungszugängen: Fernwartungszugänge bestehen in größeren Unternehmen sowohl für interne Zwecke als auch für externe Service- und Wartung. Analog zum Risiko des unerlaubten Eindringens in ein Gebäude, stellen auch solche Wartungszugänge ein latentes Risiko für die IT und für die informationstechnischen Einrichtungen zur Steuerung von Maschinen und Anlagen dar.

## 5.2. Technische Umsetzung

Abschottung von Teilnetzen wird als Option kontroversiell gesehen, weil Betreiber vor der Installation von Sicherheitsmaßnahmen eine gewisse Scheu haben. Eine Begründung dafür könnte der große Aufwand sein, den IT bewährte Sicherheitslösungen mit sich bringen. Abgesehen von den meist erheblichen Kosten ist ein großer Konfigurationsaufwand für Firewalls, Router, Benutzerkonten etc. erforderlich. Bereits in der IT bekannte Maßnahmen lassen sich oft nicht 1:1 auf den Schutz von Netzwerken der Automatisierungstechnik übertragen, ohne dass deren Verfügbarkeit beeinträchtigt wird. Abschottung zum Zweck des Datenschutzes wiederspricht auch der Idee nach einer weltweiten Vernetzung der Produktion.

Die Hauptidee bei der technischen Umsetzung des Modells ist, selektive Abschottungen vorzusehen, bei denen nur ganz bestimmte Daten für die Interaktion mit benachbarten Systemen freigegeben werden.

Grundsätzlich wird davon ausgegangen, dass unzulässige Veränderungen von Speicherinhalten für Fehlreaktionen bzw. Fehlfunktionen verantwortlich gemacht werden können.

Für die Umsetzung bedeutet das, dass die auf diese Art und Weise verbundenen Einheiten als eigene Subbereiche („Inseln“) mit einer eigenen Sicherheitszone ausgestattet werden, in der ein Monitoring auch innerhalb solcher „Trusted Zonen“ stattfindet.

In der modernen Fertigungstechnik, insbesondere nach den Konzepten von Industrie 4.0, existiert eine hohe Anzahl von Zugangspunkten zum Netzwerk. Die steigende Vernetzung intelligenter Geräte und Komponenten machen auch innerhalb von Automatisierungsnetzwerken das sicherheitsrelevante Monitoring notwendig. Es geht dabei grundsätzlich um die Kenntnis, wie der Datenaustausch innerhalb der Automatisierungsnetze erfolgt und welche Informationen nach außen weitergegeben werden müssen.

Aus der Sichtweise der Automatisierungstechnik steht die Produktionssicherheit im Vordergrund: der kontinuierliche Betrieb muss sichergestellt sein. Aus Sicht der IT gilt, dass Verfügbarkeit und Sicherheit gegeben sein müssen.

Dabei ist der Zustand im Netzwerk zu beachten, um Anomalien frühzeitig und möglichst vor einem Ausfall zu erkennen. Durch so genannte Intrusion-Detection-Systeme kann die Anwesenheit unbekannter Teilnehmer im Netzwerk festgestellt werden. Durch das Beobachten der Netzwerkauslastung lassen sich gezielte Angriffe auf bestimmte Teilnehmer z.B. durch vermehrte Anfragen (Denial of Service) feststellen. Auch Programmierzugriff auf Steuerungssysteme können damit erkannt werden.

## 5.3. Modellbaukasten

Zur Risikobehandlung müssen nach der Identifikation und Bewertung der Risiken Gegenstrategien sowohl für den Fall des Eintritts als auch zur Reduktion der Wahrscheinlichkeit des Eintritts entwickelt und implementiert werden. Im Regelfall sind es technische Maßnahmen, wie z.B. bauliche Sicherheit oder redundante Auslegung sensibler Systeme. Zusätzlich sind organi-

satorische Maßnahmen, wie die Sensibilisierung der Mitarbeiter*innen im Rahmen von Awareness-Trainings oder die Entwicklung von Standards für die Dokumentation von bestimmten Handlungen, wie die Vergabe von Rechten oder die Durchführung von Backups und Updates notwendig.

### 5.3.1. Baustein Sperren für Zugangswege von Schadprogrammen

Einer der Hauptzugangswege von Schadprogrammen sind Web-Seiten und der E-Mailverkehr. Angriffsträger sind dazu oft verbreitete Software-Produkte, wie z.B. Programme der Microsoft-Office-Familie, wo vergleichsweise einfach möglichst viele Computer-Systeme mit Schadsoftware infiziert werden können.

Ausgenutzt werden dazu Schwachstellen oder unsichere Konfigurationen von Standardfunktionen von Büro-Software, wobei Makro-Funktionen oder aktive HTML-Anzeigen genutzt werden. Abhilfe schafft dabei eine sichere Konfiguration. Darüber hinaus kann auch durch eine Sperre bestimmter Dateianhänge im E-Mailverkehr das Risiko vermindert werden.

Das BSI hat in [BSI19-1] Empfehlungen zur sicheren Konfiguration von Microsoft-Office-Produkten veröffentlicht.

In der internen Serviceseite des Universitäts-Rechen- und Medienzentrum der Universität Erfurt [URMZ20] wird mitgeteilt, dass der Austausch von Anhängen in bestimmten Dateiformaten per E-Mail gesperrt worden ist.

Grundsätzlich ist davon auszugehen, dass nur ausgewählte Funktionalitäten im Geschäftsbetrieb zur Erfüllung der dort anfallenden Aufgaben notwendig sind. Deshalb kann die Sicherheit durch selektives Sperren von Programmen firmenintern und arbeitsplatzbezogen reguliert werden, wie auch z.B. der Zugang zum Internet.

### 5.3.2. Baustein Maschinen- und Anlagensicherheit

Der Baustein Maschinen- und Anlagensicherheit fokussiert Sicherheit im Sinne von Safety, wo der Personen- und Anlagenschutz im Vordergrund der Bertachtungsweise steht. Da es absolute Sicherheit nicht geben wird, wird mit Hilfe des Begriffes des so genannten Grenzrisikos festgelegt, dass Maschinen- bzw. Anlagensicherheit dann gegeben ist, wenn das verbleibende Risiko einer Schädigung geringer als das Grenzrisiko ist. In diesem Zusammenhang wird von einem vertretbaren Risiko gesprochen.[23]

Im Bereich der Technik insbesondere im Zusammenhang mit der Risikoanalyse bei Anlagen und Maschinen (Maschinensicherheit) werden nach der IEC 62061 sogenannte Risikoparameter (S: Schwere des Schadens, F: Häufigkeit, W: Wahrscheinlichkeit des Auftretens und P: Möglichkeit der Vermeidung) verwendet, um mit Hilfe einer Formel die Risikozahl

[23] Im Online-Artikel „Risiko, Sicherheit und Gefahr“ [SP o.J.] vom Springer-Verlag werden die genannten Begriffe ausführlich diskutiert.

R=S*K=S*(F+W+P) zu ermitteln. Das Ergebnis dieser Berechnung ist ein Zahlenwert, mit Hilfe dessen die notwendigen Maßnahmen festgelegt werden.

Ganz allgemein gilt, dass zum Sicherstellen der Maschinensicherheit technische Maßnahmen gesetzt werden. Im einfachsten Fall sind das Abschrankungen, die mit Hilfe diverser elektronischer Systeme überwacht werden. Diese Systeme sind mit den Steuerungen vernetzt und tauschen kontinuierlich mit diesen Daten über den aktuellen Sicherheitsstatus aus.

Betrachtet man den typischen Aufbau einer Maschinensteuerung, werden auf Grund der dort herrschenden Umweltbedingungen, wie z.B. Vibrationen, erhöhte Temperatur, Feuchtigkeit und Staub, industrietaugliche Rechnersysteme wie Industrie-PCs, Leittechnik-Systeme und speicherprogrammierbare Steuerungen (SPS) eingesetzt.

Der hohe Automatisierungsgrad moderner Fertigungen bringt es mit sich, dass vielfach eine Vielzahl technischer Prozesse von vernetzten Rechnersystemen kontrolliert werden, die sich über alle Prozessführungsebenen erstrecken. Auch Sicherheitssteuerungen sind in diese Systeme integriert. Für die Sicherheitssteuerungen muss dabei sichergestellt werden, dass diese völlig unabhängig vom Status der übrigen Rechnersysteme arbeiten, und dass Sicherheitsschaltungen der Sicherheitssteuerung durch die übrigen Systeme nicht wechselseitig beeinflusst werden können. Es ist daher zweckmäßig, Sicherheitskomponenten bezüglich ihrer Wirkungsweise autark zu betreiben und nur Statusmeldungen an die übrigen Steuerungs- und Überwachungssysteme zuzulassen.

### 5.3.3. Baustein Kommunikationssicherheit

Die Technik, ein eigenständig abgeschirmtes Netzwerk als Pufferzone innerhalb eines IT-Netzwerkes zu errichten, ist als DMZ-Technik (Demilitarized Zone) bekannt. Die DMZ ist damit ein speziell kontrolliertes Netzwerk, das sich zwischen dem externen Netzwerk (Internet) und dem internen Netz befindet. Es wird dadurch eine Pufferzone gebildet, die die Netze durch strenge Kommunikationsregeln und Firewalls voneinander trennt. Diese Technik gilt als sicher, weil eine Schutzzone für die Unternehmens-Server und Netzwerkkomponenten aufgebaut wird.

Die Wirkungsweise der Schutzmechanismen gegen Angriffe oder unberechtigten Zugriff erfolgen durch die Einrichtung einer äußeren und einer inneren Firewall, die nach dort festgelegten Regeln den Datenverkehr kontrollieren.

Durch das Festlegen von Regeln als Filtermechanismen lässt sich bestimmen, welche Daten abgefragt werden können, indem nicht zulässige Abfragen praktisch durch Sperren nicht durchführbar gemacht werden.

### 5.3.4. Baustein Speicherschutz („memory protect“)

Die Steuerungen in industriellen IT-Anwendungen unterscheiden sich von Geräten für den kommerziellen Bereich. Die dort eingesetzten Prozessoren sind für Steuerungsaufgaben optimiert. Bei den für Maschinensteuerungen eingesetzten SPS sind die Prozessoren oft Eigenent-

wicklungen der Hersteller dieser Steuerungen. Auch die dort genutzten Betriebssysteme unterscheiden sich von jenen, die in der PC-Welt genutzt werden. Daneben werden in industriellen Steuerungssystemen auch Bedien-Terminals und andere Geräte verwendet, die auch typische PC-Komponenten und Betriebssysteme nutzen.

Generell gilt, dass im Zentrum eines industriellen Steuerungssystems die SPS steht, die mit diversen Peripheriegeräten Daten austauscht. Dieser Datenaustausch erfolgt auf der so genannten Feldebene über Feldbussysteme. In [KG17] werden Aspekte der Automatisierung in der Produktion ausführlicher behandelt.

Angriffe auf industrielle Steuerungssysteme betreffen in erster Linie die Speicherorte in den Steuerungssystemen. Nur dort können etwa Schadprogramme gespeichert werden oder Steuerungsdaten in Schädigungsabsicht manipuliert werden. Teilweise wurde in Steuerungssystemen der Speicherschutz durch z.B. Schlüsselschalter als „memory protect“ Funktion realisiert, um zumindest die Manipulation des Anwenderprogramms zu verhindern bzw. zu erschweren. Bereits in der ersten SPS (MODICON 084) wurde von seinem Entwickler, Dick Morly, ein Schlüsselschalter für den Speicherschutz vorgesehen.[24]

Die Funktion „memory protect“ ist der Ausgangspunkt für die weiteren Überlegungen. In handelsüblichen Prozessoren, wie diese in PCs genutzt werden, sind in der Regel auch Schaltkreise zur Speicherverwaltung bzw. zum Zugriff auf Speicherbereiche implementiert. Der Speicherschutz (memory protect unit MPU) ist normalerweise Teil einer Zentraleinheit (central prozessing unit CPU). Die MPU regelt per Software, Speicherbereiche festzuglegen und diesen Bereichen durch das Setzen von Attributen Berechtigungen für den Zugriff zuzuweisen. Je nach Prozessor variiert die Anzahl der unterstützten Speicherbereiche.

Ähnlich dem oben genannten Speicherschutz können intelligente Filterelemente eingesetzt werden, die z.B. als Embedded Systems als autarke Einheiten als Netzwerkelemente vorgesehen sind, die ausschließlich die Abfrage vorher definierter Speicherbereiche lesend zulassen. Diese Einheiten sollen in erster Linie den Datenverkehr von Steuerungssystemen regeln. Durch die Einschränkung auf die Funktionalität „nur lesend“ (read only) und die Festlegung der Bereiche können Programmiereingriffe verhindert werden.

Ein derartiges Sicherungssystem ist mit der Funktionalität einer Firewall auf Hardwarebasis vergleichbar. Seine Aufgabe ist Verbindungen zuzulassen oder zu beschränken und ausgehende und eingehende Daten innerhalb des Netzwerks zu kontrollieren. Als autarke Einheit ist es ein zusätzliches System, das z.B. bei einer industriellen Steuerung und dem nach außen bestehendem Netzwerk eine Wächterfunktion zu erfüllen hat. Im weiter oben beschriebenen Schichtmodell sind diese Einheiten an den Übergängen eingesetzt. Eine derartige Funktion haben typisch handelsübliche Router, die mit hardwarebasierten Firewalls ausgestattet sind.

Im Wesentlichen geht ein solcher Ansatz davon aus, die Kontrolle über die eigenen Daten zu behalten, indem nur für den Betrieb benötigte Informationen zur Verwendung freigegeben

[24] Die Geschichte der SPS ist im Artikel aus dem Jahr 2008 „40-Jahre SPS“ redaktionell aufbereitet [SPR08].

werden, Zugriff auf andere Daten aber gesperrt werden. Vergleichbar ist eine solche Einheit mit einer maschinellen Authentifizierung, der Berechtigung auf Daten zuzugreifen. Durch derartige Einschränkungen können andere als sensibel z.B. für Angriffe von außerhalb des Netzes definierte Speicherbereiche einer industriellen Steuerung abgeschottet werden.[25]

Als weitere Möglichkeit kann überlegt werden, industrielle Steuerungen indirekt zu koppeln. Pufferelement könnte eine unabhängig agierende Einheit sein, die als Server nur ausgewählte Daten für das nachgeschaltete Netz zur Verfügung stellt.

### 5.3.5. Baustein Datendioden

Unidirektionale Netzwerkgeräte wie Datendioden dienen dazu, die Informationssicherheit bzw. den Schutz kritischer digitaler Systeme wie industrieller Steuerungssysteme vor Cyberangriffen zu gewährleisten. Die Verwendung solcher Geräte ist in Hochsicherheitsumgebungen üblich, und sind als Verbindungen zwischen zwei oder mehr Netzwerken mit unterschiedlichen Sicherheitsklassifikationen eingesetzt. Diese Technologie kann auch dazu verwendet werden, um die Einwegkommunikation zu erzwingen, so dass wenn z.B. kritische digitale Systeme über das Internet mit nicht vertrauenswürdigen Netzwerken verbunden werden sollen, unerwünschte oder „verbotene“ Verbindungen für den Datenverkehr gesperrt werden.

Durch die physische Natur unidirektionaler Netzwerke können Daten nur von einer Seite einer Netzwerkverbindung zur anderen übertragen werden und nicht umgekehrt. Damit lässt sich ein Schema für die Vertrauenswürdigkeit zwischen Netzwerkbereichen derart konstruieren, das ähnlich dem konzentrischen Zonenmodell für Sicherheitsstufen (Fig. 3 Seite 25) Abstufungen für die Vertraulichkeit sicher stellt.

Die Funktionalität ist dann attraktiv, wenn vertrauliche Daten innerhalb eines Netzwerks erzeugt werden und dennoch eine Verbindung mit dem Internet erforderlich ist. Hauptzweck der Datendiode ist, Daten für internetbasierte Eingriffe zugänglich zu machen. Damit kann ein sicherheitskritisches physisches System Daten für die Online-Überwachung zugänglich machen, ohne Angriffen ausgesetzt zu sein, die möglicherweise physischen Schaden verursachen (vgl. [JD06]).

Der Vorschlag von Jones und Bowersox [JD06] beschreibt zwei allgemeine Modelle für die Verwendung unidirektionaler Netzwerkverbindungen. Im klassischen Modell besteht der Zweck der Datendiode darin, den Export klassifizierter Daten von einer sicheren Maschine zu verhindern und gleichzeitig den Import von Daten von einer unsicheren Maschine zu ermöglichen.

[25] CFT bietet z.B. als „Smart Filter-Technologie“ ein Control System an und behauptet, dass damit unter anderem die Prozesssicherheit verbessert wird. In der Ankündigung heißt es: „*CFT Smart Filter überwacht und analysiert kontinuierlich die wichtigsten Daten der Geräte. Bei Fehlern oder Auffälligkeiten zeigt das System die relevanten Informationen in Echtzeit an*.“ [CFT20]

Kommentar: Wenn auch der Zweck des von CFT vorgestellten Gerätes einen anderen Zweck als oben beschrieben verfolgt, erscheint die Idee überlegenswert, den Datenfluss in Echtzeit zu überwachen und aus den Ergebnissen zweckdienliche Schlüsse zu ziehen, um die Datensicherheit zu gewährleisten.

Im alternativen Modell wird die Diode verwendet, um den Export von Daten von einem geschützten Computer zu ermöglichen und gleichzeitig Angriffe auf diesen Computer zu verhindern (vgl. [JD06]).

Als „Verfahren zur unidirektionalen Datenübertragung“ existiert für die Thales Management and Services Deutschland GmbH (Norbert Wingerath) ein Patent unter DE102015213400A1 (vgl. [WN17]).

### 5.3.6. Baustein Zero-Trust-Modell

Unter einem Zero-Trust-Modell wird ein IT-Sicherheitskonzept verstanden, bei dem sowohl innerhalb als auch außerhalb des Netzwerks niemandem vertraut wird. Das Zero-Trust-Modell schließt Geräte, Nutzer und Dienste ein. Dadurch bedingt sind recht umfangreiche Maßnahmen bezüglich der Authentifizierung sämtlicher Anwender und Dienste erforderlich einschließlich einer Prüfung des Netzwerkverkehrs. Ziel dieses Modells ist, das Risiko zu minimieren.

Aus dem Grundsatz, niemandem innerhalb oder außerhalb des Netzwerks zu vertrauen (Zero-Tust) ergibt sich, dass sämtliche Anwender und Anwendungen authentifiziert sein müssen und dass der Datenverkehr grundsätzlich verschlüsselt erfolgen muss. Als weitere Forderung ergibt sich, dass die benötigten Zugriffsrechte auf Anwendungen oder Geräte genau definiert sein müssen. Das Zero-Tust Modell schreibt vor, dass bei geteilten Netzen (Netzwerksegmenten) an den Netzwerkgrenzen durch Systeme der Datenverkehr analysiert wird, um gegebenenfalls den Datenaustausch zuzulassen oder zu sperren (vgl. LS18]).

Stefan Luber und Peter Schmitz führen dazu aus: *„Die praktische Umsetzung des Zero-Trust-Modells erfordert für ein Unternehmen großen Aufwand. Alle Bereiche der IT sind von dem Sicherheitskonzept betroffen und müssen kontrolliert werden.“* [LS18]

Für diesen Baustein stellt sich die Frage, ob in einer bereits bestehenden Unternehmensstruktur ein solcher Modellansatz nachträglich eingerichtet werden kann. Zu überlegen ist, ob sich der Aufwand und die damit verbundenen Kosten vertreten lassen.

Die Trust Zero Netzwerkarchitektur wurde von Forrester Research bereits 2010 vorgeschlagen. Zum Teil sind die dort veröffentlichten Grundsätze in derzeit[26] aktuelle Netzwerkarchitekturen übernommen worden. Im Bericht von [KJ et. al. 10] befassen sich die/r Autor*innen mit einer möglichen Art und Weise, wie die Konzepte des Zero Trust-Modells verwendet und in einer realen Umgebung implementiert werden können. Verfolgt wird das Ziel der Optimierung der Sicherheitsarchitektur auch mit dem Aspekt der zukünftigen Flexibilität. Im Mittelpunkt der Betrachtungsweise stehen die Daten, deshalb werden Netzwerke datenzentriert betrachtet und von innen nach außen entworfen (vgl. [KJ et. al. 10]).

[26] Jahr 2020

### 5.3.7. Methodenbaukasten für Risiken

Als Methoden zur Identifikation, Bewertung und Bewältigung von Risiken stehen zur Verfügung:

Risikofaktorenanalyse: Risiken werden mittels der Faktoren Zeit, Kosten und Budget quantitativ beurteilt. Risiken für den Faktor Zeit könnten Lieferprobleme von Lieferanten sein, die zu Produktionsschwierigkeiten im Zeitverlauf führen. Entsprechend des Faktors Kosten wäre dann in weiterer Folge die Notwendigkeit auf einen anderen, möglicherweise teureren Lieferanten ausweichen zu müssen, ein Kostenrisiko. Zuletzt könnte sich daraus das Risiko einer Budgetüberschreitung in einem laufenden Projekt entwickeln.

Unabhängig von der Art des Unternehmens oder einem betroffenen Bereich erfolgt eine Einteilung in unterschiedliche Risikokategorien. Die tatsächliche Bewertung des Risikos erfolgt qualitativ über eine Risikomatrix entsprechend den Auswirkungen in geringe, mittlere und hohe Risiken.

Im statischen Risk Assessment werden Risiken numerisch ausgedrückt. Das Risiko ergibt sich aus seiner Eintrittswahrscheinlichkeit und den daraus resultierenden Konsequenzen. Es wird versucht, potenzielle Auslöser von Schadensereignissen zu identifizieren, ihre Eintrittswahrscheinlichkeit zu ermitteln und den entstehenden Schaden zu bewerten. Statisches Risk Assessment wird für das Risikomanagement von Atomkraftwerken und anderen komplexen technologischen Einheiten verwendet. Die Eintrittswahrscheinlichkeiten von identifizierten Risiken können daher von einer Vielzahl von Variablen abhängig sein. Aus diesem Grund erfolgt die Modellierung der Wahrscheinlichkeiten auf der Basis von Ereignisbäumen, die die Bildung langer und komplexer Kausalitätsketten ermöglichen (vgl. weiter oben die Berechnung von Risikoparametern).

Das Konzept Value at Risk versucht, das Risiko für den Schadenseintritt mittels mathematischer Methoden der Wahrscheinlichkeiten zu berechnen. In der Technik werden z.B. für den Parameter W (Wahrscheinlichkeit des Auftretens) Werte mit 1 für vernachlässigbar, mit 2 für selten, mit 3 für möglich, mit 4 für wahrscheinlich und mit 5 für häufig in die Berechnungsformel eingesetzt. Die festgelegten Werte entsprechen der Einschätzung des Wertenden und enthalten daher gewisse Unsicherheiten.

Enterprise Information Security Architecture ist ein ganzheitlicher qualitativer Ansatz, der darin besteht, Sicherheit bereits in der Planung der gesamten Systemarchitektur zu berücksichtigen. In der Praxis ist dieser Ansatz auf Grund bestehender Informationssysteme in einem gewachsenen Unternehmen eher schwierig zu realisieren. Die gesamte Entwicklung der Architektur ist an den Unternehmenszielen auszurichten. Daraus werden die Elemente der Ablauf- und Aufbauorganisation abgeleitet, um die IT-Architektur mit ihren Sicherheitsbedarfen und Risiken danach zu planen, zu entwickeln und zu implementieren.

Gegenmaßnahmen (countermeasures) zu identifizierten und analysierten Risiken müssen durch geeignete Maßnahmen getroffen werden. Für die erkannten Risiken sind zielführende Gegenmaßnahmen erforderlich. Beispiele sind für die technische Sicherheit: Gebäudeschutz,

Multifaktorauthentifizierung, redundante Infrastruktur. Als organisatorische Maßnahmen sind das: definierte Prozesse für Kontrolle von Maßnahmen wie Rechte- und Rollenvergabe oder Backup- und Updatemanagement, Zutrittsregeln für Serverräume, Entwicklung von Compliance und Awareness.

Für ein Unternehmen können Annahmen getroffen werden und ein System nach dem Ansatz einer Enterprise Information Security Architecture aufgebaut werden. Bei einer historisch gewachsenen Struktur z.B. eines Großunternehmens wird das nicht so einfach möglich sein.

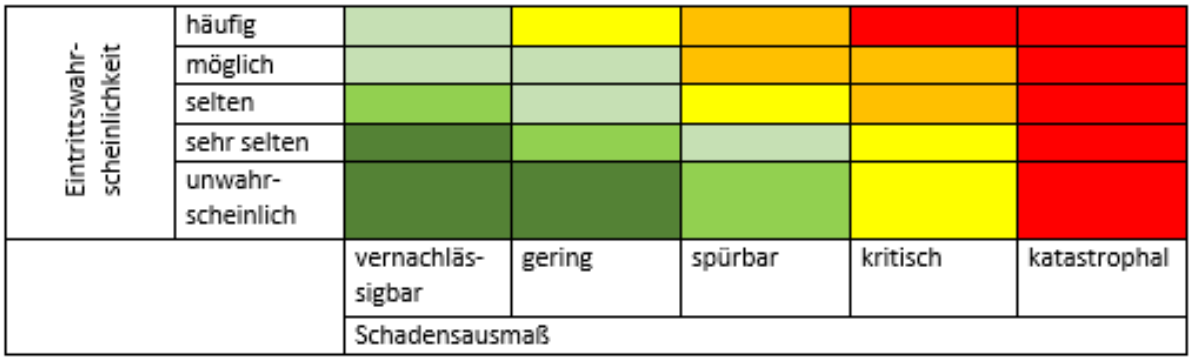
Ein zentraler Bereich eines ISMS ist die Security Awareness, auch deshalb, weil dies bis vor wenigen Jahren nicht mit der notwendigen Aufmerksamkeit betrachtet worden ist. Nachholbedarf besteht bei einer Vielzahl IT-spezifischer Risiken im Zusammenhang mit menschlichem Fehlverhalten, die nur zum Teil durch technische Sicherheit, Restriktion und Compliance-Vorgaben gelöst werden können. Beispiele sind Social Engineering und die missbräuchliche Verwendung von Fernwartungszugängen.

### 5.3.8. Einordnung der Risiken

Für die Einordnung von Risiken bietet die Risikomatrix eine gute Übersicht. In einer Risikomatrix werden Zusammenhänge verdeutlicht. Fig. 7 zeigt eine angepasste Risikomatrix. Sie stellt grafisch mögliche Risiken dar. Dadurch sind vorher definierte Schadensklassen und Klassen für die Eintrittswahrscheinlichkeit klassifizierbar. Mit Hilfe der Formel: Risiko = Schaden x Eintrittswahrscheinlichkeit lassen sich Risikowerte beziffern. In der Darstellung sind die Risikowerte in der Matrix hier nur farblich hervorgehoben. Rot bedeuten Risiken, die als sehr hoch eingestuft werden. Gelb, orange und grün stellen in der Matrix entsprechend geringere Risiken dar. Im Prinzip hängt die Einstufung jedoch auch vom betrachteten Einsatzfall ab. Aus diesem Grund wurde hier auf die Skalierung mit Zahlenwerten verzichtet.

Eine 5x5 Matrix lässt sich durch die Einführung von Zwischenstufen feiner granulieren. Vorsorgemaßnahmen kosten Zeit und Geld und durch eine feinere Aufgliederung lassen sich die benötigten Ressourcen besser einteilen.

Auch im Fall eines Totalausfalles der Infrastruktur darf es zu keinem Datenverlust kommen und es müssen bestimmte Mindestservices aufrechterhalten werden können. Es sind daher bei der Bewertung von Risiken Ereignisse zu berücksichtigen, deren Eintrittswahrscheinlichkeit denkunmöglich erscheint und dennoch katastrophale Auswirkungen für das Unternehmen haben könnten.




Skalen (Legende)

| | |
|---|---|
| häufig | Schadensereignisse, in kleineren Abständen (weniger als 1 Jahr) immer wieder vorkommen (z.B. Angriffe auf das IT-System) |
| möglich | Schadensereignisse, in größeren Abständen (1-2 Jahre) vorkommen |
| selten | Schadensereignisse sind selten aber kommen immer wieder vor (z.B. Gebrechen an Maschinen und Anlagen in der Fertigung, Geräteausfall z.B. PC) |
| sehr selten | Schadensereignisse sind nicht auszuschließen und können sehr selten vorkommen (z.B. Ausfall der Energieversorgung) |
| unwahr-scheinlich | Schadensereignisse können vorkommen, Eventualmaßnahmen sind geplant |

| | |
|---|---|
| vernachläs-sigbar | keine Auswirkungen |
| gering | betrifft keine relevanten Services, keine Einschränkung des Betriebes |
| spürbar | Einschränkungen (mit Auswirkung auf den Betrieb) |
| kritisch | massive Einschränkung (z.B. Teilstillstand) |
| katastrophal | Totalausfall (z.B. wichtiger Service, Maschine, Betriebsstillstand) |

*Fig. 7: Risikomatrix, angepasst*

ALARP (as low as reasonably practicable) besagt, dass Maßnahmen, die im Rahmen des Risikomanagements gesetzt werden, das Risiko nur so weit reduzieren sollten, soweit das mit einem vertretbaren Aufwand möglich ist. Im Umkehrschluss gilt, dass es nicht zielführend ist, Risiken durch Maßnahmen so weit zu unterdrücken, dass die Aufwendungen den eintretenden oder zu erwartenden Schaden übersteigen.

In manchen Fällen haben wirtschaftliche Erwägungen dennoch eine untergeordnete Rolle, z.B. wenn es in Bezug auf die Sicherheit Risiken mit potenziell katastrophalen Auswirkungen betrifft.

### 5.3.9. Fernzugriff

Im Sicherheitshandbuch werden als die wichtigsten Maßnahmen die erfolgreiche Authentifizierung der Benutzer*innen gegenüber ihren Endgeräten und dem Netz der Institution gesehen, dass eine Verschlüsselung der Daten auf dem Endgerät und eine regelmäßige Sicherung der Daten im Netz der Institution, um die auf dem Endgerät gespeicherten Daten vor Verlust und gegen Vertraulichkeitsverletzungen zu schützen, gegeben sein muss und das ein kryptografisch gesichertes virtuelles privates Netzwerk (virtual private network, VPN) genutzt wird,

um die Kommunikationsverbindung zwischen dem Endgerät und dem Netz der Institution vor unbefugtem Mitlesen zu schützen. [A-SIT19]

Fernzugriff wird in industriell genutzter IT zur Fernwartung genutzt. Insbesondere bei der Behebung von Störungen ist Fernwartung meist die schnellste Möglichkeit, bei Betriebsunterbrechungen die Produktion wieder in Gang zu setzen.

## 5.4. Vorgehensmodell für IACS und seine Anwendung

Das vollständige Modell ist in Fig. 8 dargestellt. Es ist je nach der Komplexität der Aufgabenstellung in mehreren Schichten aufgebaut.

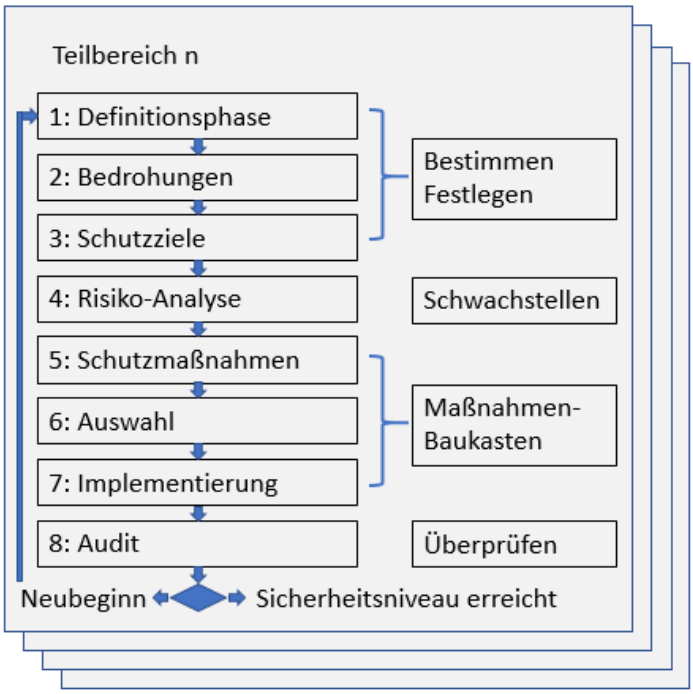



*Fig. 8: Schichtmodell für den Prozess zur Einführung und Verbesserung der Sicherheit*

Entsprechend der Struktur einer Anlage wird nach dem Festlegen der allgemeinen Sicherheitsziele und der in den Bereichen (Zonen) Schutzzielen iterativ vorgegangen. Zur besseren Übersicht werden dazu die Gesamtheit aller beteiligten elektronischen Komponenten, die in mehreren Netzwerkebenen das Gesamtsystem beschreiben, in kleinere funktionell zusammenhängende Einheiten gegliedert, die einzeln behandelt werden können.

Die Entscheidung Schutzmaßnahmen zu treffen hängt einerseits von den dazu erforderlichen finanziellen Mitteln ab und andererseits von der Wichtigkeit eines zu schützenden Bereiches. Es ist eine Unternehmensentscheidung, ob etwa besonders sensible Bereiche komplett von den übrigen IACS abgeschottet werden und im Inselbetrieb arbeiten sollen, oder ob mit der Installation der entsprechenden Sicherungsmaßnahmen das Risiko der Vernetzung tragbar ist.

Insbesondere sind die Automatisierungssysteme von Maschinen und Anlagen aufgrund der dort auftretenden Safety-Aspekte gegenüber Schadprogrammen besonders zu schützen.

Am Ende des iterativen Prozesses wird für jeden überprüften Bereich festgestellt, ob das in der Definition geforderte Sicherheitsniveau erreicht worden ist oder nicht. Wurde es nicht erreicht, muss der Vorgang wiederholt werden.

Sind alle Bereiche einzeln überprüft worden, wird am Schluss der gesamte Prozess noch einmal für die ganze Anlage durchgeführt, um eventuell noch nicht beachtete Lücken zwischen den Bereichen aufzuspüren.

Ein Vorgehensmodell für die Automatisierung insbesondere auch im Hinblick auf Industrie 4.0 ist in der VDI/VDE 2182 beschrieben. Es ist ein Modell, das den gesamten Lebenszyklus (Entwicklung, Integration, Betrieb, Migration und Außerbetriebsetzung) berücksichtigt. Das Modell beschreibt, wie die Informationssicherheit von automatisierten Maschinen und Anlagen durch die Umsetzung von konkreten Schutzmaßnahmen erreicht werden kann.

Dazu betrachtet die Richtlinie Aspekte der eingesetzten Automatisierungsgeräte, Automatisierungssysteme und Automatisierungsanwendungen. Sie definiert ein einfaches Vorgehensmodell zur Bearbeitung und Darstellung der Informationssicherheit, das aus mehreren Prozessschritten besteht (vgl. [VDI19]).

Das Modell sieht 8 Schritte vor, die wiederholt zyklisch durchlaufen werden. Das wiederholte Durchlaufen der Schritte stellt sicher, dass insbesondere Fortschritte in der technischen Entwicklung berücksichtigt werden können. Die nach [VDI19] vorgeschlagenen Schritte sind vergleichbar mit den im Ansatz bereits weiter oben beschriebenen 7 Schritte Modellansatz.

Nach [VDI19] werden folgende Schritte durchgeführt:

**Schritt 1: Definitionsphase**

Zu Beginn wird der Bestand aufgrund von vorher durchgeführten Strukturanalysen erfasst. Dazu kann z.B. auch ein einzelner Anlagenteil herangezogen werden. Diese Vorgehensweise ermöglicht es, komplexere Anlagen in kleinere Einzelbereiche aufzuteilen, um diese dann einzeln zu untersuchen. Erfasst werden alle Komponenten, in der Regel tabellarisch (vgl. [VDI19]).

**Schritt 2: Feststellen von Bedrohungen**

Im zweiten Schritt werden zu den festgestellten Komponenten die vorhandenen organisatorischen, technischen und benutzerbedingten Bedrohungen festgestellt. Vielfach gibt es zu einer Komponente auch mehrere Bedrohungen. Diese können z.B. tabellarisch zugeordnet werden. Das Feststellen von Bedrohungen erfordert eine große Erfahrung bei der Ortung potenzieller Bedrohungen. Zur Vereinfachung können Informationen und Beschreibungen aus vorhandenen Sicherheitskatalogen genutzt werden (z.B. österreichisches Informationssicherheitshandbuch [ASIT19], oder aus der Schriftenreihe des BSI stammende). Vielfach werden bei der ersten Evaluierung die relevanten Punkte aus vorgefertigten Katalogen entnommen und in weiterer Folge die daraus stammenden Bedrohungen zugeordnet und bewertet (vgl. [VDI19]).

**Schritt 3: Schutzziele**

Der dritte Teil des Vorgehensmodells beschäftigt sich mit der Ermittlung der Schutzziele des Unternehmens. Vordringlich soll als das grundlegende Schutzziel einer industriellen Organisation der reibungslose Anlagenbetrieb (Verfügbarkeit) in den Vordergrund gestellt werden. Von großer Bedeutung sind auch Vertraulichkeit und Datenschutz, die erweiternde Schutzmaßnahmen erfordern. Schutzziele werden nach ihrer Wichtigkeit priorisiert und gegeneinander in Relation gestellt und abgewogen. Es könnte z.B. der Schutz einer geheimen Rezeptur oder ganz allgemein von Forschungsergebnissen in der Produktentwicklung wichtiger sein, als das in Kauf nehmen eines Anlagenstillstands (vgl. [VDI19]).

**Schritt 4: Risiken analysieren und bewerten**

Risiken werden anhand der Wahrscheinlichkeit des Schadenseintritts und den Auswirkungen beurteilt. Genutzt werden dazu Risikomatrizen, ähnlich der in Fig. 7 vorgestellten Risikomatrix. Da die zur Risikominderung gesetzten Maßnahmen Kosten verursachen, sollte gleich auch der notwendige finanzielle Aufwand dafür der Höhe der möglichen Schadensfälle gegenübergestellt werden. Aus einer Kosten-Nutzen-Analyse kann für die Entscheidungsfindung das akzeptable Risiko bestimmt werden (vgl. [VDI19]).

**Schritt 5: Definition und Beurteilung von Schutzmaßnahmen**

Bei der Definition und Beurteilung von Schutzmaßnahmen werden zu jeder Bedrohung alle Schutzmöglichkeiten festgehalten. Diese werden den akzeptablen Risiken gegenübergestellt. Wird eine Risikoreduzierung notwendig, muss die getroffene Schutzmaßnahme mindestens so wirksam sein, dass nach dem Implementieren das akzeptable Risiko unterschritten wird. Maßnahmen, die nicht wirtschaftlich umgesetzt werden können, müssen erkannt werden und als solche definiert werden. Dazu sind überschlagsmäßige Kostenabschätzungen den einzelnen Maßnahmen zuzuordnen (vgl. [VDI19]).

**Schritt 6: Auswahl der Schutzmaßnahmen**

Die in Schritt 5 definierten Schutzmaßnahmen werden ausgewählt. Als Gründe für die Wahl eines geeigneten Schutzmechanismus stehen die Aspekte Wirtschaftlichkeit, strategischen Vorgaben und Umsetzbarkeit. Zu diesem Zeitpunkt sollten auch die Kosten bereits genauer definiert sein. In der Kostenaufstellung sollten alle Aufwendungen, wie Engineering, Implementierung, Folgekosten im Betrieb und Instandhaltungskosten berücksichtigt sein. Gegebenenfalls ist bei der Umsetzbarkeit zu berücksichtigen, dass beteiligte Personen auf neue Systeme speziell geschult werden müssen (vgl. [VDI19]).

**Schritt 7: Ausführung**

In der Ausführungsphase werden zuvor ausgewählte Schutzmechanismen implementiert. Die Durchführung muss nach dem aktuellen Stand der Technik unter Berücksichtigung von einschlägigen gesetzlichen Vorgaben erfolgen. Begleitend wird die Durchführung ständig über-

wacht, ob alle Prozessschritte richtig umgesetzt werden. Ein entsprechendes Qualitätsmanagement (z.B. nach ISO 2000) ist laut der Richtlinie empfohlen. Ergebnis dieses Prozessschritts ist der realisierte Schutz sowie ein dokumentiertes Betriebskonzept (vgl. [VDI19]).

**Schritt 8: Audit**

Die letzte Phase ist die Durchführung eines Audits, in dem alle Prozessschritte nochmals überprüft und gegebenenfalls noch bestehende Sicherheitslücken aufgezeigt werden. Existieren noch Sicherheitslücken beginnt der Prozess neuerlich bei Schritt 1. Die Prüfung sollte in regelmäßigen Abständen durch externe Personen erfolgen, die am Prozess nicht beteiligt gewesen sind. Beim Audit wird überprüft, ob alle Prozessschritte ordnungsgemäß durchgeführt und dokumentiert wurden. Ebenfalls wird kontrolliert, ob die Beurteilungen der Schutzmaßnahmen und Risiken plausibel sind. Das Endergebnis des Vorgehensmodells sollte ein umfangreicher Auditbericht mit der Aufzählung der möglichen Mängel sein (vgl. [VDI19]).

## 5.5. Zusammenfassung

Sicherheitsmodelle für die industriellen Informations - und Steuerungssysteme sind keine statischen Modelle, sondern müssen sich ständig weiterentwickeln. Bedingt ist das einerseits durch den technischen Fortschritt von in der IT genutzten Komponenten und andererseits aufgrund neuer Angriffsszenarien. Das bedeutet, dass die Überprüfung der Sicherheit von industriell genutzter IT immer wieder neu durchgeführt werden muss.

Konzeptuell stehen grundsätzliche Möglichkeiten zur Gestaltung von Schutzmodellen zur Verfügung. Bei der in dieser Arbeit verfolgten Variante wird der äußere Schutz derart umfassend gebildet, dass ein innerer Schutz nur punktuell notwendig ist. Ein solches Modell besitzt im Inneren weitere Schutzmechanismen, die für den individuellen Schutzbedarf zusätzliche Maßnahmen vorsehen, die ihrerseits erweiterte Schutzzonen schalenförmig ausbilden, die gegebenenfalls auch ihrerseits in der Tiefe geschachtelt sein können. Der individuelle Schutzbedarf zusammen mit seinen Maßnahmen sind einzelne Bausteine, die ergänzend in ein Grundschutzsystem, das allgemeingültig sein kann, eingebaut werden, um spezielle mögliche Sicherheitslücken zu schließen. Dieses Bausteinkonzept wird in Anwendungsszenarien am Beispiel der Firma RECPLAST GmbH und weiteren Beispielen untersucht, wobei angenommen wird, dass ein entsprechendes Grundschutzkonzept bereits eingeführt und umgesetzt worden ist.

Auf der anderen Seite besteht die Möglichkeit, ein Schutzkonzept von Beginn an, also zusammen mit der Konzeption einer Maschine oder Anlage aufzubauen. Dazu wird das Konzept nach der VDI/VDE 2182 als Anwendungsszenario bei einer petrochemischen Anlage untersucht.

# 6. Modellüberprüfung

Für die Modellüberprüfung wurden betriebs- und praxisnahe Anforderungen als Beispiele für die Umsetzung für unterschiedliche Unternehmen gewählt. Da Fertigungsprozesse Unternehmensgeheimnisse sind, muss in diesem Kapitel auf die Verwendung realer Unternehmensdaten verzichtet werden.

Daher wird am Beispiel von drei realitätsnahen Szenarien untersucht, wie mit Hilfe der vorgestellten Modelle die IT-Sicherheit der RECPLAST GmbH im Hinblick auf die Abteilungen Fertigung, Entwicklung und Produktion gesteigert bzw. weiter erhöht werden kann. In weiteren Beispielen werden ein Automatisierungsprojekt für eine petrochemische Anlage untersucht, wie mit Hilfe des Vorgehensmodells für die Automatisierung nach der VDI/VDE 2182 vorzugehen ist. Zuletzt wird die Sicherheit in einer Industrie 4.0 Produktion betrachtet. Ziel dabei ist es, die Modelle zu überprüfen und geplante Vorgehensweisen darzustellen.

## 6.1. Anwendungsszenario „RECPLAST GmbH“

Testumgebung ist das in [BSI18-REC] vorgestellte fiktive Beispielunternehmen RECPLAST GmbH. Das dort genutzte Managementsystem für Informationssicherheit basiert auf dem BSI-Standard 200-1: „Managementsysteme für Informationssicherheit (ISMS)“, dem BSI-Standard 200-2: „IT-Grundschutz-Methodik“ und insbesondere in den in Kapitel 4 und 5 vorgestellten Methoden, sowie aus dem Baustein ISMS.1 „Sicherheitsmanagement“ mit den zugehörigen Umsetzungshinweisen aus dem BSI IT-Grundschutz-Kompendium (vgl. [BSI18-REC]).

Der Schwerpunkt dort *„liegt auf der Initialisierung des Sicherheitsprozesses und dabei insbesondere auf dem Aufbau einer Organisationsstruktur und der Entwicklung einer Leitlinie zur Informationssicherheit*“ [BSI18-REC].

Die RECPLAST GmbH hat seine Verwaltung, Produktion und Lager in unterschiedlichen Standorten. Zusätzlich gibt es mehrere Vertriebsbüros. Fig. 9 zeigt als Übersicht den Netzplan der RECPLAST GmbH.

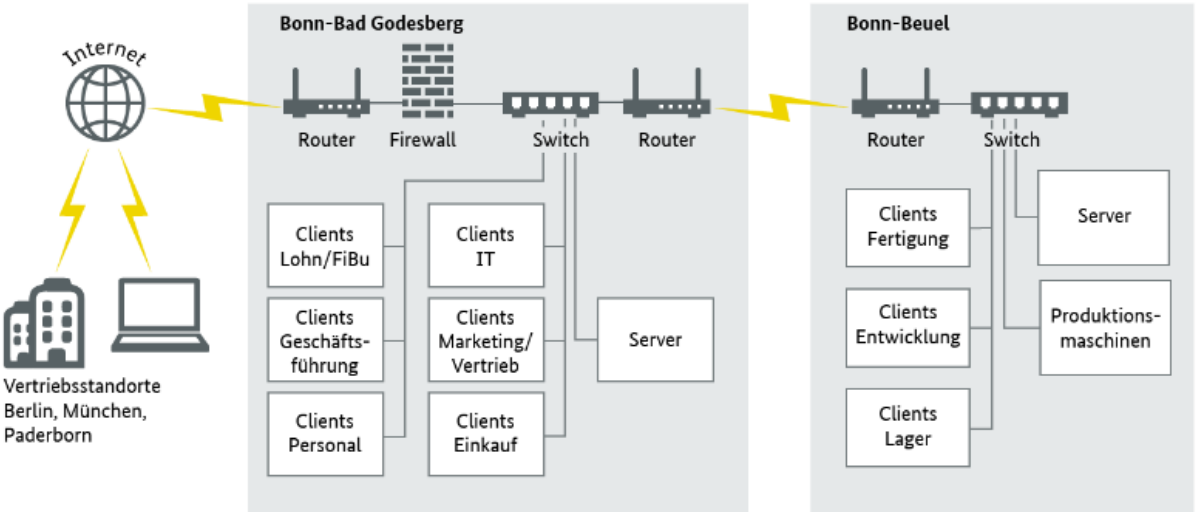



*Fig. 9: Netzplan der RECPLAST GmbH – Übersicht ([BSI18-REC], Abb. 2)*

Das in [BSI18-REC] vorgestellte fiktive Beispielunternehmen RECPLAST GmbH produziert und vertreibt etwa 400 unterschiedliche aus Recyclingmaterialien gefertigte Kunststoffprodukte, z.B. Bauelemente wie Rund- und Brettprofile, Zäune, Blumenkübel oder Abfallbehälter.

Wie Schutzkonzepte und Maßnahmen in der RECPLAST GmbH umgesetzt worden sind, ist in [BSI10-REC] bereits ausführlich dargestellt. Deshalb beschäftigen sich die weiteren Untersuchungen dieser Arbeit hauptsächlich mit Vorschlägen zur Verbesserung getroffener Maßnahmen.

Dazu ist der Standort Bonn-Bleuel von besonderem Interesse, da das vorgestellte Vorgehensmodell für Safety und Security bei der Automatisierung der verwendeten technischen Systeme die IT-Sicherheit verbessern soll. Damit rücken die Fertigung, die Entwicklung und insbesondere die Produktionsmaschinen in den Vordergrund des Interesses. Unabhängig davon wird auch eine allgemeine Sicherheitsrichtlinie für die RECPLAST GmbH vorgeschlagen.

### 6.1.1. Aktuelle Sicherheitsprozesse in der RECPLAST GmbH

In der RECPLAST GmbH sind aktuell nur die Grundelemente eines Managementsystems für Informationssicherheit dargestellt. Als Schwerpunkt wird die Initialisierung des Sicherheitsprozesses betrachtet und dabei insbesondere auf dem Aufbau einer Organisationsstruktur und auf der Entwicklung einer Leitlinie zur Informationssicherheit Wert gelegt.

Dazu ist eine Organisationsstruktur eingeführt worden, deren Aufgabe es ist die entsprechenden Vorschläge und Entscheidungsgrundlagen als Leitlinie zur Informationssicherheit festzulegen. Weiters soll ein Sicherheitskonzept bestimmt und ein Realisierungsplan vorgelegt werden. Neben der Dokumentation soll der Plan Maßnahmen zur Aufrechterhaltung der Informationssicherheit enthalten (vgl. [BSI18-REC]).

### 6.1.2. Umsetzung in der RECPLAST GmbH

Die Sicherheitsrichtlinie der RECPLAST GmbH gilt allgemein für alle Standorte und Geschäftsbereiche, wobei zusätzliche Vorgaben als erweiterte Sicherheitsziele für die Produktion sowie für die Abteilung Forschung und Entwicklung festgelegt werden. Dort wird auf die Modellbausteine Bezug genommen.

Die Formulierungen dieser Sicherheitsrichtlinie sind weitgehend allgemein gehalten, damit Vorgaben unabhängig von speziellen Lösungen sind, jedoch ausreichend spezifisch für die Umsetzung konkreter Vorgaben. Damit soll sichergestellt werden, dass sie auf Grund der rasanten Entwicklungen in der Informationstechnologie auch für neue Herausforderungen anwendbar bleibt.

Allgemeines zu den Sicherheitszielen und zur Sicherheitsrichtlinie der RECPLAST GmbH beziehen sich auf die allgemeinen Grundwerte von Informationssicherheit, die Integrität, die Verfügbarkeit und den Datenschutz. Daten müssen vollständig und unverändert bleiben sowie die zugehörigen Attribute dürfen nicht manipuliert werden. Außerdem ist die Verfügbarkeit der Funktionen, IT-Anwendungen, IT-Netze und ganz allgemein die Vertraulichkeit von Informationen sicherzustellen.

Definiert wird eine Reihe von Mindestanforderungen, die sicherstellen, dass das Handeln einer einzelnen Einrichtung keine negativen Auswirkungen auf andere Einrichtungen der RECPLAST GmbH als Gesamtunternehmen haben kann. Diese Mindestanforderungen beinhalten auch die Einhaltung von Gesetzen, Verordnungen und Compliance-Vorgaben und orientieren sich an den Interessen der RECPLAST GmbH.

Die Sicherheitsrichtlinie fordert die enge Zusammenarbeit der Standorte und Geschäftsbereiche unter Berücksichtigung der Dezentralität der IT-Infrastruktur. Durch den Austausch über IT-Sicherheitsvorfälle soll die realistische Einschätzung der Bedrohungslage und die Auswahl von Maßnahmen ermöglicht werden.

Aus der Literatur sind eine Reihe von Sicherheitsrichtlinien bekannt. Größere Institutionen haben ihre Sicherheitsrichtlinien veröffentlicht (vgl. [FUB19], [MPG17], [HSN19]).

### 6.1.3. Sicherheitsziele

Die allgemeinen Grundsätze für Informationssicherheit wurden bereits genannt. Diese gelten uneingeschränkt für den gesamten Betrieb und sind als Basissicherheit klassifiziert. Daneben gibt es Geschäftsbereiche, die für den Betrieb als sensibel einzustufen sind und deshalb zusätzliche Maßnahmen erfordern.

Unterschieden werden deshalb allgemeine Ziele, Richtlinien und Erweiterungen bezogen auf sensible Daten, insbesondere solche aus der Verwaltung, Forschung und Entwicklung sowie der Produktion. Es werden dazu Sicherheitszonen bestimmt, **Zone A** als „allgemein“ mit der Gültigkeit für das Gesamtunternehmen, **Zone V** als Zusätze für die Verwaltung, **Zone F** für die F&E Abteilung und **Zone P** für die Produktion, insbesondere für die mit der IT gekoppelten automatisierten Produktionseinrichtungen.

Erstes Sicherheitsziel ist das Sicherstellen der Verfügbarkeit von Diensten. Zur Nutzbarkeit eines Dienstes wie der Nachrichtenübertragung wird erwartet, dass seine Verfügbarkeit (availability) gegeben ist. Im Fall der Nichterfüllung wird dabei gefordert, dass es Maßnahmen zur Fehlerbehandlung (exception handling) gibt. Zusätzlich muss die Erreichbarkeit gegeben sein, also jederzeit einen andere/n Nutzer*in oder eine Maschine zu erreichen, und die Verbindlichkeit, dass ein/e Nutzer*in belangt werden kann, wenn Zusagen nicht innerhalb einer angemessenen Zeit erfüllt werden.

Zweites Sicherheitsziel ist die Integrität von Daten, das Zutreffen von Daten z.B. den Lagerbestand der RECPLAST GmbH, so darzustellen, dass ein zutreffendes Abbild des wirklichen Lagers gegeben ist. Inhaltliches Zutreffen setzt dabei voraus, dass jede Nachricht unverändert empfangen wird. Dazu kommt das Erkennen von Veränderungen und die zeitliche Korrektheit. Außerdem muss sichergestellt werden können, dass der Absender einer Nachricht authentisiert also berechtigt dazu ist.

Drittes Sicherheitsziel ist die Vertraulichkeit von Daten. Darunter fallen unter anderem Geheimhaltung, Anonymität, Rollentrennung und die Abhörsicherheit.

### 6.1.4. Anwendungsbereiche in der RECPLAST GmbH

Im oben erwähnten Konzept von Bereichen (Zonen) gibt es eine hierarchische Ordnung als allgemein gültige Basissicherheit (**Zone A**), die für das gesamte Unternehmen gilt, und darauf aufgebaut erhöhte Sicherheitsmaßnahmen für die sensibleren Geschäftsbereiche (Fig. 10).

Im Bereich der Verwaltung (**Zone V**) zählen zu den sensiblen Informationen alle Daten, die der Datenschutzgrundverordnung unterliegen. Dazu kommen noch Informationen aus der finanziellen Administration (Buchhaltung, Finanzwesen, Lohnverrechnung) sowie Daten aus dem Personalwesen und der Unternehmenskommunikation, Verkauf und Marketing. Im Bereich der Geschäftsleitung sind es Firmeninformationen, Strategien, Daten zu Geschäftsprozessen, Verträge und allfällige rechtliche Angelegenheiten, die intern als geheim eingestuft werden.

Im Bereich Forschung und Entwicklung (**Zone F**) sind es die Forschungsvorhaben zur Entwicklung neuer Produkte und deren Umsetzung sowie allfällige neue Produktionsverfahren, die dort geplant und umgesetzt werden.

Im Bereich Produktion (**Zone P**) geht es um die Vernetzung der maschinellen Einrichtungen, die einerseits Produktionsdaten erzeugen, um die Auslastung und Produktionsmengen für die Planung zur Verfügung zu stellen und andererseits auch um die Fernwartungszugänge der Maschinensteuerungen besonders gegen unbefugte Zugriffe abzusichern.

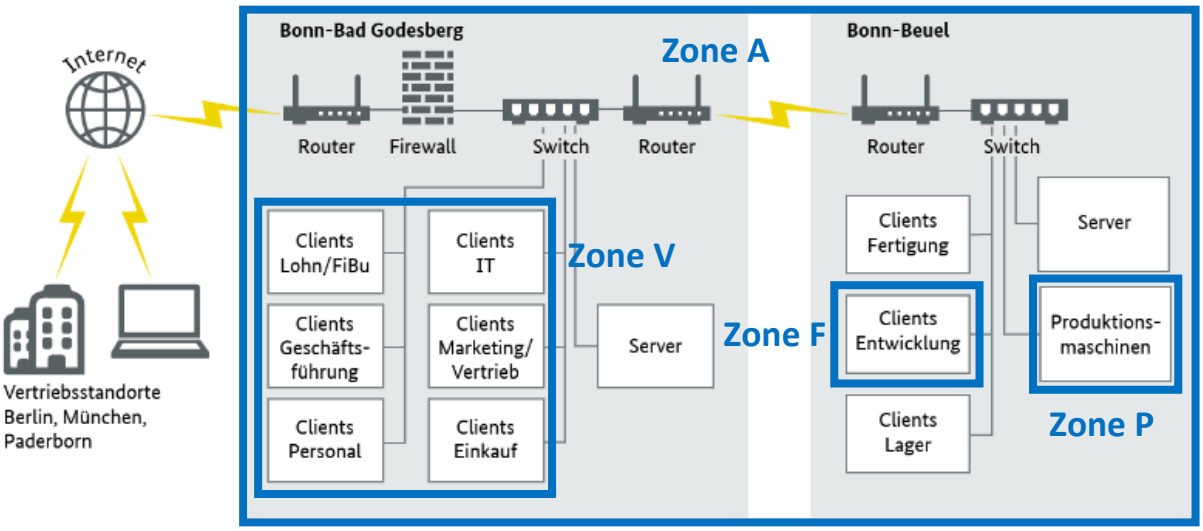



*Fig. 10: Zoneneinteilung der RECPLAST GmbH (aus [BSI18-REC], Abb. 2)*

### 6.1.5. Informationssicherheit für die genannten Bereiche

Äußerst schützenswerte Daten werden als sensibel klassifiziert und besonders abgesichert. Zugriffsrechte für solche Daten werden nur bestimmten Personen oder Personengruppen im Unternehmen eingeräumt. Dazu zählen unter anderem die Kundendaten. Dort werden über die allgemeinen Firmendaten hinaus auch Ansprechpersonen und zugehörige Zusatzinformationen gespeichert, wie z.B. Bankverbindung, Zahlungskonditionen, Zahlungsgewohnheiten, ob z.B. Zahlungen erst nach mehrmaliger Aufforderung geleistet werden, der eingeräumte Kreditrahmen, bis zu welcher Grenze geliefert wird etc. Ähnliches gilt für Personalangelegenheiten und für die weiteren Bereiche.

Einen besonders hohen Schutz müssen auch den Daten aus Forschung und Entwicklung zugemessen werden, da diese bei der Einführung neuer Entwicklungen und neuer Produkte einen Vorsprung für die Vermarktung bedeuten.

Fernwartungszugänge werden nur über verschlüsselte VPN Verbindungen zugelassen und ausschließlich für die Dauer geplanter Wartungen freigeschaltet.

### 6.1.6. Gesetzliche, regulatorische und vertragliche Vorgaben

Das Netz- und Informationssystem Sicherheitsgesetz (NIS G)[27] ist gültig für Betreiber wesentlicher Dienste, Anbieter digitaler Dienste sowie Einrichtungen der öffentlichen Verwaltung und damit keine gesetzliche Verpflichtung für die RECPLAST GmbH (entsprechend [RIS20]). Es unterstreicht jedoch die Wichtigkeit von Maßnahmen zur Verbesserung der Informationssicherheit. Einzuhalten sind die Bestimmungen des Bundesgesetzes über den Schutz personenbezogener Daten (Datenschutzgrundverordnung) (entsprechend [RIS99]).

Innerhalb der RECPLAST GmbH werden eigene Regeln und Vorgaben definiert, die als Sicherheitsrichtlinie der RECPLAST GmbH für den gesamten Betrieb gilt.

### 6.1.7. Gefährdungen bezogen auf Anwendungsbereiche

Faktor Mensch: Die Bewusstseinsbildung der Nutzer technischer Einrichtungen ist ein wichtiger Aspekt für die IT-Sicherheit. Hauptgrund dafür ist das mangelnde Vorstellungsvermögen, was kleinere Verfehlungen oder Nachlässigkeiten im eigenen Verhalten und in der Bedienung von IT-Einrichtungen für Auswirkungen bezüglich der Systemsicherheit bewirken können.

Faktor Gerätetechnik: Insbesondere die Gerätetechnik von IACS verharrt auf Grund ihrer vergleichsweise langen Lebenszeit und Einsatzdauer unverändert auf dem technischen Stand, den sie seit ihrer Ersteinführung innegehabt hatte.

Faktor Schadsoftware: Aus den Jahresberichten des BSI wird über Sicherheitsvorfälle im IT-Bereich berichtet und Maßnahmen bzw. Empfehlungen zur Erhöhung der Netzwerksicherheit vorgeschlagen. Dort wird von Vorfällen berichtet, wo teilweise existenzbedrohende Schäden Unternehmen verkraften mussten (vgl. [BSI18-1], [BSI19]).

In den exemplarischen Beispielen der Lageberichte des BSI (vgl. [BSI18-1], [BSI19]) werden darüber hinaus auch die entsprechenden Empfehlungen zur Verbesserung des IT-Sicherheit ausgesprochen.

### 6.1.8. Einführung einer Sicherheitsrichtlinie in der RECPLAST GmbH

Seitens der Geschäftsleitung wurde beschlossen, zur Erhöhung und zum Sicherstellen eines internen Standards eine eigene Sicherheitsrichtlinie zu entwickeln. Die Gültigkeit der Sicher-

[27] Dabei sind die gesetzlichen Bestimmungen des jeweiligen Staates anzuwenden, in dem die Firma ihren Sitz hat.

heitsrichtlinie wird für alle Bereiche definiert. Dazu wird die Position eines/r IT-Sicherheitsbeauftragten eingerichtet, der zusammen mit der hauseigenen IT einen entsprechenden Entwurf erstellt und diesen der Geschäftsleitung zur Prüfung und Genehmigung vorlegt.

Als Vorgaben werden dazu 4 Hauptpunkte definiert:

1. Die Sicherheitsrichtlinie muss individualisiert sein. Alle Standards werden an die Situation der einzelnen Bereiche in der RECPLAST GmbH angepasst, entsprechend dem weiter oben genannten Zonenmodell. Zweck ist, dass sich die Unternehmensleitung und die Mitarbeiter*innen in den Richtlinien wiederfinden und dass die Vorgaben als praxisnah von der gesamten Belegschaft akzeptiert werden können.

2. Die IT-Sicherheitsrichtlinien müssen in den betroffenen Bereichen durchführbar sein und dürfen Arbeitsabläufe nicht erschweren oder behindern. Wenn diese sich nicht praktisch durchführen lassen oder in Widerspruch zu anderen Vorgaben stehen, werden sie in der Regel nicht eingehalten. Die Einhaltung muss überprüfbar sein. Das zählt zum Aufgabengebiet des/der Sicherheitsbeauftragten.

3. Nach der Vorlage muss die Unternehmensleitung jede dieser (Teil-) IT-Sicherheitsrichtlinien freigeben. Nach der Freigabe werden die Anwender informiert und gegebenenfalls eingeschult. Die Gestaltung der Vorgaben muss dabei einfach und verständlich sein.

4. Jede IT-Sicherheitsrichtlinie muss aktualisiert werden, da sich nicht nur die Systeme, sondern auch die Bedrohungen in kurzen Zeitabständen verändern können. Auch das zählt zum Aufgabengebiet des/der Sicherheitsbeauftragten.

In der „Datenschutzpraxis“ [DPR20] sind die Gliederungspunkte für IT-Sicherheitsrichtlinien abrufbar.

Exemplarisch wird hier stark vereinfacht die IT-Sicherheitsrichtlinie für den Bereich Verwaltung „Behandlung von Kundendaten (Geschäftspartnern) zu Zahlungskonditionen im Mail-Versand“ der RECPLAST GmbH stichwortartig erläutert (Tab. 1). Grundsätzlich soll für alle Vorgänge, die mit der Hantierung von Daten im Zusammenhang stehen, ein Katalog von Regeln entstehen, der jeweils Geschäftsbereichen zugeordnet ist. Die Summe aller Richtlinien bilden das Regelwerk für die IT-Sicherheit im Unternehmen.

| Gliederungspunkt | Inhalt |
|---|---|
| Festlegung des Geltungsbereiches | Verkauf, Marketing, Buchhaltung |
| Betroffene Arbeitsvorgänge und Fachverfahren | Angebote, Rechnungen durch elektronische Datenübermittlung (z.B. Mailversand) |
| Betroffene Datenkategorien, Schutzbedarf und Schutzziele | Behandlung von Kundendaten (Geschäftspartnern) zu Zahlungskonditionen |
| Abzuwehrende IT-Risiken, bestehende Gefahren und mögliche Konsequenzen | Weiterleitung von Daten an unrichtigen Empfänger, Preisgabe oder Offenlegung kann Kundenbeziehung stören, Kunde geht verloren |
| Bezug zu Gesetzen, Verordnungen und Standards | DSGVO, interne Richtlinie der Geschäftsleitung |
| Verhältnis zu anderen Sicherheits- und Benutzerrichtlinien | Keine |
| Konkrete Verantwortlichkeiten für die Schutzmaßnahmen | Mitarbeiter*in |
| Zu ergreifende Schutzmaßnahmen in kurzer, verständlicher Form | Sicherstellen, dass spezielle Vereinbarungen zu Zahlungskonditionen nicht weitergegeben werden |
| Hinweis auf Schulungsangebote | Ja |
| Konsequenzen bei Nichtbeachtung der Sicherheitsrichtlinie | Verwarnung |
| Kontaktdaten von IT-Sicherheitsverantwortliche*n und Datenschutzbeauftragte*n | N.N. |

*Tab. 1: Stark vereinfachte Teil-Richtlinie. Gliederung nach [DPR20]*

### 6.1.9. Weitere Verbesserungen der Sicherheit in der RECPLAST GmbH

Das Sicherheitskonzept der RECPLAST GmbH ist nach den Grundsätzen des Grundschutzes aufgebaut. Die beiden Hauptstandorte (Verwaltung und Produktion) sind durch eine Firewall geschützt (Fig. 9). Das Zonenkonzept (Fig. 10) sieht Bereiche mit erhöhtem Schutzbedarf vor, wo zusätzliche Maßnahmen die Sicherheit verbessern können.

**Interne Bedrohungen durch kriminelle Handlungen**

Als interne Bedrohungen werden jene Bedrohungen verstanden, die von den eigenen Mitarbeitern eines Unternehmens ausgehen. Dazu zählen der Diebstahl von Unternehmensdaten oder das Verletzen der Geheimhaltung durch Durchsickern von Informationen nach außen infolge von Fahrlässigkeit, Korruption, Betrug, Absprachen oder im schlimmsten Fall durch Sabotage. Hier gibt es nur wenige Möglichkeiten, organisatorische und technische Maßnahmen zu setzen. Im Vordergrund steht hier die Auswahl des Personals und die Beschränkung des Zugangs zu Informationen und technischen Einrichtungen. Als Schutzmöglichkeit gegen Datenverlust kommt das regelmäßige Sichern auf externe Datenspeicher in Frage, die bei Kompromittierung von Datenbeständen die ursprünglichen Informationen rekonstruieren können.

Simon Alvarez [AS20] berichtet von einem Fall in der Tesla-Fabrik „Gigafactory 1“, wo für das Tesla-Model 3 Auto Akkus produziert werden. Dort sollte ein Mitarbeiter von Tesla bestochen werden, um eine bereitgestellte Malware in die Systeme des Elektroautoherstellers zu platzieren. Ziel der Hacker war es, Unternehmens- und Netzwerkdaten zu extrahieren, um Lösegeld zu erpressen. Der betroffene Mitarbeiter meldete den Vorfall. Bei den Ermittlungen durch das FBI wurde aufgedeckt, dass die Hacker bereits bei einem anderen Unternehmen diese Taktik erfolgreich praktiziert hatten (vgl. [AS20]). Solche Fälle zeigen, welchen Einfluss die Loyalität von Mitarbeiter*innen zum Unternehmen haben können.

**Gezielte Angriffe**

Gezielte Angriffe sind geplante Attacken auf IT-Systeme. Bei gezielten Angriffen kann davon ausgegangen werden, dass es Auftraggeber*in, Ausführer*in und ein Ziel als Opfer existieren. Im Unterschied zu Computerviren erfolgen gezielte Angriffe häufig auf mehrere Angriffsebenen gleichzeitig. Bei vorab erfolgten Recherchen zum Angriffsziel des Angreifers geht es um die Beschaffung von Informationen über die Schutzmechanismen, die dann gezielt attackiert werden, um diese auszuschalten. Der unbefugte Zugang zu Informationen erfolgt meist durch Social Engineering.

Da Social Engineering auf der Ausnutzung des menschlichen Faktors basiert, kann durch Aufklärung und das Festlegen von internen Regelungen die Beschaffung von Informationen für Angreifer*innen erschwert werden. Gegen mögliche Attacken auf Online-Ressourcen existieren spezialisierte Schutzmechanismen, z.B. Attack Killer [IW20] oder Qurator [QU20].

**Angriffe auf die Automatisierungstechnik**

Angriffe auf die Automatisierungstechnik von Industrieanlagen sind geplante Aktionen, die unter der Beteiligung von externen Angreifern und zum Teil auch Mitarbeiter*innen erfolgen. Der Zweck liegt oft darin, die Parameter von technologischen Prozessen zu verändern oder Prozesse zu unterbrechen.

Problem dabei ist, dass Sicherheitslösungen nicht schnell genug angepasst werden und deshalb mit neuen Bedrohungen nicht Schritt halten können. Insbesondere gilt das für intelligente Sensoren. Dazu kommt, dass Anlagenhersteller, Betriebspersonal und Sicherheitsexpert*innen unterschiedliche Sichtweisen zu den Sicherheitsanforderungen der Automatisierungstechnik in Industrieanlagen entwickelt haben. Deshalb reagieren manche Hersteller von Baugruppen für die Automatisierungstechnik nicht ausreichend schnell genug auf bekannt gewordene Schwachstellen. Dazu kommt, dass Sicherheitslösungen für Industrieanlagen eine ganze Reihe von Testläufen benötigen, um deren Wirksamkeit zu verifizieren, und dass darüber hinaus jede Automatisierungslösung individuell an den jeweiligen Prozess angepasst werden muss.

Fernwartungszugänge können eine Schwachstelle im Sicherheitskonzept einer Automatisierungsanlage sein. Im Folgenden werden weitere Maßnahmen behandelt und den weiter oben festgelegten Bereichen zugeordnet (vgl. Zonenkonzept nach Fig. 10).

### Generelle Maßnahmen (Zone A)

Generelle Maßnahmen gelten für das gesamte System. In der Zoneneinteilung nach Fig. 10 wurde diese als Zone A bezeichnet.

Interne Bedrohungen durch kriminelle Handlungen und gezielte Angriffe lassen sich grundsätzlich nicht verhindern. Durch das Missachten von Sicherheitsrichtlinien und das Umgehen von Vorgaben kann das gezielte Angreifen auf Systeme erleichtert werden. Im Wesentlichen meint Christian Schaaf in [SC13] dazu, dass durch fehlende Awareness sogar erst ermöglicht wird, gezielt von außen anzugreifen und mittels eines technischen Angriffs zu versuchen, Trojaner einzuschleusen. Fehlende Awareness kann auch dazu führen, dass Mitarbeiter*innen durch Social-Engineering ausgefragt Firmengeheimnisse preisgeben. Hier hilft es nur, alle Mitarbeiter*innen im Unternehmen zu sensibilisieren, damit diese Bedrohungen erkennen und entsprechend darauf reagieren. Vielfach sind Mitarbeiter*innen zu gutgläubig, um Fehlverhalten Dritter zu erkennen oder Handlungen Dritter kritisch zu bewerten. Das hängt oft damit zusammen, dass ihnen die Vorstellung darüber fehlt, dass durch das Negieren von Vorgaben und Regeln Schäden hervorgerufen werden können.

Mangelnde Loyalität oder die potenzielle Neigung zur Kriminalität von Mitarbeiter*innen ist auf Anhieb optisch nicht zu erkennen. Verschiedene Anzeichen können darauf hindeuten, wie Überschuldung, Lebensstil und Desinteresse an Unternehmenszielen.

Schaaf fasst zusammen, dass eine vernünftige Unternehmenskultur die Loyalität fördert, dass standardisierte Prüfregularien bei Neueinstellungen vorhanden sein sollten und dass Awareness-Maßnahmen im Unternehmen durchgeführt werden. Im Verdachtsfall sollte unmittelbar professionelle Aufklärung und Forensik betrieben werden (vgl. [SC13]).

Julia Weber hat in [BKA17] eine Studie zur sogenannten Innentäterschaft in Unternehmen veröffentlicht. An der ersten Stelle der vorgeschlagenen Maßnahmen werden das Schaffen guter Arbeitsbedingungen und die Bindung von Mitarbeiter*innen an das Unternehmen angeführt, gefolgt von guter Ausbildung. Die Stärkung von Awareness und Sensibilisierung der Mitarbeiter*innen zur Meldung von verdächtigen Aktionen ist ein wichtiger Schritt zur Erhöhung der Sicherheit. Durch die laufende Kontrolle von Systemen und die Beschränkung des Zugriffs auf spezifisches Wissen kann auch der Know-How-Schutz gestärkt werden (vgl. [BKA17]).

### Diskussion

Weil die Informationstechnik und damit verbundene Sicherheitsaspekte komplex sind, werden in der Regel die weniger gut ausgebildeten Benutzer*innen auch trotz Sensibilisierung und Schulung mit der Einhaltung von Sicherheitsrichtlinien vielfach überfordert. Es wird auf das möglichst frühe Erkennen von internen Angriffen oder das Fehlverhalten von Mitarbeiter*innen ankommen und auf das professionelle Reagieren im Falle eines Cyber-Angriffs. Um den Schaden bei Datenverlust oder Kompromittierung von Daten zu minimieren, sollten entsprechende Back-ups vorgehalten werden.

**Datenverbindung der Standorte**

Die Verwaltung ist am Hauptstandort, die Forschung und Entwicklung sind zusammen mit der Produktion im zweiten Standort der RECPLAST GmbH untergebracht (Fig. 10). Die Kommunikation zwischen den genannten Abteilungen erfolgt über eine Standleitung.

**Diskussion**

Der besondere Schutzbedarf besteht darin, dass die Vertraulichkeit der ausgetauschten Informationen sichergestellt sein muss (z.B. durch Verschlüsselung). Daten aus der Verwaltung in Bezug auf Steuerung der Produktion und der aktuelle Status müssen übertragen werden. In der Regel sind für solche Daten die Echtzeitanforderungen eher niedrig, sodass ein geringer Zeitverlust bei Authentifizierung und Verschlüsselung bzw. Entschlüsselung der Daten in Kauf genommen werden kann.

**Ergänzende Maßnahmen im Bereich der Forschung und Entwicklung (Zone F)**

Insbesondere im Bereich der Forschung und Entwicklung sind die Anforderungen an die Vertraulichkeit besonders hoch, da, wie weiter oben beschrieben, dem Know-How-Schutz eine besondere Bedeutung zukommt.

**Diskussion**

Es stellt sich grundsätzlich dabei die Frage, inwieweit die Notwendigkeit besteht, Ergebnisse von Forschung und Entwicklung an die Geschäftsleitung auf elektronischem Wege zu übermitteln. In Bezug auf die externe Datensicherheit können Bausteine wie die Datendiode oder die Abschottung durch eine demilitarisierte Zone Angriffe von außen erheblich erschweren.

**Ergänzende Maßnahmen im Bereich der Produktion (Zone P)**

Die Produktion ist automatisiert. Die Produktion übernimmt die Aufträge und die Daten für die Auftragssteuerung aus der Marketing- und Vertriebsabteilung.

Angriffe auf die Automatisierungstechnik können bis zum Stillstand der Produktion oder zu erheblichen Schäden führen.

**Diskussion**

In Bezug auf die Datensicherheit sind ähnliche Maßnahmen zielführend, wie diese zuvor für den Bereich Forschung und Entwicklung vorgeschlagen worden sind.

In der Folge wird das Herstellen von Cyber Security für Automatisierungssysteme etwas genauer betrachtet.

**Cyber Security für die Prozessleittechnik**

Im Wesentlichen geht es bei Cyber Security von Automatisierungsanlagen darum, den Schutz vor externen und internen Angreifern sicherzustellen sowie um das Aufrechterhalten eines Servicenetzwerkes. Dazu kommt der Datenaustausch mit anderen Steuerungssystemen z.B. in

anderen Niederlassungen oder anderen Produktionsbereichen entsprechend der Industrie 4.0 Konzepte, der Unternehmenszentrale etc.

Bei der hierarchischen Betrachtungsweise der Automatisierung wird diese oft als sogenannte Automatisierungspyramide dargestellt, an deren Spitze die IT steht. Die IT-Sicherheit wird durch Informationsmanagementsysteme, wie diese bereits weiter oben beschrieben worden sind, behandelt.

Untergeordnet ist die Betriebstechnik (Operational Technology, OT), die mithilfe ihrer Hard- und Software die physikalischen Prozesse der Produktion steuert und überwacht. Dazu werden industrielle Steuerungssysteme, meist speicherprogrammierbare Steuerungen, eingesetzt, die als spezielle Rechnersysteme für die Automatisierungsaufgaben besonders geeignet sind.

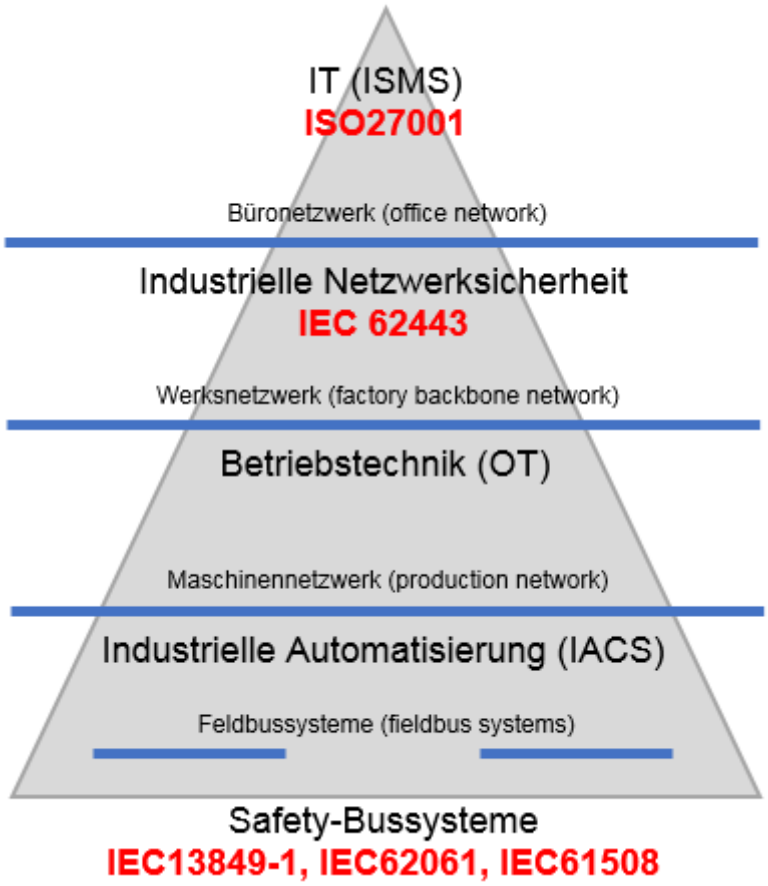



*Fig. 11: Netzwerk Hierarchie in der Automatisierungspyramide*

Fig. 11 zeigt die in die Netzwerkhierarchie eingeordneten Netzwerke in die Automatisierungspyramide. Dargestellt sind die zugehörigen Normen, z.B. Für Information Sicherheitsmanagementsysteme ist die Normenreihe der ISO2700x zu beachten, bei den Sicherheit-Bussystemen die Nomen IEC13849-1 etc. Werden die Hierarchieebenen betrachtet, gilt die horizontale Vernetzung und der darin transportierte Datenfluss hierarchisch als gleichwertig. Unter vertikaler Integration wird verstanden, dass die dargestellten Netze auch untereinander Daten austauschen.

Allgemein gilt die IEC 62443 als ganzheitlicher Ansatz für Industrial Security im Produktions- und Automatisierungsbereich, der sich mittlerweile als international anerkannter Standard für Security im Umfeld der Prozess- und Automatisierungsindustrie etabliert hat und in ihrer Anwendung unterschiedliche Industriebereiche und die kritischen Infrastrukturen abdeckt (vgl. [TÜV20]).

Die Daten im Industrienetzwerk dienen zur Vernetzung von Maschinen und Anlagen. Darüber hinaus sind die Produktionsnetze mit den unternehmensweiten Netzwerken im Office-Bereich und damit auch mit dem Internet verbunden. Der Umfang von fertigungsbedingten Daten für den Office-Bereich ist überschaubar. Als Schutzmechanismus für die dort stattfindende vertikale Datenintegration wird das Defense-in-Depth Prinzip als ausreichend betrachtet.

Bei diesem Prinzip existieren mehrere Netzwerkschichten, die untereinander durch Zugangsbeschränkungen abgesichert sind. Nur die äußerste Schicht ist direkt mit dem Internet verbunden (die am wenigsten vertrauenswürdige Ebene). Die hierarchisch unterste Netzwerkebene ist jene mit dem höchsten Schutzbedarf. Deshalb sollte zwischen dem Office-Netzwerk und dem Maschinen-Netzwerk eine demilitarisierte Zone (DMZ) zur Absicherung eingerichtet werden.

Solange es nur darum geht, dass Produktionsdaten weitergeleitet werden, kann die Sicherheit durch Datendioden verbessert werden.

Kritisch können jedoch Wartungszugriffe auf die Steuerungen sein, da damit unmittelbar auf Maschinenfunktionen eingegriffen wird. In der Regel erfolgen Wartungszugriffe im Rahmen einer Fernwartung, die von externen Personen des Anlagen- oder Maschinenherstellers durchgeführt werden.

## 6.2. Anwendungsszenario „IACS für einen technologischen Prozess“

*„Die Raffinerie in Schwechat bei Wien zählt zu den größten und komplexesten Binnenraffinerien Europas: Sie deckt rund die Hälfte des Bedarfs an Mineralölprodukten in Österreich. Im April 2018 feiert die Raffinerie Schwechat ihren 60. Geburtstag.“* [OMV20]. Im Bereich der Raffinerie sind eine Reihe weiterer Unternehmen angesiedelt, die petrochemische Grundstoffe weiterverarbeiten.

### 6.2.1. Anlagenkonzept

Für die Untersuchung wird angenommen, dass im Zuge einer Neuerrichtung eines fiktiven Anlagenteils ein chemisch technologischer Prozess automatisiert werden soll. Die neue Anlage ist als autarke Produktionsstätte vorgesehen. Es soll dabei Rohöl mittels fraktioneller Destillation aufgetrennt werden. Insbesondere dabei entstehende Dämpfe erfordern, dass in der Anlage explosionsgefährdete Zonen festgelegt sind, für die spezielle Richtlinien für die Ausführung der elektrischen Betriebsmittel zu beachten sind. Deshalb sind für bestimmte Anlagenfunktionen sicherheitsgerichtete Steuerkreise vorgesehen. Die Bedienung der Anlage soll zentral aus einer ständig besetzten Messwarte erfolgen.

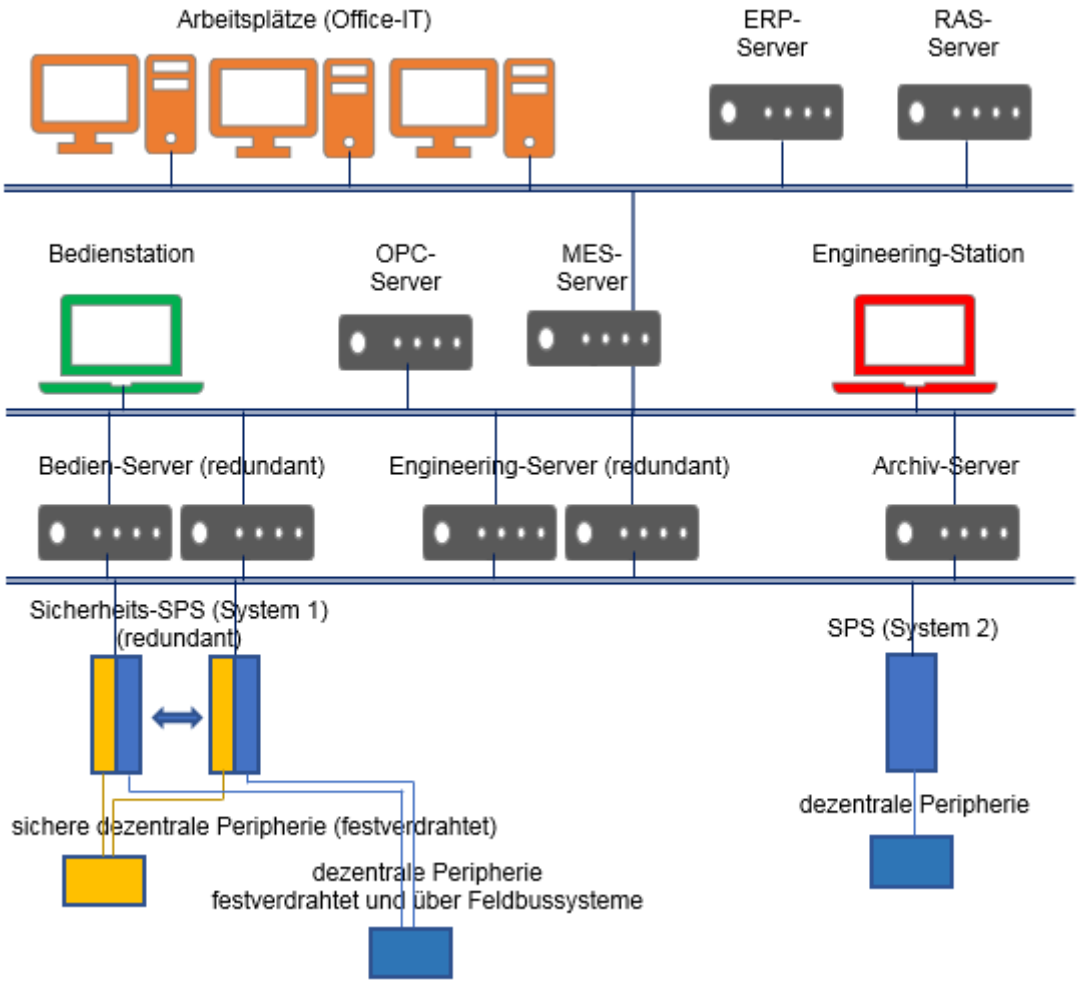



*Fig. 12: Vereinfachte Netzwerkinfrastruktur für die Automatisierung einer Anlage*

Eine grobe Netzwerkinfrastruktur des gesamten Automatisierungssystems zeigt Fig. 12. Die Anordnung ähnelt der so genannten Automatisierungspyramide. Hierarchisch gesehen sind in der obersten Ebene die Office-Arbeitsplätze und die Anbindung an das Internet, in der untersten Ebene die Feldbussysteme mit der angeschlossenen Peripherie und den zugehörigen Sensoren und Aktoren angeordnet. Die Sicherheitsfunktionen werden durch redundante Sicherheits-SPS [28] (System 1) abgearbeitet, die einschließlich aller notwendigen Trennverstärker für den explosionsgefährdeten Bereich durch Safety-Bussysteme entsprechend den einschlägigen technischen Anforderungen mit der Peripherie verbunden sind. Zwischen diesen Ebenen sind die Bedienstation und die Engineering-Station angeordnet.

Es kann vorausgesetzt werden, dass als verfahrenstechnische Anlage, diese sich innerhalb eines abgesperrten Betriebsgeländes befindet, das eingezäunt ist und durch mehrere Kameras

[28] SPS ist die Abkürzung für speicherprogrammierbare Steuerung. Speicherprogrammierbare Steuerungen sind Automatisierungssysteme, die in Anlagen und in der Fertigungstechnik eingesetzt werden. Sicherheit-SPS sind spezielle SPS, die ausgestattet mit entsprechender Hardware in Sicherheitsschaltungen (z.B. für Not-Abschaltsysteme) eingesetzt werden. Allgemeines zu SPS ist z.B. in [KG17] enthalten.

vor unberechtigten Zutritt überwacht wird. Zutritt wird nach einer entsprechenden Sicherheitsunterweisung und Kontrolle der Berechtigung gewährt.

Mittels Prozessleitsystemen wird die Anlage gesteuert, geregelt und überwacht. Instandhaltungsarbeiten können auch während des laufenden Betriebs erfolgen, wobei besonders geschultes Personal dazu vorgesehen ist. Neben den allgemeinen Aufgaben zur Steuerung und Überwachung dient ein übergeordnetes ERP-System[29] für die Unternehmensleitung, um aktuelle Statusinformationen und Produktionsdaten zur Verfügung zu stellen (Fig. 12: ERP-Server).

Zutritt zu elektrischen Betriebsräumen bzw. Serverräumen wird über Zutrittssysteme dem berechtigten Personal ermöglicht. Für alle Mitarbeiter gelten firmeninterne Richtlinien.

Für die Kopplung an das externe Netzwerk sowie die verschiedenen Anlagenteile sind Firewalls eingerichtet, das interne Netzwerk wird ebenfalls durch Firewalls untereinander segmentiert. Angenommen wird, dass PCs und Server (Office-PCs, Datenserver und Bedienstation) einheitlich mit aktuellen Betriebssystemen (z.B. Microsoft Windows) betrieben werden, wobei Update- und Backup-System zentral über einen Server erfolgt.

Mit dem Remote Access Service kann eine Verbindung mit Clients erfolgen, die sich außerhalb des geschützten lokalen Netzwerks befinden (Fig. 12: RAS-Server).

Auf Grund der höheren Verfügbarkeit sind mehrere Komponenten redundant aufgebaut ((Fig. 12: Bedien-Server, Engineering-Server, SPS-System 1 mit Sicherheits-SPS). Derartige petrochemische Anlagen müssen in der Regel kontinuierlich arbeiten. Die Sicherheits-SPS überwachen sich gegenseitig durch ständigen Austausch von Prozess- und Statusinformationen.

### 6.2.2. Sicherheitskonzept technologischer Prozess

Im Folgenden werden die Schritte entsprechend dem Modell nach VDI/VDE 2182 mit dem oben beschriebenen Anlagenteil eines automatisierten chemisch technologischen Prozesses in Verbindung gebracht. Es geht dabei in erster Linie um Grundsätze und um Überlegungen zum Aufwand und der Machbarkeit. Auf das Eingehen auf Details wird dabei weitgehend verzichtet.

Vorab soll dabei die Anlage als Ganzes betrachtet und der örtliche Schutzbedarf beleuchtet werden. Dieser ist bereits durch Abzäunung, Videoüberwachung des Geländes und der Betriebsräume bzw. Zutrittskontrollen abgedeckt. Soll an dieser Stelle auf das genannte Schema eingegangen werden, kann man schnell feststellen, dass entweder weitere Detailannahmen getroffen werden oder die örtlichen Gegebenheiten bekannt sein müssen. Beispielsweise ist in petrochemischen Anlagen bezüglich des elementaren Schutzes mit leicht entflammbaren und sogar explosiven Stoffen zu rechnen. Zum Explosionsschutz kommt der Brandschutz hinzu, wobei bei einem Brand spezielle Löschmittel benötigt werden. In Bezug auf die meist im Freien aufgestellten Anlagenteile ist zu bemerken, dass auch ein entsprechender Blitzschutz benötigt wird. Atmosphärische Entladungen, wie z.B. Blitze, können die Funktionsweise

[29] Unter einem ERP-System (ERP: Enterprise Resource Planning) wird ein IT-gestütztes System aus Softwarelösungen verstanden, das einen Überblick über vorhandene Ressourcen und Geschäftsprozesse bereitstellt.

der verwendeten elektronischen Geräte empfindlich stören und insbesondere bei der Datenübertragung bei Messgeräten, Sensoren und Aktoren zu Fehlinformationen führen. Deshalb wird für die weiteren Untersuchungen angenommen, dass die Anlage industrietauglich ist und dass ergänzende Schutzmaßnahmen nicht notwendig werden.

**Schritt 1: Definitionsphase**

Aus dem vorgestellten Anlagenkonzept können zumindest die dort genannten Hauptkomponenten erfasst werden. Typisch für die genannten Anlagen ist es, Büroräumlichkeiten, die Hauptsteuerwarte, Räume für die Server und für die Steuerungstechnik sowie die zentrale Prozessleittechnik in einem Gebäude unterzubringen, den Rest der Anlage im Freien, wobei die Steuerung mittels einer zentralen Peripherie an das Prozessleitsystem angebunden ist. Da alle verwendeten Elemente eine Funktion erfüllen, die Einfluss auf die Gesamtsicherheit und damit auf das Sicherheitskonzept haben, müssten diese genau bekannt sein. Das ist hier nicht der Fall, deshalb beschränkt sich diese Untersuchung auf die Informationssicherheit und setzt dabei voraus, dass die Sensordaten korrekt sind und dass auch die zugehörigen Aktoren funktionsgerecht arbeiten.

Exemplarisch sollen die beiden SPS-Systeme betrachtet werden.

Laut VDI/VDE 2182 interessieren dazu die Beschreibung von Komponenten und Geräten, von denen Bedrohungen im Fehlerfall ausgehen können, die Beschreibung interner und externer Kommunikationsbeziehungen und die Beschreibung der Rechtsposition des Unternehmens (vgl. [VDI19]).

Im Anlagenkonzept betrifft das die SPS und die Sicherheits-SPS (und dazu die Firmware, das Programm und den Arbeitsspeicher), netzwerkfähige Frequenzumrichter und Feldgeräte, Netzwerkkomponenten (Switch, Firewall, Router) sowie externe Gerätespeicher (z.B. Memory-Cards der SPS).

Zu betrachten sind dazu auch die Kommunikationskanäle des Prozessleitsystems mit der Außenwelt, IP-basierte Programmierschnittstellen (für die Programmierung, Diagnose und Parametrierung), weiters IP-basierte Feldbussysteme wie PROFINET I/O mit zyklischen und azyklischen Übertragungen und die Anbindung für Wartungs- und Engineering PCs/Laptops sowie die Anbindung zur Fernwartung und zu übergeordneten Systemen wie dem ERP-Server.

Dazu kommt eine allfällige Produkthaftung für die erzeugten Produkte, der Schutz des Verfahrens Know-How, die Abwehr von Haftungsansprüchen, die Gewährleistung der funktionalen Sicherheit, die Gewährleistung von Behördenvorgaben bezüglich des Umweltschutzes.

Auf Grund des Umfanges werden hier nur einige der wichtigen Geräte, die für industriellen Anlagen spezifisch sind, weiter behandelt.

Geräte wurden nach der eingesetzten Technologie (IP basierter Vernetzung) und den Risiken in einem petrochemischen Betrieb ausgewählt. Das oberste Ziel der Anlage ist der Schutz des Menschen, der Umwelt sowie die Verfügbarkeit. Deshalb werden außer den Geräten für die

Automatisierung Aspekte der Kommunikationsstrukturen, Rechtspositionen und logischen Funktionen der Anlage betrachtet.

**Geräte für die Automatisierung**

| Gerät, System, Prozess | Anmerkung, Beschreibung |
|---|---|
| SPS | Basisfunktion, offene Ethernet Programmierschnittstelle, steckbarer Programmspeicher |
| Feldgeräte, FU | Basisfunktionen, Maschinenbewegung |
| IP-basiertes Interface | Programm und Parameter laden und lesen |

**Kommunikationsstruktur**

| | |
|---|---|
| virtuelle private Netzwerke (VPN) | Fernwartung |
| PROFINET I/O | Feldbusfunktionalität |

**Rechtspositionen**

| | |
|---|---|
| Know-How Schutz | Maschinenparameter in der Visualisierung, SPS Know-How |
| Gewährleistung der funktionalen Sicherheit | Schutz der Mitarbeiter im Betrieb vor Fehlfunktionen und der Anlage |

**Logische Funktionen der Anlage**

| | |
|---|---|
| Operator-Server-Systemprozess | Basisfunktion der Anlage |
| Konfigurationsdaten | Basisfunktion der Anlage |
| Bereitstellung und Bedienung der MES-Daten | Ziele und KPIs (KPI: Key Performance Indicator) einer Anlage bereitstellen |

*Tab. 2: Auswahl von Funktionen im SPS-System (exemplarische Auswahl)*

**Schritt 2: Feststellen von Bedrohungen**

Zu den festgestellten Komponenten werden die vorhandenen organisatorischen, technischen und benutzerbedingten Bedrohungen festgestellt. Diese werden von den beteiligten Akteuren (z.B. Prozessleittechniker, Verfahrenstechniker, Betriebsleitung, IT-Administrator) der Anlage gemeinsam bestimmt und resultierende Risiken ermittelt.

Die effektivste, aber auch aufwendigste Methode zum Erkennen von Bedrohung ist die Schwachstellenanalyse. Damit können im System vorhandene Sicherheitslücken wie Implementierungsfehler, Organisationsfehler, Designfehler oder Konfigurationsfehler aufgedeckt werden. Für eine SPS ist die Schwachstellenanalyse z.B. die Analyse des Quellcodes nach semantischen Fehlern. Bei Feldgeräten mit PROFINET I/O Anbindung können Gerätestammdateien (GSD-Dateien) untersucht werden, um z.B. Konfigurationsfehler aufzudecken.

**Beispiele**

| Gerät, System, Prozess | Anmerkung, Beschreibung |
|---|---|
| Ausfall der SPS | Anlage ist nicht betriebsfähig, Produktionszeit geht verloren, Schaden an der Anlage und Umgebung sind möglich |
| Angriffe auf Netzwerkkomponenten | Performance der Anlage sinkt bis hin zu Anlagenstillstand |
| Verletzung des Know-How Schutzes durch unautorisiertes Auslesen des SPS-Programms | Spionage, Know-how Verlust an Dritte |
| Operator-Server-Systemprozess: Fehlfunktionen durch Schadsoftware | negative Beeinflussung der Prozessfunktionen durch Schadsoftware |

*Tab. 3: Beispiele möglicher Fehler im SPS-System (exemplarische Auswahl)*

**Schritt 3: Schutzziele**

Zur Ermittlung von Schutzzielen wird zuerst festgelegt, mit welcher Priorität einzelne Anlagenkomponenten zu behandeln sind. Dazu werden die ermittelten Risiken bestimmt und den akzeptablen gegenübergestellt. Als Beispiele werden im Bereich der Anlagensteuerung identifizierte Störungen bzw. Schadensfälle das SPS-System 1 betreffend unterstellt.[30]

**Beispiel**

| | | |
|---|---|---|
| SPS-System 1<br>Unzureichende Verschlüsselung, Absicherung der VPN-Verbindung | Mögliche Folgen<br>Anlagenstillstand, Produktionsschaden durch unkontrollierten Prozess | Abschätzung der Kosten [31]<br>Anlage wird gestoppt und ist für eine Zeit nicht verfügbar (Kosten 100.000 €/h), Anlage erzeugt unbrauchbares Medium, Reinigung der Rohrleitungen, Entsorgung des unbrauchbaren Mediums (Kosten 600.000 €) |
| SPS-System 1<br>unautorisierte Veränderung des SPS-Programms | Mögliche Folgen<br>negative Beeinflussung der Safety-Funktionen von Prozesseinrichtungen | Abschätzung der Kosten<br>Anlage gefährdet Umwelt und Mensch (Kosten 30,000.000 €), negative öffentliche Wirkung (Imageschaden) |

*Tab. 4: Beispiele: Fehler mit Folgen und Kosten im SPS-System (exemplarische Auswahl)*

**Schritt 4: Risiken analysieren und bewerten**

Zusätzlich muss das Risiko bewertet werden, etwa mit einer Skalierung der Wahrscheinlichkeit für das Auftreten eines Risikos als z.B. kein Risiko mit dem Wert 0 und extrem hohen Risiko mit dem Wert 100. Genauso wird dem Schadensausmaß eine Skala zugewiesen, z.B. Schaden ausgeschlossen mit dem Wert 0 bis zu extremen Schadensausmaß mit dem Wert 5. Für das

[30] Die genannten Kosten sind Schätzwerte. Auf Grund des Umstandes, dass das SPS-System 1 redundant aufgebaut ist, ist die Wahrscheinlichkeit eines Totalausfalls gemindert.

[31] Die Kosten für Folgen sind Annahmen und orientieren sich an worst-case Szenarien.

identifizierte Risiko wird dann der Wert für die Wahrscheinlichkeit mit dem Faktor für das Schadensausmaß multipliziert. Dieselbe Berechnung wird nach der Reduzierung des Risikos nach den vorgesehenen Verbesserungen durchgeführt. Die Risikoreduktion errechnet sich aus der Differenz.

**Schritt 5: Definition und Beurteilung von Schutzmaßnahmen**

Nach der Bewertung und dem Setzen von Prioritäten werden die verschiedenen Schutzmaßnahmen aufgezeigt. Dazu werden die ungefähren finanziellen Aufwendungen bestimmt und die Wirksamkeit von geplanten Maßnahmen bewertet. Schutzmaßnahmen können auch gegen mehrere Bedrohungen wirksam sein. Andererseits wird es auch vorkommen, dass mehrere Schutzmaßnahmen notwendig werden.

**Schritt 6 und 7: Auswahl der Schutzmaßnahmen, Ausführung**

Die in Schritt 5 definierten Schutzmaßnahmen werden ausgewählt und in der Ausführungsphase implementiert und getestet, ob die eingesetzten Maßnahmen die Risiken möglichst abdecken. Ist das nicht der Fall muss der Prozess neuerlich durchgeführt werden.

**Schritt 8: Audit**

Beim Audit werden alle Prozessschritte nochmals überprüft und gegebenenfalls noch bestehende Sicherheitslücken aufgezeigt.

## 6.3. Szenario „Sicherheit in der Industrie 4.0 Produktion“

In diesem Abschnitt wird nur angedeutet, dass der Umfang zur Erstellung eines Sicherheitskonzepts für Sicherheit in der Industrie 4.0 Produktion ein Vielfaches von den vorher diskutierten Vorschlägen ausmacht.

Schlick et. al. haben in ihren Beitrag: „PRODUKTION 2020 - Auf dem Weg zur 4. industriellen Revolution“ [SJ et. al. 13] Cyber-Physische Systeme (CPS) beschrieben, wie diese heute [32] als Stand der Technik etabliert sind. *„Cyber-Physische Systeme sind verteilte, intelligente Objekte, die miteinander über Internettechnologien vernetzt sind. Im Bereich der Produktionstechnik können dies z.B. einzelne Prozessmodule bis hin zu Anlagen und Einrichtungen aber auch individuelle intelligente Produkte umfassen. Sie werden auch als Cyber-Physische Produktionssysteme (CPPS) bezeichnet“* [SJ et. al. 13]

[32] 2020

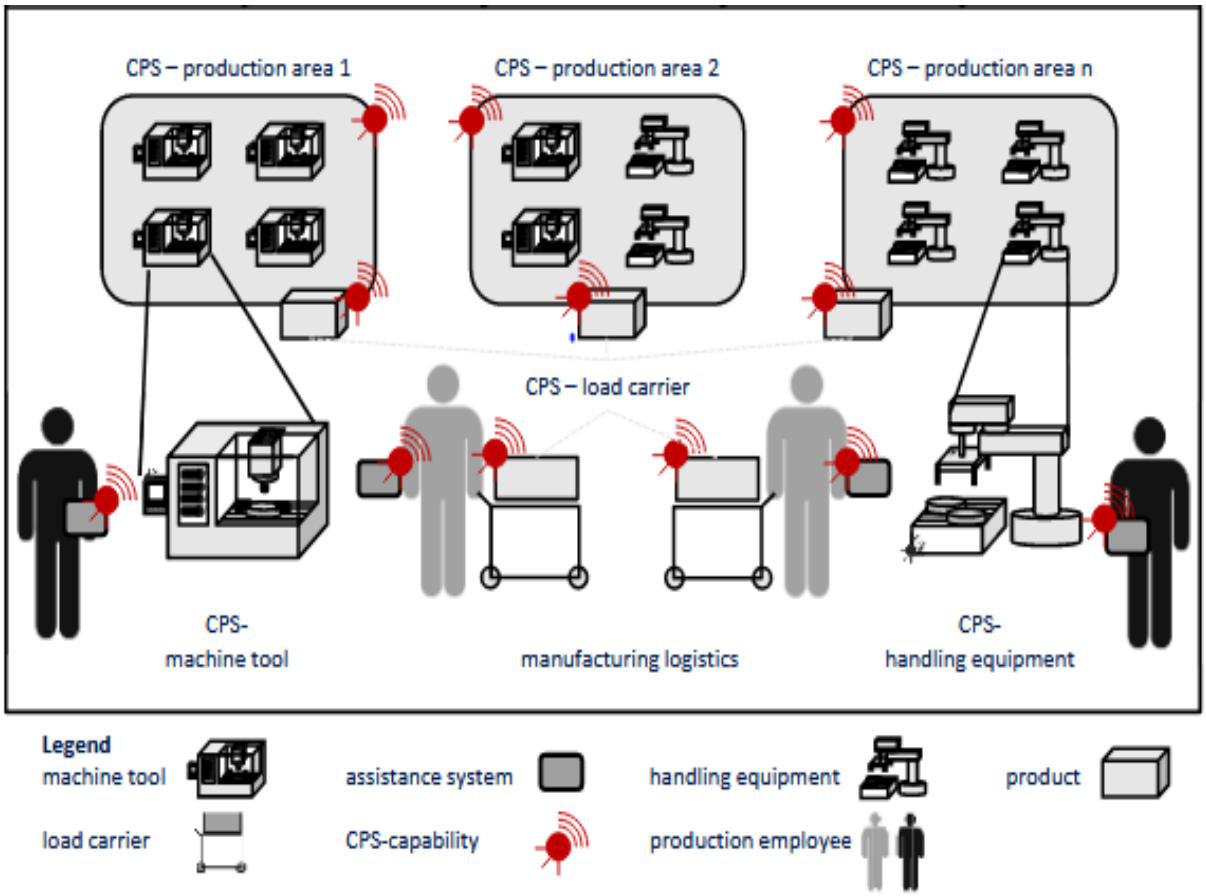



*Fig. 13: Getriebefertigung als Industrie 4.0 Fertigung [TK et. al. 16]*

Fig. 13 zeigt ein cyber-physisches Produktionssystem mit einem cyber-physischen Logistiksystem. Es ist die vereinfachte Darstellung einer Getriebeproduktion, die nach dem Industrie 4.0 Konzept eingerichtet worden ist. Mehrere Produktionsbereiche sind zu einen Gesamtsystem zusammengestellt. Ziel des Unternehmens war die Errichtung einer effizienten, schlanken Produktion mit vielen Produktvarianten. Das System nutzt cyber-physische Lastträger mit Sensorik, die sich selbst lokalisieren und die Umgebungsbedingungen überwachen, die die Komponenten beeinflussen (z.B. Temperatur, Beschleunigung). Das Produkt kennt durch gespeicherte Daten, welche Produktionseinrichtung welche Arbeitsschritte in welcher Reihenfolge durchzuführen hat. Der Transport erfolgt hier durch das Personal (vgl. [TK et. al. 16]).

In Cyber-Physischen Produktionssystemen (CPPS) ist einerseits die Vernetzung innerhalb der Betriebstechnik mit den Automatisierungsebenen und andererseits mit dem Internet sehr hoch und nimmt mit der steigenden Komplexität solcher Anlagen immer weiter zu. Dadurch werden Anlagen anfällig für Sabotage und Manipulationen, z.B. durch Schadsoftware. Deshalb muss im Zuge der Planung solcher Anlagen ein entsprechendes Sicherheitskonzept entwickelt werden.

Eine Intention von Industrie 4.0 ist es, auch Einzelprodukte, Prototypen oder Kleinserien industriell zu fertigen. Dazu werden meist mehrere CPPS zu einem Anlagenverbund zusammengefasst und mit einer intelligenten Transporttechnik miteinander verbunden. In Industrie 4.0

Anlagen sind nicht nur die einzelnen Arbeitsmaschinen sondern auch die Produktträger mit einer Teil-Intelligenz ausgestattet, insoweit, dass die Produktträger (und damit auch das Produkt) Kenntnisse mit sich führt, welche Arbeitsschritte von welcher Fertigungsanlage benötigt werden, damit das gewünschte Ergebnis erzielt wird. In einer solchen automatisierten Fertigung sollte der Produktdurchlauf optimiert gestaltet sein. Es ist deshalb eine ständige Interaktion zwischen den Produktträgern bzw. dem Produkt und den Fertigungseinrichtungen erforderlich, um etwa zu bestimmen, zu welchem Zeitpunkt ein Fertigungsschritt erfolgen kann, in welcher Reihenfolge Fertigungsschritte benötigt werden, ob die Fertigungsanlage gerüstet werden muss oder ob es reicht, wenn die entsprechenden Prozessparameter vom Produkt an die Fertigungsanlage übertragen werden.

Die Komplexität einer Industrie 4.0 Fertigung ist besonders hoch, weil mehrere Fertigungssysteme (CPPS), mehrere Produktträger (für unterschiedliche Produkte), entsprechende Lager mit deren Transportsystemen zur Bereitstellung von Vorprodukten oder Materialien zusammen mit einer übergeordneten Leittechnik erst die Fabrikation sicherstellen. Zwischen allen diesen Geräten ist der Austausch von Daten notwendig. Neben lokalen Netzwerken sind auch Funknetze in solchen Anlagen üblich. Die Mensch-Maschine-Kommunikation erfolgt nicht nur durch die Leittechnik, sondern auch über mobile Endgeräte, wie z.B. Tablets.

**Anmerkungen zum Sicherheitskonzept**

Für die Erstellung eines Sicherheitskonzept einer solchen Fertigung ist das Spezialwissen unterschiedlicher Disziplinen erforderlich, beginnend beim Betreiber und seinen technologischen Vorgaben, über IT-Experten, den Anlagen und Maschinenherstellern mit seiner Expertise zur Automatisierungstechnik und weitere. Das Sicherheitskonzept ist entsprechend vielschichtig.

Ein erster Ansatz könnte sein, die einzelnen erforderlichen Prozess-Schritte in Sicherheitsbereiche aufzuteilen bzw. die einzelnen CPS-Bereiche als Sicherheitszellen (die Summe der im Produktionsbereich vorhandenen Einzelanlagen) zu definieren, die Schnittstellen zu den übrigen Komponenten der Fertigungseinrichtung besitzen. Das Problem bei einer derartigen Aufteilung ist, dass auch die Interaktion zwischen den Anlagenteilen einzeln behandelt werden sollte, damit die Kommunikation planmäßig behandelt werden kann. Zusätzlich zur Informationssicherheit gelten die Sicherheitsrichtlinien für Maschinen und Anlagen.

Angelehnt an Fig. 13 ist die kleinste Einheit einer CPS-Produktionszelle eine CPS-Maschine. Übergeordnet zu jedem CPS-Bereich werden Leitsysteme benötigt, die mit dem Leitsystem der Fertigungslogistik im ständigen Datenaustausch stehen. Die Fertigungslogistik steht in der Hierarchie ganz oben, den sie übernimmt aus der Office-IT die Aufträge und gibt den Arbeitsfortschritt und weitere Informationen zu den einzelnen Aufträgen zurück.

### 6.3.1. Anlagenkonzept

Wie weiter oben beschrieben wird die Gesamtanlage in kleinere Bereiche aufgeteilt. Um effizient zu arbeiten sind mehrere Aufträge zeitgleich im Gesamtsystem in Bearbeitung.

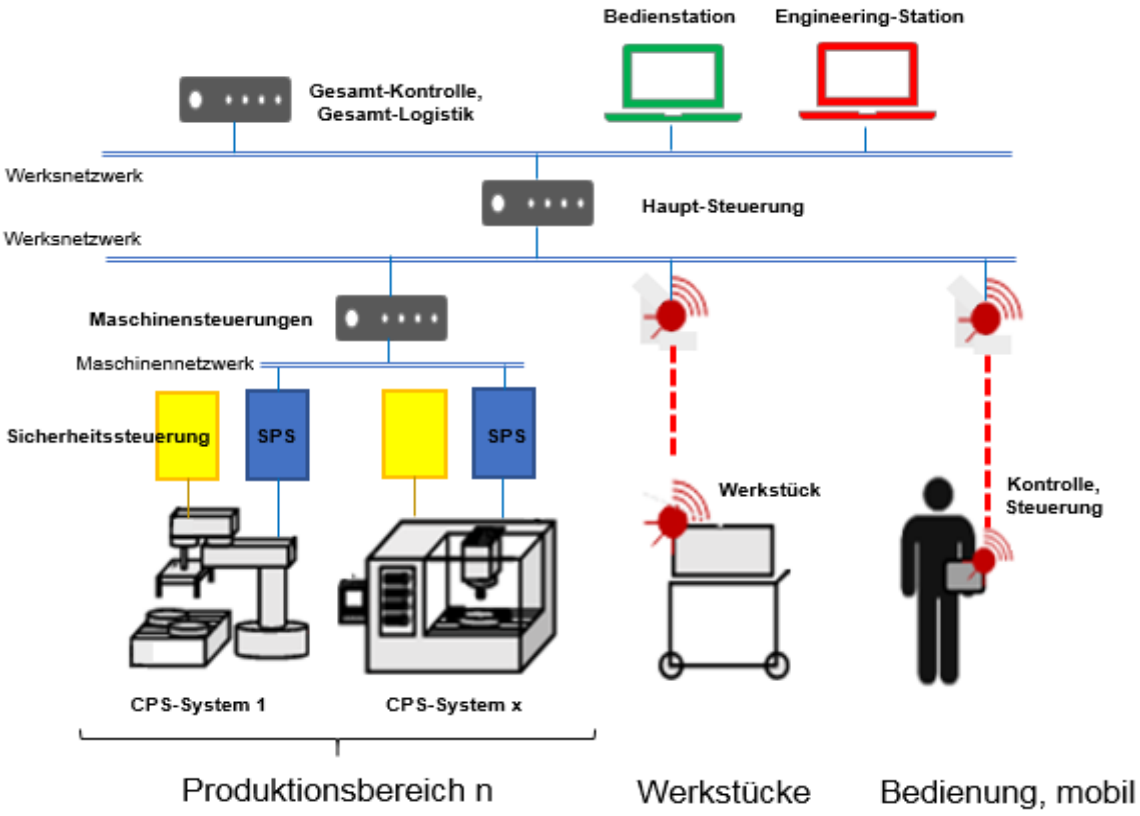



*Fig. 14: Netzwerkplan (symbolisiert) einer Industrie 4.0 Fertigung (nach [TK et. al. 16])*

Fig. 14 zeigt den Netzwerkplan stark vereinfacht. Die Fertigungslogistik übernimmt die Gesamtkontrolle. Die Maschinen werden je Produktionsbereich kontrolliert. Die Kontrolle der Produktionsbereiche sammelt alle relevanten Daten (z.B. Kapazitätsauslastung, aktuelle Maschinenparameter etc.). Die Hauptsteuerung übermittelt an die unterschiedlichen CPS, die z.B. Bearbeitungszentren sind, notwendige Einstellungen, wie ein für das Getriebe notwendiges Zahnrad zu fertigen ist (z.B. Abmessungen, Anzahl der Zähne, Art der Verzahnung etc.) und errechnet die Fertigungszeit in Abhängigkeit vom Werkzeugzustand (ob z.B. ein Werkzeugwechsel erforderlich ist). Für die Sicherheit der einzelnen CPS sind Sicherheitssteuerungen vorgesehen, die unabhängig von der Ablaufsteuerung arbeiten. Durch die strikte Trennung der Funktionen ist die Rückwirkungsfreiheit von Beginn an sichergestellt.

Aus der Leittechnik der CPS-Produktionszelle stammen Zustandsmeldungen der CPS-Maschinen wie frei oder beschäftigt mit den zugehörigen Informationen zum Arbeitsfortschritt und weiteren Parametern.[33] Die Assistenzsysteme sind Tablets, die einerseits wichtige Prozessdaten anzeigen, andererseits Eingriffe des Bedienpersonals ermöglichen.

Bei der erforderlichen Software für Leitsysteme, den einzelnen Fertigungseinrichtungen und dem Transportsystem ist sicherzustellen, dass nur die erforderlichen Softwarebestandteile

[33] Bei Werkzeugmaschinen muss z.B. nach einer bestimmten Anzahl von Bearbeitungen das Werkzeug gewechselt werden, bevor weitergearbeitet werden kann (Abnutzung). Bei Messvorrichtungen wird die Qualität geprüft und gegebenen falls ein fehlerhaftes Werkstück nachgearbeitet oder ersetzt. Messvorrichtungen müssen auch fallweise neu eingestellt oder kalibriert werden.

und Funktionen, die zur Aufgabenerfüllung benötigt werden, installiert sind. Auch entsprechende Schnittstellen der Hardware müssen geschlossen sein genauso wie nicht genutzte Ports. Im Wesentlichen geht es darum, mögliche Angriffspunkte zu minimieren.

Die funktionale Sicherheit muss gegeben sein, d.h. die Anlage muss derartig aufgebaut sein, dass sie im Gefahrenfall in einen sicheren Zustand übergeht (oder abschaltet).

### 6.3.2. Sicherheitskonzept Produktionsanlage

Auch hier wird der Prozess schrittweise durchlaufen. Ergänzend können auch die weiter oben diskutierten Bausteine entsprechend der Auswertung der Untersuchung als Maßnahmen berücksichtigt werden.

Insbesondere bei einer komplexen Anlage, wie diese weiter oben skizziert worden ist, muss schrittweise vorgegangen werden. Gerade deshalb, weil bei der Vielzahl von Anlagen der Überblick leicht verloren geht, sollten die einzelnen Prozessschritte beginnend bei der Definitionsphase mehrfach kontrolliert werden, um bereits von Beginn an möglichst keine Lücken im Konzept zu haben.

Begleitend sollte das Team, das später im Unternehmen für den Betrieb der Anlage und für die Sicherheitsaspekte zuständig ist, in den Prozess der Erstellung des Sicherheitskonzeptes mit eingebunden werden.

Eine besondere Bedeutung kommt dem letzten Schritt, der Evaluation durch einen unabhängigen Sachverständigen zu, um zu verifizieren, dass alle Risiken im Sicherheitskonzept berücksichtigt worden sind. Speziell bei so umfangreichen Projekten werden mehrere Durchläufe notwendig werden. Das Hauptproblem dabei wird sein, dass insbesondere die getroffenen Sicherheitsmaßnahmen zur Maschinensicherheit entsprechend überprüft und auf ihre Funktionsweise getestet werden müssen. Da diese Überprüfung erst am Schluss, also wenn eine Anlage bereits vollständig fertiggestellt ist, durchgeführt werden kann, entsteht ein hoher Zeitdruck, weil die Übergabe und Freigabe der Anlage erst nach der erfolgten Bestätigung oder Zertifizierung erfolgen kann.

Eine besondere Herausforderung sind dabei die Funkverbindungen für die Datenübertragung, wie die Kommunikation zwischen Werkstücken und Panels zur Hauptsteuerung über das WLAN (wireless local area network).

Bei der Einrichtung des Funknetzes ist zu prüfen, ob Dateninformationen innerhalb eines gegeben Zeitfensters zuverlässig übertragen werden können, weil hier das räumliche Umfeld die Qualität einer Verbindung beeinflussen kann. Das gilt hauptsächlich für die mobilen Bedienungseinrichtungen aber auch für die Kommunikation der Werkstücke mit dem Leitsystem, weil diese unter Echtzeitbedingungen erfolgen sollte. Günstige örtliche Bedingungen sind in der Fabrik-Automatisierung nicht immer anzutreffen, weil mit reflektierenden Metallteilen (z.B. Maschinen) zu rechnen ist. Durch Unterbrechungen im Funkverkehr kann es daher auch zur Beeinträchtigung der Funktion und im schlechtesten Fall der Sicherheit kommen. Auch über das Funknetz können auf Grund der Struktur des Netzes Angriffe auf das System erfolgen. Eine Möglichkeit zur Sicherung gegen Angriffe von Dritten ist, einerseits die Reichweite der

WLAN Verbindung so einzuschränken, dass diese für den reibungslosen Betrieb ausreichend ist und andererseits die Fabrikationsumgebung entsprechend abzuschirmen, dass Angreifer von außen keine Verbindung zum internen Funknetz aufbauen können. [34]

[34] Anmerkung: Die Richtlinie VDI/VDE 2185 beschreibt die Kriterien über die Anforderungen an die Funkkommunikation in der Automatisierungstechnik. Funkstrecken sind offene Verbindungen, deshalb ist die Abhörsicherheit und der Schutz gegen unberechtigte Zugriffe entscheidend. Dazu existierende Sicherheitsmechanismen sind in der IEEE 802.11 beschrieben.

# 7. Diskussion der Ergebnisse

Diese Arbeit hat als Schwerpunkt die Untersuchung von Vorgehensmodellen für Safety und Security behandelt, wie diese in der Automatisierung technischer Systeme genutzt werden können, um ganz allgemein die Informationssicherheit zu betrachten. Die Ergebnisse dieser Untersuchung werden zuerst den aufgeworfenen Fragestellungen gegenübergestellt und danach unter dem Aspekt der aus den Szenarien gewonnen Erkenntnisse diskutiert.

## 7.1. Nutzen und Nutzbarkeit der Modelle

Die Grundidee dieser Arbeit war, ein Sicherheitsmodell aus einzelnen Bausteinen aufzubauen, die gezielt zum Schließen von Sicherheitslücken eingesetzt werden sollen. In diesem Abschnitt werden Erkenntnisse bezogen auf die Forschungsfragen in Relation zum generellen Nutzen und der Nutzbarkeit der Modelle beleuchtet.

### 7.1.1. Aufgeworfene Forschungsfragen

Zuerst wurde die Frage aufgeworfen, welche zusätzlichen Sicherheitsmaßnahmen zum Schutz der technischen Systeme in der Produktion implementierbar sind.

In jedem Sicherheitsmodell geht es darum, Sicherheitsrisiken zu identifizieren und entsprechende Gegenmaßnahmen vorzunehmen, um ein bestehendes Risiko zu minimieren. Je feiner und detaillierter Abstufungen in einem Modell zur Einschätzung von Risiken getroffen werden, desto treffsicherer werden Risiken bewusst und damit sichtbar gemacht, da nur erkannte Risiken gemindert werden können. Im Wesentlichen hat sich die Arbeit dazu auf jene Risiken beschränkt, die über das IT-Netz die daran angeschlossenen Komponenten betreffen, sei es dadurch, dass deren Funktion beeinträchtigt wird oder dadurch, dass speziell bei sicherheitskritischen Anwendungen durch Fehlfunktionen Schaden entsteht.

Ganz allgemein gilt für Anlagen und insbesondere für Produktionsmaschinen die Maschinensicherheitsrichtlinie, die das gesetzliche Rahmenwerk bildet, um Personenschäden aber auch Schäden an den Einrichtungen selbst und die Umwelt zu verhindern. Insbesondere gilt es dabei zu verhindern, dass die in derartigen Anlagen verwendeten Sicherheitseinrichtungen wie Sicherheitssteuerungen oder andere Sicherheitseinrichtungen unzulässig durch Angriffe über das IT-Netz außer Funktion gesetzt werden können. Dazu wurden mehrere Bausteine als Maßnahmen vorgeschlagen, die entweder einzeln oder auch in Kombination geeignet erscheinen, die Sicherheit zu erhöhen. Einen besonderen Stellenwert nimmt dabei die Auftrennung des Netzwerkes in Zonen ein, die aufgrund von sehr strengen Kommunikationsregeln Schad-Programmen den Zugang auf die Rechnersysteme der Steuerung verwehren.

Selbst wenn man davon ausgeht, dass Steuerungen für Automatisierungsaufgaben ausreichend verifiziert und durch umfangreiches Testen als validiert anzusehen sind, sind in den Steuerungsprogrammen eine ganze Reihe von Parametern verankert, die von Auftrag zu Auftrag variiert werden müssen. Dass ein Computerwurm erfolgreich Daten einer Industriesteu-

erung verändern kann, beweist ein bekannt gewordener Vorfall (vgl. [IDG2014]). [35] Im seinerzeit bekannt gewordenen Fall wurde das Schadprogramm über das Leitsystem in die Steuerung eingeschleust.

Um die Möglichkeit der Übertragung von Parameterdaten in eine Steuerung zu erschweren, kann ein Baustein für den Speicherschutz der Steuerung beitragen. Solange die Funktion des Speicherschutzes aktiv ist, ist ein Zugriff auf die Steuerung selbst nicht möglich. Eine weitere Möglichkeit, Parameter-Daten auf Plausibilität zu prüfen, ist vielfach in den Steuerungssystemen selbst nur erschwert möglich, könnte aber durch eine externe Prüfeinheit die als Filter, die eine Anbindung des Fabrik-Netzes zur Steuerung selbst herstellt, realisiert werden. Das wurde in dieser Arbeit jedoch nicht weiter ausgeführt.

Als weiterer Baustein, insbesondere auch um den Datenverkehr von Steuerungssystemen zu den übergeordneten Leitsystemen zu kontrollieren, wurden Datendioden vorgeschlagen. Diese lassen nur den Datenverkehr in eine Richtung zu, z.B. von der Steuerung zu anderen Teilnehmern, und sind daher bezogen auf die Steuerung rückwirkungsfrei.

Beim Baustein Zero-Trust-Modell ist es eher fraglich, ob die Datenverschlüsselung zwischen einzelnen Netzwerkgrenzen einfach implementiert werden kann. Es stellt sich dabei auch die Frage, ob etwa ein über ein Feldbussystem eingeschleustes Schadprogramm erfolgreich von den übrigen Systemen getrennt werden kann.

Wie bereits erwähnt ist die Risikoanalyse ein Eckpunkt dafür, ob sich der Aufwand und der daraus resultierende Nutzen für einzelne Maßnahmen lohnt und welche alternativen Maßnahmen mit geringerem Aufwand umsetzbar sind und dennoch vergleichbare Ergebnisse erzielen können.

Davon unabhängig wurde ein weiteres Vorgehensmodell für die Automatisierung diskutiert, dass in acht Schritten jeweils zyklisch zu durchlaufen ist und schrittweise beginnend von der Definition der Gerätschaften über die Feststellung von möglichen Bedrohungen nach der Bestimmung von Schutzzielen anhand einer Risikoanalyse mit entsprechender Kostenanalyse die Umsetzung von Schutzmaßnahmen vorsieht. In diesem Modell ist die Kosten-Nutzen-Analyse bereits Teil des Vorganges. Dieses Modell sieht weiter vor, dass gesetzte Maßnahmen von externen Experten evaluiert werden, die eine Sicherheitsfreigabe erteilen oder weitere Verbesserungsmaßnahmen fordern.

Selbst wenn zu einem bestimmten Zeitpunkt die Sicherheit attestiert worden ist, bedeutet das nicht, dass der Vorgang nicht wiederholt werden muss, wenn neue Erkenntnisse über die Sicherheitslage oder neue Bedrohungen bekannt werden. Das gilt grundsätzlich für alle Modellansätze.

[35] Das Schadprogramm Stuxnet beschädigte Turbinen in einer Uranaufbereitungsanlage. Der Angriff erfolgte über ein System zur Überwachung und Steuerung (SCADA-System) durch Manipulation von Maschinenparametern in einer Simatic S7 SPS des Herstellers Siemens [IDG14].

Zur weiteren Frage, welche Möglichkeiten für die technische und organisatorische Nach- bzw. Aufrüstung technischer Systeme im Bereich der Automatisierungstechnik existieren, ist zu bemerken, dass die Lebensdauer von Anlagen und Maschinen in der Regel deutlich größer ist als jene der Steuerungssysteme. Oftmals bedeutet das, dass die Steuerungssysteme ersetzt werden müssen, wenn z.B. keine Ersatzteile mehr für Steuerungskomponenten erhältlich sind. In diesem Fall spricht man von Retrofit. Im Idealfall kann beim Austausch der Steuerungssysteme das ursprüngliche Steuerungsprogramm mit Anpassungen übernommen werden. Obwohl das den Aufwand vermindert, ist der Austausch wesentlicher Komponenten in einer Maschine oder Anlage so zu betrachten, als hätte eine Neuerrichtung stattgefunden.

Grundsätzlich ist es wünschenswert, im Zuge des Retrofit auch die Sicherheitsmaßnahmen auf den Stand der Technik nach zu führen. Das bedeutet, dass die gesamte Beurteilung der Sicherheit der Maschine bzw. Anlage beginnend vom Anfang an neu zu bewerten ist und ein neues Sicherheitsmodell erstellt werden muss. Einzelne Komponenten aus dem genannten Modellbaukasten können dazu geeignete Maßnahmen sein.

Zur nächsten Frage, wie ein Maßnahmenpaket aus Einzelmaßnahmen in einen Modellbaukasten eingeordnet werden kann, wurde kein Teilmodell modelliert. Dazu folgen weiter unten noch einige Anmerkungen.

In Bezug auf mögliche Abwehrmaßnahmen alle Bereiche betreffend wird auf den BSI-Grundschutz und dem BSI-Grundschutz Katalog verwiesen. [36]

Die Fragestellung nach der technischen Umsetzbarkeit der vorgeschlagenen Maßnahmen kann auf die Frage nach der Kosten-Nutzen Relation reduziert werden. Betrachtet man die in der Literatur veröffentlichen Vorfälle zu Schadenfällen, werden Investitionen in Sicherheitskonzepte für Unternehmen immer wichtiger.

Zur abschließenden Frage, wie einzelne Maßnahmen, Teilmodelle und Modelle zur Erhöhung der Sicherheit in Bezug auf ihre Wirksamkeit verifiziert werden können ist zu bemerken, dass die Überprüfung und Evaluierungen jedenfalls von unabhängigen Experten zu beurteilen sind, die nicht an der Erstellung und Implementierung der gesetzten Sicherheitsmaßnahmen beteiligt gewesen sind.

### 7.1.2. Diskussion

Die genannten Schutzmaßnahmen sind im Wesentlichen darauf aufgebaut, das Automatisierungsnetz von der übrigen IT in einem Unternehmen möglichst gut abzuschotten. Die Idee dabei ist, mögliche Schädigungen durch Malware von den Automatisierungssystemen fernzuhalten. Prinzipiell gilt diese Strategie auch für weitere kritische Bereiche, die im Bereich der IT angesiedelt sind, wie z.B. besonders schützenswerte Abteilungen wie die Buchhaltung, Geschäftsleitung oder Forschung und Entwicklung. Prinzipiell können dort auch Abschottungen durch Teilung der Netze in Bereiche eingeführt werden. Demgegenüber steht die Intention des IT-Grundschutzes, der vom BSI verfolgt wird, nämlich von vorhinein den Zugang durch

[36] Hier sei insbesondere auf die Edition 2020 des IT-Grundschutz-Kompendiums [BSI20] verwiesen.

entsprechende Firewalls zwischen dem Internet und dem IT-Netz eines Unternehmens so stark zu machen, dass damit das gesamte System geschützt werden kann. Die Idee dahinter ist, wenn das Eindringen von Malware in das Netz verhindert werden kann, kann es auch innerhalb dieses Netzes angeordnete Automatisierungssysteme nicht beeinflussen.

Dennoch werden Automatisierungssysteme üblicherweise mit zusätzlichen Schutzmaßnahmen versehen, weil speziell bei Industrie 4.0 Anlagen die dort befindlichen Produktionseinheiten stark vernetzte Systeme sind, wo es relativ schwierig ist, alle Zugangswege zu den Systemen wirksam zu kontrollieren. Auch diese Arbeit erhebt nicht den Anspruch, alle möglichen Risiken behandelt zu haben. Es gilt nach wie vor der Grundsatz, dass es absolute Sicherheit nicht geben kann.

Betrachtet man die Schadensfälle, dann kann im Fehlerfall ein gestörtes IT-Bürosystem verantwortlich für einen enormen finanziellen Schaden sein, ein gestörtes IT-Netz für ein Automatisierungssystem neben enormen finanziellen Schäden auch Schäden an Personen und an der Umwelt hervorrufen. Diese Überlegungen laufen schlussendlich wieder zu der Frage zum Verhältnis Risiko-Kosten-Nutzen gegenüber Prioritäten zur Sicherheit hinaus.

## 7.2. Kritische Betrachtung der Analysen

Im Abschnitt 2.2 sind existierende Lösungsansätze und Entwicklungen vorgestellt worden, die die Entwicklung des Modells und der Vorgehensweise inspiriert haben. In drei Anwendungsszenarien wurde in Kapitel 6 untersucht, wie Verbesserungsmaßnahmen zur Erhöhung der Sicherheit eingeführt werden können und wo entsprechende Ansatzpunkte dazu zu finden sind. Im Folgenden werden die daraus gewonnenen Erkenntnisse diskutiert.

### 7.2.1. Ergebnisse zum Szenario „RECPLAST GmbH“

Für die RECPLAST GmbH liegt in der Veröffentlichung [BSI18-REC] bereits das Konzept für das gesamte Sicherheitsmanagement dieses Unternehmens vor. Die in weiterer Folge vorgeschlagenen Sicherheitsmaßnahmen orientieren sich am Modellbaukasten und den darin enthaltenen Bausteinen.

Ergänzend wurde vorgeschlagen, in ein Sicherheitshandbuch bezogen auf jede Tätigkeit und jeden Arbeitsplatz Sicherheitsrichtlinien festzulegen, die als Teil der Arbeitsplatzbeschreibung genutzt werden können und zusätzlich in ihrer Summe das gesamte Regelwerk für die IT-Sicherheit im Unternehmen ergänzen.

Weiters wurde vorgeschlagen, das allgemeingültige Sicherheitskonzept insoweit zu spezifizieren, in dem im gegebenen Fall bestimmte Geschäftsbereiche als Zonen mit erhöhtem Sicherheitsbedarf definiert werden.

Genauso, wie später auch bei den anderen Szenarien, existieren gesetzliche, regulatorische und vertragliche Vorgaben, die einzuhalten sind.

Da der Faktor Mensch als Risikoquelle einen hohen Stellenwert in der Beurteilung von Risiken ausmacht, insbesondere dann, wenn diese Risiken auf unbewusstes oder bewusstes Handeln

zurückgehen, kann versucht werden das Gefährdungspotenzial etwa durch Zugangsbeschränkungen so weit wie möglich zu minimieren. In erster Linie werden jedoch Maßnahmen wie die Stärkung der Awareness und Sensibilisierung der Mitarbeiter*innen zur Erhöhung der Sicherheit beitragen.

Das Festlegen von Regeln, was im Falle eines erfolgten Cyber-Angriffs zu tun ist, könnte in Notfallplänen beschrieben werden.

Besonders schützenswert ist die Datenverbindung der beiden Firmenstandorte. In Bezug auf den benötigten Datenaustausch kann überlegt werden, welche Daten wo benötigt werden und den unbeschränkten Zugriff von einem Standort auf den anderen aber auch zwischen den einzelnen Abteilungen und innerhalb der Abteilungen auf das notwendige Maß einzuschränken.

Ergänzende Maßnahmen sind entsprechend des eingeführten Zonenkonzepts für bestimmte Geschäftsbereiche definiert. Die entsprechenden Maßnahmen orientieren sich dabei am Bausteinmodell, wo die einzelnen der dort vorgeschlagenen Bausteine den Bereichen zugeordnet worden sind.

Insbesondere hervorgehoben ist dabei die Betriebstechnik. Ähnlich der Automatisierungspyramide wurde vorgeschlagen, das Netzwerk zu segmentieren und gegeneinander abgesicherte Teilnetze vorzusehen. Auch hier wurde der Ansatz verfolgt, dass nur jener Datenaustausch freigegeben werden sollte, der dem Betriebszweck dient oder anders ausgedrückt, dass ein freier unbeschränkter Datenaustausch durch entsprechende Filtermaßnahmen verhindert wird.

Insbesondere ist bei Automatisierungsanlagen die Fernwartung durch den Hersteller jene Option, die bei Betriebsstörungen oder sonstigen Wartungsarbeiten Betriebsunterbrechungen möglichst verhindern soll oder helfen soll, gestörte Anlagen möglichst schnell wieder in den Produktionszyklus einzugliedern.

**Diskussion**

Durch die Anwendung der im Modell beschriebenen Bausteine werden Einzelmaßnahmen gesetzt, die zwar abgestimmt die Situation in einem bestimmten Bereich verbessern, aber dennoch nur stückweise durchgeführt werden. Bei den vorgeschlagenen Maßnahmen wurde nur auf deren Nutzen geachtet, die Kostenfrage jedoch nicht angeschnitten. Damit kann keine Kosten-Nutzen Relation hergestellt werden, denn alle Eingriffe in das System sind mit erheblichen Kosten verbunden, die von der Unternehmensleitung bereitgestellt bzw. bewilligt werden müssen.

### 7.2.2. Ergebnisse zum Szenario „IACS für einen technologischen Prozess“

Auf dem Gelände einer Raffinerie, wie z.B. das in Schwechat der Fall ist, existieren eine ganze Reihe von Teilbetrieben und Firmen, die Raffinerieprodukte in chemisch technologischen Prozessen erzeugen oder weiterverarbeiten. Die fraktionelle Destillation erzeugt leicht brennbare

Komponenten, deren Dämpfe hochexplosiv sind. Es existieren in solchen Anlagen explosionsgefährdete Bereiche, die ganz besondere Schutzmaßnahmen in Bezug auf die Überwachung und Steuerungstechnik benötigen. Deshalb sind im Anlagenkonzept redundant ausgeführte Steuerungen vorhanden, die sich gegenseitig überwachen. Die Redundanz ist deshalb erforderlich, weil die Verfügbarkeit solcher Anlagen besonders hoch sein muss.

Im Gegensatz zur sonst üblichen Steuerungstechnik ist die dezentrale Peripherie (Aktoren, wie z.B. Absperrungsorgane, sowie Sensoren, wie z.B. Stellung der Absperrungsorgane, Messsysteme etc.) nicht über Bussysteme gekoppelt, sondern direkt mit den Steuerungen verdrahtet. Parallel dazu existieren auch Bereiche, die nicht explosionsgefährdet sind und wie in sonst üblichen Anlagen auch über Feldbussysteme mit den Steuerungen verbunden sind.

Aufgrund der Wichtigkeit der Station sind auch weitere Geräte redundant ausgeführt. Insgesamt ist in der vereinfachten Netzinfrastruktur die Übersicht über die wesentlichen Komponenten gegeben.

Betrachtet worden ist die Netzsicherheit mittels des von der VDI/VDE 2182 vorgeschlagenen 8-Schritte Schemas exemplarisch für die speicherprogrammierbaren Steuerungen (SPS).

Dazu werden in der Definitionsphase zuerst alle Komponenten aufgestellt und danach mögliche Bedrohungen jeder Komponente mit den daraus resultierenden Folgen bei Schadenseintritt festgestellt. Um einen Überblick darüber zu bekommen, wie viele Komponenten zum Aufbau eines SPS-Systems benötigt werden, sei festgestellt, dass neben Komponenten wie der Zentraleinheit, Speicherkarten, Coprozessoren, Ein- und Ausgangskarten, das SPS-interne Bussystem etc. einzeln angeführt und bewertet werden muss. Ergänzt wird das Ganze dann noch mit den im Feld verbauten Geräten (Aktoren und Sensoren).

Bei der Definition der Schutzziele werden Prioritäten festgelegt. Fällt beispielsweise eine Eingangskarte bei einem redundanten System aus, kann diese auch im laufenden Betrieb ersetzt werden solange die parallellaufende zweite SPS ihre Aufgabe erfüllt. Betrifft der Ausfall jedoch beide SPS-Steuerungen, kommt es zu einem Anlagenstillstand und den daraus folgenden Schäden. Dementsprechend muss bei erkannten Fehlern schnell reagiert werden, und deshalb steht bei solchen Anlagen auch das Wartungspersonal meist 24 Stunden in Bereitschaft.

In der Risikobewertung sind mögliche Ausfälle entsprechend beziffert. Im gegebenen Fall wurde eine Skala eingeführt, die jedem Risiko einem bestimmten Zahlenwert zuweist.

Zu jedem Risiko sind auch mögliche Schutzmaßnahmen zuzuordnen gewesen, wobei auch finanzielle Aufwendungen für das Vorhalten von Schutzmaßnahmen festgelegt werden. Wird als Beispiel „defekte Eingangskarte“ mit einem bestimmten Risikowert definiert, kann dieser Risikowert durch das Vorhalten entsprechender Ersatzteile reduziert werden. Die sich daraus ergebende Differenz ist das sogenannte Restrisiko. Dazu werden die entsprechenden Schutzmaßnahmen ausgewählt, die vorher abgeschätzten Kosten für die Durchführung der Schutzmaßnahmen budgetiert und nach Genehmigung durch die Geschäftsleitung durchgeführt.

Am Ende des Prozesses wird die Sicherheit der Anlage von unabhängigen Experten evaluiert und abgenommen.

In dieses Konzept können für die weiter oben genannten Schutzmaßnahmen auch die im Modell vorgeschlagenen Bausteine zur Minderung der Risiken eingesetzt werden.

**Diskussion**

Grundsätzlich ist die Vorgehensweise nach dem 8-Schritte Schema ein sehr aufwendiger Prozess, bei dem jeder Anlagenteil einzeln bewertet werden muss. In dieser Arbeit sind nur Risiken, die die IT-Sicherheit betrachten untersucht worden und allfällige mechanische Gebrechen an der Anlage selbst unberücksichtigt geblieben. Es ist leicht abzuschätzen, dass der benötigte Aufwand dieses Prozesses entsprechend der Größe und im Umfang von solchen Anlagen sehr hoch ist.

### 7.2.3. Ergebnisse zum Szenario „Sicherheit in der Industrie 4.0 Produktion“

In der genannten Industrie 4.0 Produktion wurde ebenfalls nach dem 8-Schritte Schema vorgegangen. Im Unterschied von zuvor sind es viel mehr Teilanlagen und dem entsprechend auch viel mehr Komponenten.

Aus dem Netzwerkplan ergibt sich, dass eine Reihe von CPS-Systemen existieren, die grundsätzlich getrennt zu untersuchen sind, aber auch gewisse Parallelitäten besitzen, so dass sich die Untersuchungsschemen für die unterschiedlichen Produktionsbereiche ähneln.

Identisch sind sowohl die Anknüpfung der Werkstücke an die Hauptsteuerung als auch die Anknüpfung der mobilen Bedienung und Überwachung. Bei den notwendigen Kostenabschätzungen können die ermittelten Zahlenwerte einfach multipliziert werden. Eine kleine Kostenreduktion ist auch dadurch zu erwarten, dass eine allfällige Ersatzteilhaltung aufgrund ähnlicher Steuerungskomponenten und sonstiger Geräte optimiert werden kann.

Die maschinelle Ausstattung der einzelnen CPS-Systeme wurde nicht definiert. Wurde die Ausstattung geschickt gewählt, würde der Ausfall eines dieser Systeme zwar die Produktionskapazität vermindern aber der Arbeitsanfall könnte von anderen Stationen übernommen werden. Auf diese Art und Weise kann ein Revisionsplan für allfällige Wartungen aufgestellt werden.

Ein sicherheitskritisches Element sind dort vorgesehene WLAN-Kopplungen. Aus der Gesamtübersicht ist erkennbar, dass in dem diskutierten Konzept auch innerhalb der CPS-Systeme WLAN-Verbindungen bestehen können. In diesem Zusammenhang wurde vorgeschlagen, die Sendeleistung der Funkverbindungen so zu dimensionieren, dass die Abhörsicherheit im gesamten Fabriksgelände gegeben ist, sodass über die ohnehin gesicherten WLAN-Verbindungen der Zugriff von außen nahezu unmöglich gemacht wird.

**Diskussion**

Aufgrund einer Vielzahl von Anlagen in einer Industrie 4.0 Produktion ist der Aufwand entsprechend höher. Das Produkt z.B. ein Getriebe kennt seine Evolutionsstadien und kann auf Grund dieser Kenntnis mit den CPS kommunizieren, um z.B. entsprechende Bearbeitungszeitfenster zugeteilt zu erhalten. Dazu muss das Produkt die Reihenfolge der benötigten Ferti-

gungsschritte kennen. Parallel dazu sind die benötigten Vormaterialien aus der Lagerverwaltung zeitgerecht bereitzustellen etc. Es herrscht damit ein ständiger interner und externer Datenaustausch einerseits zu den CPS in Bezug auf deren Auslastung, andererseits zum Lager bezüglich der Beschaffung und zu Nachbestellung bei Vorlieferanten und darüber hinaus zur Auftragsbearbeitung und zu den Kunden.

Zur Systemabsicherung sind umfangreiche Maßnahmen notwendig. Insbesondere auf Grund der Vielfalt möglicher Kommunikationskanäle müssen diese nicht nur einzeln überprüft, sondern auch alle nicht für den Betrieb erforderlichen Verbindungen aufgedeckt und eliminiert werden.

## 7.3. Schlussfolgerungen

Das allgemeine Problem für IT-Sicherheit ist, dass eine Vielzahl unterschiedlicher Programme verschiedener Hersteller Daten verarbeiten, die von den unterschiedlichsten Systemen bereitgestellt oder auch in einem Unternehmen erzeugt werden. Was alles innerhalb von Datensätzen enthalten ist, die zwischen einer Vielzahl von Rechnersystemen ausgetauscht werden, wird nicht überprüft solange eine gewünschte Funktionalität gegeben ist. Im Grunde genommen interessiert es die Nutzer auch nicht, was etwa in einem Datei-Overhead für Informationen enthalten sind.

Ein Fehler in einem Programm, ein Fehler in einer Datei etc. fällt niemandem auf, solange er keine Auswirkungen hat. Es kann durchaus vorkommen, dass in Programmen „Datei Müll“ enthalten ist, wenn etwa beim Ändern eines Programmes nicht mehr genutzte Teile ungewollt oder unbewusst nicht entfernt worden sind, die ihrerseits so lange nichts bewirken, solange sie nicht von Rechnersystemen angesprochen werden. Das könnte auch nie der Fall sein. Andererseits könnte auch der Fall eintreten, dass nach einem Softwareupdate solche eigentlich unbrauchbaren Programmsegmente angesprochen werden und zu Fehlern führen.[37]

Angriffe auf ein System können effektiv bekämpft werden, wenn Sicherheitslücken oder Angriffsmechanismen bekannt sind. Das bedeutet, dass bei der Risikoanalyse sowohl die Gerätetechnik und deren Sicherheitsmechanismen als auch die Unsicherheitsquelle „Mensch“[38] in die Untersuchungen mit einbezogen werden müssen.

Unabhängig davon ist festzustellen, dass beginnend von der Definition der Anforderungen an die IT-Sicherheit bis hin zu seiner Umsetzung und Evaluierung eine Vielzahl von Arbeitsschritten erforderlich sind. Je nach Umfang einer Anlage wird ein hoher Zeitaufwand dafür benötigt. Es erscheint daher zweckmäßig zu sein, gleich von Beginn an bei der Konzeption von Maschinen und Anlagen und der Konzeption der kompletten IT die Sicherheitsfragen mit zu bedenken und bereits zu diesem Zeitpunkt mit der Arbeit zu beginnen. Die begleitende Entwicklung von

[37] In „Software - das unterschätzte Sicherheitsrisiko“ ist in [LS93] z.B. ein Artikel veröffentlicht, der diese Problematik beschreibt.

[38] z.B. durch das Negieren oder Unterschätzen von Risiken, mangelnde Vorstellung von Folgen einer Handlung etc.

Sicherheitskonzepten hat den Vorteil, dass allfällige Änderungen bei der Ausführungsplanung bekannt sind und in die Sicherheitskonzepte eingearbeitet werden können.

Im Überprüfungsfall bei bestehenden Anlagen ist es notwendig, neben den Gegebenheiten im Unternehmen auch die Arbeitsweise und Abläufe des Geschäftsbetriebes zu berücksichtigen. Werden firmenfremde Personen mit der Überprüfung beauftragt, sollten Kontaktpersonen im Unternehmen namhaft gemacht werden.

# 8. Zusammenfassung und Ausblick

Ein Grundsatz bei der erforderlichen Software für Leitsysteme ist, dass nur die erforderlichen Softwarebestandteile und Funktionen, die zur Aufgabenerfüllung benötigt werden, installiert sind. Betrachtet man die typische Office-Welt der Arbeitsplätze für die unterschiedlichen Büroanwendungen, kann festgestellt werden, dass die dort installierte Software aufgrund ihres universellen Charakters weitaus mehr Möglichkeiten bietet als die für die unmittelbare Aufgabenerfüllung benötigte Funktionalität.[39]

## 8.1. Büroarbeitsplätze

In größeren Unternehmen sind IT-Abteilungen für die Einrichtung der Arbeitsplätze und der gesamten IT-Infrastruktur zuständig. Diese bieten auch Supportleistungen für die übrigen Bereiche und Arbeitsplätze an. In der Regel werden von der IT-Abteilung auch die Rechte als Administratoren verwaltet, so dass bei den Arbeitsplatzrechnern die Eingriffsmöglichkeiten der dort Beschäftigten entsprechend beschränkt ist. Von einer derartigen Konstellation wird im Folgenden ausgegangen.

Bezogen auf jeden Arbeitsplatz kann gefragt werden, ob etwa der Zugang zum Internet für jede mögliche Stellenbeschreibung in vollem Umfang erforderlich ist. Es ist bekannt, dass Schadprogramme unter anderem auch über das Internet in ein Büronetzwerk eingeschleust werden können. Sperrt man den Internetzugang dort, wo er für den Betriebsablauf nicht benötigt wird, kann von diesem bestimmten Rechner aus gesehen eine Infektion mithilfe eines Schadprogramms erst gar nicht erfolgen. Maßnahmen dieser Art erfordern allerdings einen hohen Aufwand in der IT-Abteilung eines Unternehmens, deshalb werden die typischen Office-Programme in der Regel für die Nutzer*innen in ihrem vollen Funktionsumfang zur Verfügung gestellt. Ähnlich liegt der Fall beim E-Mailverkehr, wo zum Beispiel mittels geeigneter Maßnahmen bestimmte Dateianhänge gefiltert werden können oder aus dem Inhalt interaktive Links automatisiert entfernt werden.

Es ist bekannt, dass schädliche Websites sowohl Schadinhalte übertragen können als auch unbemerkt von Nutzer*innen Daten sammeln. Um vor derartigen Sicherheitsgefährdungen zu warnen, können manche Office-Programme derart konfiguriert werden, dass Warnungen angezeigt werden. Ist der Zugang zum Internet bei einem derartigen Arbeitsplatz nicht von vornherein gesperrt, können in den Voreinstellungen Listen von vertrauenswürdigen Websites konfiguriert werden, für welche der Internetzugang ermöglicht wird. Bei Dokumenten können z.B. Acrobat und Acrobat Reader so konfiguriert werden, dass diese eine Warnung anzeigen, sobald eine PDF-Datei versucht, eine Verbindung zu einer Website herzustellen.

[39] Anmerkung: Zur Minimierung der Angriffsmöglichkeiten soll das „Härten“ (engl. hardening) der Software erfolgen: nur benötigte Software-Funktionen werden installiert, nicht erforderliche Funktionalitäten werden entfernt oder gesperrt. Zusätzlich wird das Zero Trust Prinzip genutzt: System Kontrollen, basierend auf Richtlinien, Transparenz und Protokollierung.

Es ist davon auszugehen, dass die interne Überwachung des Datenverkehrs durch automatische Zugangssperren keine Verletzung der Persönlichkeitsrechte von Mitarbeiter*innen ist oder sonstigen gesetzlichen Regelungen widerspricht.

Wie weiter oben schon erwähnt, hat das BSI Empfehlungen zur sicheren Konfiguration von Microsoft-Office-Produkten veröffentlicht (vgl. [BSI19-1]).

## 8.2. Leitrechner in der Automatisierung

Bei Leitrechnern in Automatisierungssystemen werden üblicherweise die Daten und Befehle zwischen dem Leitsystem und der Steuerung ausgetauscht. Typisch für solche Systeme ist, dass aus diesen Systemen Aufträge, wie z.B. das in Betrieb setzen von Anlagenfunktionen, das Schalten von Antrieben etc. und gegebenenfalls das Übertragen von Parametern an die Steuerungssysteme weitergeleitet werden.

Auf der anderen Seite werden Daten vom Betriebszustand zur Weiterleitung an das Leitsystem abgefragt. Die abgefragten Daten sind in den Steuerungssystemen in reservierten Speicherbereichen zusammengestellt. Um den Weg eines Schadprogramms aus dem Steuerungssystem in das Leitsystem zu sperren, kann der Datenverkehr insoweit gefiltert werden, indem die zu übertragenden Daten, die sich im Wesentlichen auf Zahlenwerte beschränken lassen, im empfangenden System nur als Zahlenwerte interpretiert werden. Prinzipiell lassen sich auch Betriebszustände als Zahlenwerte darstellen. Mit dem entsprechend erhöhten Programmieraufwand kann überprüft werden, ob valide Daten vorliegen oder nicht.

Eine Maßnahme zur Verbesserung der Abhörsicherheit ist die Verwendung von Lichtwellenleitern (zusammen mit den entsprechenden Umsetzern). Zur Erhöhung der Datensicherheit können Redundanzen bei der Datenerfassung (Sensorik) und Kontrollberechnungen (Software) die Datensicherheit erhöhen. Eine vergleichsweise einfache Möglichkeit ist das Festlegen von Grenzwerten, die bei Über- oder Unterschreitung einerseits alarmieren und anderseits Sicherheitsreaktionen auslösen (Software).

## 8.3. Ausblick

Absolute Sicherheit kann nicht erreicht werden. Das ist einerseits damit begründet, dass, um Sicherheit zu erreichen, zuerst alle möglichen Gefährdungen und Schwachstellen in einem System bekannt sein müssen, damit die entsprechenden Gegenmaßnahmen geplant werden können. Wurden derartige Gegenmaßnahmen gefunden und implementiert, muss wiederum sichergestellt werden, dass deren Wirksamkeit dauerhaft gegeben ist. Im Zuge der technischen Weiterentwicklung wird es immer wieder neue Geräte und Prozesse geben, sodass neue Anforderungen an die Sicherheit gestellt werden müssen und an dieser Stelle beginnt der Prozess von neuem. Maßnahmen zur Überprüfung der Sicherheit und zum Schließen von Sicherheitslücken sind ein sich ständig wiederholende Prozess, der nicht endet.

Damit sind die in dieser Arbeit vorgeschlagenen Maßnahmen als Momentaufnahme zu betrachten. Wird allgemein die Thematik Sicherheit in industriellen Anlagen betrachtet, stellen

sich immer wieder Fragen wie: „Wann ist eine Anlage sicher?“ oder „Wie sicher ist eine Anlage?“ oder „Ist die Sicherheit so weit gegeben, dass sie als ausreichend betrachtet werden kann?“.

Wurde ein bestimmter Sicherheitsstatus erreicht, bei dem eine industrielle Anlage als sicher eingestuft worden ist, existieren mehrere Aspekte. Der erste Aspekt ist allgemein gültig und betrifft Regeln und Anforderungen, die sich aus dem Stand der Technik ergeben und die als gesetzliche Bestimmungen, wie z.B. die Verordnungen zur Maschinensicherheit für die technische Ausrüstung der Produktion oder die Datenschutz Grundverordnung für den Bereich der kommerziell genutzten IT, einzuhalten sind. Betrachtet man den Datenschutz entsprechend der Datenschutz Grundverordnung bezieht sich dieser ausschließlich auf die personenbezogene Datenverarbeitung. In der Regel sind dabei die von den Fabrikationsanlagen erzeugten Daten, wie z.B. Betriebsdaten aus der Produktion, der Warenwirtschaft und zum Zustand der Produktionseinrichtungen ausgenommen. Dennoch sind auch diese Daten als hoch sensibel einzuschätzen, weil daraus auch Daten zur Leistungsfähigkeit eines Unternehmens abgeleitet werden können.

Daraus ergibt sich der zweite Aspekt. Daten aus der Produktion gelten als Betriebsgeheimnisse und werden sie offengelegt, kann das zu Nachteilen für ein Unternehmen führen. Auf der anderen Seite zählt es auch zu den Betriebsgeheimnissen, wie sich Unternehmen gegenüber möglichen Angreifern schützen. Daraus ergibt sich, dass tatsächlich getroffene Sicherheitsmaßnahmen im industriellen Umfeld für Außenstehende kaum zugänglich sind und dass daher von den üblichen, dem Stand der Technik entsprechenden Vorkehrungen auszugehen ist.

Der dritte Aspekt liegt im Unternehmen selbst und behandelt die Fragestellung, wie wichtig ist der Schutz der eigenen industriellen Anlagen und wie kann mit technischen Mitteln den äußeren Bedrohungen des eigenen Schutzstatus entgegengewirkt werden.[40] Schutzmaßnahmen zu implementieren, um bestimmte Schutzziele zu erreichen, ist ein aufwendiger Prozess. Dieser Prozess erfordert nicht nur die entsprechenden Ressourcen, sondern auch einen sich ständig wiederholenden Aufwand, um Schritt haltend dem Stand der Technik folgen zu können. Ein Dilemma liegt dabei bei den nicht unerheblichen Kosten, die das Einführen von Sicherheitsmaßnahmen mit sich bringen. Dazu kommt, dass ein Wettlauf entsteht, wie ständig neu hinzukommende Bedrohungen mit ergänzenden Sicherheitsmaßnahmen abgewehrt werden können. Das kann sogar soweit führen, dass aus betriebswirtschaftlicher Sicht die anfallenden Kosten den Nutzen übersteigen.

Weiter oben wurde der Stand der Technik erwähnt. Dazu ist festzustellen, dass die Entwicklung der kommerziell genutzten IT deutlich schneller voranschreitet und deshalb vergleichsweise kurzlebig gegenüber den industriell genutzten Steuerungssystemen ist, die langlebig sind und nur langsam modernisiert werden. Daraus ergeben sich Diskrepanzen im Sicherheitsstatus industriell genutzter gegenüber den kommerziellen Systemen.

[40] Anmerkung: Es existieren auch innere Bedrohungen, die hier nicht weiter behandelt werden.

Jedenfalls trägt zur Verbesserung des Sicherheitsstatus eines Systems bei, Absicherungsmaßnahmen so zu gestalten, dass ein Angriff auf ein System derart erschwert wird, dass sich der Aufwand für potenzielle Angreifer nicht lohnt. Erfolgversprechend bei IACS ist, die Daten der Produktion unattraktiv für Angreifer zu machen. Dort erzeugte Daten könnten so stark selektiert, überwacht und zusätzlich verschlüsselt werden, dass diese zwar für die Steuerungsfunktionen innerhalb des Unternehmens ausreichend sind, aber nach außen hin kaum Information über Produktionsabläufe preisgeben.

Insbesondere das überwachte Selektieren nach den Inhalten von Datensätzen erscheint geeignet, den Infektionsweg von Schadsoftware zu den übergeordneten Systemen der IACS zu unterbinden, indem als „suspekt“ klassifizierte Daten in Quarantäne genommen werden, zusammen mit der Ausgabe von Warnmeldungen oder Handlungsanweisungen.

# Literatur


[AS20] Alvarez Simon: „Tesla employee foregoes $1M payment, works with FBI to thwart cybersecurity attack“, 27.08.2020, https://www.teslarati.com/tesla-employee-fbi-thwarts-russian-cybersecurity-attack/, online abgefragt 08.09.2020

[ASIT19] A-SIT: „Österreichisches Informationssicherheitshandbuch“, Version 4.1.1 vom 19.12.2019, https://www.sicherheitshandbuch.gv.at/downloads/sicherheitshandbuch.pdf, online abgefragt 20.08.2020

[BBC14] BBC News: „Hack attack causes ‘massive damage’ at steel works“, https://www.bbc.com/news/technology-30575104, online abgefragt 10.02.2020

[BO19] Bendel Oliver: „Definition: Was ist „Industrie 4.0“?“, Gablers Wirtschaftslexikon, https://wirtschaftslexikon.gabler.de/definition/industrie-40-54032/version-368841, Revision von Industrie 4.0 vom 07.01.2019 - 17:27, online abgefragt 24.02.2020

[BM15] Bertovic Marija: “Human Factors in Non-Destructive Testing (NDT): Risks and Challenges of Mechanised NDT” - Scientific Figure on ResearchGate, 2015, Available from: https://www.researchgate.net/figure/Risk-management-process-ISO-310002009-reproduced-with-permission-of-DIN-Deutsches_fig6_282365896, online abgefragt 23.04.2020

[BJ et. al. 17] FireEye, Inc.601 McCarthy Blvd. Milpitas, CA 95035: “Malware ICS Security”, Attackers Deploy New ICS Attack Framework “TRITON” and Cause Operational Disruption to Critical Infrastructure, December 14, 2017, Blake Johnson, Dan Caban, Marina Krotofil, Dan Scali, Nathan Brubaker, Christopher Glyer, https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html, online abgefragt 10.02.2020

[BSI11] BSI IT-Grundschutz-Kataloge: 12. EL Stand 2011: „Gefährdungskatalog Elementare Gefährdungen“, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Gefaehrdungskatalog-G0-Elementare-Gefaehrdungen.pdf?__blob=publicationFile&v=1, online abgefragt 23.04.2020

[BSI13] Bundesamt für Sicherheit in der Informationstechnik: „ICS-Security-Kompendium“, 2013, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf;jsessionid=10777467E7553F677655A90277BC190F.1_cid360?__blob=publicationFile&v=2, online abgefragt 21.02.2020

[BSI18] Bundesamt für Sicherheit in der Informationstechnik (BSI), Referat WG 24: „On-line-Kurs IT-Grundschutz“, 2018, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/OnlinekursITGrundschutz2018/Lektion_3_Strukturanalyse/Lektion_3_01/Lektion_3_01_node.html, online abgefragt 06.02.2020

[BSI18-1] Bundesamt für Sicherheit in der Informationstechnik: „Die Lage der IT-Sicherheit in Deutschland 2018“, 2018, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2018.pdf?__blob=publicationFile&v=6, online abgefragt 10.02.2020

[BSI18-REC] Bundesamt für Sicherheit in der Informationstechnik (BSI): „Beschreibung des Beispielunternehmens RECPLAST GmbH“, 2018, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Webkurs/Recplast_Onlinekurs2018.pdf;jsessionid=B572E3BE112D5A7535EAA9FA229AD621.2_cid501?__blob=publicationFile&v=7, online abgefragt 19.08.2020

[BSI19] Bundesamt für Sicherheit in der Informationstechnik: „Die Lage der IT-Sicherheit in Deutschland 2019“, 2019, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf?__blob=publicationFile&v=7, online abgefragt 10.02.2020

[BSI19-1] Bundesamt für Sicherheit in der Informationstechnik Pressemitteilung: „BSI veröffentlicht Empfehlungen zur sicheren Konfiguration von Microsoft-Office-Produkten“, 19.06.2019, https://www.bsi.bund.de/DE/Home/home_node.html;jsessionid=43CB59D17E8E4D102AE8FBF08A728015.1_cid502, abgefragt 03.09.2020

[BSI20] Bundesamt für Sicherheit in der Informationstechnik: „Edition 2020 des IT-Grundschutz-Kompendiums“, 03.02.2020, ISBN: 978-3-8462-0906-6, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2020.html, online abgefragt 21.06.2020

[BSI20-IND] Bundesamt für Sicherheit in der Informationstechnik: „Edition 2020 des IT-Grundschutz-Kompendiums“, Abschnitt IND: Industrielle IT, 03.02.2020, ISBN: 978-3-8462-0906-6, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2020.html, online abgefragt 17.08.2020

[BSI20-NET] Bundesamt für Sicherheit in der Informationstechnik: „Edition 2020 des IT-Grundschutz-Kompendiums“, Abschnitt NET: Netze und Kommunikation, 03.02.2020, ISBN: 978-3-8462-0906-6, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2020.html, online abgefragt 17.08.2020

[BSI20-1] Bundesamt für Sicherheit in der Informationstechnik, „ISMS: Sicherheitsmanagement“, BSI Grundschutz, https://www.bsi.bund.de/DE/Themen/IT-Grundschutz/ITGrundschutzKompendium/bausteine/ISMS/ISMS_Uebersicht_node.html, online abgefragt 25.04.2020

[BSI20-2] Bundesamt für Sicherheit in der Informationstechnik, „BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS)“. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_1.pdf?__blob=publicationFile&v=8, online abgefragt 24.04.2020

[BSI20-3] Bundesamt für Sicherheit in der Informationstechnik, „BSI-Standard 200-2 IT-Grundschutz-Vorgehensweise“, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_2.pdf?__blob=publicationFile&v=7, online abgefragt 24.04.2020

[BSI20-4] Bundesamt für Sicherheit in der Informationstechnik, „BSI-Standard 200-3 Risikoanalyse auf der Basis von IT-Grundschutz“, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_3.pdf?__blob=publicationFile&v=7, online abgefragt 24.04.2020

[BSI20-5] Bundesamt für Sicherheit in der Informationstechnik, „BSI-Standard 100-4: Notfallmanagement Version 1.0“, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSIStandard_1004.pdf?__blob=publicationFile&v=1, online abgefragt 24.04.2020

[BSI20-6] Bundesamt für Sicherheit in der Informationstechnik, „Aktueller Informationsstand zur Weiterentwicklung des BSI-Standards 200-4“, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BCM/BCM_20190416_Infomail.pdf?__blob=publicationFile&v=2, online abgefragt 24.04.2020

[BSI20-7] Bundesamt für Sicherheit in der Informationstechnik, „BSI-IT-Grundschutz-Katalog“, 2016, https://download.gsb.bund.de/BSI/ITGSK/IT-Grundschutz-Kataloge_2016_EL15_DE.pdf, online abgefragt 24.04.2020

[BKA17] Bundeskriminalamt, Weber, Julia: „Innentäter in Unternehmen - Zusammenstellung aktueller inländischer Forschungsbeiträge zum Forschungsstand und Handlungsempfehlun-gen zur sogenannten Innentäterschaft“, 04.08.2017, https://www.wirtschaftsschutz.info/SharedDocs/Artikel/DE/BKA-Monitoringbericht-Innentaeter.pdf?__blob=publicationFile&v=2, online abgefragt 08.09.2020

[DPR20] Datenschutzpraxis, „Mustergliederung einer IT-Sicherheitsrichtlinie“. https://www.datenschutz-praxis.de/praxishilfen/muster-gliederung-it-sicherheitsrichtlinie/, online abgefragt 23.08.2020

[CFT20] CFT GmbH Compact Filter Technic, Produktvorstellung, 2020, https://cft-gmbh.de/en/smart-filter-technology, online abgefragt 31.08.2020

[DH11] Dirnberger Herbert: „Entwicklung eines Zellen-basierten Frameworks für Industrial Information Security“, Diplomarbeit, Juni 2011, Ferdinand Porsche FernFH, https://www.cybersecurityaustria.at/images/pdf/Dirnberger2011.pdf, online abgefragt 05.02.2020

[DSG2000] 165. Bundesgesetz: Datenschutzgesetz 2000 – DSG 2000, in der gelenden Fassung, https://www.ris.bka.gv.at/Dokumente/BgblPdf/1999_165_1/1999_165_1.pdf, online abgefragt 25.07.2020

[EK19] EUROPÄISCHE KOMMISSION Generaldirektion Binnenmarkt, Industrie, Unternehmertum und KMU Industrieller Wandel und moderne Wertschöpfungsketten—Fortgeschrittene Ingenieurstechnik- und Fertigungssysteme, 2019, https://www.bmas.de/SharedDocs/Downloads/DE/Thema-Arbeitsschutz/leitfaden-fuer-anwendung-maschinenrichtlinie-2006-42-eg.pdf;jsessionid=31F9FAA6F8EE90BC5A31962C86369D8D?__blob=publicationFile&v=2, online abgefragt 17.08.2020

[EX18] onlinesicherheit.gv.at, „Experteninformation - Sicherheitsmanagement - Informationssicherheits-Managementsystem“, 25.05.2018, https://www.onlinesicherheit.gv.at/experteninformation/sicherheitsmanagement/informationssicherheits-managementsystem/71260.html, online abgefragt 24.04.2020

[FG20] Fraunhofer-Gesellschaft: „Strategie- und Positionspapier Cyber-Sicherheit 2020: Herausforderungen für die IT-Sicherheitsforschung“, 2020, https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Cyber_Security_2020.pdf?_=1394197956, online abgefragt 24.02.2020

[FUB19] Freie Universität Berlin, „IT-Sicherheitsrichtlinie der Freien Universität Berlin“, Apr. 04, 2019, https://www.fu-berlin.de/sites/it-sicherheit/downloads/IT-Sicherheitsrichtlinie.pdf, online abgefragt 21.08.2020

[HSN19] Hochschule Niederrhein, „Leitlinie zur Informationssicherheit“, Feb. 02, 2019. https://www.hs-niederrhein.de/fileadmin/dateien/dez_st/amtliche_bekanntmachungen/Satzungen_und_Ordnungen/Leitlinie_Informationssicherheit_V2.1.pdf, online abgefragt 21.08.2020

[IDG2014] IDG Business Media GmbH: „Computerwurm Stuxnet wurde nicht über USB-Stick verbreitet“, 12.11.2014“, München, https://www.computerwoche.de/a/computerwurm-stuxnet-wurde-nicht-ueber-usb-stick-verbreitet,3071344, abgefragt 12.09.2020

[IW20] InfoWatch Attack Killer – Custom Code Scanner, 2020, https://infowatch.com/products/attack_killer/ccs, online abgefragt 07.09.2020

[JD06] Jones Douglas W., Bowersox Tom C.: „Secure Data Export and Auditing using Data Diodes“, Department of Computer Science, University of Iowa, Paper, 2006, https://www.usenix.org/legacy/events/evt06/tech/full_papers/jones/jones_html/, online abgefragt 05.09.2020

[KJ et. al. 10] Kindervag John, Balaouras Stephanie, Colt Lindsey: „Build Security Into Your Network’s DNA: The Zero Trust Network Architecture“, Forrester Research Inc., 05.11.2010, http://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf, online abgefragt 03.09.2010

[KG12] Kucera Gernot.: „Elektrische Signalbeeinflussung in technischen Prozessen“, Buch, FH Campus Wien, ISBN: 987-3-902614-23-0, 2012

[KG17] Kucera Gernot: „Automatisierung in der Produktion: Steuerung von Fertigungsautomaten“, FH Campus Wien, 2017, ISBN 9783902614353

[KW20] Winfried Krieger: „Just in Time (JIT)“, Gabler Wirtschaftslexikon, 2020, https://wirtschaftslexikon.gabler.de/definition/just-time-jit-38670/version-262091, online abgefragt 21.06.2020

[LT et. al. 20] Theo Lins, Ricardo Augusto, Rabelo Oliveira: “Cyber-physical production systems retrofitting in context of industry 4.0”, Elsevier, Computers & Industrial Engineering, Volume 139, January 2020, 106193, https://www.sciencedirect.com/science/article/pii/S036083521930662X, online abgefragt 21.06.2020

[LS93] Bev Littlewood und Lorenzo Strigini: „Software - das unterschätzte Sicherheitsrisiko“, in Druckschrift: Spektrum der Wissenschaft 1 / 1993, Seite 64, Spektrum der Wissenschaft Verlagsgesellschaft mbH 1993, https://www.spektrum.de/magazin/software-das-unterschaetzte-sicherheitsrisiko/820585, abgefragt 13.09.2020

[LS18] Luber Stefan, Schmitz Peter: „Was ist ein Zero-Trust-Modell?“ in Security Insider, 04.10.2018, https://www.security-insider.de/was-ist-ein-zero-trust-modell-a-752389/, online abgefragt 03.09.2020

[MRL06] Maschinenrichtlinie: „RICHTLINIE 2006/42/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES“ vom 17. Mai 2006 über Maschinen und der Änderung der Richtlinie 95/16/EG, https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:32006L0042, online abgefragt 05.02.2020

[MPG17] mpg.de: „IT-Sicherheitsrichtlinie der Max-Planck-Gesellschaft“, Juni 21, 2017, https://www.mpg.de/12104234/it-sicherheitsrichtlinie-der-mpg.pdf, online abgefragt 21.08.2020

[MQJ19] Müller-Quade Jörn [Hrsg.]: „Cybersecurity Research: Challenges and Course of Action“, Forschungsbericht, 06.02.2019, KIT, Karlsruhe, DOI: 10.5445/IR/1000090060, https://publikationen.bibliothek.kit.edu/1000090060, online abgefragt 21.02.2020

[NV et. al. 18] Nigam V., Pretschner A., Ruess H.: „Model-Based Safety and Security Engineering”, White Paper, 2018, arXiv:1810.04866 [cs.LO], https://arxiv.org/abs/1810.04866v2, online abgefragt 11.02.2020

[OMV20] OMV Aktiengesellschaft: „Über uns“, Homepage 2020, https://www.omv.at/de-at/ueber-uns/raffinerie-schwechat, online abgefragt 02.09.2020

[QU20] QURATOR 2021 – Conference on Digital Curation Technologies, 2020, https://qurator.ai/conference-qurator-2021/, online abgefragt 07.09.2020

[RIS99] Rechtsinformationssystem des Bundes, „Bundesgesetz über den Schutz personenbezogener Daten“, 1999, https://www.ris.bka.gv.at/Dokumente/BgblPdf/1999_165_1/1999_165_1.pdf, online abgefragt 23.08.2020

[RIS18] Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG), StF: BGBl. I Nr. 111/2018 (NR: GP XXVI RV 369 AB 418 S. 53. BR: AB 10099 S. 887.) [CELEX-Nr.: 32016L1148], https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010536, online abgefragt 05.02.2020

[RIS19] Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Maschinen-Sicherheitsverordnung 2010, Fassung vom 22.12.2019, https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20005922, online abgefragt 05.02.2020

[RIS20] Rechtsinformationssystem des Bundes, „Netz- und Informationssystem Sicherheitsgesetz (NIS G)“, 2020, https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010536 , online abgefragt 23.08.2020

[RA16] Roth, Armin [Hrsg.]: „Einführung und Umsetzung von Industrie 4.0: „Grundlagen, Vorgehensmodell und Use Cases aus der Praxis“, Springer-Verlag Berlin Heidelberg, 2016, Print ISBN: 978-3-662-48504-0, Online ISBN: 978-3-662-48505-7

[SC13] Schaaf, Christian: „Mitarbeiterkriminalität wirksam bekämpfen - Ursachen und An-zeichen rechtzeitig erkennen“, SecuMedia-Verlags-GmbH, 2013, Seite 16, https://www.kes.info/archiv/leseproben/2013/13-1-016/, online abgefragt 08.09.2020

[SP o.J.] Springer: „Risiko, Sicherheit und Gefahr“, o.J., https://link.springer.com/content/pdf/10.1007%2F978-3-8348-9429-8_11.pdf, online abgefragt 28.08.2020

[SPR08] smart-production.de: „40 Jahre SPS“, VDE GmbH Verlag, 2008, https://www.smart-production.de/open-automation/news-detailansicht/nsctrl/detail/News/40-jahre-sps-20081014/, online abgefragt 1.9.2020

[SJ et. al. 13] Schlick, Jochen, Stephan, Peter, Zühlke, Detlef: „PRODUKTION 2020 - Auf dem Weg zur 4. industriellen Revolution“, im Sammelband von Scheer, August-Wilhelm [Hrsg.]: „Industrie 4.0 – Wie sehen Produktionsprozesse im Jahr 2020 aus?“, 2013, ISBN 978-3-9815833-2-8, online: https://www.researchgate.net/profile/August_Wilhelm_Scheer/publication/277717764_Industrie_40_-_Wie_sehen_Produktionsprozesse_im_Jahr_2020_aus/links/55ee9e5608ae0af8ee1a1d72/Industrie-40-Wie-sehen-Produktionsprozesse-im-Jahr-2020-aus.pdf, online abgefragt 10.09.2020

[SU19] Schneider, Ulla: „7 Tipps für den idealen Aufbau Ihrer IT Infrastruktur“, Web-Media4Business GmbH, 86441 Zusmarshausen, 15. April 2019, https://www.business-netz.com/Unternehmensfuehrung/Der-ideale-Aufbau-Ihrer-IT-Infrastruktur, abgefragt 04.11.2020,

[SC14] Swedish Civil Contingencies Agency (MSB) SE-651 81 Karlstad Phone +46 (0)771-240 240 www.msb.se, Order No. MSB766 - November 2014 ISBN 978-91-7383-500-8, online: https://www.msb.se/RibData/Filer/pdf/27473.pdf, online abgefragt 04.02.2020

[TC et. al. 10] C. Ten, G. Manimaran and C. Liu: “Cybersecurity for Critical Infrastructures: Attack and Defense Modeling,” in IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, vol. 40, no. 4, pp. 853-865, July 2010, doi: 10.1109/TSMCA.2010.2048028, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.475.2858&rep=rep1&type=pdf, online abgefragt 12.02.2020

[TW17] Technik und Wirtschaft: „Retrofit: Definition und Vorteile“, item Redaktion, 8. Jun. 2017, https://www.produktion.de/technik/retrofit-definition-und-vorteile-345.html, online abgefragt 21.06.2020

[TK et. al. 16] Thoben, Klaus-Dieter, Wiesner, Stefan, Wuest, Thorsten: “Industrie 4.0” and Smart Manufacturing– A Review of Research Issues and Application Examples, Paper, 2016, https://www.researchgate.net/publication/312069858, online abgefragt 10.09.2020

[TÜV20] TÜV Informationstechnik GmbH: „IEC 62443: Security für industrielle Steuerungs- und Automatisierungssysteme“, White Paper, https://www.tuvit.de/de/themen/industrie-40/iec-62443/?gclid=EAIaIQobChMI373G6KPc6wIVAeztCh2zow7WEAAYASAAEgJVEfD_BwE, online abgefragt 09.09.2020

[URMZ20] Universität Erfurt, Rechen- und Medienzentrum, interne Serviceseiten: „Sperrung von Dateianhängen in E-Mails“, 2020, https://www.uni-erfurt.de/en/universitaetsrechen-und-medienzentrum/ueber-uns/aktuelles/news/news-detail/sperrung-von-dateianhaengen-in-e-mails, online abgefragt 03.09.2020

[VDI19] VDI Verein Deutscher Ingenieure: „Informationssicherheit in der industriellen Automatisierung“, Pressemitteilung 10.12.2019, https://www.presseportal.de/pm/16368/4463767, online abgefragt 04.09.2020

[VSE18] Verband Schweizerischer Elektrizitätsunternehmen VSE: „Handbuch Grundschutz für «Operational Technology» in der Stromversorgung“, Ausgabe Juli 2018, https://www.strom.ch/sites/default/files/media/documents/20180611-hb-grundschutz-operational-technology-stromversorgung.pdf, online abgefragt 1..09.6.2020

[WKW19] Wirtschaftskammer Wien: „FAQ zur Maschinenrichtlinie-Antworten aus Sicht des Herstellers und des Betreibers von Maschinen“, https://www.wko.at/service/innovation-technologie-digitalisierung/faq-zur-maschinenrichtlinie.html, online abgefragt 05.02.2020

[WS et. al. 16] Windmann, Stefan, Niggemann, Oliver, Trsek, Henning: „Konzepte zur Erhöhung der IT Sicherheit in industriellen Automatisierungssystemen“, 2016, Conference Paper, https://www.researchgate.net/publication/304525200_Konzepte_zur_Erho-hung_der_IT_Sicherheit_in_industriellen_Automatisierungssystemen/citation/download, online abgefragt 23.04.2020

[WN17] Wingerath Norbert: „Verfahren zur unidirektionalen Datenübertragung“, Deutsches Patentamt, 19.01.2017, https://patents.google.com/patent/DE102015213400A1/de, online abgefragt 05.09.2020

[ZS19] Zimmermann Steffen: „VDMA Industrial Security: Menschliches Fehlverhalten und Sabotage sind die größten Bedrohungen“, Faktenpapier, 09.07.2019, https://industrialsecurity.vdma.org/viewer/-/v2article/render/37164217, online abgefragt 21.02.2020